TISAX AL3
Requirements Reference Catalogue

Control specification, evidence expectations and auditor preparation for all 160 documents of the ISMS library V6.2

Version 6.2 · 14 November 2026 · Classification C1 · INTERNAL
Document owner: Aurélien Husson, CISO

Status of this catalogue. It consolidates the Annex A added to each Word document. It is a working reference for audit preparation. It is not published by VDA or ENX, it does not replace the official VDA ISA workbook, and it does not itself demonstrate TISAX conformity. Question-level applicability and ISA numbering must be confirmed against the ISA edition of the assessment order, and baseline parameters (deadlines, frequencies, thresholds) must be confirmed or tightened by the approving authority.

Contents

1 AL3 in practice 7

2 Coverage matrix by ISA area 8

2b ISA control to document mapping 15

3 Control specifications 21

ISMS-OPS-VULN-001 — Vulnerability and patch management 22

ISMS-CRY-POLITIQUE-001 — Cryptography, keys and certificates 25

ISMS-OPS-CHANGES-001 — IT change management 27

ISMS-OPS-DURCISSEMENT-001 — Secure configuration and hardening 29

ISMS-OPS-MALWARE-001 — Malware protection 31

ISMS-OPS-JOURNAUX-001 — Security logging and monitoring 33

ISMS-OPS-SAUVEGARDE-001 — Backup and restoration policy 35

ISMS-OPS-RESEAU-001 — Network security policy 37

ISMS-OPS-CLOUD-001 — Cloud services security policy 39

ISMS-DEV-SDLC-001 — Secure procurement and development lifecycle 41

ISMS-POL-SSI-002 — Full information security policy 43

ISMS-POL-SSI-001 — Shareable information security policy 45

ISMS-ORG-PERIMETRE-001 — ISMS scope and boundaries 47

ISMS-ORG-ROLES-001 — Information security roles and RACI 49

ISMS-ORG-DEROGATIONS-001 — Security exceptions management 51

ISMS-ACT-CLASSIF-001 — Information classification and handling 53

ISMS-ACT-INVENTAIRE-001 — Asset management and inventory 55

ISMS-RSK-METHODE-001 — Information security risk methodology 57

ISMS-PRJ-SECURITE-001 — Security in projects 59

ISMS-AUD-PROGRAMME-001 — Internal audit, self-assessment and management review 61

ISMS-INC-PROC-001 — Information security incident management 63

ISMS-INC-CRISE-001 — Crisis management and communications 65

ISMS-CLI-EXIGENCES-001 — Customer information security requirements 67

ISMS-RH-CYCLE-001 — Employee joiner-mover-leaver lifecycle 69

ISMS-RH-SENSIBILISATION-001 — Security awareness and training programme 71

ISMS-RH-CHARTE-001 — Employee IT acceptable-use charter 73

ISMS-RH-TELETRAVAIL-001 — Remote and mobile work policy 75

ISMS-RH-MOBILE-001 — Mobile device and BYOD controls 77

ISMS-PHY-ZONES-001 — Physical security zones and premises 79

ISMS-PHY-SUPPORTS-001 — Physical media handling and disposal 81

ISMS-PRA-PCA-001 — Business impact analysis and continuity plan 83

ISMS-PRA-PRA-001 — IT disaster recovery plan 85

ISMS-PRA-TESTS-001 — Business continuity, recovery and restore tests 87

ISMS-IAM-POLITIQUE-001 — Identity and access management policy 89

ISMS-IAM-CYCLE-001 — User account lifecycle management 91

ISMS-IAM-AUTH-001 — Authentication and multi-factor authentication 93
ISMS-IAM-PRIV-001 — Privileged and administrative access 95
ISMS-IAM-REVUE-001 — Periodic access certification 97
ISMS-FOU-POLITIQUE-001 — Supplier security management policy 99
ISMS-CON-CONFORMITE-001 — Legal, regulatory and contractual compliance 101
ISMS-CLI-FICHE-001 — Customer security fact sheet 103
ISMS-CLI-QUESTIONNAIRE-001 — Approved customer security responses 105
ISMS-CLI-ANNEXE-001 — Customer contractual security annex 107
ISMS-CLI-INCIDENT-001 — Customer incident notification procedure 109
ISMS-INF-HEB-002 — Customer-facing data-location statement 111
ISMS-FOU-CHARTE-001 — Supplier security requirements 113
ISMS-RGP-DPA-001 — Data processing agreement template 115
ISMS-RH-NDA-001 — Confidentiality agreement template 117
ISMS-RH-CHARTE-002 — IT acceptable-use charter for contractors 118
ISMS-PUB-CONFIANCE-001 — Public security trust page 120
ISMS-AUD-FIELDWORK-001 — AL3 assessment fieldwork and on-site readiness plan 121
ISMS-AUD-SAMPLE-001 — Audit evidence population and sampling standard 123
ISMS-AUD-MATURITY-001 — ISA maturity assessment and sustained-operation test 125
ISMS-AUD-CLOSURE-001 — Assessment finding remediation and independent closure testing 127
ISMS-ORG-SOA-001 — Control applicability and documented rationale statement 129
ISMS-ORG-INTERFACES-001 — Cross-site shared control and handoff assurance 131
ISMS-ORG-ATTEST-001 — Control owner attestation and independent challenge 133
ISMS-FOU-ASSURANCE-002 — High-risk supplier assurance dossier and evidence validity 135
ISMS-INC-EXERCISE-001 — Cyber crisis tabletop and decision exercise programme 137
ISMS-AUD-EVIDENCE-001 — Evidence chain of custody, minimisation and secure disclosure 139
ISMS-CLI-DIFFUSION-001 — Security-evidence disclosure procedure 141
ISMS-CLI-TISAX-001 — TISAX assessment-result sharing procedure 143
ISMS-CLI-SECURITE-002 — Supplier qualification questionnaire 145
ISMS-ORG-DOC-001 — ISMS document control 147
ISMS-ORG-OBJECTIFS-001 — Security objectives and metrics 149
ISMS-ORG-GOUVERNANCE-001 — Security steering committee and decisions 151
ISMS-ORG-SITES-001 — Multi-site security operating model 153
ISMS-ORG-ISA-001 — VDA ISA coverage and applicability matrix 155
ISMS-RSK-REGISTRE-001 — Information security risk register 157
ISMS-RSK-TRAITEMENT-001 — Risk treatment plan 159
ISMS-ACT-FLUX-001 — Information-flow and data-flow maps 160
ISMS-ACT-TRANSFERT-001 — Secure information exchange and transfer 162
ISMS-ACT-CONSERVATION-001 — Information retention and destruction 164
ISMS-ORG-MENACES-001 — Threat intelligence and risk context 166
ISMS-ORG-ECARTS-001 — Nonconformity and corrective action 168
ISMS-CLI-ENGAGEMENTS-001 — Register of customer security commitments 170

ISMS-ORG-CONTROLES-001 — Internal security control testing plan 172
ISMS-INC-PRESERVATION-001 — Incident evidence collection and preservation 174
ISMS-RH-TIERS-001 — External workforce security management 176
ISMS-RH-POSTES-001 — Sensitive roles and segregation of duties 178
ISMS-RH-FORMATION-001 — Role-based training curriculum 180
ISMS-RH-DEPLACEMENTS-001 — Travel and off-site equipment use 182
ISMS-PHY-BADGES-001 — Physical access badge management 184
ISMS-PHY-VISITEURS-001 — Visitor and on-site contractor procedures 186
ISMS-PHY-ENV-001 — Environmental and facilities risk controls 188
ISMS-PHY-MATERIEL-001 — Equipment maintenance, transport and removal 190
ISMS-PHY-INSPECTIONS-001 — Periodic premises inspections 192
ISMS-IAM-PRIV-002 — Privileged access management (PAM/PIM) 193
ISMS-IAM-SERVICE-001 — Service, API and machine identities 195
ISMS-IAM-TIERS-001 — Third-party and supplier access control 197
ISMS-IAM-DISTANT-001 — Remote access and interconnections 199
ISMS-IAM-URGENCE-001 — Emergency break-glass access 201
ISMS-IAM-FEDERATION-001 — Single sign-on, federation and SaaS access 203
ISMS-OPS-ARCHI-001 — Security architecture and technical diagrams 205
ISMS-OPS-CMDB-001 — Systems and software configuration register 207
ISMS-OPS-EOL-001 — End-of-life technologies and exceptions 209
ISMS-OPS-ENDPOINT-001 — Endpoint and server security baseline 211
ISMS-OPS-EMAIL-001 — Messaging and collaboration protection 213
ISMS-OPS-EXPO-001 — Internet-facing service security 215
ISMS-OPS-SEGMENT-001 — Network segmentation and firewall rule register 217
ISMS-OPS-WIFI-001 — Wi-Fi and guest network security 219
ISMS-OPS-SIEM-001 — Security detection and SOC use cases 220
ISMS-OPS-TEMPS-001 — Clock synchronization and forensic time quality 222
ISMS-OPS-RESTORE-001 — Detailed restoration operating procedures 223
ISMS-OPS-BACKUP-002 — Tamper-resistant and isolated backups 224
ISMS-OPS-SECRETS-001 — Secrets vault and key rotation 226
ISMS-OPS-CONFIG-001 — Continuous configuration compliance 228
ISMS-OPS-PENTEST-001 — Penetration testing programme 230
ISMS-OPS-OUTILS-001 — Administrative tooling and remote maintenance security 232
ISMS-OPS-DLP-001 — Data loss prevention and external sharing 234
ISMS-OPS-SUPPRESSION-001 — Secure logical data and system erasure 236
ISMS-OPS-CLOUD-002 — Cloud posture review and service exit 238
ISMS-DEV-RELEASE-001 — Secure releases and CI/CD 240
ISMS-DEV-TESTS-001 — Application security verification 242
ISMS-DEV-EXTERNE-001 — Third-party software and solution acquisition 243
ISMS-FOU-REGISTRE-001 — Supplier register and criticality 245
ISMS-FOU-EVALUATION-001 — Supplier security due diligence 247

ISMS-FOU-SUIVI-001 — Ongoing supplier security assurance 249
ISMS-FOU-SOUS-TRAITANCE-001 — Subcontractor chain and external information flows 251
ISMS-FOU-SORTIE-001 — Supplier exit and reversibility 253
ISMS-FOU-INCIDENT-001 — Supplier alerts and incident management 254
ISMS-CON-VEILLE-001 — Legal and standards watch 256
ISMS-CON-DONNEES-001 — Confidentiality obligations management 258
ISMS-CON-RETENTION-001 — Audit record retention and archiving 260
ISMS-CON-CONTROLES-001 — Contractual compliance testing 262
ISMS-ORG-AI-001 — AI services and sensitive-information security handling 264
ISMS-PRO-GOUV-001 — Prototype security governance and customer requirements 266
ISMS-PRO-ZONES-001 — Prototype facilities and restricted zones 268
ISMS-PRO-TRACABILITE-001 — Prototype lifecycle traceability 270
ISMS-PRO-TRANSPORT-001 — Prototype secure transport and storage 272
ISMS-PRO-IMAGE-001 — Prototype photography and media handling 274
ISMS-PRO-DESTRUCTION-001 — Prototype return, destruction and recycling 276
ISMS-PRO-VEHICULES-001 — Protected test vehicles and trials 278
ISMS-PRO-RECON-001 — Prototype inventory reconciliation and missing-item response 280
ISMS-RGP-REGISTRE-001 — Personal data processing records 282
ISMS-RGP-PIA-001 — Data protection impact assessment (DPIA) 284
ISMS-RGP-DROITS-001 — Data-subject rights procedure 286
ISMS-RGP-VIOLATION-001 — Personal data breach response 288
ISMS-RGP-TRANSFERTS-001 — International personal data transfers 290
ISMS-RGP-RETENTION-001 — Personal data retention and disposal 292
ISMS-OT-INVENTAIRE-001 — OT and industrial asset inventory 294
ISMS-OT-ZONES-001 — Industrial zones and conduits architecture 296
ISMS-OT-ACCES-001 — Secure industrial remote maintenance 298
ISMS-OT-CORRECTIFS-001 — OT vulnerability and patch management 300
ISMS-OT-CHANGES-001 — Industrial change management 302
ISMS-OT-PRA-001 — Production continuity and OT recovery 304
ISMS-OT-FOURNISSEURS-001 — OT integrator and manufacturer security 306
ISMS-OT-IEC62443-001 — IEC 62443 applicability and gap review 308
ISMS-OT-SESSION-002 — OT privileged remote session release and forensic record 310
ISMS-ORG-CONTEXTE-001 — Organisational context and interested parties 312
ISMS-RH-DISCIPLINE-001 — Disciplinary procedure for security breaches 314
ISMS-RH-ANTECEDENTS-001 — Background verification and screening 316
ISMS-OPS-LOGICIELS-001 — Software installation and approval 318
ISMS-OPS-ENVIRONNEMENTS-001 — Environment separation and test data 320
ISMS-PHY-BUREAU-001 — Clean desk and screen lock 322
ISMS-OPS-PURVIEW-001 — Microsoft Purview labelling and DLP configuration register 324
ISMS-ORG-AUTORITES-001 — Contacts with authorities and special interest groups 326
ISMS-ORG-COMMUNICATION-001 — Information security communication plan 328

ISMS-OPS-CAPACITES-001 — Capacity and availability management 330
4 Evidence master index 332
5 Auditor question bank 348
6 Indicator dashboard definition 362
7 Baseline parameter register (ISMS-ORG-PARAMETRES-001) 376
8 AL3 readiness checklist 378

1 AL3 in practice

Assessment Level 3 (AL3) is the most rigorous TISAX assessment level. The requirement catalogue is the VDA ISA; what changes with the level is the audit method. At AL3 the audit provider verifies implementation through document review, interviews and an on-site inspection, rather than a remote plausibility check only. Every applicable control question is scored on a maturity scale from 0 to 5, and a TISAX label requires maturity level 3 or better for each applicable control; unmet controls become findings that must be remediated through a corrective action plan.

Maturity levels as applied in this library

LEVEL	NAME	MEANING FOR THIS LIBRARY
0	Incomplete	Control absent or not performed.
1	Performed	Done informally; ad hoc; typically no consistent evidence. A manual that nobody follows lands here.
2	Managed	Planned and tracked for part of the scope; evidence incomplete or inconsistent.
3	Established	Defined, implemented across the whole scope, consistently followed and demonstrably tested during the audit. Minimum for the label.
4	Predictable	Measured and controlled with quantitative targets (not required for the label).
5	Optimising	Continuously improved based on measurement (not required for the label).

How an AL3 assessment unfolds

- Preparation: scope and objectives agreed with the provider; self-assessment against the VDA ISA; evidence staged (ISMS-AUD-FIELDWORK-001).
- Document review: policies, procedures and registers are read for completeness and consistency; the version actually in use is assessed.
- Interviews: IT management, ISMS manager, HR, facility, data protection and control owners are asked the same questions independently; answers must agree with documents and each other.
- On-site inspection: premises, security zones, server rooms, offices and delivery areas are walked; clean desk, access control, screen lock and media handling are spot-checked.
- Technical verification: live system queries, configurations, logs and tickets are examined; populations are sampled (ISMS-AUD-SAMPLE-001).
- Findings and remediation: nonconformities are classified, corrective actions are planned and closure is verified (ISMS-AUD-CLOSURE-001).

Evidence principles

- Native, timestamped, system-generated records beat screenshots and reconstructed documents.
- Show sustained operation: at least two cycles or three months of records for recurring controls.
- One person per control can explain scope, frequency and exceptions; a deputy gives the same account.
- Do not back-date or rebuild records; label post-order remediation as such.
- Minimise personal and customer data in evidence (ISMS-AUD-EVIDENCE-001).

Role of the Word documents and this catalogue

Each Word document keeps its operating sections 1 to 9 and now ends with Annex A (AL3 control specification): framework mapping, numbered mandatory requirements, activities and accountability, records and evidence register, indicators with escalation triggers, maturity level 3 criteria, auditor questions, frequent nonconformities, on-site readiness and interfaces. This catalogue reproduces that content in one place and adds cross-document indexes.

2 Coverage matrix by ISA area

Control numbers are those of the official VDA ISA 6.0.3 workbook (chapters 1 IS policies and organisation, 2 human resources, 3 physical security, 4 identity and access management, 5 IT security and cyber security, 6 supplier relationships, 7 compliance, 8 prototype protection, 9 data protection). Business continuity sits in controls 1.6.3, 5.2.8 and 5.2.9. Applicability and maturity are decided in the workbook for the assessment order and recorded in ISMS-ORG-SOA-001. Source: VDA ISA © ENX Association, CC BY-ND 4.0; this mapping is a derivative not approved by ENX or VDA.

DOCUMENT	TITLE	ISA 6.0.3 CONTROLS	ISO 27001:2022 (LEAD)	CLASS
ISMS-OPS-VULN-001	Vulnerability and patch management	5.2.5	A.8.8 Management of technical vulnerabilities …	C2
ISMS-CRY-POLITIQUE-001	Cryptography, keys and certificates	5.1.1, 5.1.2	A.8.24 Use of cryptography …	C1
ISMS-OPS-CHANGES-001	IT change management	5.2.1, 5.2.2	A.8.32 Change management …	C1
ISMS-OPS-DURCISSEMENT-001	Secure configuration and hardening	5.2.1, 5.2.6	A.8.9 Configuration management …	C2
ISMS-OPS-MALWARE-001	Malware protection	5.2.3	A.8.7 Protection against malware …	C1
ISMS-OPS-JOURNAUX-001	Security logging and monitoring	5.2.4	A.8.15 Logging …	C2
ISMS-OPS-SAUVEGARDE-001	Backup and restoration policy	5.2.9	A.8.13 Information backup …	C1
ISMS-OPS-RESEAU-001	Network security policy	5.2.7, 5.3.2	A.8.20 Network security …	C2
ISMS-OPS-CLOUD-001	Cloud services security policy	1.3.3, 1.2.4, 5.3.3, 5.3.4	A.5.23 Information security for use of cloud services …	C1
ISMS-DEV-SDLC-001	Secure procurement and development lifecycle	5.3.1, 5.2.2	A.8.25 Secure development life cycle …	C1
ISMS-POL-SSI-002	Full information security policy	1.1.1	A.5.1 Policies for information security …	C1
ISMS-POL-SSI-001	Shareable information security policy	1.1.1	A.5.1 Policies for information security …	C0
ISMS-ORG-PERIMETRE-001	ISMS scope and boundaries	1.2.1	Clause 4.3 Determining the scope of the ISMS …	C2
ISMS-ORG-ROLES-001	Information security roles and RACI	1.2.2, 9.2.1	A.5.2 Information security roles and responsibilities …	C1
ISMS-ORG-DEROGATIONS-001	Security exceptions management	1.2.1, 1.4.1	A.5.1 Policies …	C1
ISMS-ACT-CLASSIF-001	Information classification and handling	1.3.2	A.5.12 Classification of information …	C1
ISMS-ACT-INVENTAIRE-001	Asset management and inventory	1.3.1	A.5.9 Inventory of information and other associated assets …	C2
ISMS-RSK-METHODE-001	Information security risk methodology	1.4.1	Clauses 6.1.2 and 6.1.3 Risk assessment and treatment …	C1
ISMS-PRJ-SECURITE-001	Security in projects	1.2.3, 5.3.1	A.5.8 Information security in project management …	C1
ISMS-AUD-PROGRAMME-001	Internal audit, self-assessment and management review	1.5.1, 1.5.2	Clause 9.2 Internal audit …	C1

DOCUMENT	TITLE	ISA 6.0.3 CONTROLS	ISO 27001:2022 (LEAD)	CLASS
ISMS-INC-PROC-001	Information security incident management	1.6.1, 1.6.2	A.5.24 Incident management planning …	C2
ISMS-INC-CRISE-001	Crisis management and communications	1.6.3	A.5.29 Information security during disruption …	C2
ISMS-CLI-EXIGENCES-001	Customer information security requirements	7.1.1	A.5.31 Legal, statutory, regulatory and contractual requirements …	C2
ISMS-RH-CYCLE-001	Employee joiner-mover-leaver lifecycle	2.1.1, 2.1.2, 4.2.1	A.6.1 Screening …	C1
ISMS-RH-SENSIBILISATION-001	Security awareness and training programme	2.1.3, 9.7.2, 8.2.3	A.6.3 Awareness, education and training …	C1
ISMS-RH-CHARTE-001	Employee IT acceptable-use charter	2.1.2	A.5.10 Acceptable use of information and other assets …	C1
ISMS-RH-TELETRAVAIL-001	Remote and mobile work policy	2.1.4	A.6.7 Remote working …	C1
ISMS-RH-MOBILE-001	Mobile device and BYOD controls	2.1.4, 3.1.4	A.8.1 User endpoint devices …	C1
ISMS-PHY-ZONES-001	Physical security zones and premises	3.1.1	A.7.1 Physical security perimeters …	C2
ISMS-PHY-SUPPORTS-001	Physical media handling and disposal	3.1.3, 3.1.4	A.7.10 Storage media …	C1
ISMS-PRA-PCA-001	Business impact analysis and continuity plan	1.6.3, 5.2.8	A.5.29 Information security during disruption …	C2
ISMS-PRA-PRA-001	IT disaster recovery plan	5.2.8, 5.2.9	A.5.30 ICT readiness for business continuity …	C2
ISMS-PRA-TESTS-001	Business continuity, recovery and restore tests	5.2.8, 5.2.9	A.5.30 ICT readiness for business continuity …	C2
ISMS-IAM-POLITIQUE-001	Identity and access management policy	4.2.1	A.5.15 Access control …	C1
ISMS-IAM-CYCLE-001	User account lifecycle management	4.2.1, 4.1.3	A.5.16 Identity management …	C1
ISMS-IAM-AUTH-001	Authentication and multi-factor authentication	4.1.2, 4.1.3	A.5.17 Authentication information …	C1
ISMS-IAM-PRIV-001	Privileged and administrative access	4.2.1	A.8.2 Privileged access rights …	C2
ISMS-IAM-REVUE-001	Periodic access certification	4.2.1	A.5.18 Access rights …	C1
ISMS-FOU-POLITIQUE-001	Supplier security management policy	6.1.1, 1.2.4	A.5.19 Information security in supplier relationships …	C1
ISMS-CON-CONFORMITE-001	Legal, regulatory and contractual compliance	7.1.1, 7.1.2	A.5.31 Legal, statutory, regulatory and contractual requirements …	C1
ISMS-CLI-FICHE-001	Customer security fact sheet	7.1.1, 6.1.1	A.5.14 Information transfer …	C1
ISMS-CLI-QUESTIONNAIRE-001	Approved customer security responses	7.1.1	A.5.31 Legal requirements …	C2

DOCUMENT	TITLE	ISA 6.0.3 CONTROLS	ISO 27001:2022 (LEAD)	CLASS
ISMS-CLI-ANNEXE-001	Customer contractual security annex	6.1.1, 6.1.2, 7.1.1	A.5.20 Addressing information security in supplier agreements …	C1
ISMS-CLI-INCIDENT-001	Customer incident notification procedure	1.6.2, 1.6.3	A.5.24 Incident management planning …	C1
ISMS-INF-HEB-002	Customer-facing data-location statement	1.3.3, 5.3.4, 9.5.3	A.5.23 Cloud services …	C1
ISMS-FOU-CHARTE-001	Supplier security requirements	6.1.1	A.5.19 and A.5.20 Supplier relationships …	C1
ISMS-RGP-DPA-001	Data processing agreement template	9.5.2, 9.8.1, 7.1.2	A.5.34 Privacy and protection of PII …	C1
ISMS-RH-NDA-001	Confidentiality agreement template	6.1.2, 2.1.2, 9.7.1, 8.2.1	A.6.6 Confidentiality or non-disclosure agreements …	C1
ISMS-RH-CHARTE-002	IT acceptable-use charter for contractors	2.1.2, 6.1.1	A.5.10 Acceptable use …	C1
ISMS-PUB-CONFIANCE-001	Public security trust page	1.1.1, 7.1.1	A.5.31 …	C0
ISMS-AUD-FIELDWORK-001	AL3 assessment fieldwork and on-site readiness plan	1.5.1	Clause 9.2 Internal audit …	C2
ISMS-AUD-SAMPLE-001	Audit evidence population and sampling standard	1.5.1	A.5.35 Independent review …	C1
ISMS-AUD-MATURITY-001	ISA maturity assessment and sustained-operation test	1.5.1	Clause 9.1 Monitoring, measurement, analysis and evaluation …	C1
ISMS-AUD-CLOSURE-001	Assessment finding remediation and independent closure testing	1.5.1	Clause 10.2 Nonconformity and corrective action …	C2
ISMS-ORG-SOA-001	Control applicability and documented rationale statement	1.2.1, 1.5.1	Clause 6.1.3 Statement of applicability …	C2
ISMS-ORG-INTERFACES-001	Cross-site shared control and handoff assurance	1.2.4, 1.2.2	A.5.2 Roles and responsibilities …	C1
ISMS-ORG-ATTEST-001	Control owner attestation and independent challenge	1.5.1	Clause 9.3 Management review …	C2
ISMS-FOU-ASSURANCE-002	High-risk supplier assurance dossier and evidence validity	6.1.1, 1.3.3	A.5.22 Monitoring, review and change management of supplier services …	C2
ISMS-INC-EXERCISE-001	Cyber crisis tabletop and decision exercise programme	1.6.3	A.5.24 Incident management planning …	C1
ISMS-AUD-EVIDENCE-001	Evidence chain of custody, minimisation and secure disclosure	7.1.1, 1.5.2	A.5.28 Collection of evidence …	C2
ISMS-CLI-DIFFUSION-001	Security-evidence disclosure procedure	1.3.2, 5.1.2	A.5.14 Information transfer …	C1
ISMS-CLI-TISAX-001	TISAX assessment-result sharing procedure	7.1.1, 1.5.2	A.5.31 Legal and contractual requirements …	C1
ISMS-CLI-SECURITE-002	Supplier qualification questionnaire	6.1.1, 1.3.3	A.5.19 Information security in supplier relationships …	C1

DOCUMENT	TITLE	ISA 6.0.3 CONTROLS	ISO 27001:2022 (LEAD)	CLASS
ISMS-ORG-DOC-001	ISMS document control	1.1.1	Clause 7.5 Documented information …	C1
ISMS-ORG-OBJECTIFS-001	Security objectives and metrics	1.2.1	Clause 6.2 Information security objectives …	C1
ISMS-ORG-GOUVERNANCE-001	Security steering committee and decisions	1.2.1, 1.2.2	Clause 5.1 Leadership …	C1
ISMS-ORG-SITES-001	Multi-site security operating model	1.2.1, 3.1.1	A.5.2 Roles and responsibilities …	C1
ISMS-ORG-ISA-001	VDA ISA coverage and applicability matrix	1.5.1	Clause 6.1.3 Statement of applicability …	C2
ISMS-RSK-REGISTRE-001	Information security risk register	1.4.1	Clause 6.1.2 Information security risk assessment …	C2
ISMS-RSK-TRAITEMENT-001	Risk treatment plan	1.4.1	Clause 6.1.3 Risk treatment …	C2
ISMS-ACT-FLUX-001	Information-flow and data-flow maps	1.3.1, 5.1.2	A.5.9 Inventory of information …	C2
ISMS-ACT-TRANSFERT-001	Secure information exchange and transfer	5.1.2	A.5.14 Information transfer …	C1
ISMS-ACT-CONSERVATION-001	Information retention and destruction	7.1.1	A.5.33 Protection of records …	C1
ISMS-ORG-MENACES-001	Threat intelligence and risk context	1.4.1	A.5.7 Threat intelligence …	C2
ISMS-ORG-ECARTS-001	Nonconformity and corrective action	1.5.1	Clause 10.2 Nonconformity and corrective action …	C1
ISMS-CLI-ENGAGEMENTS-001	Register of customer security commitments	7.1.1	A.5.31 Legal and contractual requirements …	C2
ISMS-ORG-CONTROLES-001	Internal security control testing plan	1.5.1	A.5.35 Independent review …	C2
ISMS-INC-PRESERVATION-001	Incident evidence collection and preservation	1.6.2	A.5.28 Collection of evidence …	C2
ISMS-RH-TIERS-001	External workforce security management	2.1.1, 2.1.2, 6.1.1	A.6.1 Screening …	C1
ISMS-RH-POSTES-001	Sensitive roles and segregation of duties	2.1.1, 1.2.2	A.5.3 Segregation of duties …	C2
ISMS-RH-FORMATION-001	Role-based training curriculum	2.1.3, 9.7.2	A.6.3 Awareness, education and training …	C1
ISMS-RH-DEPLACEMENTS-001	Travel and off-site equipment use	2.1.4, 3.1.4	A.6.7 Remote working …	C1
ISMS-PHY-BADGES-001	Physical access badge management	3.1.1, 4.1.1	A.7.2 Physical entry …	C1
ISMS-PHY-VISITEURS-001	Visitor and on-site contractor procedures	3.1.1	A.7.2 Physical entry …	C1
ISMS-PHY-ENV-001	Environmental and facilities risk controls	3.1.1, 5.2.8	A.7.5 Protecting against physical and environmental threats …	C2
ISMS-PHY-MATERIEL-001	Equipment maintenance, transport and removal	3.1.3, 3.1.4	A.7.8 Equipment siting …	C1
ISMS-PHY-INSPECTIONS-001	Periodic premises inspections	3.1.1	A.7.4 Physical security monitoring …	C1
ISMS-IAM-PRIV-002	Privileged access management (PAM/PIM)	4.2.1	A.8.2 Privileged access rights …	C2

DOCUMENT	TITLE	ISA 6.0.3 CONTROLS	ISO 27001:2022 (LEAD)	CLASS
ISMS-IAM-SERVICE-001	Service, API and machine identities	4.1.3, 4.2.1	A.5.16 Identity management …	C2
ISMS-IAM-TIERS-001	Third-party and supplier access control	4.2.1, 6.1.1	A.5.19 Supplier relationships …	C2
ISMS-IAM-DISTANT-001	Remote access and interconnections	4.1.2, 5.2.7	A.8.20 Network security …	C2
ISMS-IAM-URGENCE-001	Emergency break-glass access	4.2.1	A.8.2 Privileged access rights …	C3
ISMS-IAM-FEDERATION-001	Single sign-on, federation and SaaS access	4.1.2, 1.3.3	A.5.16 Identity management …	C1
ISMS-OPS-ARCHI-001	Security architecture and technical diagrams	5.2.7, 5.3.1	A.8.27 Secure system architecture …	C3
ISMS-OPS-CMDB-001	Systems and software configuration register	1.3.1, 5.2.1	A.8.9 Configuration management …	C2
ISMS-OPS-EOL-001	End-of-life technologies and exceptions	5.2.5, 1.3.4	A.8.8 Management of technical vulnerabilities …	C1
ISMS-OPS-ENDPOINT-001	Endpoint and server security baseline	5.2.3, 3.1.4, 5.1.1	A.8.1 User endpoint devices …	C2
ISMS-OPS-EMAIL-001	Messaging and collaboration protection	5.1.2, 5.2.3	A.5.14 Information transfer …	C1
ISMS-OPS-EXPO-001	Internet-facing service security	5.2.5, 5.2.7	A.8.20 …	C2
ISMS-OPS-SEGMENT-001	Network segmentation and firewall rule register	5.2.7	A.8.22 Segregation of networks …	C3
ISMS-OPS-WIFI-001	Wi-Fi and guest network security	5.2.7	A.8.20 …	C1
ISMS-OPS-SIEM-001	Security detection and SOC use cases	5.2.4, 1.6.1	A.8.16 Monitoring activities …	C2
ISMS-OPS-TEMPS-001	Clock synchronization and forensic time quality	5.2.4	A.8.17 Clock synchronisation …	C1
ISMS-OPS-RESTORE-001	Detailed restoration operating procedures	5.2.9	A.8.13 Information backup …	C2
ISMS-OPS-BACKUP-002	Tamper-resistant and isolated backups	5.2.9	A.8.13 …	C2
ISMS-OPS-SECRETS-001	Secrets vault and key rotation	4.1.3, 5.1.1	A.5.17 Authentication information …	C3
ISMS-OPS-CONFIG-001	Continuous configuration compliance	5.2.1, 5.2.6	A.8.9 Configuration management …	C2
ISMS-OPS-PENTEST-001	Penetration testing programme	5.2.6, 5.2.5	A.8.8 …	C2
ISMS-OPS-OUTILS-001	Administrative tooling and remote maintenance security	4.2.1, 5.2.6	A.8.18 Use of privileged utility programs …	C2
ISMS-OPS-DLP-001	Data loss prevention and external sharing	5.1.2, 1.3.2	A.8.12 Data leakage prevention …	C1
ISMS-OPS-SUPPRESSION-001	Secure logical data and system erasure	3.1.3, 5.3.3	A.8.10 Information deletion …	C1
ISMS-OPS-CLOUD-002	Cloud posture review and service exit	1.3.3, 5.3.3, 5.3.4	A.5.23 Cloud services …	C2
ISMS-DEV-RELEASE-001	Secure releases and CI/CD	5.2.1, 5.3.1	A.8.32 Change management …	C1
ISMS-DEV-TESTS-001	Application security verification	5.3.1, 5.2.2	A.8.29 Security testing …	C2
ISMS-DEV-EXTERNE-001	Third-party software and solution acquisition	1.3.4, 5.3.1, 6.1.1	A.8.30 Outsourced development …	C1

DOCUMENT	TITLE	ISA 6.0.3 CONTROLS	ISO 27001:2022 (LEAD)	CLASS
ISMS-FOU-REGISTRE-001	Supplier register and criticality	6.1.1	A.5.19 …	C2
ISMS-FOU-EVALUATION-001	Supplier security due diligence	6.1.1, 1.3.3	A.5.19 …	C1
ISMS-FOU-SUIVI-001	Ongoing supplier security assurance	6.1.1	A.5.22 Monitoring, review and change management of supplier services …	C1
ISMS-FOU-SOUS-TRAITANCE-001	Subcontractor chain and external information flows	6.1.1	A.5.19 …	C1
ISMS-FOU-SORTIE-001	Supplier exit and reversibility	5.3.3, 6.1.1	A.5.20 …	C1
ISMS-FOU-INCIDENT-001	Supplier alerts and incident management	1.6.2, 6.1.1	A.5.24 …	C1
ISMS-CON-VEILLE-001	Legal and standards watch	7.1.1	A.5.31 Legal, statutory, regulatory and contractual requirements …	C1
ISMS-CON-DONNEES-001	Confidentiality obligations management	6.1.2, 7.1.1	A.6.6 Confidentiality agreements …	C2
ISMS-CON-RETENTION-001	Audit record retention and archiving	7.1.1	A.5.33 Protection of records …	C1
ISMS-CON-CONTROLES-001	Contractual compliance testing	7.1.1, 1.5.1	A.5.36 Compliance with policies …	C1
ISMS-ORG-AI-001	AI services and sensitive-information security handling	1.3.3, 1.3.4, 5.1.2	A.5.10 Acceptable use …	C1
ISMS-PRO-GOUV-001	Prototype security governance and customer requirements	8.2.1, 8.2.2, 8.2.3, 8.2.4, 8.2.5, 8.5.1	A.5.2 …	C3
ISMS-PRO-ZONES-001	Prototype facilities and restricted zones	8.1.1, 8.1.2, 8.1.3, 8.1.4, 8.1.5, 8.1.6, 8.1.7, 8.1.8	A.7.1 …	C3
ISMS-PRO-TRACABILITE-001	Prototype lifecycle traceability	8.3.1	A.5.9 …	C3
ISMS-PRO-TRANSPORT-001	Prototype secure transport and storage	8.3.1, 8.3.2	A.7.9 …	C3
ISMS-PRO-IMAGE-001	Prototype photography and media handling	8.2.6, 8.2.7, 8.5.2	A.7.6 …	C3
ISMS-PRO-DESTRUCTION-001	Prototype return, destruction and recycling	8.3.2	A.7.14 …	C3
ISMS-PRO-VEHICULES-001	Protected test vehicles and trials	8.4.1, 8.4.2, 8.4.3	A.7.9 …	C3
ISMS-PRO-RECON-001	Prototype inventory reconciliation and missing-item response	8.3.1, 1.6.2	A.5.9 …	C3
ISMS-RGP-REGISTRE-001	Personal data processing records	9.3.1, 9.2.1, 9.1.1	A.5.34 Privacy and protection of PII …	C2
ISMS-RGP-PIA-001	Data protection impact assessment (DPIA)	9.4.1	A.5.34 …	C2
ISMS-RGP-DROITS-001	Data-subject rights procedure	9.6.1	A.5.34 …	C1
ISMS-RGP-VIOLATION-001	Personal data breach response	9.6.2	A.5.24 …	C2
ISMS-RGP-TRANSFERTS-001	International personal data transfers	9.5.1, 9.5.3	A.5.34 …	C1
ISMS-RGP-RETENTION-001	Personal data retention and disposal	9.3.1, 9.1.1	A.5.34 …	C1

DOCUMENT	TITLE	ISA 6.0.3 CONTROLS	ISO 27001:2022 (LEAD)	CLASS
ISMS-OT-INVENTAIRE-001	OT and industrial asset inventory	1.3.1	A.5.9 …	C2
ISMS-OT-ZONES-001	Industrial zones and conduits architecture	5.2.7	A.8.22 …	C3
ISMS-OT-ACCES-001	Secure industrial remote maintenance	4.2.1, 5.2.7	A.8.2 …	C2
ISMS-OT-CORRECTIFS-001	OT vulnerability and patch management	5.2.5	A.8.8 …	C2
ISMS-OT-CHANGES-001	Industrial change management	5.2.1	A.8.32 …	C2
ISMS-OT-PRA-001	Production continuity and OT recovery	5.2.8, 5.2.9	A.5.30 …	C2
ISMS-OT-FOURNISSEURS-001	OT integrator and manufacturer security	6.1.1	A.5.19 …	C2
ISMS-OT-IEC62443-001	IEC 62443 applicability and gap review	—	IEC 62443-2-1 …	C2
ISMS-OT-SESSION-002	OT privileged remote session release and forensic record	4.2.1, 5.2.4	A.8.2 …	C2
ISMS-ORG-CONTEXTE-001	Organisational context and interested parties	1.2.1, 1.1.1	Clause 4.1 Understanding the organisation and its context …	C1
ISMS-RH-DISCIPLINE-001	Disciplinary procedure for security breaches	2.1.2	A.6.4 Disciplinary process …	C1
ISMS-RH-ANTECEDENTS-001	Background verification and screening	2.1.1	A.6.1 Screening …	C1
ISMS-OPS-LOGICIELS-001	Software installation and approval	1.3.4, 5.2.3	A.8.19 Installation of software on operational systems …	C1
ISMS-OPS-ENVIRONNEMENTS-001	Environment separation and test data	5.2.2, 5.3.1	A.8.31 Separation of development, test and production environments …	C1
ISMS-PHY-BUREAU-001	Clean desk and screen lock	3.1.1, 2.1.3	A.7.7 Clear desk and clear screen …	C1
ISMS-OPS-PURVIEW-001	Microsoft Purview labelling and DLP configuration register	1.3.2, 5.1.2	A.5.12 Classification of information …	C2
ISMS-ORG-AUTORITES-001	Contacts with authorities and special interest groups	1.6.1, 1.6.3	A.5.5 Contact with authorities …	C1
ISMS-ORG-COMMUNICATION-001	Information security communication plan	1.2.2, 2.1.3, 1.6.3	Clause 7.4 Communication …	C1
ISMS-OPS-CAPACITES-001	Capacity and availability management	5.2.8, 5.2.1	A.8.6 Capacity management …	C1

2b ISA control to document mapping

Each ISA 6.0.3 control with its ISA2027.1 number and the library documents that address it. Prototype controls 8.2.4, 8.3 to 8.5 are removed in ISA2027; ISA2027 adds 8.1.1, 8.1.2, 8.1.4, 8.1.11, 8.1.12 and 8.1.13 (last rows).

MODULE	ISA 6	QUESTION	ISA2027	DOCUMENTS
Information security	1.1.1	To what extent are information security policies available?	1.1.1	ISMS-POL-SSI-001 ; ISMS-PUB-CONFIANCE-001 ; ISMS-POL-SSI-002 ; ISMS-ORG-DOC-001 ; ISMS-ORG-PARAMETRES-001 ; ISMS-ORG-CONTEXTE-001
Information security	1.2.1	To what extent is information security managed within the organization?	1.2.1	ISMS-ORG-PERIMETRE-001 ; ISMS-ORG-DEROGATIONS-001 ; ISMS-ORG-OBJECTIFS-001 ; ISMS-ORG-PARAMETRES-001 ; ISMS-ORG-GOUVERNANCE-001 ; ISMS-ORG-SITES-001 ; ISMS-ORG-SOA-001 ; ISMS-ORG-CONTEXTE-001
Information security	1.2.2	To what extent are information security responsibilities organized?	1.2.2	ISMS-ORG-ROLES-001 ; ISMS-ORG-GOUVERNANCE-001 ; ISMS-RH-POSTES-001 ; ISMS-ORG-INTERFACES-001 ; ISMS-ORG-COMMUNICATION-001
Information security	1.2.3	To what extent are information security requirements considered in projects?	1.2.3	ISMS-PRJ-SECURITE-001
Information security	1.2.4	To what extent are the responsibilities between external IT service providers and the own organization defined?	6.1.3	ISMS-OPS-CLOUD-001 ; ISMS-FOU-POLITIQUE-001 ; ISMS-ORG-INTERFACES-001
Information security	1.3.1	To what extent are information assets identified and recorded?	1.3.1	ISMS-ACT-INVENTAIRE-001 ; ISMS-ACT-FLUX-001 ; ISMS-OPS-CMDB-001 ; ISMS-OT-INVENTAIRE-001
Information security	1.3.2	To what extent are information assets classified and managed in terms of their protection needs?	1.3.2	ISMS-CLI-DIFFUSION-001 ; ISMS-ACT-CLASSIF-001 ; ISMS-OPS-DLP-001 ; ISMS-OPS-PURVIEW-001
Information security	1.3.3	To what extent is it ensured that only evaluated and approved external IT services are used for processing the organization’s information assets?	1.3.3	ISMS-INF-HEB-002 ; ISMS-CLI-SECURITE-002 ; ISMS-IAM-FEDERATION-001 ; ISMS-OPS-CLOUD-001 ; ISMS-OPS-CLOUD-002 ; ISMS-FOU-EVALUATION-001 ; ISMS-FOU-ASSURANCE-002 ; ISMS-ORG-AI-001
Information security	1.3.4	To what extent is it ensured that only evaluated and approved software is used for processing the organization’s information assets?	1.3.4	ISMS-OPS-EOL-001 ; ISMS-DEV-EXTERNE-001 ; ISMS-ORG-AI-001 ; ISMS-OPS-LOGICIELS-001
Information security	1.4.1	To what extent are information security risks managed?	1.4.1	ISMS-ORG-DEROGATIONS-001 ; ISMS-RSK-METHODE-001 ; ISMS-RSK-REGISTRE-001 ; ISMS-RSK-TRAITEMENT-001 ; ISMS-ORG-MENACES-001
Information security	1.5.1	To what extent is compliance with information security ensured in procedures and processes?	1.5.1	ISMS-AUD-PROGRAMME-001 ; ISMS-ORG-ISA-001 ; ISMS-ORG-ECARTS-001 ; ISMS-ORG-CONTROLES-001 ; ISMS-CON-CONTROLES-001 ; ISMS-AUD-FIELDWORK-001 ; ISMS-AUD-SAMPLE-001 ; ISMS-AUD-MATURITY-001 ; ISMS-AUD-CLOSURE-001 ; ISMS-ORG-SOA-001 ; ISMS-ORG-ATTEST-001

MODULE	ISA 6	QUESTION	ISA2027	DOCUMENTS
Information security	1.5.2	To what extent is the ISMS reviewed by an independent authority?	1.5.2	ISMS-CLI-TISAX-001 ; ISMS-AUD-PROGRAMME-001 ; ISMS-AUD-EVIDENCE-001
Information security	1.6.1	To what extent are information security relevant events or observations reported?	1.6.1	ISMS-INC-PROC-001 ; ISMS-OPS-SIEM-001 ; ISMS-ORG-AUTORITES-001
Information security	1.6.2	To what extent are reported security events managed?	1.6.2	ISMS-CLI-INCIDENT-001 ; ISMS-INC-PROC-001 ; ISMS-INC-PRESERVATION-001 ; ISMS-FOU-INCIDENT-001 ; ISMS-PRO-RECON-001
Information security	1.6.3	To what extent is the organization prepared to handle crisis situations?	1.6.3	ISMS-CLI-INCIDENT-001 ; ISMS-INC-CRISE-001 ; ISMS-PRA-PCA-001 ; ISMS-INC-EXERCISE-001 ; ISMS-ORG-AUTORITES-001 ; ISMS-ORG-COMMUNICATION-001
Information security	2.1.1	To what extent is the qualification of employees for sensitive work fields ensured?	2.1.1	ISMS-RH-CYCLE-001 ; ISMS-RH-TIERS-001 ; ISMS-RH-POSTES-001 ; ISMS-RH-ANTECEDENTS-001
Information security	2.1.2	To what extent is all staff contractually bound to comply with information security policies?	2.1.2	ISMS-RH-NDA-001 ; ISMS-RH-CHARTE-002 ; ISMS-RH-CYCLE-001 ; ISMS-RH-CHARTE-001 ; ISMS-RH-TIERS-001 ; ISMS-RH-DISCIPLINE-001
Information security	2.1.3	To what extent is staff made aware of and trained with respect to the risks arising from the handling of information?	2.1.3	ISMS-RH-SENSIBILISATION-001 ; ISMS-RH-FORMATION-001 ; ISMS-PHY-BUREAU-001 ; ISMS-ORG-COMMUNICATION-001
Information security	2.1.4	To what extent is mobile work regulated?	2.1.4	ISMS-RH-TELETRAVAIL-001 ; ISMS-RH-MOBILE-001 ; ISMS-RH-DEPLACEMENTS-001
Information security	3.1.1	To what extent are security zones managed to protect information assets?	3.1.1	ISMS-ORG-SITES-001 ; ISMS-PHY-ZONES-001 ; ISMS-PHY-BADGES-001 ; ISMS-PHY-VISITEURS-001 ; ISMS-PHY-ENV-001 ; ISMS-PHY-INSPECTIONS-001 ; ISMS-PHY-BUREAU-001
Information security	3.1.2	Superseded by 1.6.3, 5.2.8 and 5.2.9		
Information security	3.1.3	To what extent is the handling of supporting assets managed?	3.1.3	ISMS-PHY-SUPPORTS-001 ; ISMS-PHY-MATERIEL-001 ; ISMS-OPS-SUPPRESSION-001
Information security	3.1.4	To what extent is the handling of mobile IT devices and mobile data storage devices managed?	3.1.4	ISMS-RH-MOBILE-001 ; ISMS-RH-DEPLACEMENTS-001 ; ISMS-PHY-SUPPORTS-001 ; ISMS-PHY-MATERIEL-001 ; ISMS-OPS-ENDPOINT-001
Information security	4.1.1	To what extent is the use of identification means managed?	4.1.1	ISMS-PHY-BADGES-001
Information security	4.1.2	To what extent is the user access to IT services and IT systems secured?	4.1.2	ISMS-IAM-AUTH-001 ; ISMS-IAM-DISTANT-001 ; ISMS-IAM-FEDERATION-001
Information security	4.1.3	To what extent are user accounts and login information securely managed and applied?	4.1.3	ISMS-IAM-CYCLE-001 ; ISMS-IAM-AUTH-001 ; ISMS-IAM-SERVICE-001 ; ISMS-OPS-SECRETS-001

MODULE	ISA 6	QUESTION	ISA2027	DOCUMENTS
Information security	4.2.1	To what extent are access rights assigned and managed?	4.2.1	ISMS-RH-CYCLE-001 ; ISMS-IAM-POLITIQUE-001 ; ISMS-IAM-CYCLE-001 ; ISMS-IAM-PRIV-001 ; ISMS-IAM-REVUE-001 ; ISMS-IAM-PRIV-002 ; ISMS-IAM-SERVICE-001 ; ISMS-IAM-TIERS-001 ; ISMS-IAM-URGENCE-001 ; ISMS-OPS-OUTILS-001 ; ISMS-OT-ACCES-001 ; ISMS-OT-SESSION-002
Information security	5.1.1	To what extent is the use of cryptographic procedures managed?	5.1.1	ISMS-CRY-POLITIQUE-001 ; ISMS-OPS-ENDPOINT-001 ; ISMS-OPS-SECRETS-001
Information security	5.1.2	To what extent is information protected during transfer?	5.1.2	ISMS-CLI-DIFFUSION-001 ; ISMS-ACT-FLUX-001 ; ISMS-ACT-TRANSFERT-001 ; ISMS-CRY-POLITIQUE-001 ; ISMS-OPS-EMAIL-001 ; ISMS-OPS-DLP-001 ; ISMS-ORG-AI-001 ; ISMS-OPS-PURVIEW-001
Information security	5.2.1	To what extent are changes managed?	5.2.1	ISMS-OPS-CHANGES-001 ; ISMS-OPS-DURCISSEMENT-001 ; ISMS-OPS-CMDB-001 ; ISMS-OPS-CONFIG-001 ; ISMS-DEV-RELEASE-001 ; ISMS-OT-CHANGES-001 ; ISMS-OPS-CAPACITES-001
Information security	5.2.2	To what extent are development and testing environments separated from operational environments?	5.2.2	ISMS-OPS-CHANGES-001 ; ISMS-DEV-SDLC-001 ; ISMS-DEV-TESTS-001 ; ISMS-OPS-ENVIRONNEMENTS-001
Information security	5.2.3	To what extent are IT systems protected against malware?	5.2.3	ISMS-OPS-MALWARE-001 ; ISMS-OPS-ENDPOINT-001 ; ISMS-OPS-EMAIL-001 ; ISMS-OPS-LOGICIELS-001
Information security	5.2.4	To what extent are event logs recorded and analysed?	5.2.4	ISMS-OPS-JOURNAUX-001 ; ISMS-OPS-SIEM-001 ; ISMS-OPS-TEMPS-001 ; ISMS-OT-SESSION-002
Information security	5.2.5	To what extent are vulnerabilities identified and addressed?	5.2.5	ISMS-OPS-VULN-001 ; ISMS-OPS-EOL-001 ; ISMS-OPS-EXPO-001 ; ISMS-OPS-PENTEST-001 ; ISMS-OT-CORRECTIFS-001
Information security	5.2.6	To what extent are IT systems and services technically checked (system and service audit)?	5.2.6	ISMS-OPS-DURCISSEMENT-001 ; ISMS-OPS-CONFIG-001 ; ISMS-OPS-PENTEST-001 ; ISMS-OPS-OUTILS-001
Information security	5.2.7	To what extent is the network of the organization managed?	5.2.7	ISMS-IAM-DISTANT-001 ; ISMS-OPS-RESEAU-001 ; ISMS-OPS-ARCHI-001 ; ISMS-OPS-EXPO-001 ; ISMS-OPS-SEGMENT-001 ; ISMS-OPS-WIFI-001 ; ISMS-OT-ZONES-001 ; ISMS-OT-ACCES-001
Information security	5.2.8	To what extent is continuity planning for IT services in place?	5.2.8	ISMS-PRA-PCA-001 ; ISMS-PRA-PRA-001 ; ISMS-PRA-TESTS-001 ; ISMS-PHY-ENV-001 ; ISMS-OT-PRA-001 ; ISMS-OPS-CAPACITES-001

MODULE	ISA 6	QUESTION	ISA2027	DOCUMENTS
Information security	5.2.9	To what extent is the backup and recovery of data and IT services ensured?	5.2.9	ISMS-PRA-PRA-001 ; ISMS-PRA-TESTS-001 ; ISMS-OPS-SAUVEGARDE-001 ; ISMS-OPS-RESTORE-001 ; ISMS-OPS-BACKUP-002 ; ISMS-OT-PRA-001
Information security	5.3.1	To what extent is information security considered in new or further developed IT systems?	5.3.1	ISMS-PRJ-SECURITE-001 ; ISMS-DEV-SDLC-001 ; ISMS-OPS-ARCHI-001 ; ISMS-DEV-RELEASE-001 ; ISMS-DEV-TESTS-001 ; ISMS-DEV-EXTERNE-001 ; ISMS-OPS-ENVIRONNEMENTS-001
Information security	5.3.2	To what extent are requirements for network services defined?	5.3.2	ISMS-OPS-RESEAU-001
Information security	5.3.3	To what extent is the return and secure removal of information assets from external IT services regulated?	5.3.3	ISMS-OPS-CLOUD-001 ; ISMS-OPS-SUPPRESSION-001 ; ISMS-OPS-CLOUD-002 ; ISMS-FOU-SORTIE-001
Information security	5.3.4	To what extent is information protected in shared external IT services?	5.3.4	ISMS-INF-HEB-002 ; ISMS-OPS-CLOUD-001 ; ISMS-OPS-CLOUD-002
Information security	6.1.1	To what extent is information security ensured among contractors and cooperation partners?	6.1.1	ISMS-CLI-FICHE-001 ; ISMS-CLI-ANNEXE-001 ; ISMS-FOU-CHARTE-001 ; ISMS-RH-CHARTE-002 ; ISMS-CLI-SECURITE-002 ; ISMS-RH-TIERS-001 ; ISMS-IAM-TIERS-001 ; ISMS-DEV-EXTERNE-001 ; ISMS-FOU-POLITIQUE-001 ; ISMS-FOU-REGISTRE-001 ; ISMS-FOU-EVALUATION-001 ; ISMS-FOU-SUIVI-001 ; ISMS-FOU-SOUS-TRAITANCE-001 ; ISMS-FOU-SORTIE-001 ; ISMS-FOU-INCIDENT-001 ; ISMS-OT-FOURNISSEURS-001 ; ISMS-FOU-ASSURANCE-002
Information security	6.1.2	To what extent is non-disclosure regarding the exchange of information contractually agreed?	6.1.2	ISMS-CLI-ANNEXE-001 ; ISMS-RH-NDA-001 ; ISMS-CON-DONNEES-001
Information security	7.1.1	To what extent is compliance with regulatory and contractual provisions ensured?	7.1.1	ISMS-CLI-FICHE-001 ; ISMS-CLI-QUESTIONNAIRE-001 ; ISMS-CLI-ANNEXE-001 ; ISMS-PUB-CONFIANCE-001 ; ISMS-CLI-TISAX-001 ; ISMS-CLI-EXIGENCES-001 ; ISMS-ACT-CONSERVATION-001 ; ISMS-CLI-ENGAGEMENTS-001 ; ISMS-CON-CONFORMITE-001 ; ISMS-CON-VEILLE-001 ; ISMS-CON-DONNEES-001 ; ISMS-CON-RETENTION-001 ; ISMS-CON-CONTROLES-001 ; ISMS-AUD-EVIDENCE-001
Information security	7.1.2	To what extent is the protection of personally identifiable data considered when implementing information security?	7.1.2	ISMS-RGP-DPA-001 ; ISMS-CON-CONFORMITE-001
Prototype protection	8.1.1	To what extent is a security concept available describing minimum requirements regarding the physical and environmental security for prototype protection?	8.2.1	ISMS-PRO-ZONES-001
Prototype protection	8.1.2	To what extent is perimeter security existent preventing unauthorized access to protected property objects?	8.2.2	ISMS-PRO-ZONES-001

MODULE	ISA 6	QUESTION	ISA2027	DOCUMENTS
Prototype protection	8.1.3	To what extent is the outer skin of the protected buildings constructed such as to prevent removal or opening of outer-skin components using standard tools?	8.2.3	ISMS-PRO-ZONES-001
Prototype protection	8.1.4	To what extent is view and sight protection ensured in defined security areas?	8.2.4	ISMS-PRO-ZONES-001
Prototype protection	8.1.5	To what extent is the protection against unauthorized entry regulated in the form of access control?	8.2.5	ISMS-PRO-ZONES-001
Prototype protection	8.1.6	To what extent are the premises to be secured monitored for intrusion?	8.2.6	ISMS-PRO-ZONES-001
Prototype protection	8.1.7	To what extent is a documented visitor management in place?	8.1.8	ISMS-PRO-ZONES-001
Prototype protection	8.1.8	To what extent is on-site client segregation existent?	8.2.7	ISMS-PRO-ZONES-001
Prototype protection	8.2.1	To what extent are non-disclosure agreements/obligations existent according to the valid contractual law?	8.1.5	ISMS-RH-NDA-001 ; ISMS-PRO-GOUV-001
Prototype protection	8.2.2	To what extent are requirements for commissioning subcontractors known and fulfilled?	8.1.6	ISMS-PRO-GOUV-001
Prototype protection	8.2.3	To what extent do employees and project members evidently participate in training and awareness measures regarding the handling of prototypes?	8.1.3	ISMS-RH-SENSIBILISATION-001 ; ISMS-PRO-GOUV-001
Prototype protection	8.2.4	To what extent are security classifications of the project and the resulting security measures known?	removed	ISMS-PRO-GOUV-001
Prototype protection	8.2.5	To what extent is a process defined for granting access to security areas?	8.1.7	ISMS-PRO-GOUV-001
Prototype protection	8.2.6	To what extent are regulations for image recording and handling of created image material existent?	8.1.10	ISMS-PRO-IMAGE-001
Prototype protection	8.2.7	To what extent is a process for carrying along and using mobile video and photography devices in(to) defined security areas established?	8.1.9	ISMS-PRO-IMAGE-001
Prototype protection	8.3.1	To what extent are transports of vehicles, components or parts classified as requiring protection arranged according to the customer requirements?	removed	ISMS-PRO-TRACABILITE-001 ; ISMS-PRO-TRANSPORT-001 ; ISMS-PRO-RECON-001
Prototype protection	8.3.2	To what extent is it ensured that vehicles, components, and parts classified as requiring protection are parked/stored in accordance with customer requirements?	removed	ISMS-PRO-TRANSPORT-001 ; ISMS-PRO-DESTRUCTION-001
Prototype protection	8.4.1	To what extent are the predefined camouflage regulations implemented by the project members?	removed	ISMS-PRO-VEHICULES-001
Prototype protection	8.4.2	To what extent are measures for protecting approved test and trial grounds observed/implemented?	removed	ISMS-PRO-VEHICULES-001
Prototype protection	8.4.3	To what extent are protective measures for approved test and trial drives in public observed/implemented?	removed	ISMS-PRO-VEHICULES-001
Prototype protection	8.5.1	To what extent are security requirements for presentations and events involving vehicles, components or parts classified as requiring protection known?	removed	ISMS-PRO-GOUV-001
Prototype protection	8.5.2	To what extent are the protective measures for film and photo shootings involving vehicles, components or parts classified as requiring protection known?	removed	ISMS-PRO-IMAGE-001

MODULE	ISA 6	QUESTION	ISA2027	DOCUMENTS
Data protection	9.1.1	To what extent do data protection policies exist?	9.1.1	ISMS-RGP-REGISTRE-001 ; ISMS-RGP-RETENTION-001
Data protection	9.2.1	To what extent are the responsibilities for data protection organized?	9.2.1	ISMS-ORG-ROLES-001 ; ISMS-RGP-REGISTRE-001
Data protection	9.3.1	To what extent are processing activities identified and recorded?	9.3.1	ISMS-RGP-REGISTRE-001 ; ISMS-RGP-RETENTION-001
Data protection	9.4.1	To what extent is adequate handling of high-risk processing activities ensured (data protection impact assessment)?	9.4.1	ISMS-RGP-PIA-001
Data protection	9.5.1	To what extent is the transfer of data managed?	9.5.1	ISMS-RGP-TRANSFERTS-001
Data protection	9.5.2	To what extent are contractual obligations passed through to and enforced at subcontractors and cooperation partners?	9.5.2	ISMS-RGP-DPA-001
Data protection	9.5.3	To what extent are data transfers to third countries managed?	9.5.3	ISMS-INF-HEB-002 ; ISMS-RGP-TRANSFERTS-001
Data protection	9.6.1	To what extent are data subject requests processed?	9.6.1	ISMS-RGP-DROITS-001
Data protection	9.6.2	To what extent are data protection incidents processed?	9.6.2	ISMS-RGP-VIOLATION-001
Data protection	9.7.1	To what extent are employees obliged to maintain confidentiality?	9.7.1	ISMS-RH-NDA-001
Data protection	9.7.2	To what extent are employees trained in data protection?	9.7.2	ISMS-RH-SENSIBILISATION-001 ; ISMS-RH-FORMATION-001
Data protection	9.8.1	To what extent are instructions of processing relationships handled?	9.8.1	ISMS-RGP-DPA-001
Prototype protection (new in ISA2027.1)	—	To what extent are regulations for prototype protection defined within the organization and responsibilities established?	8.1.1	ISMS-PRO-GOUV-001
Prototype protection (new in ISA2027.1)	—	To what extent are order-specific requirements and specifications for handling prototypes regulated?	8.1.2	ISMS-PRO-GOUV-001
Prototype protection (new in ISA2027.1)	—	To what extent is the qualification of employees for working in prototype areas ensured?	8.1.4	ISMS-PRO-GOUV-001 ; ISMS-RH-ANTECEDENTS-001 ; ISMS-RH-FORMATION-001
Prototype protection (new in ISA2027.1)	—	To what extent are incident management requirements regulated?	8.1.11	ISMS-PRO-RECON-001
Prototype protection (new in ISA2027.1)	—	To what extent is comprehensive documentation and traceability of vehicles and components requiring special protection ensured throughout the entire processing procedure?	8.1.12	ISMS-PRO-TRACABILITE-001
Prototype protection (new in ISA2027.1)	—	To what extent is it ensured that vehicles, components, parts and relevant tools classified as in need of protection that are no longer needed are disposed of/ recycled/ returned in accordance with the client's specifications?	8.1.13	ISMS-PRO-DESTRUCTION-001

3 Control specifications

One section per document. Requirement IDs are stable and cited in internal audit and evidence indexes.

ISMS-OPS-VULN-001 — Vulnerability and patch management

Classification C2 · CONFIDENTIAL · Format PROCEDURE · Applicability Core

Objective

Ensure that technical vulnerabilities in every in-scope system are identified, prioritised by real exposure, treated within defined timeframes and verified as closed, so that systems handling protected information are not exploitable through known weaknesses.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	IT security: vulnerability management, patching and technical review of IT systems (chapter 5)
ISO/IEC 27001:2022	A.8.8 Management of technical vulnerabilities; A.8.9 Configuration management; A.8.19 Installation of software on operational systems; A.8.34 Protection of information systems during audit testing
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
VUL-01	A complete inventory of in-scope hardware, operating systems, firmware, applications, containers and cloud workloads shall be the scan target population; every scanner population shall be reconciled to the inventory at least monthly.	Reconciliation report with counts of unscanned, orphaned and duplicate assets and owner sign-off.
VUL-02	Authenticated vulnerability scans shall run at least weekly on internet-facing systems and at least monthly on internal systems, and after any significant change.	Scan schedule export and last 12 months of scan job history.
VUL-03	Vendor security advisories and threat feeds relevant to the installed software shall be monitored by a named role and logged on receipt.	Advisory log with receipt date, product and triage decision.
VUL-04	Each finding shall be triaged within 2 working days using exploitability (known exploitation, public exploit), exposure, asset protection need and compensating controls; CVSS is an input only.	Finding records with documented rationale and priority.
VUL-05	Baseline remediation deadlines from triage shall be: actively exploited or critical on exposed system 72 hours; critical or high 14 days; medium 60 days; low 120 days or next planned release.	Sample of closed findings showing detection date, due date, closure date.
VUL-06	Operating-system and security patches shall be deployed through a tested channel with a rollback path; emergency patches follow the emergency path of ISMS-OPS-CHANGES-001.	Change tickets linked to findings.
VUL-07	Where a patch cannot be applied in time, a time-limited risk acceptance with compensating controls shall be approved under ISMS-ORG-DEROGATIONS-001; it shall not exceed 90 days without re-approval.	Exception register entries with expiry and approver.
VUL-08	Closure of a finding shall be verified by an independent rescan or an equivalent configuration check by a person other than the implementer.	Closure evidence referencing rescan ID or configuration snapshot.
VUL-09	End-of-life and unsupported software shall be listed with a replacement plan and isolation measures; no unsupported system shall process information of high or very high protection need without an approved exception.	EOL register cross-checked to the asset inventory (ISMS-OPS-EOL-001).
VUL-10	Internet-facing assets shall undergo an external attack-surface review at least quarterly, and independent penetration testing at least annually and after major change.	External scan reports and penetration test report with tracked findings (ISMS-OPS-PENTEST-001).
VUL-11	Vulnerability testing shall not disrupt production or exceed the authorised scope; OT and prototype systems are tested only under written plant or programme approval.	Test authorisation records.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Maintain scan coverage and schedule	Platform / security engineer	IT Operations service owner	Asset owners; ISMS manager
Triage findings and set priority	Vulnerability analyst	Information security officer	Service owner; business owner
Deploy patch or mitigation	System administrator	Service owner	Change authority
Approve risk acceptance	Service owner (proposal)	Change authority / business service owner	CISO; customer programme where applicable
Verify closure independently	Second engineer or ISMS reviewer	ISMS manager	Service owner
Report indicators to management review	ISMS manager	CISO	Top management

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Asset-to-scanner reconciliation	CMDB and scanner export; IT Operations	Monthly	3 years
Scan results and job history	Scanner platform; security engineering	Weekly / monthly	3 years
Triage and priority record	Ticketing system; vulnerability analyst	Per finding	3 years
Patch deployment and change record	Change system; service owner	Per change	3 years
Independent closure evidence	Ticket plus rescan ID; ISMS reviewer	Per finding	3 years
Risk acceptance and EOL exceptions	Exception register; CISO	Per exception	Exception life + 3 years
Penetration test reports and retest	Document store; CISO	Annual	6 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Critical/high findings closed within deadline	≥ 95% each quarter	< 90% in a quarter: root-cause review at ISMS meeting
Mean age of open critical findings	≤ 7 days	Any critical finding open beyond 30 days goes to CISO
Asset coverage by authenticated scan	≥ 98% of in-scope assets	< 95%: coverage remediation plan within 14 days
Open risk acceptances past expiry	0	Any expired acceptance escalates to top management
Sampled closures verified independently	100% of sample	Any miss reopens the finding and the sample doubles

Auditor questions to prepare

- Show me how you know the scanner sees every in-scope asset. Who reconciles it and when was the last time something was found missing?
- Pick a critical finding from the last quarter: when was it detected, who triaged it, when was it fixed and who verified it?
- How do you handle a vulnerability that cannot be patched? Show me the register and one example with its compensating control.
- Which systems are end-of-life today and how are they isolated?
- How do you test systems you must not scan, such as OT or prototype equipment?
- What happened the last time a critical advisory was published for software you run?

Frequent nonconformities

- Scanner covers only part of the estate and nobody can show the reconciliation.
- CVSS alone drives priority; exposure and exploitation are ignored.
- Findings closed by the implementer without independent verification.
- Risk acceptances without expiry date or approver.
- Cloud workloads, endpoints of remote staff and supplier-managed devices missing from the population.

On-site readiness

- Be ready to demonstrate a live scan result and trace one finding end to end on screen, including the ticket and the rescan.
- Demonstrate patch compliance for a server and an endpoint selected by the auditor on the day.

Interfaces: ISMS-OPS-CHANGES-001, ISMS-OPS-CMDB-001, ISMS-OPS-EOL-001, ISMS-OPS-PENTEST-001, ISMS-OPS-DURCISSEMENT-001, ISMS-ORG-DEROGATIONS-001, ISMS-RSK-REGISTRE-001, ISMS-AUD-CLOSURE-001

ISMS-CRY-POLITIQUE-001 — Cryptography, keys and certificates

Classification C1 · INTERNAL · Format PROCEDURE · Applicability Core

Objective

Protect confidentiality, integrity and authenticity of information with approved cryptographic algorithms, sound key management and a controlled certificate lifecycle.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	IT security: cryptography, encryption in transit and at rest, key management (chapter 5)
ISO/IEC 27001:2022	A.8.24 Use of cryptography; A.8.5 Secure authentication; A.5.14 Information transfer; A.8.11 Data masking
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
CRY-01	Approved algorithms and minimum key lengths shall be defined and follow current national guidance (for example BSI TR-02102 or NIST SP 800-57): AES-256 or AES-128 minimum for symmetric, RSA ≥ 3072 or ECC ≥ 256 bit, SHA-256 or stronger; deprecated algorithms (MD5, SHA-1, 3DES, RC4) are prohibited.	Cryptographic standard and scan results.
CRY-02	C2 and C3 data at rest shall be encrypted on servers, endpoints, mobile devices, backups and removable media.	Encryption status reports.
CRY-03	Data in transit shall use TLS 1.2 or higher with approved cipher suites, and TLS 1.3 where supported; plain protocols are prohibited for C2/C3 data.	TLS scan results.
CRY-04	Cryptographic keys shall be generated, stored, rotated, backed up, archived and destroyed under a documented lifecycle, using HSM or managed key services for high-value keys.	Key lifecycle records.
CRY-05	Key custodians shall be named; keys for C3 data shall use split knowledge or dual control.	Custodian list.
CRY-06	Certificates shall be inventoried with owner and expiry; renewal shall begin at least 30 days before expiry, with monitoring and alerts.	Certificate inventory.
CRY-07	Customer-held keys or customer-specified encryption requirements shall be respected and documented.	Customer requirement mapping.
CRY-08	Cryptographic measures shall be reviewed at least annually against evolving guidance.	Annual review.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Define crypto standard	Security architect	CISO	IT; legal
Manage keys and certificates	Platform engineering	IT manager	Security architect
Monitor expiry and algorithms	Security engineering	CISO	Service owners

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Cryptographic standard	Document system; architect	Annual	3 years
Key inventory and lifecycle log	KMS/HSM; platform engineering	Continuous	Key life + 3 years
Certificate inventory	CLM or CMDB; platform engineering	Continuous	Cert life + 1 year
Encryption and TLS compliance scans	Scanner; security engineering	Quarterly	3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Certificates expired in production	0	Incident
C2/C3 stores encrypted	100%	Any exception via exception procedure
Deprecated algorithms in use	0	Remediation plan within 30 days

Auditor questions to prepare

- How are your keys protected and who can access them?
- Show me the certificate inventory and next expiries.
- What encryption protects backups?

Frequent nonconformities

- No key inventory.
- Encryption claimed but not evidenced.
- Weak TLS on internal services.

Interfaces: ISMS-OPS-SECRETS-001, ISMS-OPS-SAUVEGARDE-001, ISMS-OPS-RESEAU-001, ISMS-OPS-EMAIL-001, ISMS-ACT-CLASSIF-001

ISMS-OPS-CHANGES-001 — IT change management

Classification C1 · INTERNAL · Format PROCEDURE · Applicability Core

Objective

Ensure that all changes to production systems are assessed, approved, tested, implemented and reviewed in a controlled and traceable way.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	IT security: change management and separation of environments (chapter 5)
ISO/IEC 27001:2022	A.8.32 Change management; A.8.31 Separation of development, test and production; A.8.19 Installation of software; A.8.9 Configuration management
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
CHG-01	Every change to in-scope production systems shall be recorded in a change ticket with description, reason, risk, test result, back-out plan and implementation window.	Change tickets.
CHG-02	Changes shall be classified (standard, normal, emergency) with defined approval levels; the approver shall not be the implementer.	Approval matrix and ticket evidence.
CHG-03	Security impact shall be assessed for every normal change; changes affecting security controls require security approval.	Security assessment field.
CHG-04	Emergency changes shall be approved retrospectively within 2 working days and reviewed.	Emergency change review.
CHG-05	Development, test and production shall be separated logically or physically; production data shall not be used in test without equivalent protection or masking.	Environment architecture and data masking evidence.
CHG-06	Success and failure of changes shall be reviewed and failed changes analysed.	Post-implementation review.
CHG-07	Unauthorised changes shall be detected by configuration monitoring and handled as incidents.	Drift detection alerts.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Raise and test changes	Change requester	Service owner	Security
Approve changes	Change authority	IT manager	CISO for security-related
Implement	Engineers	Service owner	Change manager
Review emergencies	Change manager	IT manager	CISO

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Change tickets	ITSM; change manager	Per change	3 years
CAB minutes	ITSM; change manager	Weekly	3 years
Emergency reviews	ITSM; change manager	Per emergency	3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Changes with approval before implementation	100%	Any miss is an incident review
Failed or rolled-back changes	≤ 5%	> 10%: root cause
Emergency changes share	≤ 5%	Rising trend reviewed

Auditor questions to prepare

- Pick a recent change: show request, test, approval, implementation, review.
- How do you detect unauthorised changes?
- How do you separate test and production data?

Frequent nonconformities

- Implementer approves own change.
- No back-out plan.
- Production data in test.

Interfaces: ISMS-OPS-CONFIG-001, ISMS-OPS-DURCISSEMENT-001, ISMS-OPS-VULN-001, ISMS-DEV-RELEASE-001, ISMS-DEV-SDLC-001

ISMS-OPS-DURCISSEMENT-001 — Secure configuration and hardening

Classification C2 · CONFIDENTIAL · Format PROCEDURE · Applicability Core

Objective

Ensure all systems are built and maintained from a secure, documented baseline and that deviations are detected and corrected.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	IT security: secure configuration and hardening (chapter 5)
ISO/IEC 27001:2022	A.8.9 Configuration management; A.8.19 Software installation; A.8.7 Protection against malware; A.8.20 Network security
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
HRD-01	Hardening baselines shall exist for each platform class (operating systems, databases, containers, network devices, cloud services) based on recognised benchmarks such as CIS or vendor guidance.	Baseline documents with version.
HRD-02	New systems shall be deployed from approved images or infrastructure-as-code templates.	Pipeline or image records.
HRD-03	Unneeded services, ports, accounts and software shall be removed; default credentials changed.	Compliance scans.
HRD-04	Compliance with baselines shall be measured at least monthly using automated tooling, with deviations tracked.	Compliance reports.
HRD-05	Baselines shall be reviewed at least annually and upon new releases.	Baseline review.
HRD-06	Deviations shall be approved as exceptions with compensating controls.	Exception register.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Maintain baselines	Platform engineers	IT manager	Security architect
Measure compliance	Security engineering	CISO	Platform engineers
Remediate drift	System administrators	Service owners	Security engineering

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Baseline catalogue	Repository; platform engineering	Annual	3 years
Compliance scan results	Compliance tool; security engineering	Monthly	3 years
Deviation approvals	Exception register; CISO	Per exception	Life + 3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Systems compliant with baseline	≥ 95%	< 90%: remediation plan
Critical deviations open > 30 days	0	CISO
Systems built from approved images	100%	Rebuild

Auditor questions to prepare

- Which benchmark do you use and how do you measure compliance?
- Show me a deviation and how it was approved.
- How do you build a new server?

Frequent nonconformities

- Baselines not versioned.
- No measurement of compliance.
- Defaults unchanged on network devices.

Interfaces: ISMS-OPS-CONFIG-001, ISMS-OPS-CHANGES-001, ISMS-OPS-VULN-001, ISMS-OPS-CMDB-001, ISMS-OPS-CLOUD-001

ISMS-OPS-MALWARE-001 — Malware protection

Classification C1 · INTERNAL · Format PROCEDURE · Applicability Core

Objective

Prevent, detect and respond to malicious code on endpoints, servers, email, web and cloud workloads.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	IT security: protection against malware (chapter 5)
ISO/IEC 27001:2022	A.8.7 Protection against malware; A.8.23 Web filtering; A.8.16 Monitoring activities
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
MAL-01	Endpoint protection with behavioural detection (EDR or equivalent) shall be installed on all supported endpoints and servers, centrally managed and tamper-protected.	Coverage report from console.
MAL-02	Signatures and engines shall update at least daily; agents unhealthy for more than 24 hours shall alert.	Update and health report.
MAL-03	Email and web gateways shall scan attachments and links, and block executable and macro-enabled content by default.	Gateway configuration.
MAL-04	Removable media and downloads shall be scanned before use.	Policy and tool evidence.
MAL-05	Detections shall be triaged and handled within defined timeframes: high severity within 1 hour of alert during support hours.	Alert tickets.
MAL-06	Systems that cannot run agents (OT, appliances) shall have compensating controls documented.	Exception list.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Operate endpoint protection	Security engineering	CISO	IT operations
Triage alerts	SOC / security analyst	CISO	Service owners
Document exceptions	Platform owners	IT manager	Security engineering

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Coverage and health reports	EDR console; security engineering	Weekly	12 months
Detection tickets	Ticket/SIEM; analyst	Per alert	3 years
Exceptions	Exception register; CISO	Per exception	Life + 3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Endpoints with healthy agent	≥ 99%	< 97%: remediation within 7 days
High alerts triaged within 1 hour	≥ 95%	Staffing review
Signature age > 48h	0	Investigate

Auditor questions to prepare

- How do you know every server has protection?
- Show me the last malware detection and response.
- How are non-agent systems protected?

Frequent nonconformities

- Agents disabled by users.
- No coverage report.
- Servers excluded without exceptions.

Interfaces: ISMS-OPS-ENDPOINT-001, ISMS-OPS-EMAIL-001, ISMS-OPS-JOURNAUX-001, ISMS-INC-PROC-001

ISMS-OPS-JOURNAUX-001 — Security logging and monitoring

Classification C2 · CONFIDENTIAL · Format PROCEDURE · Applicability Core

Objective

Generate, protect, retain and review security-relevant logs so that events can be detected, investigated and proven.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	IT security: event logging and monitoring (chapter 5)
ISO/IEC 27001:2022	A.8.15 Logging; A.8.16 Monitoring activities; A.8.17 Clock synchronisation; A.5.28 Collection of evidence
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
LOG-01	A logging standard shall define which events are logged per system class: authentication, privilege use, account changes, administrative actions, access to C3 data, security alerts, configuration changes, and failures.	Logging standard and per-system matrix.
LOG-02	Logs shall be centralised to a protected platform with restricted access, integrity protection and synchronised time (ISMS-OPS-TEMPS-001).	SIEM source list and time-sync evidence.
LOG-03	Log retention shall be at least 12 months with at least 3 months immediately available, unless law or contracts require otherwise.	Retention configuration.
LOG-04	Administrators shall not be able to delete or alter their own audit logs.	Access control on log platform.
LOG-05	Use cases and alert rules shall be defined and reviewed at least annually; alerts shall be handled within defined times.	Rule catalogue and handling records.
LOG-06	Log source coverage shall be reconciled with the asset inventory at least quarterly.	Coverage reconciliation.
LOG-07	Log review of critical sources shall be carried out and recorded at defined frequency (daily for alerts, weekly for dashboards).	Review records.
LOG-08	Logging of personal data shall be minimised.	Privacy review.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Maintain logging standard	Security architect	CISO	IT; DPO
Operate log platform	Security engineering	IT manager	CISO
Monitor and triage	SOC	CISO	Service owners

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Logging standard	Document system; architect	Annual	3 years
Source coverage reconciliation	SIEM; security engineering	Quarterly	3 years
Alert handling tickets	SIEM / ticket; SOC	Per alert	3 years
Log archives	Log platform; security engineering	Continuous	12 months minimum

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
In-scope systems sending logs	≥ 98%	Remediate within 14 days
Critical alerts handled within target	≥ 95%	Review
Time drift above 1 second	0	Fix within 24 hours

Auditor questions to prepare

- Show me what you log for privileged access and where it is stored.
- What happens if someone deletes a log?
- Show me a detection and how you followed it.

Frequent nonconformities

- Logs retained only locally.
- No review of logs.
- Admins can alter logs.

Interfaces: ISMS-OPS-SIEM-001, ISMS-OPS-TEMPS-001, ISMS-INC-PROC-001, ISMS-IAM-PRIV-001, ISMS-AUD-EVIDENCE-001

ISMS-OPS-SAUVEGARDE-001 — Backup and restoration policy

Classification C1 · INTERNAL · Format STANDARD · Applicability Core

Objective

Ensure that data and system configurations can be restored within the recovery point and time objectives after loss, corruption or ransomware.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	IT security: backup and restore; business continuity (chapters 3 and 5)
ISO/IEC 27001:2022	A.8.13 Information backup; A.8.14 Redundancy; A.5.30 ICT readiness; A.8.24 Use of cryptography
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
BKP-01	Backup scope, frequency, retention and target RPO shall be defined per service from the BIA.	Backup matrix.
BKP-02	Backups shall follow the 3-2-1 principle with at least one copy offline, immutable or logically isolated from production credentials.	Architecture and immutability setting.
BKP-03	Backups shall be encrypted in transit and at rest, with keys stored separately.	Encryption configuration.
BKP-04	Backup job failures shall alert and be corrected within 1 working day.	Job reports and tickets.
BKP-05	Restore tests shall be performed at least quarterly for critical systems and annually for others, with measured restore times (ISMS-OPS-RESTORE-001).	Restore test records.
BKP-06	Backup administration shall use separate privileged accounts with MFA.	Account evidence.
BKP-07	Backups of customer data shall respect customer retention and location requirements.	Mapping.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Operate backups	Backup administrator	IT manager	Service owners
Verify restores	Backup administrator	IT manager	CISO
Define RPO/RTO	Service owners	BCM manager	Top management

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Backup job reports	Backup tool; administrator	Daily	12 months
Restore test results	ITSM; administrator	Quarterly	3 years
Backup matrix	Document system; IT manager	Annual	3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Successful backup jobs	≥ 99%	< 97%: review
Critical systems with successful restore test in last quarter	100%	Immediate test
Immutable copies available	100% of critical data	Remediation

Auditor questions to prepare

- Show me a restore test and how long it took.
- What protects your backups from ransomware?
- How are backups encrypted?

Frequent nonconformities

- Backups never restore-tested.
- Backups reachable with admin credentials.
- Retention conflicts with customer needs.

Interfaces: ISMS-OPS-RESTORE-001, ISMS-OPS-BACKUP-002, ISMS-PRA-PRA-001, ISMS-CRY-POLITIQUE-001, ISMS-OPS-SUPPRESSION-001

ISMS-OPS-RESEAU-001 — Network security policy

Classification C2 · CONFIDENTIAL · Format STANDARD · Applicability Core

Objective

Protect the network and its services through segmentation, filtering, secure remote access and monitoring so that compromise of one segment does not expose protected information.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	IT security: network management, network segregation and services (chapter 5)
ISO/IEC 27001:2022	A.8.20 Network security; A.8.21 Security of network services; A.8.22 Segregation of networks; A.8.23 Web filtering; A.8.26 Application security requirements
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
NET-01	Current network diagrams and data-flow diagrams shall exist for all in-scope networks and be updated within 30 days of change.	Diagrams with version.
NET-02	Networks shall be segmented by trust and protection need (user, server, management, guest, OT, prototype, supplier); inter-segment traffic shall be denied by default and allowed by documented rule.	Firewall rule base with owners.
NET-03	Firewall rules shall have owner, purpose, requester and expiry or review date and shall be reviewed at least semi-annually.	Rule review records.
NET-04	Remote access shall use encrypted VPN or ZTNA with MFA and device compliance check.	Access configuration.
NET-05	Guest and wireless networks shall be separated from the internal network; unmanaged devices shall be prevented from reaching it (ISMS-OPS-WIFI-001).	Segmentation evidence.
NET-06	Network devices shall be hardened, patched, backed up and managed via secure protocols from a management network.	Device compliance.
NET-07	Network intrusion detection or equivalent monitoring shall cover boundaries and critical segments.	IDS/NDR deployment.
NET-08	Network services provided by third parties shall have security terms and service levels.	Contracts.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Maintain diagrams and rules	Network engineering	IT manager	Security architect
Review firewall rules	Network engineering	CISO	Service owners
Monitor network	SOC	CISO	Network engineering

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Network and data-flow diagrams	Document system; network engineering	On change	Life + 3 years
Firewall rule reviews	Firewall manager; network engineering	Semi-annual	3 years
Remote access reports	VPN/ZTNA; network engineering	Monthly	12 months

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Rules with owner and review date	100%	Review within 14 days
Overly permissive (any-any) rules	0	Immediate
Diagrams older than 12 months	0	Update

Auditor questions to prepare

- Explain how the prototype or customer segment is separated.
- Show me the last firewall rule review.
- How is remote access secured?

Frequent nonconformities

- Flat network.
- Stale firewall rules.
- Diagrams not matching reality.

Interfaces: ISMS-OPS-SEGMENT-001, ISMS-OPS-WIFI-001, ISMS-OPS-EXPO-001, ISMS-OPS-JOURNAUX-001, ISMS-IAM-AUTH-001

ISMS-OPS-CLOUD-001 — Cloud services security policy

Classification C1 · INTERNAL · Format STANDARD · Applicability Core

Objective

Ensure cloud services are selected, configured, operated and exited in a way that preserves the protection of information and the customer's requirements, with clear shared responsibility.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	IT security and supplier relationships: use of external IT services and cloud (chapters 5 and 6)
ISO/IEC 27001:2022	A.5.23 Information security for use of cloud services; A.5.19-A.5.22 Supplier relationships; A.8.9 Configuration management; A.8.24 Cryptography
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
CLD-01	Cloud services shall be registered in an approved-service list with data classification allowed, data location, provider, shared-responsibility matrix and owner.	Cloud register.
CLD-02	A security assessment shall be completed before onboarding, including certifications (ISO 27001, SOC 2, TISAX or C5), data location, sub-processors, incident duties and exit.	Assessment record.
CLD-03	Data of C2/C3 shall remain in contractually agreed regions and use customer-managed or provider-managed keys with encryption.	Configuration evidence.
CLD-04	Tenants shall be hardened using benchmarks and continuous posture monitoring with alerts for public storage, excessive permissions and missing logging.	CSPM reports.
CLD-05	Identity and access for cloud shall follow ISMS-IAM-PRIV-001 and use MFA and just-in-time administration.	Role listings.
CLD-06	Backup, logging and incident contacts shall be arranged with the provider; exit and data return plan shall exist.	Contract and exit plan.
CLD-07	Shadow IT shall be detected and handled.	Discovery reports.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Assess and onboard cloud	Service owner	IT manager	CISO; legal
Operate cloud posture	Cloud engineering	IT manager	CISO
Review provider assurance annually	Supplier manager	CISO	Service owner

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Cloud service register	CMDB; cloud owner	Quarterly	Life + 3 years
Onboarding assessments	Supplier files; supplier manager	Per service	Contract life + 3 years
Posture reports	CSPM; cloud engineering	Weekly	12 months
Provider assurance reports	Supplier files; supplier manager	Annual	3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Cloud services registered and assessed	100%	Unregistered service blocked or assessed within 30 days
Critical posture findings open > 14 days	0	CISO
Provider certificates in date	100%	Request evidence

Auditor questions to prepare

- Where does C3 data reside in the cloud and who can access it?
- Show me how you assessed your last cloud provider.
- What is your exit plan?

Frequent nonconformities

- Unregistered SaaS.
- Public storage buckets.
- Region not controlled.

Interfaces: ISMS-OPS-CLOUD-002, ISMS-FOU-POLITIQUE-001, ISMS-FOU-ASSURANCE-002, ISMS-CRY-POLITIQUE-001, ISMS-INF-HEB-002

ISMS-DEV-SDLC-001 — Secure procurement and development lifecycle

Classification C1 · INTERNAL · Format PROCEDURE · Applicability Core

Objective

Build security into acquisition and development of software and systems through requirements, secure design, secure coding, testing and controlled release.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	IT security: security requirements in new systems and secure development (chapter 5)
ISO/IEC 27001:2022	A.8.25 Secure development life cycle; A.8.26 Application security requirements; A.8.27 Secure system architecture; A.8.28 Secure coding; A.8.29 Security testing; A.8.30 Outsourced development; A.8.33 Test information
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
SDL-01	Security requirements shall be defined for every software project and purchase, based on risk and protection need, and traced to tests.	Requirements and traceability.
SDL-02	Threat modelling shall be performed for new systems and major changes handling C2/C3 data.	Threat model records.
SDL-03	Secure coding guidelines shall exist and developers shall be trained annually.	Guidelines and training.
SDL-04	Source code shall be in version-controlled repositories with branch protection, mandatory peer review and signed commits for release branches.	Repository settings.
SDL-05	Static analysis, dependency and secret scanning shall run on every merge; critical findings shall block release or require approved exception.	Pipeline results.
SDL-06	Dynamic or penetration testing shall be performed before go-live of internet-facing or high-risk applications.	Test reports.
SDL-07	Third-party and open-source components shall be inventoried (SBOM) and monitored for vulnerabilities and licences.	SBOM and alerts.
SDL-08	Production credentials shall not be in code; test data shall not contain production personal data or customer secrets without masking.	Scan results and data policy.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Define requirements	Product owner	Business owner	Security architect
Develop and review	Developers	Engineering manager	Security champion
Run security tests	Security engineering	CISO	Engineering manager
Approve release	Release manager	Service owner	CISO

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Requirements and threat models	Repository; architect	Per project	Product life + 3 years
Pipeline security results	CI/CD; engineering	Per build	12 months
Penetration tests	Document system; CISO	Per release / annual	6 years
SBOM	Repository; engineering	Per release	Product life + 3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Releases with completed security gates	100%	Block
Critical dependency vulnerabilities open > 14 days	0	Escalation
Developers trained in last 12 months	≥ 95%	Plan

Auditor questions to prepare

- Show me how a security requirement flows into tests.
- What blocks a release with a critical vulnerability?
- How do you handle secrets in code?

Frequent nonconformities

- Gates optional.
- No SBOM.
- Production data in test.

Interfaces: ISMS-DEV-TESTS-001, ISMS-DEV-RELEASE-001, ISMS-DEV-EXTERNE-001, ISMS-PRJ-SECURITE-001, ISMS-OPS-CHANGES-001

ISMS-POL-SSI-002 — Full information security policy

Classification C1 · INTERNAL · Format STANDARD · Applicability Core

Objective

Provide a management-approved information security policy that sets direction, objectives and responsibilities for the whole TISAX scope and is the parent of every procedure in the library.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Information security policies and organisation: policy framework (chapter 1)
ISO/IEC 27001:2022	A.5.1 Policies for information security; A.5.2 Roles and responsibilities; Clause 5.2 Policy; Clause 5.1 Leadership
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
POL-01	The policy shall be approved by top management, dated, versioned and signed or electronically approved, and shall name the scope by reference to ISMS-ORG-PERIMETRE-001.	Approval record with approver identity and date.
POL-02	The policy shall state information security objectives that are measurable and reviewed at least annually (ISMS-ORG-OBJECTIFS-001).	Objectives register with owner, target, last measurement.
POL-03	The policy shall commit to compliance with applicable legal, contractual and customer requirements, including TISAX and the VDA ISA, and to continual improvement.	Policy text; link to ISMS-CON-CONFORMITE-001.
POL-04	The policy shall define the information classification scheme and handling duty (ISMS-ACT-CLASSIF-001) and the protection-need levels used by TISAX.	Cross-reference present and consistent.
POL-05	The policy shall be communicated to all employees and relevant external parties and acknowledged on joining and after each material change.	Acknowledgement log with completion rate.
POL-06	The policy shall be reviewed at least annually and after significant organisational, technical or threat change; each review shall be recorded even if no change results.	Review minutes or document control history.
POL-07	A hierarchy of supporting policies and procedures shall exist, each with owner, version and next review date, held in a controlled register (ISMS-ORG-DOC-001).	Document register export.
POL-08	Deviations from the policy shall only be allowed through the exception procedure (ISMS-ORG-DEROGATIONS-001).	Exception register sample.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Draft and maintain policy	ISMS manager	CISO	Legal; HR; IT; works council where applicable
Approve policy	Top management	Managing director	Staff representatives
Communicate and collect acknowledgement	HR and ISMS manager	CISO	All staff
Annual review	CISO	Top management	Control owners

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Approved policy with version history	Document management system; CISO	On change / annual	Superseded versions kept 6 years
Acknowledgement records	HR system or LMS; HR	Joining and on change	Employment + 3 years
Annual policy review record	Management review minutes; CISO	Annual	6 years
Policy exception register	Exception register; CISO	Continuous	Exception life + 3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Policy reviewed within 12 months	100%	Overdue by > 30 days: CISO to top management
Staff acknowledgement of current version	≥ 98% within 30 days of release	< 90%: HR reminder campaign
Objectives with measured result	100%	Unmeasured objective is a management review item

Auditor questions to prepare

- Where is your current approved policy and who approved it?
- How do you know every employee has read it? Show me the data.
- How does top management steer the ISMS beyond signing the policy?
- Show me one change to the policy and how it was communicated.

Frequent nonconformities

- Policy signed by the CISO instead of top management.
- No evidence of review in the last 12 months.
- Policy contradicts a procedure (for example on retention or classification).
- Several policy versions in circulation.

Interfaces: ISMS-POL-SSI-001, ISMS-ORG-OBJECTIFS-001, ISMS-ORG-GOUVERNANCE-001, ISMS-ORG-DOC-001, ISMS-ACT-CLASSIF-001, ISMS-AUD-PROGRAMME-001

ISMS-POL-SSI-001 — Shareable information security policy

Classification C0 · PUBLIC · Format STANDARD · Applicability Core

Objective

Provide a shareable policy statement that can be given to customers and auditors without disclosing internal detail, and that remains consistent with the internal policy.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Information security policies and organisation (chapter 1); information given to customers
ISO/IEC 27001:2022	A.5.1 Policies for information security; A.5.14 Information transfer; A.5.19 Information security in supplier relationships
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
PUB-01	The shareable policy shall be a derivative of ISMS-POL-SSI-002 and shall not contain any statement that is stricter or looser than the internal policy.	Side-by-side consistency check signed by the CISO.
PUB-02	It shall be approved for public release (C0) by the owner and top management before publication, and the approval shall be recorded.	Publication approval record.
PUB-03	It shall exclude internal system names, network detail, personal data and customer names.	Pre-release content review checklist.
PUB-04	It shall carry version, date and next review date, and the version on the website, in the data room and in customer packages shall be identical.	Version comparison across channels.
PUB-05	Customers shall receive the version in force at the time of request; superseded versions shall be retained.	Distribution log.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Prepare shareable version	ISMS manager	CISO	Legal; communications
Approve release	CISO	Top management	Legal
Publish and withdraw	Communications	CISO	Customer managers

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Release approval	Document system; CISO	Per version	6 years
Consistency check	ISMS workspace; ISMS manager	Per version	6 years
Distribution log	Customer register; account owner	Per release	3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Channels carrying the current version	100%	Any stale copy removed within 5 working days
Review on time	100%	Overdue: CISO notified

Auditor questions to prepare

- Is this the same policy you work to internally?
- Who approved it for external publication?
- How do you ensure customers get the current version?

Frequent nonconformities

- Published text differs from the internal policy.
- Unapproved publication.
- Expired version still available online.

Interfaces: ISMS-POL-SSI-002, ISMS-PUB-CONFIANCE-001, ISMS-CLI-FICHE-001, ISMS-ACT-CLASSIF-001

ISMS-ORG-PERIMETRE-001 — ISMS scope and boundaries

Classification C2 · CONFIDENTIAL · Format REGISTER · Applicability Core

Objective

Define precisely which legal entities, sites, networks, systems, processes and assets are in the TISAX assessment scope so that the audit provider can verify that every protected asset is covered and every exclusion is justified.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Scope of the assessment and organisation of information security (chapter 1); assessment objectives (Confidential, Strictly Confidential, Availability)
ISO/IEC 27001:2022	Clause 4.3 Determining the scope of the ISMS; A.5.9 Inventory of information and other associated assets
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
SCP-01	The scope statement shall list legal entities, locations (address level), organisational units, processes and IT services, with the TISAX Participant ID and the scope ID per location.	Scope register reconciled to ENX portal data.
SCP-02	Each scope element shall state the assessment objectives requested by customers (for example Confidential, Strictly Confidential, Availability, prototype protection, data protection).	Objective-to-scope matrix.
SCP-03	Interfaces and dependencies to other sites, cloud providers and suppliers shall be documented, with the party responsible for each control at each interface (ISMS-ORG-INTERFACES-001).	Interface register.
SCP-04	Exclusions shall be listed with rationale, approved by top management and agreed with the audit provider before the assessment.	Exclusion record and provider correspondence.
SCP-05	The scope shall be re-validated at least annually and on any acquisition, relocation, new customer programme or new hosting arrangement.	Review log.
SCP-06	The scope shall be consistent with the asset inventory, network diagrams, data-flow diagrams and the contract with the customer.	Reconciliation evidence.
SCP-07	Sites shall be physically identifiable on a plan showing security zones (ISMS-PHY-ZONES-001).	Site plans with zone marking.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Maintain scope register	ISMS manager	CISO	Facility; IT; legal
Approve scope and exclusions	Top management	Managing director	CISO; audit provider
Keep ENX portal data aligned	ISMS manager	CISO	Account manager
Review on change events	CISO	Top management	Site managers

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Scope register and boundary diagram	ISMS workspace; ISMS manager	Annual / on change	6 years
Exclusion approvals	Document system; CISO	Per exclusion	6 years
ENX portal scope extract	ENX portal; ISMS manager	Per assessment	6 years
Interface register	ISMS workspace; ISMS manager	Quarterly	3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Scope elements with named owner	100%	Orphan element assigned within 10 days
Scope review on time	100%	Overdue: CISO escalates
Unreconciled assets between scope and CMDB	0	Any gap raised as ISMS action

Auditor questions to prepare

- Walk me through your scope. What is explicitly outside and why?
- Where does your data leave the scope and who protects it there?
- Show that every site in the ENX portal is in your register.
- What changed since the last assessment?

Frequent nonconformities

- Scope diagram does not match actual networks.
- Exclusions justified only by convenience.
- A site or cloud tenant missing from scope.

Interfaces: ISMS-ORG-INTERFACES-001, ISMS-ACT-INVENTAIRE-001, ISMS-PHY-ZONES-001, ISMS-ORG-SOA-001, ISMS-AUD-FIELDWORK-001

ISMS-ORG-ROLES-001 — Information security roles and RACI

Classification C1 · INTERNAL · Format PROCEDURE · Applicability Core

Objective

Assign every information security responsibility to a named role and person with sufficient authority, and prevent conflicts of duty.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Organisation of information security: roles, responsibilities and segregation of duties (chapter 1)
ISO/IEC 27001:2022	A.5.2 Information security roles and responsibilities; A.5.3 Segregation of duties; A.6.3 Awareness; Clause 5.3
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
ROL-01	A top management representative shall be accountable for information security, and a CISO or equivalent shall be appointed in writing with a deputy.	Appointment letters.
ROL-02	A RACI matrix covering at least governance, risk, assets, access, operations, incidents, suppliers, audits and prototype protection shall exist and name individuals.	Current RACI export with names.
ROL-03	Each control owner shall have accepted the role in writing and shall have the competence and time required.	Acceptance record; competence record.
ROL-04	Conflicting duties (request versus approve, develop versus release to production, administer versus audit) shall be separated or compensated with documented controls.	Segregation of duties matrix with exceptions.
ROL-05	Roles shall be reviewed at least annually and on every personnel change; vacancies shall have a named stand-in.	Review log.
ROL-06	Security responsibilities shall be included in job descriptions and contracts.	HR templates.
ROL-07	Contact paths to authorities, customers and special interest groups shall be named (ISMS-CLI-INCIDENT-001).	Contact register.
ROL-08	Responsibilities for data protection (ISA 9.2.1) shall be assigned: a data protection officer or equivalent responsible person shall be named with deputy, tasks and reporting line, and the RACI shall show how data protection and information security cooperate.	RACI entries and DPO appointment.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Maintain RACI	ISMS manager	CISO	HR; department heads
Appoint CISO and deputy	Managing director	Top management	HR
Review segregation of duties	IAM owner	CISO	Internal audit
Onboard role holders	HR	Department head	CISO

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Appointment letters	HR system; HR	On change	Employment + 6 years
RACI matrix	ISMS workspace; ISMS manager	Annual	3 years
Segregation of duties analysis	IAM tooling; IAM owner	Semi-annual	3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Roles with named holder and deputy	100%	Vacancy filled or covered within 30 days
SoD conflicts without compensating control	0	CISO decision within 10 days

Auditor questions to prepare

- Who is accountable for information security at top-management level?
- Who stands in when the CISO is absent?
- Show me a segregation-of-duties conflict and how you handled it.

Frequent nonconformities

- Roles described generically without names.
- CISO also acts as sole auditor of own controls.
- No deputy named.

Interfaces: ISMS-ORG-GOUVERNANCE-001, ISMS-IAM-REVUE-001, ISMS-RH-CYCLE-001, ISMS-AUD-PROGRAMME-001

ISMS-ORG-DEROGATIONS-001 — Security exceptions management

Classification C1 · INTERNAL · Format PROCEDURE · Applicability Core

Objective

Allow deviations from security requirements only through a controlled, time-limited, risk-based decision with compensating controls and a defined exit.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Organisation and risk management: handling of deviations and residual risk (chapters 1)
ISO/IEC 27001:2022	A.5.1 Policies; Clause 6.1.3 Risk treatment; Clause 8.3 Risk treatment; A.5.36 Compliance with policies and standards
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
EXC-01	No exception shall be valid without a written request stating requirement, reason, affected assets, impact, compensating controls, duration and exit plan.	Exception record template completed.
EXC-02	Risk assessment of the exception shall be performed by someone other than the requester.	Reviewer identity on record.
EXC-03	Approval authority shall depend on residual risk: low – service owner; medium – CISO; high or any exception affecting customer requirements – top management and, where the contract requires, the customer.	Approval matrix and signed records.
EXC-04	Every exception shall expire within 12 months at most (90 days for vulnerabilities) and shall be re-approved, closed or converted into a risk-treatment plan before expiry.	Register with expiry dates.
EXC-05	The exception register shall be reviewed monthly by the CISO and reported in management review.	Review minutes.
EXC-06	Exceptions affecting TISAX-relevant controls shall be disclosed to the audit provider on request and reflected in ISMS-ORG-SOA-001.	Disclosure log.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Request exception	Control owner	Service owner	CISO
Assess residual risk	ISMS manager	CISO	Risk owner
Approve exception	Approver per matrix	Top management	Customer programme
Monitor expiry	ISMS manager	CISO	Control owners

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Exception requests and approvals	Exception register; CISO	Per exception	Life + 3 years
Monthly register review	Meeting minutes; CISO	Monthly	3 years
Expiry and closure evidence	Ticket system; ISMS manager	Per exception	Life + 3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Expired exceptions still active	0	Immediate CISO escalation
Exceptions older than 12 months	0	Top management review
Exceptions with compensating controls tested	100%	Untested control reopens exception

Auditor questions to prepare

- How many exceptions are active? Show me the register.
- Show an exception that expired. What happened?
- Who may approve a high-risk exception?

Frequent nonconformities

- Open-ended exceptions.
- Exceptions approved by the requester's own line manager only.
- Exceptions not reflected in the risk register.

Interfaces: ISMS-RSK-REGISTRE-001, ISMS-RSK-TRAITEMENT-001, ISMS-OPS-VULN-001, ISMS-ORG-SOA-001, ISMS-AUD-CLOSURE-001

ISMS-ACT-CLASSIF-001 — Information classification and handling

Classification C1 · INTERNAL · Format PROCEDURE · Applicability Core

Objective

Ensure information is classified by protection need, labelled and handled accordingly through its life cycle, including customer-defined markings.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Asset management: classification and handling of information; protection needs 'confidential' and 'strictly confidential' (chapter 1)
ISO/IEC 27001:2022	A.5.12 Classification of information; A.5.13 Labelling of information; A.5.10 Acceptable use of information; A.7.10 Storage media
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
CLS-01	A four-level scheme (C0 public, C1 internal, C2 confidential, C3 strictly confidential) shall be mapped to the TISAX protection needs and to customer marking schemes.	Mapping table approved by the CISO.
CLS-02	The owner of each information asset shall assign the classification at creation or receipt and review it at least annually or on change of use.	Asset register classification column with owner and date.
CLS-03	Classification markings shall be applied in documents (header/footer), sensitivity labels in the productivity suite, and in storage and transfer controls.	Label configuration export and sample documents.
CLS-04	Handling rules (storage, transfer, printing, disposal, remote access, sharing with suppliers) shall be defined per level and be technically enforced where possible.	DLP and encryption policy exports.
CLS-05	Customer-supplied markings shall be preserved and shall take precedence over internal labels.	Sample of customer documents with preserved markings.
CLS-06	Information of level C3 shall be limited to named individuals and logged for access.	Access list and access log.
CLS-07	Staff shall be trained on classification at onboarding and annually.	Training record.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Define scheme	CISO	Top management	Legal; customers
Classify information assets	Information owners	Department heads	ISMS manager
Configure labels and DLP	IT operations	IT manager	CISO
Verify labelling by sampling	ISMS reviewer	CISO	Information owners

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Classification scheme and mapping	Document system; CISO	Annual	3 years
Asset classifications	Asset register; asset owners	Annual	3 years
Label and DLP configuration	Security console; IT operations	Quarterly	3 years
Labelling sample results	ISMS workspace; reviewer	Semi-annual	3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Sampled documents correctly labelled	≥ 95%	< 90%: awareness action
Assets with owner-assigned classification	100%	Unclassified assets closed within 30 days
C3 information accessed outside named list	0	Incident procedure

Auditor questions to prepare

- Show me a C3 document and tell me who can read it and how that is enforced.
- How do you handle a customer's own marking?
- How do you detect mislabelled data?

Frequent nonconformities

- Scheme exists but is not applied on stored data.
- No mapping to customer schemes.
- Labels optional with no technical enforcement for the highest levels.

Interfaces: ISMS-ACT-INVENTAIRE-001, ISMS-OPS-DLP-001, ISMS-CRY-POLITIQUE-001, ISMS-PHY-SUPPORTS-001, ISMS-CLI-EXIGENCES-001

ISMS-ACT-INVENTAIRE-001 — Asset management and inventory

Classification C2 · CONFIDENTIAL · Format REGISTER · Applicability Core

Objective

Maintain a complete, owned and current inventory of information and supporting assets, so that protection measures, access reviews and vulnerability management cover every in-scope item.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Asset management: inventory and ownership of information, applications and IT systems (chapter 1)
ISO/IEC 27001:2022	A.5.9 Inventory of information and other associated assets; A.5.11 Return of assets; A.8.1 User endpoint devices; A.7.14 Secure disposal
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
AST-01	The inventory shall cover information assets, applications, servers, endpoints, network devices, cloud services, OT components and supplier-hosted assets in scope.	Inventory export reconciled to scope register.
AST-02	Each asset shall have owner, classification, location, criticality, supporting service, lifecycle status and support end date.	Mandatory field completeness report.
AST-03	The inventory shall be updated on acquisition, change and disposal, and shall be reconciled with discovery tools (network, endpoint, cloud) at least monthly.	Reconciliation log.
AST-04	Unknown or unmanaged devices detected on the network shall be investigated within 5 working days.	Discovery alert tickets.
AST-05	Assets shall be returned or sanitised on leaving the organisation or being retired, with disposal certificates for media (ISMS-OPS-SUPPRESSION-001).	Return and disposal records.
AST-06	The inventory shall feed access review, vulnerability management, backup and risk assessment.	Evidence of use in those processes.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Maintain inventory	IT operations / CMDB owner	IT manager	Asset owners
Confirm ownership annually	Asset owners	Department heads	ISMS manager
Run discovery reconciliation	Security engineering	CISO	IT operations
Dispose of assets	IT operations	IT manager	ISMS manager

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Asset inventory with attributes	CMDB; CMDB owner	Continuous	Life + 3 years
Reconciliation reports	CMDB and scanners; engineering	Monthly	3 years
Disposal certificates	Procurement files; IT operations	Per disposal	6 years
Ownership confirmation	Asset register; asset owners	Annual	3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Assets with complete mandatory attributes	≥ 98%	< 95%: data quality plan
Discovery exceptions open > 5 days	0	CISO notified
Assets without owner	0	Assign within 10 days

Auditor questions to prepare

- How do you know your inventory is complete?
- Pick a server and show me owner, classification and patch state.
- How are cloud and personal devices captured?

Frequent nonconformities

- Spreadsheet inventory not reconciled to tools.
- No owner for shared systems.
- Assets still listed after disposal.

Interfaces: ISMS-OPS-CMDB-001, ISMS-ACT-CLASSIF-001, ISMS-OPS-VULN-001, ISMS-OPS-SUPPRESSION-001, ISMS-IAM-REVUE-001

ISMS-RSK-METHODE-001 — Information security risk methodology

Classification C1 · INTERNAL · Format STANDARD · Applicability Core

Objective

Define a repeatable, documented risk methodology that identifies, analyses, evaluates and treats information security risks for the whole scope and produces comparable results over time.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Information security risk management: assessment, treatment and acceptance (chapter 1)
ISO/IEC 27001:2022	Clauses 6.1.2 and 6.1.3 Risk assessment and treatment; Clause 8.2; A.5.7 Threat intelligence
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
RSM-01	The methodology shall define scales for likelihood and impact (including legal, customer and safety impact), the risk-acceptance criteria and who decides.	Methodology with scales and approved criteria.
RSM-02	A complete assessment shall be performed at least annually and on significant change, covering assets, threats, vulnerabilities, existing controls and protection needs.	Assessment report dated within 12 months.
RSM-03	Each risk shall have an owner, a treatment decision (reduce, avoid, transfer, accept) and a due date.	Risk register entries.
RSM-04	Residual risks above the acceptance threshold shall be accepted by top management in writing.	Acceptance records.
RSM-05	Risk treatment shall link to controls in the statement of applicability and be verified for effectiveness.	Control-to-risk mapping.
RSM-06	Results shall be reported in management review and used for audit planning and objectives.	Management review inputs.
RSM-07	Threat information relevant to automotive and supply-chain risks shall be considered at least quarterly.	Threat review notes.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Define methodology	CISO	Top management	Risk owners
Run assessments	Risk coordinator	CISO	Asset and process owners
Treat risks	Risk owners	Department heads	ISMS manager
Accept residual risk	Risk owners	Top management	CISO

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Risk methodology	Document system; CISO	Annual	3 years
Risk assessment reports	Risk tool; risk coordinator	Annual / on change	6 years
Risk register	Risk tool; ISMS manager	Continuous	6 years
Residual-risk acceptances	Document system; top management	Per decision	6 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Risks with owner and treatment date	100%	Unassigned risks escalated at next meeting
High risks overdue for treatment	0	Top management review
Risk assessment within 12 months	100%	Triggers audit finding

Auditor questions to prepare

- How did you decide which risks to accept?
- Show me how a new threat entered the register.
- Who is the risk owner for your prototype data?

Frequent nonconformities

- Risk assessment has not been updated for over a year.
- Risk scales not applied consistently.
- Acceptance by the CISO without top management.

Interfaces: ISMS-RSK-REGISTRE-001, ISMS-RSK-TRAITEMENT-001, ISMS-ORG-MENACES-001, ISMS-ORG-SOA-001, ISMS-AUD-PROGRAMME-001

ISMS-PRJ-SECURITE-001 — Security in projects

Classification C1 · INTERNAL · Format PROCEDURE · Applicability Core

Objective

Integrate information security into every project and change to products, services and infrastructure from initiation, so security requirements are defined, built and verified before go-live.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Organisation of information security: information security in projects (chapter 1); security requirements in new systems
ISO/IEC 27001:2022	A.5.8 Information security in project management; A.8.25 Secure development life cycle; A.8.26 Application security requirements; A.8.29 Security testing
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
PRJ-01	A security classification and risk screening shall be completed at project initiation and shall determine required security activities.	Completed screening form per project.
PRJ-02	Security requirements shall be documented, traceable to the risk assessment and customer requirements, and approved before design freeze.	Requirements list with approval.
PRJ-03	Security review gates shall exist at design, before testing and before go-live; go-live shall require signed security approval.	Gate records.
PRJ-04	Projects handling protected information or customer prototypes shall state data locations, suppliers and access models in the project plan.	Project documentation.
PRJ-05	Residual security risks at closure shall be handed to the service owner and recorded in the risk register.	Handover record.
PRJ-06	Project security status shall be reported to the CISO at least quarterly for active projects.	Status report.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Screen project risk	Project manager	Project sponsor	CISO
Define security requirements	Security architect	CISO	Project team
Approve go-live security	CISO delegate	CISO	Service owner
Hand over residual risk	Project manager	Service owner	ISMS manager

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Security screening	Project portal; project manager	Per project	6 years
Security requirements and approvals	Project portal; architect	Per project	6 years
Gate and go-live approvals	Change system; CISO delegate	Per gate	6 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Projects with completed screening	100%	Stop-work for missing screening
Go-lives with security approval	100%	Emergency path only with CISO sign-off
Security defects open at go-live	0 high	Waiver via exception procedure

Auditor questions to prepare

- Show me a recent project and its security approvals.

- How are security requirements derived?
- What happens if a project wants to go live without approval?

Frequent nonconformities

- Screening done after design.
- Go-live approval by project manager only.
- No handover of residual risks.

Interfaces: ISMS-DEV-SDLC-001, ISMS-OPS-CHANGES-001, ISMS-RSK-METHODE-001, ISMS-FOU-POLITIQUE-001

ISMS-AUD-PROGRAMME-001 — Internal audit, self-assessment and management review

Classification C1 · INTERNAL · Format PROCEDURE · Applicability Core

Objective

Verify at regular intervals, independently and with documented evidence, that the ISMS conforms to requirements and is effective, and feed results into management review and continual improvement.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Assessments: compliance with requirements, independent review of information security, management review (chapter 1)
ISO/IEC 27001:2022	Clause 9.2 Internal audit; Clause 9.3 Management review; A.5.35 Independent review; A.5.36 Compliance with policies
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
AUD-01	A three-year audit programme shall cover every ISA control area and every site at least once, with higher-risk areas audited at least annually.	Programme with coverage matrix.
AUD-02	Auditors shall be independent of the audited activity and shall be competent.	Auditor competence and independence declaration.
AUD-03	Each audit shall have a plan, criteria, sample, evidence list and a report with findings classified by severity and maturity impact.	Audit plan and report.
AUD-04	An ISA self-assessment with maturity scoring shall be performed at least annually and before every TISAX assessment.	Self-assessment workbook.
AUD-05	Findings shall be tracked to verified closure with owner and due date (ISMS-AUD-CLOSURE-001).	Finding register.
AUD-06	Management review shall take place at least annually, with prescribed inputs (audit results, incidents, risks, objectives, supplier status, customer feedback, changes) and recorded decisions.	Management review minutes.
AUD-07	Management review decisions shall have owners and be tracked.	Action log.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Plan audit programme	ISMS manager	CISO	Top management
Conduct audits	Internal or external auditor	ISMS manager	Auditees
Close findings	Finding owners	Department heads	Reviewer
Chair management review	CISO	Managing director	Control owners

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Audit programme and plans	Audit tool; ISMS manager	Annual	6 years
Audit reports and evidence	Audit tool; auditors	Per audit	6 years
Management review minutes	Document system; CISO	Annual	6 years
Findings register	Audit tool; ISMS manager	Continuous	6 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Planned audits delivered	100%	Slippage explained to top management
Findings closed on time	≥ 90%	< 80%: management review item
Repeat findings	0	Root-cause analysis required

Auditor questions to prepare

- Show me last year's audit programme and what was actually audited.
- Who audits the ISMS manager's work?
- Which decision did management take from the last review?

Frequent nonconformities

- Auditors audit own work.
- Management review without prescribed inputs.
- Findings closed without verification.

Interfaces: ISMS-AUD-CLOSURE-001, ISMS-AUD-MATURITY-001, ISMS-AUD-SAMPLE-001, ISMS-ORG-OBJECTIFS-001, ISMS-RSK-REGISTRE-001

ISMS-INC-PROC-001 — Information security incident management

Classification C2 · CONFIDENTIAL · Format PROCEDURE · Applicability Core

Objective

Detect, report, assess, contain, eradicate and learn from information security events and incidents in a timeframe that satisfies customer, legal and contractual notification duties.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Incident and crisis management: reporting of events, incident handling and learning (chapter 1)
ISO/IEC 27001:2022	A.5.24 Incident management planning; A.5.25 Assessment of events; A.5.26 Response; A.5.27 Learning; A.5.28 Evidence collection; A.6.8 Event reporting
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
INC-01	All staff and contractors shall be able to report events through at least two channels available 24/7 and shall be told they will not be penalised for good-faith reporting.	Reporting channel descriptions and awareness material.
INC-02	Events shall be logged and classified within 4 hours of receipt using defined severity criteria including confidentiality impact on customer data and prototypes.	Incident tickets with timestamps.
INC-03	Roles for incident commander, technical lead, communications and legal shall be assigned with deputies and on-call coverage.	On-call roster.
INC-04	Customers with contractual notification duties shall be notified within the contractual period, and in any case within 24 hours of confirming a breach of their information unless stricter terms apply (ISMS-CLI-INCIDENT-001).	Notification records.
INC-05	Evidence shall be preserved under chain of custody before containment where feasible (ISMS-INC-PRESERVATION-001).	Evidence log.
INC-06	Each major incident shall have a post-incident review within 10 working days with root cause, actions and lessons.	Review report.
INC-07	The procedure shall be exercised at least annually (ISMS-INC-EXERCISE-001).	Exercise report.
INC-08	Incident statistics and trends shall be reported to management quarterly.	Quarterly report.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Receive and classify event	Service desk / SOC	Incident manager	CISO
Contain and eradicate	Technical lead	Incident manager	Service owners
Notify customers and authorities	Communications and legal	CISO	Top management
Run post-incident review	ISMS manager	CISO	Participants

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Incident tickets and timeline	Ticket system; incident manager	Per incident	6 years
Notification records	Document system; CISO	Per incident	6 years
Post-incident review	ISMS workspace; ISMS manager	Per major incident	6 years
Evidence log	Evidence vault; incident manager	Per incident	Per legal need

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Events classified within 4 hours	≥ 95%	< 90%: staffing review
Customer notifications within contract time	100%	Any miss reported to top management
Post-incident reviews within 10 days	≥ 90%	Overdue list at ISMS meeting

Auditor questions to prepare

- Walk me through your last incident from detection to review.
- How do staff know how to report?
- How did you decide whether to notify the customer?
- When did you last exercise this?

Frequent nonconformities

- Events handled by email with no ticket.
- No classification criteria for customer-data events.
- Lessons learned not tracked.

Interfaces: ISMS-CLI-INCIDENT-001, ISMS-INC-CRISE-001, ISMS-INC-PRESERVATION-001, ISMS-INC-EXERCISE-001, ISMS-OPS-JOURNAUX-001, ISMS-OPS-SIEM-001

ISMS-INC-CRISE-001 — Crisis management and communications

Classification C2 · CONFIDENTIAL · Format PROCEDURE · Applicability Core

Objective

Provide a crisis organisation able to take decisions and communicate internally and externally when an incident threatens business operations, safety, customer trust or legal standing.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Incident and crisis management: crisis organisation and communication (chapter 1); business continuity link (chapter 3)
ISO/IEC 27001:2022	A.5.29 Information security during disruption; A.5.30 ICT readiness for business continuity; A.5.5 Contact with authorities
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
CRI-01	Crisis criteria and the activation authority shall be defined; activation shall be possible 24/7.	Activation criteria and on-call contact list.
CRI-02	A crisis team with named members and deputies shall be defined, including top management, CISO, IT, legal, communications and HR.	Crisis team roster.
CRI-03	Communication templates and approved spokespersons shall exist for customers, authorities, staff and media.	Template set.
CRI-04	Alternative communication channels independent of the compromised systems shall be available.	Out-of-band channel test.
CRI-05	Crisis decisions and timelines shall be logged contemporaneously.	Decision log.
CRI-06	The crisis plan shall be exercised annually and updated after exercises and real events.	Exercise records and updates.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Activate crisis	Incident manager	CISO	Top management
Lead crisis team	CISO	Managing director	Crisis team
Communicate externally	Communications	Managing director	Legal; customers

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Crisis plan and roster	Document system; CISO	Semi-annual	3 years
Crisis log	Crisis log tool; secretary	Per crisis	6 years
Exercise report	ISMS workspace; ISMS manager	Annual	3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Crisis roster verified	Twice yearly	Unreachable members replaced within 5 days
Exercise performed	Annual	Missed exercise is an audit finding

Auditor questions to prepare

- Who can declare a crisis and how fast can the team assemble?
- How would you communicate if email was down?
- Show me what you learned from your last exercise.

Frequent nonconformities

- Crisis roster outdated.
- No out-of-band channel.
- Plan never exercised.

Interfaces: ISMS-INC-PROC-001, ISMS-INC-EXERCISE-001, ISMS-PRA-PCA-001, ISMS-CLI-INCIDENT-001

ISMS-CLI-EXIGENCES-001 — Customer information security requirements

Classification C2 · CONFIDENTIAL · Format PROCEDURE · Applicability Core

Objective

Capture, interpret, assign and monitor information security requirements imposed by customers so that none is missed and each is mapped to a control and an owner.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Compliance and organisation: contractual and customer requirements (chapters 1 and 7)
ISO/IEC 27001:2022	A.5.31 Legal, statutory, regulatory and contractual requirements; A.5.19 and A.5.20 Supplier relationships; A.5.34 Privacy
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
CRQ-01	Every customer contract, security annex and specification shall be reviewed within 10 working days of receipt and its security obligations extracted into a register.	Requirements register with source references.
CRQ-02	Each requirement shall be mapped to an ISMS control, an owner and a verification method.	Mapping and owner fields.
CRQ-03	Conflicts between customer requirements, or with internal policy, shall be escalated to the CISO and resolved in writing.	Conflict log.
CRQ-04	Customer-specific markings, notification times, location restrictions and audit rights shall be flowed down to suppliers where applicable.	Flow-down records.
CRQ-05	The register shall be reviewed at least semi-annually and on contract change.	Review log.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Extract requirements	Contract manager	Customer account owner	ISMS manager
Map to controls	ISMS manager	CISO	Control owners
Resolve conflicts	CISO	Top management	Legal

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Customer requirements register	ISMS workspace; ISMS manager	Per contract / semi-annual	Contract life + 6 years
Conflict decisions	Document system; CISO	Per conflict	Contract life + 6 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Contracts reviewed within 10 days	100%	Escalate delay to CISO
Requirements without mapped control	0	Mapped within 10 days

Auditor questions to prepare

- How do you know what your customers require?
- Show me one customer requirement and the control that meets it.
- How do you flow requirements to suppliers?

Frequent nonconformities

- Requirements read once and never tracked.
- No owner for customer obligations.
- Flow-down missing.

Interfaces: ISMS-CLI-ENGAGEMENTS-001, ISMS-CLI-ANNEXE-001, ISMS-FOU-POLITIQUE-001, ISMS-CON-CONFORMITE-001

ISMS-RH-CYCLE-001 — Employee joiner-mover-leaver lifecycle

Classification C1 · INTERNAL · Format PROCEDURE · Applicability Core

Objective

Control the full employment lifecycle (screening, joining, role change, leaving) so that trust, access, equipment and knowledge are granted, adjusted and withdrawn on time and with evidence.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Human resources: screening, contractual obligations, termination and change of employment (chapter 2)
ISO/IEC 27001:2022	A.6.1 Screening; A.6.2 Terms and conditions of employment; A.6.5 Responsibilities after termination; A.5.11 Return of assets; A.5.18 Access rights
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
JML-01	Background screening proportionate to role and protection need, and lawful in the country concerned, shall be completed before access to C2 or C3 information is granted.	Screening completion record per sampled hire.
JML-02	Employment contracts and contractor agreements shall contain confidentiality and information security obligations that survive termination.	Contract templates and signed samples.
JML-03	Joiner access shall be requested by the line manager on a role template and approved by the data owner; no access shall be granted before start date and signed obligations.	Access request ticket dates versus start date.
JML-04	Role changes shall trigger access re-evaluation within 5 working days and removal of rights no longer needed.	Mover tickets.
JML-05	Leavers' access shall be disabled no later than the end of the last working day (immediately for dismissal for cause), and assets returned and recorded.	HR leaving date versus account disable timestamp.
JML-06	Leavers shall receive a reminder of continuing confidentiality duties and an exit checklist signed by manager.	Exit checklist.
JML-07	HR leaver data shall be reconciled to the identity system monthly to find orphan accounts.	Reconciliation report.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Screen candidates	HR	HR manager	Line manager; legal
Provision joiners	IT service desk	IAM owner	Line manager; data owners
Process role changes	Line manager	Department head	IAM owner
Deprovision leavers	IT service desk	IAM owner	HR; line manager

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Screening results (minimal)	HR system; HR	Per hire	Employment + 1 year or as law allows
Signed obligations	HR system; HR	Per hire	Employment + 6 years
Joiner/mover/leaver tickets	Ticket system; service desk	Per event	3 years
Exit checklist and asset return	HR system; line manager	Per leaver	3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Leaver accounts disabled on last day	100%	Any miss is an incident review
Joiners with completed screening before access	100%	Stop access until completed
Orphan accounts found per month	0	Root-cause analysis

Auditor questions to prepare

- Pick three leavers: show the leaving date, account disable time and asset return.
- How do you screen people who handle prototypes?
- How do you detect that a person changed role and kept old access?

Frequent nonconformities

- Accounts disabled days after leaving.
- Screening after access was granted.
- Contractors outside HR process.

Interfaces: ISMS-IAM-CYCLE-001, ISMS-IAM-REVUE-001, ISMS-RH-NDA-001, ISMS-RH-CHARTE-001, ISMS-RH-SENSIBILISATION-001

ISMS-RH-SENSIBILISATION-001 — Security awareness and training programme

Classification C1 · INTERNAL · Format STANDARD · Applicability Core

Objective

Make all personnel competent and aware of their information security responsibilities through role-appropriate, tracked and measured training and awareness activities.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Human resources: awareness and training of employees (chapter 2)
ISO/IEC 27001:2022	A.6.3 Awareness, education and training; A.5.4 Management responsibilities; A.6.8 Event reporting
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
AWR-01	Every employee and contractor shall complete security induction within 10 working days of joining and before access to C2/C3 data.	Training records by hire date.
AWR-02	All staff shall complete refresher training at least annually; completion shall be tracked and escalated to the line manager and top management at 30 and 60 days overdue.	LMS completion report.
AWR-03	Role-based modules shall exist for administrators, developers, HR, reception/security, managers with C3 data, and prototype handlers.	Curriculum and attendance.
AWR-04	Phishing and social-engineering simulations shall be run at least twice yearly with measured click and report rates.	Simulation results and follow-up.
AWR-05	Content shall be reviewed annually against incident trends and the threat picture.	Content review record.
AWR-06	Effectiveness shall be assessed, for example through tests, simulations and incident metrics, and results used to improve the programme.	Effectiveness report.
AWR-07	Awareness of TISAX specifics (labels, customer markings, prototype rules, reporting duty) shall be demonstrated by interview sample.	Interview sample results.
AWR-08	Staff who process personal data (ISA 9.7.2) shall complete data protection training at induction and at least annually covering principles, data subject rights, breach reporting and processor instructions, with completion tracked and escalated like security training.	Data protection training records.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Design programme	ISMS manager	CISO	HR; department heads
Deliver training	HR / training provider	HR manager	ISMS manager
Chase completion	Line managers	Department heads	HR
Run simulations	Security engineering	CISO	HR; works council

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Training completion	LMS; HR	Per course	3 years
Simulation results	Phishing platform; engineering	Semi-annual	3 years
Programme review	ISMS workspace; ISMS manager	Annual	3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Annual training completion	≥ 98%	< 95%: top management notice
Phishing simulation report rate	≥ 60%	< 40%: targeted campaign
Click rate	≤ 5%	> 10%: remedial training

Auditor questions to prepare

- Show completion rates for the last cycle and what you did about laggards.
- What training do your administrators get?
- Ask any employee: how do you report an incident?

Frequent nonconformities

- Generic training for everyone.
- No tracking of contractors.
- No link between incidents and content.

Interfaces: ISMS-RH-CYCLE-001, ISMS-INC-PROC-001, ISMS-RH-CHARTE-001, ISMS-PRO-RECON-001

ISMS-RH-CHARTE-001 — Employee IT acceptable-use charter

Classification C1 · INTERNAL · Format AGREEMENT · Applicability Core

Objective

Give employees clear, enforceable rules for the acceptable use of information, systems and devices, acknowledged in writing.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Human resources: contractual obligations and acceptable use (chapter 2); handling of assets
ISO/IEC 27001:2022	A.5.10 Acceptable use of information and other assets; A.6.2 Terms and conditions; A.8.1 User endpoint devices; A.5.14 Information transfer
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
ACU-01	The charter shall cover use of devices, accounts, email, internet, removable media, personal devices, AI tools and external sharing services, and the reporting duty.	Charter text.
ACU-02	Each person shall accept the charter before receiving access and after every material version, and the acceptance shall be recorded.	Acceptance log.
ACU-03	Breach consequences shall be defined and consistent with employment law; a disciplinary process shall exist.	HR procedure.
ACU-04	Use of generative AI tools with company or customer information shall be restricted to approved tools (ISMS-ORG-AI-001).	AI use rules.
ACU-05	The charter shall be reviewed annually.	Review record.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Maintain charter	ISMS manager	CISO	HR; legal; works council
Collect acceptance	HR	HR manager	Line manager
Handle breaches	HR	HR manager	CISO

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Signed charter acceptance	HR system; HR	Joining / on change	Employment + 3 years
Breach cases	HR case system; HR	Per case	As law allows

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Staff with current acceptance	100%	Access reviewed for missing acceptance
Review on time	100%	CISO notified

Auditor questions to prepare

- Show me an employee's acceptance record.
- What may staff not do with customer data?
- How are breaches handled?

Frequent nonconformities

- Acceptance only at hiring, never refreshed.

- No AI tool rules.
- Rules not enforceable under local law.

Interfaces: ISMS-RH-CYCLE-001, ISMS-RH-TELETRAVAIL-001, ISMS-RH-MOBILE-001, ISMS-ORG-AI-001, ISMS-OPS-DLP-001

ISMS-RH-TELETRAVAIL-001 — Remote and mobile work policy

Classification C1 · INTERNAL · Format STANDARD · Applicability Core

Objective

Ensure information remains protected when people work outside controlled premises, including at home, in transit and at customer or third-party sites.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Human resources: mobile working and teleworking (chapter 2); physical security of mobile devices (chapter 3)
ISO/IEC 27001:2022	A.6.7 Remote working; A.7.9 Security of assets off-premises; A.8.1 User endpoint devices; A.8.20 Network security
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
REM-01	Remote work with C2/C3 information shall be permitted only on managed, encrypted devices with MFA and a company VPN or equivalent zero-trust access.	Endpoint and access policy exports.
REM-02	Staff shall not work on C3 information in public places, and shall use privacy screens, lock screens within 5 minutes and never leave devices unattended.	Policy and awareness evidence.
REM-03	Home-office minimum conditions (private space, secure Wi-Fi, no shared use of the device) shall be acknowledged by the employee.	Signed declaration.
REM-04	Printing, local storage and use of personal cloud storage for company data shall be blocked or prohibited.	DLP configuration.
REM-05	Remote work from outside the approved countries shall require prior approval and a risk assessment.	Approval records.
REM-06	Lost or stolen devices shall be reported immediately and remotely wiped or locked.	Device loss tickets and MDM logs.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Define rules	ISMS manager	CISO	HR; works council
Enforce device controls	IT operations	IT manager	CISO
Approve foreign working	Line manager	Department head	CISO; legal

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Remote-work declaration	HR system; HR	Joining / annual	Employment + 3 years
MDM compliance report	MDM; IT operations	Monthly	3 years
Foreign-working approvals	Ticket system; line managers	Per case	3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Remote devices compliant with policy	≥ 98%	< 95%: access conditional block
Lost devices wiped within 4 hours of report	100%	Incident review

Auditor questions to prepare

- How do you protect a laptop with C3 data lost in a train?
- How do you know staff at home use a secure network?
- Can someone work from abroad? Show me an approval.

Frequent nonconformities

- Personal devices used without controls.
- No evidence of encryption.
- Foreign working allowed without approval.

Interfaces: ISMS-RH-MOBILE-001, ISMS-OPS-ENDPOINT-001, ISMS-IAM-AUTH-001, ISMS-OPS-WIFI-001, ISMS-OPS-DLP-001

ISMS-RH-MOBILE-001 — Mobile device and BYOD controls

Classification C1 · INTERNAL · Format PROCEDURE · Applicability Core

Objective

Control the security of smartphones, tablets and privately owned devices (BYOD) that access company information.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Mobile devices and teleworking (chapters 2 and 3); user endpoint protection
ISO/IEC 27001:2022	A.8.1 User endpoint devices; A.6.7 Remote working; A.7.9 Off-premises assets; A.5.10 Acceptable use
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
MOB-01	All mobile devices accessing company data shall be enrolled in a mobile device management or container solution before access.	MDM enrolment export versus access logs.
MOB-02	Minimum baseline shall be enforced: device encryption, PIN or biometric, OS within the supported and patched versions, jailbreak/root detection, remote wipe.	MDM compliance policies.
MOB-03	BYOD shall be limited to the corporate container; C3 information shall not be stored on private devices.	BYOD policy and technical restriction.
MOB-04	Non-compliant devices shall lose access within 24 hours.	Conditional access logs.
MOB-05	Device loss, theft and leaving shall result in wipe of company data and recorded in tickets.	Wipe records.
MOB-06	Cameras and recording in prototype areas shall follow ISMS-PRO-RECON-001.	Policy reference.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Run MDM	IT operations	IT manager	CISO
Approve BYOD exceptions	Line manager	CISO	HR; legal
Respond to loss	Service desk	IT manager	CISO

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Enrolment and compliance report	MDM; IT operations	Monthly	3 years
Wipe actions	MDM and ticket; service desk	Per event	3 years
BYOD approvals	Ticket system; line manager	Per device	Device life + 1 year

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Mobile devices compliant	≥ 98%	< 95%: access restriction
Wipe completed within 4 hours	100%	Incident review

Auditor questions to prepare

- How do you stop an unmanaged phone from reading mail?
- Show me a non-compliant device and what happened.
- What may BYOD users store?

Frequent nonconformities

- Mail accessible from unmanaged devices.
- No remote wipe evidence.
- No distinction by classification.

Interfaces: ISMS-RH-TELETRAVAIL-001, ISMS-OPS-ENDPOINT-001, ISMS-IAM-AUTH-001, ISMS-PRO-RECON-001

ISMS-PHY-ZONES-001 — Physical security zones and premises

Classification C2 · CONFIDENTIAL · Format PROCEDURE · Applicability Core

Objective

Protect premises, rooms and facilities holding or processing protected information through defined security zones, entry control, monitoring and environmental protection verified on site.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Physical security: security zones, protection against external and environmental threats, visitor and delivery handling (chapter 3)
ISO/IEC 27001:2022	A.7.1 Physical security perimeters; A.7.2 Physical entry; A.7.3 Securing offices; A.7.4 Physical security monitoring; A.7.5 Environmental threats; A.7.6 Working in secure areas; A.7.8 Equipment siting
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
PHY-01	Security zones shall be defined per site (for example public, office, restricted, high-security) with the information classification permitted in each and shown on site plans.	Zone plans and rules.
PHY-02	Entry to non-public zones shall use an access-control system with individual credentials; shared keys and codes shall not protect C2/C3 areas.	Access-control system export.
PHY-03	Access rights to restricted zones shall be reviewed quarterly by the zone owner and removed on leaving.	Review record.
PHY-04	Visitors shall be registered, identified, badged and escorted in non-public zones; the visitor log shall be kept for 12 months.	Visitor log sample.
PHY-05	Entry events shall be logged, with alarm for forced doors and doors held open; intrusion detection and (where lawful) video monitoring shall cover restricted zones, with defined retention.	Alarm tests and log extracts.
PHY-06	Server rooms and network cabinets shall have restricted access, fire detection and suppression, temperature and humidity monitoring, and UPS and power-failure protection tested at least annually.	Maintenance and test certificates.
PHY-07	Deliveries and shipping shall be received in a controlled area and not given direct access to restricted zones (ISMS-PHY-SUPPORTS-001).	Delivery procedure and samples.
PHY-08	Clean-desk, locked cabinets, screen lock and secure printing shall be enforced and checked by spot checks at least quarterly.	Spot-check reports.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Operate access control	Facility management	Site manager	CISO
Review zone access	Zone owners	Department heads	Facility management
Test environmental protection	Facility management	Site manager	IT operations
Spot-check clean desk	ISMS reviewer	CISO	Department heads

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Zone register and plans	ISMS workspace; facility manager	Annual / on change	3 years
Access-control logs and reviews	Access system; facility management	Quarterly review	12 months logs; 3 years reviews
Visitor log	Visitor system; reception	Daily	12 months
Fire, UPS and climate test records	Facility files; facility manager	Annual	6 years
Spot-check results	ISMS workspace; reviewer	Quarterly	3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Restricted-zone access reviews on time	100%	Overdue review: facility manager escalation
Unescorted visitors found	0	Incident
Environmental tests in date	100%	Overdue test is a finding

Auditor questions to prepare

- Walk us to the server room: who can enter and how do you know who entered last week?
- Show the zone plan and what is allowed in each zone.
- How do you handle a visitor who needs to enter a restricted area?
- Show the last UPS and fire test.

Frequent nonconformities

- Shared door codes.
- Visitor not escorted.
- Server room with storage clutter or no fire suppression test.
- Access list not reviewed.

On-site readiness

- Prepare a walk-through route covering reception, an office floor, the server room, a restricted zone and the delivery area; the auditor may change the route.
- Expect door, window, cabinet and clean-desk spot checks; test alarms in advance.

Interfaces: ISMS-PHY-SUPPORTS-001, ISMS-PRO-RECON-001, ISMS-PRO-ZONES-001, ISMS-IAM-REVUE-001, ISMS-PRA-PCA-001

ISMS-PHY-SUPPORTS-001 — Physical media handling and disposal

Classification C1 · INTERNAL · Format PROCEDURE · Applicability Core

Objective

Prevent disclosure, modification or loss of information on physical media and printed material during storage, transport, reuse and disposal.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Physical security: handling of media, data carriers and mobile storage (chapter 3); secure disposal
ISO/IEC 27001:2022	A.7.10 Storage media; A.7.14 Secure disposal or re-use of equipment; A.8.10 Information deletion; A.5.10 Acceptable use
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
MED-01	Removable media shall be blocked by default; use shall be authorised, encrypted and registered.	Endpoint control and registry.
MED-02	Media containing C2/C3 data shall be stored locked and transported in tamper-evident containers by authorised couriers with tracking.	Transport records.
MED-03	Media and printed material shall be destroyed or sanitised to a recognised standard (for example NIST SP 800-88 or DIN 66399 security level suited to classification) and certified.	Destruction certificates.
MED-04	Devices shall be sanitised before reuse or return to lessor, with a verification record.	Sanitisation logs.
MED-05	Paper copies of C3 shall be numbered and logged, and destroyed with cross-cut shredders or via certified service.	C3 copy register.
MED-06	Secure disposal bins shall be emptied under control, and providers shall be contractually bound (ISMS-OPS-SUPPRESSION-001).	Provider contract and handover receipts.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Authorise media	IT operations	IT manager	CISO
Destroy media	IT operations / provider	Facility manager	ISMS manager
Audit destruction	ISMS reviewer	CISO	Facility manager

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Media register	Asset tool; IT operations	Per media	Life + 3 years
Destruction certificates	Procurement files; facility manager	Per batch	6 years
C3 copy register	Document control; document owners	Per copy	6 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Media with destruction certificate	100%	Missing certificate is an incident
Unauthorised removable media events	0	Investigation

Auditor questions to prepare

- Show me the destruction certificate for the last retired disk.
- How do you transport backup media?

- How do you stop USB data copying?

Frequent nonconformities

- No certificates for destroyed media.
- USB open on endpoints.
- C3 prints unlogged.

Interfaces: ISMS-OPS-SUPPRESSION-001, ISMS-ACT-CLASSIF-001, ISMS-OPS-DLP-001, ISMS-PHY-ZONES-001

ISMS-PRA-PCA-001 — Business impact analysis and continuity plan

Classification C2 · CONFIDENTIAL · Format STANDARD · Applicability Core

Objective

Identify critical processes and information systems and define the recovery objectives, strategies and plans that keep or restore operations within the time customers can tolerate.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Business continuity and disaster recovery: business impact analysis and continuity planning (chapter 3); availability objective
ISO/IEC 27001:2022	A.5.29 Information security during disruption; A.5.30 ICT readiness for business continuity; Clause 8.1; A.8.14 Redundancy of information processing facilities
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
BCP-01	A business impact analysis shall be performed at least annually and on major change, identifying critical processes, dependencies, maximum tolerable downtime, RTO and RPO per process and system.	BIA report with approved values.
BCP-02	Continuity strategies shall be defined for loss of premises, IT, staff, key suppliers and communications, with resource needs.	Strategy documents.
BCP-03	Continuity plans shall contain activation criteria, roles, contact details, step-by-step recovery actions and alternative workplaces.	Current plans.
BCP-04	Plans shall be available offline and to the crisis team in a location independent of the failed systems.	Offline copy check.
BCP-05	Customer availability requirements shall be reflected in objectives and contracts and tested (availability label).	Mapping to customer requirements.
BCP-06	Plans shall be reviewed annually and updated after exercises and organisational change.	Review log.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Perform BIA	Process owners	CISO / BCM manager	IT; finance
Maintain plans	BCM manager	CISO	Service owners
Approve RTO/RPO	Top management	Managing director	Customers where applicable

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
BIA and RTO/RPO table	BCM workspace; BCM manager	Annual	6 years
Continuity plans	Document system; BCM manager	Annual	6 years
Review and update log	BCM workspace; BCM manager	Annual	3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Critical processes with approved RTO/RPO	100%	Gaps added to risk register
Plans reviewed within 12 months	100%	Overdue: CISO
RTO targets supported by tested capability	≥ 90%	Gap treatment plan

Auditor questions to prepare

- What is the maximum downtime of your most critical process and who agreed it?

- Where is the plan if systems are down?
- How are customers' availability needs considered?

Frequent nonconformities

- RTO values never validated by tests.
- Plans not available offline.
- BIA outdated.

Interfaces: ISMS-PRA-PRA-001, ISMS-PRA-TESTS-001, ISMS-INC-CRISE-001, ISMS-OPS-SAUVEGARDE-001, ISMS-FOU-POLITIQUE-001

ISMS-PRA-PRA-001 — IT disaster recovery plan

Classification C2 · CONFIDENTIAL · Format STANDARD · Applicability Core

Objective

Restore IT services, data and infrastructure within the recovery objectives after loss of systems, data centres or cloud regions.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Business continuity and disaster recovery: IT disaster recovery (chapter 3)
ISO/IEC 27001:2022	A.5.30 ICT readiness for business continuity; A.8.13 Information backup; A.8.14 Redundancy of information processing facilities
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
DRP-01	Recovery procedures shall exist per critical service with dependencies, order of recovery, owner, RTO and RPO.	Runbooks per service.
DRP-02	Redundancy and replication shall be designed to meet RTO and RPO; single points of failure for critical services shall be recorded in the risk register.	Architecture and SPOF list.
DRP-03	Recovery shall include secure rebuild from trusted images, credentials reset and integrity checks.	Runbook steps.
DRP-04	Backup copies shall include an offline or immutable copy and be tested (ISMS-OPS-RESTORE-001).	Backup configuration.
DRP-05	Disaster recovery shall be tested at least annually for each critical service, with measured recovery time and results compared to RTO and RPO.	Test reports.
DRP-06	Failures during tests shall result in tracked corrective actions.	Action log.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Maintain DR runbooks	Service owners	IT manager	BCM manager
Execute DR tests	IT operations	IT manager	Service owners; CISO
Approve test results	BCM manager	CISO	Top management

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
DR runbooks	Document system; service owners	Annual	3 years
DR test reports	BCM workspace; IT manager	Annual	6 years
Corrective actions	Ticket system; IT manager	Per test	3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Critical services DR-tested in last 12 months	100%	Untested service is a finding
Measured recovery time within RTO	≥ 90% of tests	Failure triggers redesign

Auditor questions to prepare

- Show me the last DR test and recovery time against RTO.
- What if your cloud region fails?
- What are your single points of failure?

Frequent nonconformities

- DR never tested end to end.
- RTO unknown.
- Runbook outdated.

Interfaces: ISMS-PRA-PCA-001, ISMS-PRA-TESTS-001, ISMS-OPS-RESTORE-001, ISMS-OPS-SAUVEGARDE-001, ISMS-OPS-CLOUD-001

ISMS-PRA-TESTS-001 — Business continuity, recovery and restore tests

Classification C2 · CONFIDENTIAL · Format STANDARD · Applicability Core

Objective

Prove through recurring, realistic tests that continuity, recovery and restore capabilities meet the stated objectives.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Business continuity: testing and exercising of plans (chapter 3)
ISO/IEC 27001:2022	A.5.30 ICT readiness for business continuity; A.8.13 Information backup; Clause 9.1 Monitoring and measurement
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
TST-01	An annual test plan shall cover continuity, DR, restore and crisis communication, with scope, scenario, success criteria and date.	Approved test plan.
TST-02	Each test shall be documented with participants, timeline, measured recovery time, deviations and lessons.	Test report.
TST-03	At least one test per year shall simulate loss of the main site or system without prior warning to operational teams where safe.	Unannounced or scenario test record.
TST-04	Test results shall be reviewed by the CISO and top management, and findings tracked to closure.	Management review input and tracked actions.
TST-05	Plans shall be revised within 30 days of a failed test, and the failed part shall be retested.	Revision and retest record.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Plan tests	BCM manager	CISO	Service owners
Run tests	Service owners	IT manager	BCM manager
Evaluate and report	BCM manager	CISO	Top management

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Test plan	BCM workspace; BCM manager	Annual	3 years
Test reports	BCM workspace; BCM manager	Per test	6 years
Corrective actions	Ticket system; owners	Per test	3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Planned tests performed	100%	Missed test escalated
Test findings closed on time	≥ 90%	Escalation

Auditor questions to prepare

- Which tests did you run last year and what failed?
- How do you know your backups can be restored?
- Show me the corrective action from the last test.

Frequent nonconformities

- Tests only on paper.
- No success criteria.
- Findings not tracked.

Interfaces: ISMS-PRA-PCA-001, ISMS-PRA-PRA-001, ISMS-OPS-RESTORE-001, ISMS-INC-EXERCISE-001

ISMS-IAM-POLITIQUE-001 — Identity and access management policy

Classification C1 · INTERNAL · Format STANDARD · Applicability Core

Objective

Set the principles for granting, using and withdrawing access so that only identified and authorised persons and systems reach information, on a need-to-know and least-privilege basis.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Identity and access management: access control policy, user access, privileged access (chapter 4)
ISO/IEC 27001:2022	A.5.15 Access control; A.5.16 Identity management; A.5.17 Authentication information; A.5.18 Access rights; A.8.2 Privileged access rights; A.8.3 Information access restriction
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
IAP-01	Access shall be granted on the basis of role, need-to-know and least privilege, approved by the data/system owner, and documented.	Role model and approval records.
IAP-02	Every user shall have a unique identity; shared and generic accounts shall be prohibited unless exceptions are approved, technically controlled and attributable.	Account inventory with exception list.
IAP-03	Role-based access models shall be defined for critical applications, and business-owned roles shall have named owners.	Role catalogue.
IAP-04	Access to C3 information shall be explicitly approved per person and reviewed at least quarterly.	C3 access list and review.
IAP-05	External parties shall receive time-limited accounts under an agreement with an internal sponsor.	Account expiry data.
IAP-06	All access decisions shall be logged and retained.	Access logs.
IAP-07	The policy shall be reviewed annually.	Policy review record.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Define access principles	IAM owner	CISO	Data owners
Approve access	Data / system owner	Department head	IAM owner
Provision	IT operations	IAM owner	Line manager
Review	Data owners	CISO	IAM owner

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Role catalogue	IAM tool; IAM owner	Semi-annual	3 years
Access approvals	Ticket / IAM system; data owners	Per request	3 years
Account inventory with exceptions	IAM tool; IAM owner	Monthly	3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Shared accounts without exception	0	Immediate remediation
Access requests with documented approval	100%	Review of approver
External accounts without expiry	0	Disable within 5 days

Auditor questions to prepare

- Pick a user and tell me who approved each of their rights.
- Do you have shared accounts? Show the register.
- How do you manage external users?

Frequent nonconformities

- Approval by IT rather than data owner.
- Generic accounts used for admin work.
- No expiry for suppliers.

Interfaces: ISMS-IAM-CYCLE-001, ISMS-IAM-AUTH-001, ISMS-IAM-PRIV-001, ISMS-IAM-REVUE-001, ISMS-RH-CYCLE-001

ISMS-IAM-CYCLE-001 — User account lifecycle management

Classification C1 · INTERNAL · Format PROCEDURE · Applicability Core

Objective

Manage user, service and technical accounts from creation to deletion so that each account is attributable, correctly privileged and removed when no longer needed.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Identity and access management: user access provisioning, change and removal (chapter 4)
ISO/IEC 27001:2022	A.5.16 Identity management; A.5.18 Access rights; A.8.5 Secure authentication
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
ACL-01	Account creation shall require a ticket with business justification, approval by the data owner and verification of identity.	Ticket sample.
ACL-02	Service and technical accounts shall have an owner, purpose, rotation schedule and restricted interactive login.	Service-account register.
ACL-03	Dormant accounts inactive for 90 days shall be disabled and removed after 180 days unless exempted.	Dormancy report.
ACL-04	Account changes shall be logged with actor, time and approval, and the logs protected from tampering.	IAM audit log.
ACL-05	Emergency (break-glass) accounts shall be sealed, monitored and their use reviewed within 24 hours.	Break-glass log reviews.
ACL-06	Directory and HR data shall be reconciled monthly.	Reconciliation.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Create and change accounts	Service desk	IAM owner	Data owner
Disable dormant accounts	IAM engineering	IAM owner	CISO
Own service accounts	Technical owners	IT manager	IAM owner

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Account tickets	Ticket system; service desk	Per event	3 years
Service account register	IAM tool; technical owners	Quarterly	Life + 1 year
Dormancy report	IAM tool; IAM engineering	Monthly	3 years
Break-glass reviews	SIEM and ticket; CISO	Per use	3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Dormant accounts older than 90 days	0	Disable within 5 days
Service accounts with owner	100%	Assign within 10 days
Break-glass uses reviewed	100%	Incident

Auditor questions to prepare

- Show me service accounts and their owners.
- How many dormant accounts do you have?

- How is break-glass use monitored?

Frequent nonconformities

- Orphan service accounts.
- No dormancy handling.
- No log of who changed rights.

Interfaces: ISMS-IAM-POLITIQUE-001, ISMS-IAM-PRIV-001, ISMS-IAM-REVUE-001, ISMS-RH-CYCLE-001, ISMS-OPS-JOURNAUX-001

ISMS-IAM-AUTH-001 — Authentication and multi-factor authentication

Classification C1 · INTERNAL · Format PROCEDURE · Applicability Core

Objective

Ensure the strength and protection of authentication so that identities cannot be impersonated, with multi-factor authentication where information protection needs or exposure require it.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Identity and access management: identification means, authentication and secret handling (chapter 4)
ISO/IEC 27001:2022	A.5.17 Authentication information; A.8.5 Secure authentication; A.5.16 Identity management; A.8.20 Network security
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
ATH-01	MFA shall be mandatory for all remote access, cloud and SaaS administration, privileged accounts, email access from outside managed devices and access to C3 information.	MFA enforcement configuration and coverage report.
ATH-02	Phishing-resistant MFA (FIDO2/passkeys or certificate-based) shall be used for administrators and C3 access where technically possible.	Method inventory.
ATH-03	Password rules shall follow current guidance: minimum 14 characters or passphrase, screening against breached lists, no forced periodic change without compromise, lockout or throttling.	Password policy export.
ATH-04	Initial and reset credentials shall be delivered securely, identity verified and changed at first use.	Reset procedure and samples.
ATH-05	Secrets shall not be stored in clear text or shared by chat or email; password managers or vaults shall be used (ISMS-OPS-SECRETS-001).	Vault usage.
ATH-06	Authentication failures and anomalies shall be logged and monitored.	Alerts and review.
ATH-07	Legacy authentication protocols shall be disabled.	Tenant configuration.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Configure authentication	IAM engineering	IAM owner	CISO
Verify identity for resets	Service desk	IT manager	IAM owner
Monitor anomalies	SOC	CISO	IAM owner

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Authentication policy configuration	IdP console; IAM engineering	Quarterly	3 years
MFA coverage report	IdP; IAM engineering	Monthly	3 years
Reset requests	Ticket system; service desk	Per event	1 year

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Users covered by MFA	100% in scope	Any gap blocked within 5 days
Admins with phishing-resistant MFA	≥ 90%	Plan to 100%
Legacy protocol logins	0	Investigate

Auditor questions to prepare

- Show me MFA coverage: who is exempt and why?
- How do you verify the user for a password reset?
- Which legacy protocols remain enabled?

Frequent nonconformities

- MFA exceptions without approval.
- SMS only for admins.
- Password reset by email only.

Interfaces: ISMS-IAM-POLITIQUE-001, ISMS-IAM-PRIV-001, ISMS-OPS-SECRETS-001, ISMS-OPS-JOURNAUX-001, ISMS-RH-TELETRAVAIL-001

ISMS-IAM-PRIV-001 — Privileged and administrative access

Classification C2 · CONFIDENTIAL · Format PROCEDURE · Applicability Core

Objective

Strictly control, monitor and minimise privileged access because compromise of a privileged account affects every protected asset.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Identity and access management: privileged users and administrative access (chapter 4)
ISO/IEC 27001:2022	A.8.2 Privileged access rights; A.8.18 Use of privileged utility programs; A.8.15 Logging; A.5.18 Access rights
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
PAM-01	Privileged access shall be separate from daily accounts, individually assigned, approved and time-bound where technically feasible (just-in-time).	Admin account inventory.
PAM-02	Administration shall be done from hardened admin workstations or bastion hosts with MFA; direct admin from user workstations shall be prohibited.	Admin path architecture and logs.
PAM-03	Privileged sessions shall be recorded or fully logged and reviewed on a risk basis, and at least monthly sampled.	Session logs and review notes.
PAM-04	Privileged group membership shall be recertified quarterly.	Recertification.
PAM-05	Default and built-in administrator accounts shall be renamed or disabled, and shared secrets rotated after each use.	Configuration evidence.
PAM-06	Cloud and SaaS administrator roles shall be minimised, with at most the defined number of global administrators and break-glass accounts.	Role counts.
PAM-07	Privileged use shall be alerted in SIEM for abnormal times, sources and actions.	Alert rules.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Grant privileged access	IAM engineering	IAM owner	System owner; CISO
Review sessions	Security officer	CISO	IAM owner
Recertify admins	System owners	IT manager	CISO

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Privileged account inventory	PAM/IAM tool; IAM engineering	Monthly	3 years
Session recordings and reviews	PAM tool; security officer	Monthly	12 months recordings; 3 years reviews
Recertification	IAM tool; system owners	Quarterly	3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Admins using separate accounts	100%	Remediation within 10 days
Privileged accounts recertified in quarter	100%	Disable unconfirmed
Standing global admins above target	0	Reduce within 14 days

Auditor questions to prepare

- How many administrators do you have and who reviews their activity?
- Show me one privileged session and its review.
- How do you protect admin workstations?

Frequent nonconformities

- Daily and admin accounts identical.
- No review of privileged activity.
- Domain admins on user PCs.

Interfaces: ISMS-IAM-POLITIQUE-001, ISMS-IAM-AUTH-001, ISMS-IAM-REVUE-001, ISMS-OPS-JOURNAUX-001, ISMS-OPS-DURCISSEMENT-001

ISMS-IAM-REVUE-001 — Periodic access certification

Classification C1 · INTERNAL · Format PROCEDURE · Applicability Core

Objective

Verify periodically that every access right is still needed, appropriate and approved, and remove those that are not.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Identity and access management: review of access rights (chapter 4)
ISO/IEC 27001:2022	A.5.18 Access rights; A.8.2 Privileged access rights; A.5.15 Access control
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
REV-01	All accounts and entitlements to applications holding C2/C3 data shall be reviewed by the data owner at least semi-annually; privileged and C3 access quarterly.	Review campaign records.
REV-02	Reviewers shall receive complete data: user, role, last login, approver and justification.	Review extract.
REV-03	Rights not confirmed within 14 days shall be revoked.	Revocation evidence.
REV-04	Review results and removals shall be recorded and rights removed within 5 working days of the decision.	Removal tickets.
REV-05	Reviews shall be done by someone with knowledge of the business need, not by IT alone, and not by the user themselves.	Reviewer assignment.
REV-06	Completeness of the reviewed population shall be reconciled with the account inventory.	Reconciliation.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Prepare review data	IAM engineering	IAM owner	Data owners
Review entitlements	Data owners	Department heads	CISO
Remove rights	Service desk	IAM owner	Data owners

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Review campaigns	IAM tool; IAM owner	Quarterly / semi-annual	3 years
Revocation tickets	Ticket system; service desk	Per removal	3 years
Population reconciliation	IAM tool; IAM engineering	Per campaign	3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Reviews completed on time	100%	Revoke unconfirmed rights
Rights removed within 5 days	100%	Escalation
Share of rights revoked per campaign	Tracked	Very low rate triggers review quality check

Auditor questions to prepare

- Show last campaign and the number of rights removed.
- Who reviews privileged access?
- How do you ensure the review list was complete?

Frequent nonconformities

- Review by IT without business owner.
- No removals ever (rubber stamping).
- Population incomplete.

Interfaces: ISMS-IAM-POLITIQUE-001, ISMS-IAM-PRIV-001, ISMS-IAM-CYCLE-001, ISMS-RH-CYCLE-001

ISMS-FOU-POLITIQUE-001 — Supplier security management policy

Classification C1 · INTERNAL · Format STANDARD · Applicability Core

Objective

Select, contract, monitor and exit suppliers and service providers so that information shared with them is protected to the level required by customers and the ISMS.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Supplier relationships: information security among contractors and service providers (chapter 6)
ISO/IEC 27001:2022	A.5.19 Information security in supplier relationships; A.5.20 Addressing security in supplier agreements; A.5.21 ICT supply chain; A.5.22 Monitoring and review of supplier services; A.5.23 Cloud services
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
SUP-01	A supplier register shall list every supplier with access to or processing of company or customer information, its criticality and the data classes involved.	Supplier register.
SUP-02	Suppliers shall be risk-tiered; due diligence proportional to tier shall be performed before contract and renewed at least annually for high tier.	Assessments by tier.
SUP-03	Contracts shall include confidentiality, security requirements, incident notification, audit rights, sub-supplier flow-down, data return and deletion, and TISAX requirements where relevant.	Contract clauses.
SUP-04	Suppliers handling C3 data or prototypes shall hold a valid TISAX label at the appropriate level or be audited directly.	Label verification in ENX portal.
SUP-05	Supplier performance and security shall be monitored; changes, incidents and certificates shall be reviewed at least annually.	Review records.
SUP-06	Supplier access shall be time-limited, logged and removed at contract end.	Access records.
SUP-07	Exit shall include data return, deletion certificate and access removal.	Exit record.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Maintain supplier register	Procurement	Procurement manager	CISO
Assess supplier risk	Supplier manager	CISO	Service owner
Verify TISAX labels	Supplier manager	CISO	Procurement
Offboard supplier	Service owner	Department head	Procurement; IAM

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Supplier register	Procurement system; procurement	Continuous	Contract + 6 years
Due-diligence files	Supplier repository; supplier manager	Annual	Contract + 6 years
Contracts and clauses	Contract system; legal	Per contract	Contract + 10 years
Exit evidence	Supplier files; service owner	Per exit	6 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
High-tier suppliers assessed in last 12 months	100%	Overdue triggers CISO decision
Suppliers with data access and signed security terms	100%	Block access
Expired labels or certificates	0	Remediation request within 5 days

Auditor questions to prepare

- Which of your suppliers can see C3 data and how did you assess them?
- Show me a supplier whose assessment found gaps.
- How do you check a supplier's TISAX label?

Frequent nonconformities

- Register incomplete.
- Contracts without security terms.
- No monitoring after onboarding.

Interfaces: ISMS-FOU-CHARTE-001, ISMS-FOU-ASSURANCE-002, ISMS-OPS-CLOUD-001, ISMS-RGP-DPA-001, ISMS-RH-NDA-001

ISMS-CON-CONFORMITE-001 — Legal, regulatory and contractual compliance

Classification C1 · INTERNAL · Format PROCEDURE · Applicability Core

Objective

Identify, interpret and comply with legal, regulatory and contractual obligations affecting information security, privacy and intellectual property.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Compliance: legal and contractual requirements, intellectual property, protection of records, data protection (chapter 7)
ISO/IEC 27001:2022	A.5.31 Legal, statutory, regulatory and contractual requirements; A.5.32 Intellectual property rights; A.5.33 Protection of records; A.5.34 Privacy; A.5.36 Compliance
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
CMP-01	A register of applicable laws, regulations, standards and contractual duties shall be maintained with owner, requirement summary and control mapping, and reviewed at least annually.	Legal register.
CMP-02	Relevant regulations (for example GDPR, NIS2, export control, labour and trade-secret law) shall be assessed for applicability per country of operation.	Applicability analysis.
CMP-03	Software licences and intellectual property shall be managed, including open-source obligations.	Licence register.
CMP-04	Records shall be protected, retained and disposed per ISMS-CON-RETENTION-001.	Retention schedule.
CMP-05	Compliance monitoring shall be done through self-checks and audits with results reported to management.	Reports.
CMP-06	Changes in law shall be monitored via named sources and assessed within 30 days.	Change log.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Maintain legal register	Legal / compliance officer	CISO	DPO; department heads
Assess new requirements	Compliance officer	Top management	CISO
Verify compliance	ISMS reviewer	CISO	Control owners

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Legal and contractual register	Compliance tool; compliance officer	Annual	6 years
Compliance assessments	Compliance workspace; officer	Annual	6 years
Licence register	Asset tool; IT	Quarterly	Life + 3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Register reviewed in 12 months	100%	Overdue: top management
New requirements assessed within 30 days	100%	Escalation

Auditor questions to prepare

- How do you know which laws apply to you?

- Show me how a new regulation was handled.
- How do you manage open-source licences?

Frequent nonconformities

- No register.
- No owner.
- Law changes unknown.

Interfaces: ISMS-CON-DONNEES-001, ISMS-CON-RETENTION-001, ISMS-CON-VEILLE-001, ISMS-CLI-EXIGENCES-001, ISMS-RGP-REGISTRE-001

ISMS-CLI-FICHE-001 — Customer security fact sheet

Classification C1 · INTERNAL · Format REGISTER · Applicability Core

Objective

Provide customers with an accurate, approved and current summary of the security posture, certifications and contact points without exposing confidential details.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Compliance and supplier relationships: information to customers; TISAX label and scope (chapters 6 and 7)
ISO/IEC 27001:2022	A.5.14 Information transfer; A.5.31 Legal and contractual requirements; A.5.34 Privacy
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
FCH-01	Each statement shall be supported by a current evidence reference held internally (certificate, procedure, test).	Evidence index.
FCH-02	The fact sheet shall be approved by the CISO and legal and updated within 30 days of any change that makes a statement inaccurate.	Approval and change log.
FCH-03	It shall state TISAX Participant ID, scope, labels, validity and assessment objectives exactly as shown in the ENX portal.	Portal comparison.
FCH-04	Distribution shall follow its classification and shall be logged for named customers.	Distribution log.
FCH-05	Version and date shall be shown; outdated copies shall be withdrawn.	Versioning.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Prepare	Security communications	CISO	Legal
Approve	CISO	Top management	Legal
Distribute	Account manager	Sales manager	CISO

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Approved fact sheet	Document system; CISO	Per version	6 years
Evidence index	ISMS workspace; ISMS manager	Per version	6 years
Distribution log	CRM; account manager	Per release	3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Statements with evidence	100%	Remove unsupported statement
Fact sheet current within 30 days of change	100%	Escalation

Auditor questions to prepare

- Where does each statement come from?
- How do you keep it aligned with the TISAX portal?
- Who approved it?

Frequent nonconformities

- Overstated claims.
- Out-of-date label information.

- No evidence reference.

Interfaces: ISMS-POL-SSI-001, ISMS-CLI-QUESTIONNAIRE-001, ISMS-PUB-CONFIANCE-001, ISMS-ORG-PERIMETRE-001

ISMS-CLI-QUESTIONNAIRE-001 — Approved customer security responses

Classification C2 · CONFIDENTIAL · Format REGISTER · Applicability Core

Objective

Answer customer security questionnaires consistently, truthfully and with evidence, using a single approved answer base.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Compliance and supplier relationships: consistent information to customers (chapters 6 and 7)
ISO/IEC 27001:2022	A.5.31 Legal requirements; A.5.14 Information transfer; A.5.35 Independent review
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
QST-01	An approved answer base shall exist with owner, evidence reference and date for every answer.	Answer base.
QST-02	Answers shall be reviewed by the control owner and approved by the CISO before release; commitments beyond current practice shall not be made.	Review record.
QST-03	Answers shall be reviewed at least annually and after relevant change.	Review log.
QST-04	Each questionnaire response shall be logged, with customer, date, version and signer.	Response log.
QST-05	Inconsistencies between answers and the TISAX assessment scope or evidence shall be corrected immediately.	Correction log.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Answer	Control owners	ISMS manager	Account manager
Approve	CISO	Top management	Legal
Maintain base	ISMS manager	CISO	Control owners

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Answer base	ISMS workspace; ISMS manager	Annual	3 years
Response log	CRM; account manager	Per response	6 years
Approvals	Document system; CISO	Per response	6 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Answers with evidence and date	100%	Remove
Responses approved before release	100%	Incident

Auditor questions to prepare

- How do you ensure answers are accurate?
- Show me an answer and its evidence.
- Who may sign a questionnaire?

Frequent nonconformities

- Stale answers.

- Promises not backed by controls.
- No approval.

Interfaces: ISMS-CLI-FICHE-001, ISMS-CLI-EXIGENCES-001, ISMS-POL-SSI-001

ISMS-CLI-ANNEXE-001 — Customer contractual security annex

Classification C1 · INTERNAL · Format AGREEMENT · Applicability Core

Objective

Provide a standard contractual security annex that states the obligations applied to customer information and that can be offered consistently across customers.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Supplier relationships and compliance: contractual security requirements (chapters 6 and 7)
ISO/IEC 27001:2022	A.5.20 Addressing information security in supplier agreements; A.5.31; A.5.34
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
ANX-01	The annex shall define scope, classification, permitted processing, locations, access, subprocessors, incident notification time, audit rights, return and deletion, and liability allocation.	Template clauses.
ANX-02	Obligations in the annex shall be mapped to controls and owners before signature (ISMS-CLI-EXIGENCES-001).	Mapping.
ANX-03	Changes to the standard annex shall be approved by legal and the CISO.	Approval.
ANX-04	Deviations requested by customers shall be assessed for feasibility and recorded.	Deviation log.
ANX-05	Signed annexes shall be stored and linked to the customer record.	Contract repository.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Maintain template	Legal	General counsel	CISO
Negotiate	Account manager	Sales manager	Legal; CISO
Map obligations	ISMS manager	CISO	Control owners

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Standard annex	Contract system; legal	Annual	Contract + 10 years
Signed annexes	Contract system; legal	Per contract	Contract + 10 years
Deviations	Contract system; legal	Per contract	Contract + 10 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Signed annexes mapped to controls	100%	Mapping before delivery
Annex reviewed in 12 months	100%	Escalation

Auditor questions to prepare

- Which obligations do you owe a given customer and who is responsible?
- How are deviations approved?
- Where are signed annexes stored?

Frequent nonconformities

- Obligations not mapped.
- Unapproved deviations.

- No storage.

Interfaces: ISMS-CLI-EXIGENCES-001, ISMS-RGP-DPA-001, ISMS-CLI-INCIDENT-001, ISMS-FOU-POLITIQUE-001

ISMS-CLI-INCIDENT-001 — Customer incident notification procedure

Classification C1 · INTERNAL · Format PROCEDURE · Applicability Core

Objective

Ensure customers are informed of security incidents affecting their information within the time and in the form required by contract and law.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Incident management: communication with customers and authorities (chapter 1); supplier relationships
ISO/IEC 27001:2022	A.5.24 Incident management planning; A.5.26 Response; A.5.5 Contact with authorities; A.5.31
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
CIN-01	A customer notification matrix shall list contact, time limit, channel and content for every customer with contractual duties.	Matrix current within 6 months.
CIN-02	Notifications shall be made within the contractual limit and in any case within 24 hours after confirmation where the contract is silent; initial notification shall not wait for full analysis.	Notification records with timestamps.
CIN-03	Notifications shall contain nature, affected data, time, measures, contact and next update time, and shall be approved by the CISO and legal.	Template and approvals.
CIN-04	Regulatory notifications (for example data protection authorities within 72 hours) shall be coordinated with the DPO.	DPO log.
CIN-05	Follow-up reports shall be provided until closure and final report within the agreed period.	Reports.
CIN-06	The process shall be exercised yearly.	Exercise.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Prepare notification	Incident manager	CISO	Legal; communications
Approve and send	CISO	Managing director	Account manager
Maintain matrix	ISMS manager	CISO	Account managers

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Notification matrix	Document system; ISMS manager	Semi-annual	3 years
Notifications sent	Incident system; incident manager	Per incident	Contract + 6 years
Final reports	Incident system; CISO	Per incident	Contract + 6 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Notifications within contractual time	100%	Top management
Matrix contacts verified	Twice yearly	Update within 5 days

Auditor questions to prepare

- What is the shortest notification duty you have and how do you meet it?
- Show a notification you sent.
- Who decides to notify?

Frequent nonconformities

- Matrix outdated.
- Waiting for full analysis.
- No evidence of timing.

Interfaces: ISMS-INC-PROC-001, ISMS-INC-CRISE-001, ISMS-CLI-EXIGENCES-001, ISMS-RGP-VIOLATION-001

ISMS-INF-HEB-002 — Customer-facing data-location statement

Classification C1 · INTERNAL · Format REGISTER · Applicability Core

Objective

State accurately where customer and company data is stored, processed and accessed from, and ensure that this matches contractual and legal restrictions.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Supplier relationships and compliance: data location and external IT services (chapters 5, 6 and 7)
ISO/IEC 27001:2022	A.5.23 Cloud services; A.5.34 Privacy; A.5.31 Legal requirements; A.8.24
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
LOC-01	A data location register shall list per service and data class: storage region, processing region, support access locations, subprocessors and backup location.	Register.
LOC-02	Declared locations shall be verified against technical configuration at least semi-annually.	Verification record.
LOC-03	Changes of location or subprocessor shall be approved and notified to customers per contract before implementation.	Change and notification records.
LOC-04	Remote support access from outside permitted regions shall be technically blocked or approved case by case.	Access controls.
LOC-05	The customer-facing statement shall be approved and aligned with the register.	Approval.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Maintain register	Cloud owner	IT manager	DPO
Verify location	Security engineering	CISO	Cloud owner
Notify customers	Account manager	Sales manager	Legal

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Data location register	CMDB; cloud owner	Semi-annual	Life + 3 years
Verification results	Cloud console; engineering	Semi-annual	3 years
Customer notifications	CRM; account manager	Per change	Contract + 3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Statements verified in 6 months	100%	Correct
Unauthorised location events	0	Incident

Auditor questions to prepare

- Prove that data stays in the stated region.
- Who can access from outside?
- How do you notify location changes?

Frequent nonconformities

- Statement not verified.
- Support access from third countries.
- Unnoticed subprocessor change.

Interfaces: ISMS-OPS-CLOUD-001, ISMS-RGP-TRANSFERTS-001, ISMS-CLI-FICHE-001, ISMS-FOU-POLITIQUE-001

ISMS-FOU-CHARTE-001 — Supplier security requirements

Classification C1 · INTERNAL · Format PROCEDURE · Applicability Core

Objective

Communicate to suppliers the minimum security requirements that apply when they handle company or customer information.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Supplier relationships: requirements imposed on contractors and service providers (chapter 6)
ISO/IEC 27001:2022	A.5.19 and A.5.20 Supplier relationships; A.5.21 ICT supply chain; A.6.6 Confidentiality agreements
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
SRQ-01	Requirements shall cover governance, personnel, access, encryption, incident notification within 24 hours, subcontractors, location, audit rights, return/deletion and TISAX where required.	Requirement document.
SRQ-02	The requirements shall be attached to or referenced by every relevant contract.	Contract check.
SRQ-03	Suppliers shall confirm compliance in writing and provide evidence at onboarding and annually.	Declarations and evidence.
SRQ-04	Non-compliance shall result in corrective plans with deadlines or termination.	Corrective plans.
SRQ-05	The document shall be reviewed annually.	Review.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Maintain requirements	ISMS manager	CISO	Procurement; legal
Collect declarations	Supplier manager	Procurement manager	Service owners
Follow up gaps	Supplier manager	CISO	Service owners

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Requirements document	Document system; ISMS manager	Annual	6 years
Declarations	Supplier files; supplier manager	Annual	Contract + 6 years
Corrective plans	Supplier files; supplier manager	Per case	Contract + 3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Suppliers with declaration in 12 months	100% of tiered	Block
Corrective plans closed on time	≥ 90%	Escalation

Auditor questions to prepare

- How do you ensure suppliers know your requirements?
- Show a declaration.
- What happens when a supplier fails?

Frequent nonconformities

- Requirements not attached.
- No follow-up.
- One-off declarations.

Interfaces: ISMS-FOU-POLITIQUE-001, ISMS-FOU-ASSURANCE-002, ISMS-RH-NDA-001, ISMS-RGP-DPA-001

ISMS-RGP-DPA-001 — Data processing agreement template

Classification C1 · INTERNAL · Format AGREEMENT · Applicability Core

Objective

Provide a data processing agreement that meets data protection law and customer needs and that can be signed with processors and customers.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Compliance and data protection: processing agreements (chapter 7; data protection module)
ISO/IEC 27001:2022	A.5.34 Privacy and protection of PII; A.5.20; A.5.31
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
DPA-01	The agreement shall contain subject, duration, nature, purpose, data types, data subjects, instructions, confidentiality, security measures, subprocessor rules, assistance, deletion/return, audit and breach notification duties.	Template clauses.
DPA-02	Technical and organisational measures annexed shall correspond to actual controls and be updated at least annually.	Annex comparison.
DPA-03	Subprocessors shall be listed and changes notified with objection rights.	Subprocessor list.
DPA-04	International transfers shall be supported by valid mechanisms (ISMS-RGP-TRANSFERTS-001).	Transfer assessment.
DPA-05	Signed DPAs shall be registered.	Register.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Maintain template	Legal / DPO	General counsel	CISO
Sign	Managing director	Top management	DPO
Update TOMs	ISMS manager	CISO	DPO

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
DPA template	Contract system; DPO	Annual	Contract + 10 years
Signed DPAs	Contract system; legal	Per contract	Contract + 10 years
TOMs annex	ISMS workspace; ISMS manager	Annual	Contract + 6 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Processors with signed DPA	100%	Block processing
TOMs updated in 12 months	100%	Escalation

Auditor questions to prepare

- Show me the TOMs and the controls behind them.
- How do you handle a subprocessor change?
- Which processors do you use?

Frequent nonconformities

- TOMs generic.

- Missing DPA.
- Subprocessors not listed.

Interfaces: ISMS-RGP-REGISTRE-001, ISMS-RGP-TRANSFERTS-001, ISMS-FOU-POLITIQUE-001, ISMS-CLI-ANNEXE-001

ISMS-RH-NDA-001 — Confidentiality agreement template

Classification C1 · INTERNAL · Format AGREEMENT · Applicability Core

Objective

Bind employees, contractors, suppliers and visitors to confidentiality obligations proportionate to the information they receive.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Human resources and supplier relationships: confidentiality agreements (chapters 2 and 6)
ISO/IEC 27001:2022	A.6.6 Confidentiality or non-disclosure agreements; A.6.2 Terms and conditions; A.5.14
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
NDA-01	NDAs shall define confidential information, permitted use, duration (including after termination), return or destruction and remedies.	Template.
NDA-02	An NDA shall be signed before disclosure of C2 or C3 information to any third party.	Signed copies before first disclosure.
NDA-03	NDAs shall be registered with counterparty, date, scope and expiry; disclosures beyond scope shall be refused.	Register.
NDA-04	Template changes shall be approved by legal.	Approval.
NDA-05	Expiring NDAs shall be reviewed 60 days before expiry.	Review.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Maintain template	Legal	General counsel	CISO
Sign and register	Contract owner	Department head	Legal
Monitor expiry	Legal	General counsel	Contract owners

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
NDA register	Contract system; legal	Continuous	Expiry + 6 years
Signed NDAs	Contract system; legal	Per NDA	Expiry + 6 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Disclosures preceded by NDA	100%	Incident
NDAs expiring without review	0	Legal

Auditor questions to prepare

- Show an NDA signed before a disclosure.
- How do you track expiry?
- Who can sign?

Frequent nonconformities

- Disclosure before NDA.
- No register.
- No post-termination duty.

Interfaces: ISMS-RH-CYCLE-001, ISMS-FOU-CHARTE-001, ISMS-CLI-EXIGENCES-001

ISMS-RH-CHARTE-002 — IT acceptable-use charter for contractors

Classification C1 · INTERNAL · Format AGREEMENT · Applicability Core

Objective

Define acceptable use obligations for contractors and temporary staff who use company systems or information.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Human resources and supplier relationships: external personnel (chapters 2 and 6)
ISO/IEC 27001:2022	A.5.10 Acceptable use; A.6.2; A.5.19
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
CAC-01	Contractors shall accept the charter before access, with sponsor named.	Acceptance log.
CAC-02	Access shall be time-limited to the contract duration and reviewed monthly by the sponsor.	Expiry data.
CAC-03	Contractors shall use managed devices or approved virtual desktops for C2/C3 information.	Device evidence.
CAC-04	Contractor activities shall be logged and personal data minimised.	Logs.
CAC-05	The charter shall cover reporting duty, return of assets and confidentiality.	Charter.
CAC-06	Review annually.	Review log.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Maintain	ISMS manager	CISO	HR; legal
Sponsor	Business sponsor	Department head	IAM
Revoke access	Service desk	IAM owner	Sponsor

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Signed charters	HR/contract system; sponsor	Per contractor	Contract + 3 years
Contractor access list	IAM tool; IAM owner	Monthly	3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Contractors with acceptance and sponsor	100%	Block access
Contractor accounts past contract end	0	Disable

Auditor questions to prepare

- Who sponsors each contractor?
- How is access ended?
- Which devices do contractors use?

Frequent nonconformities

- No sponsor.
- No expiry.

- Unmanaged devices.

Interfaces: ISMS-RH-CHARTE-001, ISMS-IAM-CYCLE-001, ISMS-FOU-CHARTE-001

ISMS-PUB-CONFIANCE-001 — Public security trust page

Classification C0 · PUBLIC · Format REGISTER · Applicability Core

Objective

Publish a public trust page that is accurate, approved and consistent with the TISAX assessment and internal controls.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Compliance: public information about security (chapter 7)
ISO/IEC 27001:2022	A.5.31; A.5.14 Information transfer; Clause 7.4 Communication
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
PTP-01	Every public claim shall be supported by evidence and reviewed by the CISO and legal before publication.	Claim-evidence table.
PTP-02	The page shall display label, scope and validity exactly as in the ENX portal and link to the public TISAX information.	Portal check.
PTP-03	It shall not disclose system names, vulnerabilities, locations of sensitive areas or customer names.	Pre-publication checklist.
PTP-04	The page shall be reviewed at least quarterly and on certification change.	Review log.
PTP-05	Changes shall be versioned.	Version history.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Draft	Communications	Marketing manager	CISO
Approve	CISO	Top management	Legal
Publish	Web team	Communications	CISO

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Claim-evidence table	ISMS workspace; ISMS manager	Quarterly	3 years
Publication approvals	Document system; CISO	Per change	3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Claims with evidence	100%	Remove
Page reviewed in 90 days	100%	Escalation

Auditor questions to prepare

- Which claims on your page can you prove?
- Who approves changes?
- How does it match the portal?

Frequent nonconformities

- Overstated claims.
- Stale label data.
- Unapproved publication.

Interfaces: ISMS-POL-SSI-001, ISMS-CLI-FICHE-001, ISMS-ORG-PERIMETRE-001

ISMS-AUD-FIELDWORK-001 — AL3 assessment fieldwork and on-site readiness plan

Classification C2 · CONFIDENTIAL · Format PROCEDURE · Applicability Core supporting control

Objective

Prepare the organisation for the on-site and interview-based fieldwork of an AL3 assessment so that scope, people, evidence, systems and premises are ready and the audit provider can complete its testing without disruption.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	TISAX assessment process: assessment level 3 (on-site inspection, interviews and plausibility checks of implementation)
ISO/IEC 27001:2022	Clause 9.2 Internal audit; A.5.35 Independent review of information security; A.5.36 Compliance with policies
Target maturity	Level 3 minimum for every applicable control; the audit provider decides sampling at AL3 and may deepen testing

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
FLD-01	An assessment readiness plan shall be created at least 90 days before fieldwork with scope, sites, dates, audit team, interviewees, evidence owners and logistics.	Approved plan.
FLD-02	A pre-assessment self-check against the VDA ISA shall have been completed within 6 months and all gaps below maturity 3 shall have a dated action plan.	Self-assessment and action register.
FLD-03	Interviewees shall be nominated for every control owner and prepared by briefing (honest answers, evidence-based, no speculation).	Interview schedule and briefing record.
FLD-04	Evidence shall be staged in a controlled read-only repository organised by ISA topic with an index, minimising personal data (ISMS-AUD-EVIDENCE-001).	Repository index.
FLD-05	Every site in scope shall be walked through by the ISMS manager at least 4 weeks before the assessment using the physical checklist; defects shall be corrected.	Walk-through report.
FLD-06	Technical demonstrations (live system queries, configuration display, log retrieval) shall be rehearsed by the responsible engineers.	Rehearsal record.
FLD-07	A single point of contact and a deputy shall coordinate the auditors during fieldwork, record requests and track open items in a daily log.	Request log.
FLD-08	Provisional findings shall be reviewed daily and clarified; factual errors in the report shall be corrected within the provider's window.	Daily meeting notes.
FLD-09	After the closing meeting a corrective action plan with owners and dates shall be produced within 10 working days (ISMS-AUD-CLOSURE-001).	Action plan.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Plan fieldwork	ISMS manager	CISO	Top management; site managers
Prepare interviewees	Control owners	Department heads	ISMS manager
Host auditors	Single point of contact	CISO	Facility management
Handle findings	Finding owners	CISO	Auditor liaison

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Readiness plan	ISMS workspace; ISMS manager	Per assessment	6 years
Interview schedule and briefings	ISMS workspace; ISMS manager	Per assessment	3 years
Request log	Audit portal; point of contact	Daily during fieldwork	6 years
Walk-through report	ISMS workspace; ISMS manager	Per site	3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Controls at maturity ≥ 3 in self-assessment	100% before fieldwork	Gap plan with dates
Evidence requests answered within 4 working hours	≥ 90%	Resource increase
Sites walked through before assessment	100%	Do not start fieldwork

Auditor questions to prepare

- Who will we speak to for each control and are they available?
- Show the staged evidence for a control we pick.
- Take us to the server room and one restricted area now.

Frequent nonconformities

- Interviewees unprepared and unaware of procedures.
- Evidence assembled hastily and inconsistent.
- Site defects found by the auditor on the day.

On-site readiness

- Reserve a room for auditors with network access, printing and a secure place for materials.
- Ensure all key staff are physically available; arrange deputies for leave or absence.

Interfaces: ISMS-AUD-SAMPLE-001, ISMS-AUD-EVIDENCE-001, ISMS-AUD-MATURITY-001, ISMS-AUD-CLOSURE-001, ISMS-ORG-SOA-001, ISMS-PHY-ZONES-001

ISMS-AUD-SAMPLE-001 — Audit evidence population and sampling standard

Classification C1 · INTERNAL · Format PROCEDURE · Applicability Core supporting control

Objective

Define and document the populations from which samples are drawn so that evidence shows sustained, consistent operation of each control over the assessment period and cannot be criticised as cherry-picked.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	TISAX assessment: evidence and sample-based verification of implementation (all chapters)
ISO/IEC 27001:2022	A.5.35 Independent review; Clause 9.1 Monitoring and measurement; Clause 9.2 Internal audit
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
SMP-01	For each recurring control a population shall be defined (for example all changes, all joiners, all leavers, all findings, all incidents) with source system, period and total count.	Population register.
SMP-02	Populations shall be exported by the system owner and, where possible, extracted by the audit team directly or in their presence.	Extraction records.
SMP-03	Samples shall be selected randomly or by documented risk-based criteria; the sample size shall follow a table by population size (for example 25 items or all if fewer; 10% of populations above 250, min 25).	Sampling table and selection record.
SMP-04	The sample shall cover the whole period and all sites, teams and platforms in scope, including exceptions and failures.	Coverage analysis.
SMP-05	Each sampled item shall be traced end to end across systems and compared with the policy and parameters; deviations shall be recorded.	Test sheets.
SMP-06	Population completeness shall be checked by reconciliation with an independent source or count.	Completeness check.
SMP-07	Test results shall be summarised with deviation rate; any deviation rate above 5% triggers root-cause analysis and extended sampling.	Summary and extended sample.
SMP-08	Samples and results shall be retained for the assessment cycle.	Retention.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Define populations	ISMS manager	CISO	System owners
Extract populations	System owners	IT manager	ISMS manager
Test samples	ISMS reviewer	CISO	Control owners
Analyse deviations	ISMS manager	CISO	Control owners

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Population register	ISMS workspace; ISMS manager	Per cycle	3 years
Sample selection and test sheets	Audit tool; reviewers	Per test	3 years
Deviation analysis	Audit tool; ISMS manager	Per test	3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Controls with population defined	100%	Define before test
Samples with complete evidence	≥ 95%	Root-cause analysis
Sample deviation rate	≤ 5%	Extended sample and action

Auditor questions to prepare

- How did you select this sample and how do you know the population was complete?
- Show a deviation you found yourselves.
- Can I extract the list from the system myself?

Frequent nonconformities

- Populations supplied by the control owner only.
- Cherry-picked samples.
- Samples only from the last month.

Interfaces: ISMS-AUD-FIELDWORK-001, ISMS-AUD-MATURITY-001, ISMS-AUD-EVIDENCE-001, ISMS-AUD-PROGRAMME-001

ISMS-AUD-MATURITY-001 — ISA maturity assessment and sustained-operation test

Classification C1 · INTERNAL · Format PROCEDURE · Applicability Core supporting control

Objective

Assess the maturity of each applicable ISA control consistently and prove that controls are operated in a sustained manner over time rather than created for the assessment.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	TISAX assessment: maturity model 0 to 5 with target level 3 for each applicable control
ISO/IEC 27001:2022	Clause 9.1 Monitoring, measurement, analysis and evaluation; Clause 10.3 Continual improvement
Target maturity	Level 3 (established) required; level 4 (predictable) and 5 (optimising) are not required for the label

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
MAT-01	The organisation shall score each applicable ISA control from 0 (incomplete) to 5 (optimising) with a documented rationale and evidence reference, using the ISA maturity definitions.	Scoring sheet.
MAT-02	A control shall be scored at level 3 only if it is documented, implemented in the whole scope, supported by evidence and reviewed for effectiveness; otherwise the score shall not exceed 2.	Scoring rules.
MAT-03	Scoring shall be performed by the control owner and challenged by an independent reviewer, with differences resolved and recorded.	Challenge record.
MAT-04	Sustained operation shall be shown by at least two operating cycles or three months of continuous records, whichever longer, for each recurring control; newly introduced controls shall be flagged as such.	Cycle evidence.
MAT-05	Controls below level 3 shall have a corrective plan with owner, date and acceptance criteria and shall be retested.	Plans and retests.
MAT-06	Score trends shall be reported to management review and used to prioritise investment.	Management review input.
MAT-07	Maturity assessment shall be repeated at least annually and before each assessment.	Annual repeat.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Score controls	Control owners	Department heads	ISMS manager
Challenge scores	ISMS reviewer	CISO	Control owners
Approve results	CISO	Top management	—

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Maturity scoring sheet	ISMS workspace; ISMS manager	Annual	3 years
Challenge notes	ISMS workspace; reviewer	Annual	3 years
Operating-cycle evidence	Per control system	Per cycle	3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Applicable controls scoring ≥ 3	100%	Corrective plan
Score challenged independently	100%	Rescore
Controls with sustained records	≥ 95%	Plan

Auditor questions to prepare

- How did you score this control and who challenged it?
- What proves that it has run for more than one cycle?
- What did you do about controls scoring below 3?

Frequent nonconformities

- Self-scored 3 with no records.
- Controls introduced a week before the assessment.
- No independent challenge.

Interfaces: ISMS-AUD-SAMPLE-001, ISMS-AUD-CLOSURE-001, ISMS-ORG-ATTEST-001, ISMS-ORG-SOA-001, ISMS-AUD-PROGRAMME-001

ISMS-AUD-CLOSURE-001 — Assessment finding remediation and independent closure testing

Classification C2 · CONFIDENTIAL · Format PROCEDURE · Applicability Core supporting control

Objective

Ensure that every finding is analysed, corrected and its closure verified independently, so closed means effective.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	TISAX assessment: handling of findings and corrective action plans after assessment (assessment process)
ISO/IEC 27001:2022	Clause 10.2 Nonconformity and corrective action; Clause 10.1 Continual improvement
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
CLO-01	Each finding shall be registered with source, severity, affected control, root cause, owner and due date; severity shall follow ENX rules for minor and major nonconformities.	Finding register.
CLO-02	Root-cause analysis shall be performed for every major finding and for repeated minor findings.	Analysis.
CLO-03	Corrective plans shall be submitted to the audit provider within the period set by ENX and be realistic and dated.	Plan submission.
CLO-04	Corrective actions shall be implemented by the owner and verified by a different person with sampled evidence of operation.	Verification record.
CLO-05	Closure shall require evidence of effective operation, not only of implementation (for example one full cycle).	Closure evidence.
CLO-06	Overdue actions shall be escalated weekly to the CISO and monthly to top management.	Escalation log.
CLO-07	Reopened findings and recurrences shall be tracked and analysed.	Recurrence analysis.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Analyse and plan	Finding owner	Department head	ISMS manager
Implement	Owners	Department head	ISMS manager
Verify closure	ISMS reviewer	CISO	Owners
Escalate	ISMS manager	CISO	Top management

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Finding register	Audit tool; ISMS manager	Continuous	6 years
Root-cause analyses	Audit tool; owners	Per finding	6 years
Verification evidence	Audit tool; reviewer	Per finding	6 years
Escalation log	ISMS workspace; ISMS manager	Weekly	3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Actions closed by due date	≥ 90%	< 80%: management review
Closures independently verified	100%	Reopen
Reopened findings	0	Root cause

Auditor questions to prepare

- Show a finding from last year and its closure evidence.
- Who verified closure?
- How do you stop recurrence?

Frequent nonconformities

- Owner closes own finding.
- Closure by document only.
- Overdue findings without escalation.

Interfaces: ISMS-AUD-PROGRAMME-001, ISMS-AUD-MATURITY-001, ISMS-AUD-FIELDWORK-001, ISMS-ORG-DEROGATIONS-001

ISMS-ORG-SOA-001 — Control applicability and documented rationale statement

Classification C2 · CONFIDENTIAL · Format REGISTER · Applicability Core supporting control

Objective

Document for every ISA control (and each ISO 27001 Annex A control, if certified) whether it applies, the reason for exclusions, how it is implemented and the owner, so the audit provider can follow the logic of scope and applicability.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	TISAX assessment scope and applicability: control applicability and justification across all ISA modules (information security, prototype protection, data protection)
ISO/IEC 27001:2022	Clause 6.1.3 Statement of applicability; Clause 4.3 Scope
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
SOA-01	Every question of the ISA catalogue for the edition in use shall be listed with status: applicable, not applicable with justification, or inherited from a provider.	Complete list.
SOA-02	Each applicable control shall reference the implementing document, owner, evidence location and maturity score.	Mapping.
SOA-03	Exclusions shall be approved by top management, justified by objective facts (for example no prototype handling) and agreed with the audit provider.	Approval and correspondence.
SOA-04	The statement shall be consistent with the scope, risk assessment, interface register and customer requirements.	Consistency check.
SOA-05	The statement shall be reviewed when scope, customer requirements, risks or ISA edition change, and at least annually.	Review log.
SOA-06	The ISA edition applicable (ISA 6.0.3 for assessments ordered before 1 January 2027, ISA2027.1 for orders from 2027; ENX states March 2027 as the final date to open an initial assessment under ISA 6) shall be recorded for the assessment order.	Edition record.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Maintain statement	ISMS manager	CISO	Control owners
Approve exclusions	Top management	Managing director	CISO
Reconcile	ISMS reviewer	CISO	ISMS manager

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Statement of applicability	ISMS workspace; ISMS manager	Annual / on change	6 years
Exclusion approvals	Document system; top management	Per exclusion	6 years
Edition and order record	ENX portal; ISMS manager	Per assessment	6 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Applicable controls mapped to evidence	100%	Gap plan
Exclusions approved and justified	100%	Reassess

Auditor questions to prepare

- Why is this control not applicable?
- Show where this control is implemented.
- Which ISA edition applies to your order?

Frequent nonconformities

- Exclusions without reason.
- No mapping to evidence.
- Wrong ISA edition.

Interfaces: ISMS-ORG-PERIMETRE-001, ISMS-AUD-MATURITY-001, ISMS-ORG-INTERFACES-001, ISMS-RSK-REGISTRE-001

ISMS-ORG-INTERFACES-001 — Cross-site shared control and handoff assurance

Classification C1 · INTERNAL · Format PROCEDURE · Applicability Core supporting control

Objective

Make responsibility explicit and verifiable for every control that is shared across sites, entities, customers or providers, so that nothing is left uncovered at the boundaries.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Organisation and supplier relationships: shared and inherited controls, multi-site scope (chapters 1 and 6)
ISO/IEC 27001:2022	A.5.2 Roles and responsibilities; A.5.19 Supplier relationships; A.5.22 Monitoring supplier services
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
INT-01	A register shall list each shared or inherited control with providing party, receiving party, responsibility split and evidence source.	Interface register.
INT-02	Handoffs shall be defined by a written agreement or service description naming contacts and response times.	Agreements.
INT-03	Inherited controls shall be validated by evidence (for example a provider's assurance report or TISAX label) covering the relevant scope and period.	Validation record.
INT-04	Central functions serving multiple sites (HR, IT, security, facilities) shall demonstrate operation for each site in scope.	Per-site evidence.
INT-05	Interfaces shall be tested annually through a walk-through of a typical case across the boundary.	Walk-through record.
INT-06	Changes of provider or structure shall update the register within 30 days.	Change log.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Maintain register	ISMS manager	CISO	Site managers; supplier manager
Validate inherited controls	Supplier manager	CISO	Control owners
Test handoffs	ISMS reviewer	CISO	Site managers

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Interface register	ISMS workspace; ISMS manager	Quarterly	3 years
Validation evidence	Supplier files; supplier manager	Annual	3 years
Walk-through reports	ISMS workspace; reviewer	Annual	3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Interfaces with named parties and evidence	100%	Complete in 14 days
Validations in date	100%	Request evidence

Auditor questions to prepare

- Who is responsible for this control at the other site?
- How do you know the provider performs it?
- Show me a handoff test.

Frequent nonconformities

- Gaps between sites.
- Inherited controls assumed, not verified.
- No per-site evidence.

Interfaces: ISMS-ORG-PERIMETRE-001, ISMS-ORG-SOA-001, ISMS-FOU-POLITIQUE-001, ISMS-FOU-ASSURANCE-002

ISMS-ORG-ATTEST-001 — Control owner attestation and independent challenge

Classification C2 · CONFIDENTIAL · Format REGISTER · Applicability Core supporting control

Objective

Obtain a formal, dated and challenged statement from each control owner that the control operates as documented, giving management a reliable view before assessments and during the year.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Organisation and assessments: responsibility for control operation and independent review (chapter 1)
ISO/IEC 27001:2022	Clause 9.3 Management review; A.5.35 Independent review; A.5.36 Compliance with policies
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
ATT-01	Each control owner shall attest at least semi-annually that the control operated as described, listing exceptions, failures and open actions.	Attestation form.
ATT-02	Attestations shall be supported by metrics or evidence references, not narrative alone.	Evidence references.
ATT-03	An independent reviewer shall challenge a risk-based sample of attestations with testing.	Challenge sample.
ATT-04	Contradictions between attestation and evidence shall be raised as findings and the attestation corrected.	Finding record.
ATT-05	Attestations shall be summarised for top management.	Summary.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Attest	Control owners	Department heads	ISMS manager
Challenge	ISMS reviewer	CISO	Control owners
Report	ISMS manager	CISO	Top management

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Attestations	ISMS workspace; control owners	Semi-annual	3 years
Challenge tests	Audit tool; reviewer	Semi-annual	3 years
Summary	Management review; CISO	Semi-annual	6 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Attestations received on time	100%	Escalation
Challenged attestations confirmed	≥ 90%	Root-cause

Auditor questions to prepare

- Who attests that this control works and what do they base it on?
- Show a challenged attestation.
- What happens if the attestation is wrong?

Frequent nonconformities

- Attestation by signature only.

- No challenge.
- Attestations late.

Interfaces: ISMS-AUD-MATURITY-001, ISMS-AUD-PROGRAMME-001, ISMS-ORG-ROLES-001

ISMS-FOU-ASSURANCE-002 — High-risk supplier assurance dossier and evidence validity

Classification C2 · CONFIDENTIAL · Format PROCEDURE · Applicability Core supporting control

Objective

Obtain and keep valid, scope-matched assurance evidence for high-risk suppliers so that reliance on them is justified and visible at assessment.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Supplier relationships: monitoring and evidence for service providers handling information of high or very high protection need (chapter 6)
ISO/IEC 27001:2022	A.5.22 Monitoring, review and change management of supplier services; A.5.21 ICT supply chain; A.5.19
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
ASR-01	High-risk suppliers shall be identified using data class, access level, criticality and subcontracting depth.	Tiering record.
ASR-02	A dossier per supplier shall contain contract, security schedule, TISAX label or certificate with scope and validity, latest assessment, open findings, incident history and contacts.	Dossier.
ASR-03	Assurance evidence shall be checked for scope match (site, service, objectives, assessment level) and validity period; expired evidence shall trigger action within 14 days.	Validity check.
ASR-04	Where no adequate certification exists, an on-site or remote audit by the organisation or a third party shall be performed.	Audit report.
ASR-05	Supplier findings shall be tracked to closure with deadlines.	Findings register.
ASR-06	Dossiers shall be reviewed annually and after major incidents or changes.	Review log.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Maintain dossiers	Supplier manager	Procurement manager	CISO
Verify evidence	Supplier manager	CISO	Service owner
Audit suppliers	ISMS reviewer / third party	CISO	Supplier manager

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Supplier dossiers	Supplier repository; supplier manager	Annual	Contract + 6 years
Validity checks	Supplier repository; supplier manager	Quarterly	3 years
Supplier audits	Audit tool; reviewer	Per audit	Contract + 6 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
High-risk dossiers complete and valid	100%	Action in 14 days
Supplier findings closed on time	≥ 90%	Escalation

Auditor questions to prepare

- Show evidence that this supplier's TISAX label covers the service you use.
- What is the validity of that evidence?

- What did your last supplier audit find?

Frequent nonconformities

- Label scope not checked.
- Expired evidence.
- Supplier findings unmanaged.

Interfaces: ISMS-FOU-POLITIQUE-001, ISMS-ORG-INTERFACES-001, ISMS-OPS-CLOUD-001, ISMS-AUD-CLOSURE-001

ISMS-INC-EXERCISE-001 — Cyber crisis tabletop and decision exercise programme

Classification C1 · INTERNAL · Format PROCEDURE · Applicability Core supporting control

Objective

Test and improve the incident and crisis response of people and decision-makers through scenario-based exercises that reflect real threats.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Incident and crisis management: exercising incident handling and crisis procedures (chapters 1 and 3)
ISO/IEC 27001:2022	A.5.24 Incident management planning; A.5.29 Information security during disruption; A.5.30 ICT readiness
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
EXR-01	An annual exercise programme shall include at least one tabletop for the crisis team and one technical simulation for responders.	Programme.
EXR-02	Scenarios shall reflect the threat picture (ransomware, data exfiltration, supplier breach, loss of prototype information, insider).	Scenarios.
EXR-03	Exercises shall include decision points for customer notification, legal notification and communication.	Scenario scripts.
EXR-04	Each exercise shall have objectives, observers, a timeline and an after-action report within 10 working days.	Reports.
EXR-05	Actions shall be tracked to closure and plans updated.	Action log.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Plan exercises	ISMS manager	CISO	Top management
Run exercises	Facilitator	CISO	Crisis team
Track actions	ISMS manager	CISO	Owners

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Exercise plan and scripts	ISMS workspace; ISMS manager	Annual	3 years
After-action reports	ISMS workspace; facilitator	Per exercise	6 years
Action log	Ticket system; ISMS manager	Per exercise	3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Planned exercises held	100%	Escalation
Actions closed on time	≥ 90%	Review

Auditor questions to prepare

- What scenario did you exercise and what changed afterwards?
- Who participated?
- How were notification decisions tested?

Frequent nonconformities

- Exercise without top management.
- No actions.
- Scenarios unrealistic.

Interfaces: ISMS-INC-PROC-001, ISMS-INC-CRISE-001, ISMS-PRA-TESTS-001, ISMS-CLI-INCIDENT-001

ISMS-AUD-EVIDENCE-001 — Evidence chain of custody, minimisation and secure disclosure

Classification C2 · CONFIDENTIAL · Format PROCEDURE · Applicability Core supporting control

Objective

Handle evidence supplied to auditors, customers and authorities so that it is authentic, minimal, protected and traceable, without disclosing more than needed.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	TISAX assessment and compliance: evidence handling, disclosure of information to the audit provider (chapters 1 and 7)
ISO/IEC 27001:2022	A.5.28 Collection of evidence; A.5.14 Information transfer; A.5.34 Privacy; A.5.33 Protection of records
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
EVD-01	Evidence shall be collected from systems of record in native form, with extraction date, author and source query, and shall remain unmodified; redactions shall be marked and an original kept.	Evidence record.
EVD-02	Personal data, customer secrets and unrelated confidential data shall be minimised or redacted before disclosure, with legal and DPO guidance.	Redaction record.
EVD-03	Disclosure shall be through a controlled channel (secure data room or on-site read-only access) with named recipients, expiry and download restrictions for C2/C3.	Data-room settings and access log.
EVD-04	A chain-of-custody register shall record every evidence item given, to whom, when and why.	Register.
EVD-05	Evidence shall be withdrawn or deleted from sharing spaces after the assessment per agreement and recorded.	Withdrawal record.
EVD-06	Non-disclosure shall be agreed with the audit provider and with each customer whose data appears in evidence.	NDA.
EVD-07	Evidence integrity shall be provable (hashes or system timestamps) where disputes may arise.	Integrity evidence.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Collect evidence	Control owners	Department heads	ISMS manager
Redact and approve	ISMS manager	CISO	DPO; legal
Operate data room	ISMS manager	CISO	IT
Withdraw	ISMS manager	CISO	—

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Evidence register	ISMS workspace; ISMS manager	Per item	6 years
Data-room access logs	Data-room platform; ISMS manager	Continuous	12 months
Redaction approvals	Document system; DPO	Per release	6 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Evidence items in register	100%	Add
Items with redaction check	100%	Incident
Sharing spaces withdrawn on time	100%	Immediate

Auditor questions to prepare

- How do you ensure what you gave us is authentic?
- Who saw this evidence?
- How do you protect customer data in evidence?

Frequent nonconformities

- Evidence by email.
- No chain of custody.
- Personal data unredacted.

Interfaces: ISMS-AUD-FIELDWORK-001, ISMS-AUD-SAMPLE-001, ISMS-ACT-CLASSIF-001, ISMS-RGP-REGISTRE-001, ISMS-RH-NDA-001

ISMS-CLI-DIFFUSION-001 — Security-evidence disclosure procedure

Classification C1 · INTERNAL · Format PROCEDURE · Applicability Added

Objective

Control the disclosure of security evidence (policies, reports, test results) to customers, auditors and partners so that only approved, minimal and traceable information leaves the organisation.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Compliance and supplier relationships: information given to customers and audit providers (chapters 6 and 7)
ISO/IEC 27001:2022	A.5.14 Information transfer; A.5.34 Privacy; A.5.12 Classification of information
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
DIF-01	Every disclosure request shall be logged with requester, purpose, items and classification before release.	Disclosure log.
DIF-02	Disclosure of C2 content shall require owner approval and an NDA; C3 content shall require CISO approval and view-only access.	Approvals and NDA reference.
DIF-03	Evidence shall be redacted of personal data, system identifiers and unrelated customer data using a documented checklist.	Redaction checklist per release.
DIF-04	Release shall use a controlled channel (secure data room, expiring links) and never unencrypted email.	Channel configuration and access logs.
DIF-05	Disclosed items shall be versioned and the version given shall be retained.	Archive copy.
DIF-06	Access to shared spaces shall be removed within 30 days or at the end of the purpose.	Withdrawal record.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Receive and log request	Account manager	Sales manager	CISO
Approve release	CISO	Top management	Legal; DPO
Redact and publish	ISMS manager	CISO	Document owners

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Disclosure log	CRM; account manager	Per request	3 years
Approvals and NDAs	Document system; CISO	Per release	6 years
Data-room access logs	Data-room platform; ISMS manager	Continuous	12 months

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Disclosures with approval before release	100%	Incident
Shared spaces withdrawn on time	100%	Immediate removal
Unredacted personal data findings	0	Incident review

Auditor questions to prepare

- How do you decide what a customer may see?
- Show the log for the last disclosure.

- How do you retract access afterwards?

Frequent nonconformities

- Disclosure by email without log.
- No redaction check.

Interfaces: ISMS-AUD-EVIDENCE-001, ISMS-CLI-TISAX-001, ISMS-ACT-CLASSIF-001, ISMS-RH-NDA-001

ISMS-CLI-TISAX-001 — TISAX assessment-result sharing procedure

Classification C1 · INTERNAL · Format PROCEDURE · Applicability Added

Objective

Share TISAX assessment results with customers and partners through the ENX exchange platform in line with the sharing rules, and keep the shared label data accurate.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	TISAX participation: assessment results, labels and exchange via the ENX platform (assessment process)
ISO/IEC 27001:2022	A.5.31 Legal and contractual requirements; A.5.14 Information transfer; A.5.19 Supplier relationships
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
TSH-01	The participant record (company data, scope IDs, labels, objectives, validity) in the ENX portal shall be reviewed at least quarterly against the real scope.	Portal extract with review signature.
TSH-02	Sharing of results shall only be to recipients with a legitimate request, using the ENX platform exchange with approval by the CISO.	Sharing log.
TSH-03	The full assessment report shall not be handed out directly; only label information and, where allowed, summary content shall be shared.	Disclosure rules and log.
TSH-04	Label expiry (three years) shall be tracked and reassessment ordered at least 6 months before expiry.	Expiry calendar and order record.
TSH-05	Changes in scope, sites or ownership that affect the label shall be notified to ENX and the provider within 30 days.	Notification record.
TSH-06	Customer questions about the result shall be answered from the approved fact sheet (ISMS-CLI-FICHE-001).	Response log.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Maintain participant data	ISMS manager	CISO	Legal
Approve sharing	CISO	Top management	Account managers
Order reassessment	ISMS manager	CISO	Finance

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Portal extract and review	ENX portal; ISMS manager	Quarterly	6 years
Sharing log	ENX portal and CRM; ISMS manager	Per share	6 years
Label expiry calendar	ISMS workspace; ISMS manager	Quarterly	Until superseded + 3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Portal data correct at review	100%	Correct within 5 days
Reassessment ordered ≥ 6 months before expiry	100%	Top management
Result shares with CISO approval	100%	Incident

Auditor questions to prepare

- How is your portal scope kept consistent with reality?
- Who may share your result?
- When does your label expire and what is the plan?

Frequent nonconformities

- Stale scope in portal.
- Report distributed by email.

Interfaces: ISMS-ORG-PERIMETRE-001, ISMS-CLI-FICHE-001, ISMS-CLI-DIFFUSION-001, ISMS-AUD-FIELDWORK-001

ISMS-CLI-SECURITE-002 — Supplier qualification questionnaire

Classification C1 · INTERNAL · Format REGISTER · Applicability Added

Objective

Qualify suppliers through a consistent security questionnaire proportionate to the supplier's risk tier, with scoring and follow-up.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Supplier relationships: selection and assessment of contractors and service providers (chapter 6)
ISO/IEC 27001:2022	A.5.19 Information security in supplier relationships; A.5.21 ICT supply chain; A.5.22 Monitoring of supplier services
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
SQ2-01	The questionnaire shall have tiers (basic, standard, high) aligned with the supplier risk tier and covering governance, access, data protection, incident handling, subcontracting, physical security and continuity.	Questionnaire versions per tier.
SQ2-02	Responses shall be scored using documented criteria and reviewed by the supplier manager and, for high tier, the CISO.	Scored responses.
SQ2-03	Claims shall be verified by evidence (certificates, reports, policies) for all high-tier suppliers.	Evidence list.
SQ2-04	Gaps shall produce a corrective plan with dates before contracting, or a risk acceptance under ISMS-ORG-DEROGATIONS-001.	Plans and acceptances.
SQ2-05	Questionnaires shall be repeated at least annually for high tier and every 24 months for standard tier.	Schedule.
SQ2-06	The questionnaire content shall be reviewed annually against ISA and customer requirements.	Review record.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Send and collect	Supplier manager	Procurement manager	Service owner
Score and review	Security analyst	CISO	Supplier manager
Track gaps	Supplier manager	CISO	Supplier

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Questionnaire and score	Supplier repository; supplier manager	Per supplier	Contract + 6 years
Evidence copies	Supplier repository; supplier manager	Per supplier	Contract + 6 years
Corrective plans	Supplier repository; supplier manager	Per gap	Contract + 3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Tiered suppliers with current questionnaire	100%	Block new data sharing
High-tier answers evidenced	100%	Reopen
Plans closed on time	≥ 90%	Escalate

Auditor questions to prepare

- How do you tier suppliers and what do you ask each tier?

- Show a scored questionnaire and what you did with the gaps.
- How do you verify answers?

Frequent nonconformities

- Self-declaration accepted without evidence.
- No periodic repetition.

Interfaces: ISMS-FOU-POLITIQUE-001, ISMS-FOU-EVALUATION-001, ISMS-FOU-REGISTRE-001

ISMS-ORG-DOC-001 — ISMS document control

Classification C1 · INTERNAL · Format PROCEDURE · Applicability Added

Objective

Keep ISMS documents controlled, current, approved and reachable so that only the version in force is used and every change is traceable.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Policies and organisation: document control, communication of policies (chapter 1)
ISO/IEC 27001:2022	Clause 7.5 Documented information; A.5.1 Policies; A.5.37 Documented operating procedures; A.5.33 Protection of records
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
DOC-01	Each ISMS document shall have unique ID, title, owner, approver, version, classification, effective date and next review date.	Document register.
DOC-02	Documents shall be approved by the authority named in the approval table before use; drafts shall be marked and shall not be used operationally.	Approval records.
DOC-03	A single controlled repository shall hold the current versions with access matching classification; superseded versions shall be archived.	Repository permissions and archive.
DOC-04	Document owners shall review each document at least annually or on trigger events; overdue reviews shall be reported monthly.	Overdue report.
DOC-05	Changes shall be recorded in a revision history and communicated to affected roles with acknowledgement for policies.	Revision history and acknowledgements.
DOC-06	Markings and labels shall follow ISMS-ACT-CLASSIF-001 and be checked by sampling quarterly.	Sampling results.
DOC-07	External documents (customer specifications, standards) shall be registered and checked for currency.	External document register.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Maintain register	ISMS manager	CISO	Document owners
Approve documents	Approval authority	Top management	CISO
Review documents	Owners	Department heads	ISMS manager

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Document register	Document system; ISMS manager	Continuous	Life + 6 years
Approval records	Document system; approvers	Per version	6 years
Overdue review report	ISMS workspace; ISMS manager	Monthly	3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Documents approved and in date	≥ 98%	Overdue list to CISO
Drafts in operational use	0	Withdraw
Marking errors in sample	≤ 5%	Awareness action

Auditor questions to prepare

- How do you know staff use the current version?

- Show a document change and who approved it.
- Where are drafts kept?

Frequent nonconformities

- Several versions in circulation.
- Approver missing.

Interfaces: ISMS-POL-SSI-002, ISMS-ACT-CLASSIF-001, ISMS-ORG-GOUVERNANCE-001, ISMS-ACT-CONSERVATION-001

ISMS-ORG-OBJECTIFS-001 — Security objectives and metrics

Classification C1 · INTERNAL · Format PROCEDURE · Applicability Added

Objective

Define measurable security objectives and metrics aligned with the policy and business risk, and use them to steer the ISMS.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Organisation and assessments: objectives, measurement and management review (chapter 1)
ISO/IEC 27001:2022	Clause 6.2 Information security objectives; Clause 9.1 Monitoring, measurement, analysis and evaluation; Clause 9.3
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
OBJ-01	Objectives shall be derived from the policy, risk assessment and customer requirements, with owner, metric, target, method and date.	Objectives register.
OBJ-02	Objectives shall be reviewed at least quarterly; measurement data shall come from systems of record where possible.	Measurement data.
OBJ-03	Results below target shall trigger an analysis and a documented action.	Action records.
OBJ-04	Objectives and results shall be presented at management review and communicated to relevant staff.	Management review input.
OBJ-05	Objective set shall be updated annually and after major incidents or changes.	Update record.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Define objectives	CISO	Top management	Department heads
Measure	Metric owners	Department heads	ISMS manager
Report	ISMS manager	CISO	Top management

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Objectives register	ISMS workspace; ISMS manager	Annual	6 years
Quarterly results	ISMS dashboard; ISMS manager	Quarterly	3 years
Actions	Ticket system; owners	Per miss	3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Objectives measured on schedule	100%	Escalate
Objectives met	≥ 80%	Analysis
Objectives with named owner	100%	Assign

Auditor questions to prepare

- Which objectives did you set and how did you perform?
- Show a missed objective and the action.
- Who sees these results?

Frequent nonconformities

- Objectives not measurable.
- No action on missed targets.

Interfaces: ISMS-POL-SSI-002, ISMS-AUD-PROGRAMME-001, ISMS-ORG-GOUVERNANCE-001

ISMS-ORG-GOUVERNANCE-001 — Security steering committee and decisions

Classification C1 · INTERNAL · Format PROCEDURE · Applicability Added

Objective

Run a security steering committee that takes, records and follows up decisions on risk, investment, exceptions and compliance.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Organisation of information security: management commitment and governance (chapter 1)
ISO/IEC 27001:2022	Clause 5.1 Leadership; Clause 9.3 Management review; A.5.2 Roles and responsibilities
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
GOV-01	The committee shall include top management, the CISO and representatives of IT, HR, legal, operations and facility, and meet at least quarterly.	Charter and attendance.
GOV-02	The agenda shall cover risks, incidents, audit findings, objectives, exceptions, projects and customer requirements.	Agenda and minutes.
GOV-03	Decisions shall be recorded with owner and due date and tracked until closure.	Decision log.
GOV-04	Quorum and delegation rules shall be defined; decisions on high-risk acceptance require top management.	Charter.
GOV-05	Minutes shall be distributed within 5 working days.	Distribution record.
GOV-06	The charter shall be reviewed annually.	Review record.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Chair committee	CISO	Managing director	Members
Record minutes	ISMS manager	CISO	Members
Track decisions	ISMS manager	CISO	Owners

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Minutes	Document system; ISMS manager	Quarterly	6 years
Decision log	ISMS workspace; ISMS manager	Quarterly	6 years
Attendance	Minutes; ISMS manager	Quarterly	3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Meetings held as planned	100%	Reschedule within 14 days
Decisions closed on time	≥ 85%	Escalate
Top management attendance	≥ 80%	Discuss

Auditor questions to prepare

- Show recent minutes and decisions.
- How does top management steer security?
- How are decisions followed up?

Frequent nonconformities

- No top management presence.
- Decisions without owners.

Interfaces: ISMS-AUD-PROGRAMME-001, ISMS-ORG-OBJECTIFS-001, ISMS-ORG-DEROGATIONS-001, ISMS-RSK-REGISTRE-001

ISMS-ORG-SITES-001 — Multi-site security operating model

Classification C1 · INTERNAL · Format PROCEDURE · Applicability Added

Objective

Ensure uniform security governance across all sites, with clear central and local responsibilities and verified local operation.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Organisation of information security: multi-site organisation and local responsibilities (chapters 1 and 3)
ISO/IEC 27001:2022	A.5.2 Roles and responsibilities; A.7.1 Physical security perimeters; Clause 4.3 Scope
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
SIT-01	Each site shall have a named security contact and deputy and a local risk view.	Site contact list.
SIT-02	Central policies shall apply to all sites; local deviations shall follow the exception procedure.	Exception register.
SIT-03	Sites shall be assessed at least annually against a common checklist covering physical, IT, personnel and incident aspects.	Site assessment reports.
SIT-04	A site security report shall be sent quarterly to the CISO.	Reports.
SIT-05	New sites, closures and moves shall trigger scope and ENX portal updates before operation.	Change record.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Local operation	Site security contact	Site manager	CISO
Assess sites	ISMS reviewer	CISO	Site managers
Consolidate	ISMS manager	CISO	Top management

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Site assessments	ISMS workspace; reviewer	Annual	3 years
Quarterly reports	ISMS workspace; contacts	Quarterly	3 years
Site contact list	Document system; ISMS manager	Semi-annual	3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Sites assessed in 12 months	100%	Immediate plan
Open site findings > 60 days	0	CISO
Sites with named contact	100%	Appoint

Auditor questions to prepare

- How do you ensure every site follows the same rules?
- Show a site assessment.
- Who is responsible locally?

Frequent nonconformities

- No local contact.
- Uneven site practice.

Interfaces: ISMS-ORG-PERIMETRE-001, ISMS-ORG-INTERFACES-001, ISMS-PHY-ZONES-001, ISMS-PHY-INSPECTIONS-001

ISMS-ORG-ISA-001 — VDA ISA coverage and applicability matrix

Classification C2 · CONFIDENTIAL · Format REGISTER · Applicability Added

Objective

Document how each ISA control is covered, by which document, owner and evidence, to support assessment planning and gap management.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	TISAX assessment preparation: VDA ISA coverage and applicability (all chapters)
ISO/IEC 27001:2022	Clause 6.1.3 Statement of applicability; A.5.36 Compliance with policies
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
ISA-01	The matrix shall list every ISA control question of the ISA edition in use with applicability, owner, implementing document, evidence reference and self-assessed maturity.	Matrix.
ISA-02	The matrix shall be reconciled with ISMS-ORG-SOA-001 so that both state the same applicability.	Reconciliation.
ISA-03	Gaps shall be linked to actions with dates and tracked (ISMS-AUD-CLOSURE-001).	Action link.
ISA-04	The ISA edition and version used shall be recorded and changes in the ISA shall be assessed within 30 days of publication.	Change log.
ISA-05	The matrix shall be updated after each audit, incident and process change.	Update log.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Maintain matrix	ISMS manager	CISO	Control owners
Self-assess	Control owners	Department heads	ISMS manager
Reconcile	ISMS reviewer	CISO	ISMS manager

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
ISA matrix	ISMS workspace; ISMS manager	Quarterly	6 years
Reconciliation record	ISMS workspace; reviewer	Annual	3 years
ISA change log	ISMS workspace; ISMS manager	Per change	3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Applicable controls with evidence	100%	Plan
Controls below maturity 3	0 at assessment	Corrective plan
Matrix reviewed in quarter	100%	Escalate

Auditor questions to prepare

- How do you know all ISA controls are covered?
- Show the evidence behind one control.
- Which ISA version do you use?

Frequent nonconformities

- Matrix not aligned with SoA.
- Edition unknown.

Interfaces: ISMS-ORG-SOA-001, ISMS-AUD-MATURITY-001, ISMS-AUD-CLOSURE-001

ISMS-RSK-REGISTRE-001 — Information security risk register

Classification C2 · CONFIDENTIAL · Format REGISTER · Applicability Added

Objective

Keep a single, current and owned register of information security risks that supports treatment decisions and reporting.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Information security risk management: risk register, treatment and acceptance (chapter 1)
ISO/IEC 27001:2022	Clause 6.1.2 Information security risk assessment; Clause 8.2; A.5.7 Threat intelligence
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
RGR-01	Every risk shall record asset or process, threat, vulnerability, impact, likelihood, inherent and residual rating, owner, treatment and due date.	Register fields.
RGR-02	The register shall be reviewed quarterly by risk owners and updated on incidents, audit findings, new threats and changes.	Review records.
RGR-03	Residual risks above threshold shall be accepted by top management in writing and be time-limited.	Acceptances.
RGR-04	Risks shall be linked to controls and exceptions.	Links.
RGR-05	Closed risks shall be retained with reasons for closure.	Closed items.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Maintain register	Risk coordinator	CISO	Risk owners
Review risks	Risk owners	Department heads	Risk coordinator
Accept residual risk	Risk owners	Top management	CISO

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Risk register	Risk tool; risk coordinator	Quarterly	6 years
Acceptances	Document system; top management	Per decision	6 years
Review minutes	Meeting minutes; coordinator	Quarterly	3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Risks with owner and date	100%	Assign
High risks over treatment date	0	Top management
Register reviewed in quarter	100%	Escalate

Auditor questions to prepare

- Show your top five risks and treatment.
- How did a recent incident change the register?
- Who accepted this risk?

Frequent nonconformities

- Static register.

- No owners.

Interfaces: ISMS-RSK-METHODE-001, ISMS-RSK-TRAITEMENT-001, ISMS-ORG-DEROGATIONS-001, ISMS-ORG-MENACES-001

ISMS-RSK-TRAITEMENT-001 — Risk treatment plan

Classification C2 · CONFIDENTIAL · Format STANDARD · Applicability Added

Objective

Plan, execute and verify the treatment of risks so that residual risk falls to accepted levels.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Information security risk management: risk treatment plan (chapter 1)
ISO/IEC 27001:2022	Clause 6.1.3 Risk treatment; Clause 8.3; A.5.36
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
RTP-01	Each treated risk shall have a treatment option, selected controls, owner, budget, milestones and due date.	Treatment plan lines.
RTP-02	Treatment plan shall be approved by top management.	Approval.
RTP-03	Progress shall be tracked monthly and overdue items escalated.	Progress report.
RTP-04	After completion, effectiveness shall be verified and residual risk re-rated.	Verification.
RTP-05	Accepted residual risks shall be recorded in the register.	Register update.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Plan treatment	Risk owners	Department heads	CISO
Execute	Action owners	Risk owners	ISMS manager
Verify	ISMS reviewer	CISO	Owners

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Treatment plan	Risk tool; ISMS manager	Monthly	6 years
Verification notes	Risk tool; reviewer	Per action	6 years
Approval	Document system; top management	Annual	6 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Actions on time	≥ 85%	Escalate
Treatments verified	100%	Reopen
Overdue high-risk actions	0	Top management

Auditor questions to prepare

- Show a risk you treated and how you verified it.
- Who approved the plan?
- What is overdue?

Frequent nonconformities

- No verification.
- Plan unapproved.

Interfaces: ISMS-RSK-REGISTRE-001, ISMS-RSK-METHODE-001, ISMS-ORG-DEROGATIONS-001

ISMS-ACT-FLUX-001 — Information-flow and data-flow maps

Classification C2 · CONFIDENTIAL · Format REGISTER · Applicability Added

Objective

Document where protected information flows within and outside the scope, so that controls, suppliers and locations can be verified.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Asset management: information flows, data locations and interfaces (chapters 1, 5 and 6)
ISO/IEC 27001:2022	A.5.9 Inventory of information; A.5.14 Information transfer; A.8.20 Network security; A.8.22 Segregation
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
FLX-01	Data-flow maps shall show systems, data classes, protocols, encryption, locations, owners and third parties for every C2/C3 flow.	Diagrams.
FLX-02	Maps shall be validated against network diagrams, firewall rules and cloud configuration at least annually.	Validation record.
FLX-03	Every external flow shall have a recorded legal and contractual basis and security measure.	Flow register.
FLX-04	Changes shall update the maps within 30 days.	Change log.
FLX-05	Unknown flows detected by monitoring shall be investigated within 5 working days.	Investigation tickets.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Maintain maps	Security architect	IT manager	Service owners
Validate	Security engineering	CISO	Architect
Approve external flows	Information owners	Department heads	DPO

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Data-flow maps	Document system; architect	On change / annual	Life + 3 years
Flow register	CMDB; architect	Quarterly	Life + 3 years
Validation	ISMS workspace; engineering	Annual	3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
C2/C3 flows mapped	100%	Map within 30 days
Unknown flows open > 5 days	0	CISO
Maps validated in 12 months	100%	Escalate

Auditor questions to prepare

- Show where customer data flows from receipt to deletion.
- How do you detect an undocumented flow?
- Who approves an external flow?

Frequent nonconformities

- Maps outdated.
- Flows to third parties missing.

Interfaces: ISMS-OPS-RESEAU-001, ISMS-ACT-TRANSFERT-001, ISMS-INF-HEB-002, ISMS-ACT-INVENTAIRE-001

ISMS-ACT-TRANSFERT-001 — Secure information exchange and transfer

Classification C1 · INTERNAL · Format PROCEDURE · Applicability Added

Objective

Exchange information securely with third parties through approved channels and controls proportionate to classification.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Asset management and IT security: information transfer and exchange (chapters 1 and 5)
ISO/IEC 27001:2022	A.5.14 Information transfer; A.8.24 Use of cryptography; A.5.10 Acceptable use
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
XFR-01	Approved channels per classification shall be defined (for example C2 through encrypted email or managed file transfer; C3 through approved secure exchange only).	Channel matrix.
XFR-02	Transfers of C2/C3 information shall be encrypted in transit and, for files, at rest with keys exchanged out-of-band.	Configuration.
XFR-03	Recipients shall be verified and authorised before transfer; bulk transfers shall be logged.	Transfer log.
XFR-04	Customer-mandated platforms shall be used where required.	Customer requirement mapping.
XFR-05	Misdirected transfers shall be reported as incidents.	Incident tickets.
XFR-06	Transfer tools shall be reviewed annually.	Review.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Define channels	Security architect	CISO	IT; legal
Operate transfer tools	IT operations	IT manager	CISO
Review logs	Security analyst	CISO	IT operations

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Channel matrix	Document system; architect	Annual	3 years
Transfer logs	MFT/DLP; IT operations	Continuous	12 months
Misdirection incidents	Incident system; analyst	Per event	3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Transfers via approved channels	≥ 98%	DLP follow-up
Misdirected transfers	0	Incident
C3 transfers logged	100%	Investigate

Auditor questions to prepare

- How do you send C3 files to a customer?
- Show a transfer log.
- What if the wrong person received data?

Frequent nonconformities

- Unencrypted email.
- No transfer logs.

Interfaces: ISMS-OPS-DLP-001, ISMS-OPS-EMAIL-001, ISMS-CRY-POLITIQUE-001, ISMS-ACT-CLASSIF-001

ISMS-ACT-CONSERVATION-001 — Information retention and destruction

Classification C1 · INTERNAL · Format PROCEDURE · Applicability Added

Objective

Retain information only as long as needed or required, and destroy it securely afterwards, covering contracts, law and ISMS records.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Compliance: protection of records, retention and destruction (chapter 7)
ISO/IEC 27001:2022	A.5.33 Protection of records; A.8.10 Information deletion; A.7.14 Secure disposal; A.5.34
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
RET-01	A retention schedule shall state period, legal or contractual basis, owner and destruction method per record type.	Schedule.
RET-02	Retention shall be enforced technically where possible (lifecycle rules, automated deletion).	Configuration.
RET-03	Destruction shall be recorded and certified for C2/C3 information, including backups where feasible.	Destruction records.
RET-04	Legal holds shall suspend destruction and be recorded.	Hold register.
RET-05	Customer-specific retention shall override the default.	Mapping.
RET-06	The schedule shall be reviewed annually.	Review log.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Maintain schedule	Compliance officer	CISO	Legal; DPO
Execute deletion	IT operations	IT manager	Data owners
Verify	ISMS reviewer	CISO	Data owners

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Retention schedule	Document system; compliance officer	Annual	6 years
Destruction records	ITSM; IT operations	Per event	6 years
Legal holds	Legal files; legal	Per hold	Hold + 6 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Records beyond retention	0	Delete within 30 days
Destruction certified	100%	Incident
Schedule reviewed	100%	Escalate

Auditor questions to prepare

- How do you delete data after a contract ends?
- Show a destruction record.
- How do you handle legal holds?

Frequent nonconformities

- Indefinite retention.
- No evidence of deletion.

Interfaces: ISMS-CON-RETENTION-001, ISMS-RGP-RETENTION-001, ISMS-OPS-SUPPRESSION-001, ISMS-PHY-SUPPORTS-001

ISMS-ORG-MENACES-001 — Threat intelligence and risk context

Classification C2 · CONFIDENTIAL · Format PROCEDURE · Applicability Added

Objective

Use current threat information to keep the risk assessment and detection use cases aligned with real threats against the organisation and its customers.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Risk management and IT security: threat intelligence and context (chapters 1 and 5)
ISO/IEC 27001:2022	A.5.7 Threat intelligence; A.8.16 Monitoring activities; Clause 6.1.2
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
THR-01	Named sources (national CERT, ENX/VDA, ISAC, vendor advisories, sector reports) shall be monitored by a named role at least weekly.	Source list and log.
THR-02	Relevant threats shall be assessed for impact within 5 working days and, if relevant, added to the risk register and detection rules.	Assessment records.
THR-03	Actionable indicators shall be passed to security operations and checked retroactively in logs.	Hunt records.
THR-04	Customer and sector alerts shall be shared per agreements.	Sharing records.
THR-05	A quarterly threat summary shall be presented to the steering committee.	Summary.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Collect intelligence	Threat analyst	CISO	SOC
Assess and act	ISMS manager	CISO	Risk owners
Report	CISO	Top management	Steering committee

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Threat log	ISMS workspace; analyst	Weekly	3 years
Assessments	Ticket system; analyst	Per item	3 years
Quarterly summary	Document system; CISO	Quarterly	3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Relevant threats assessed within 5 days	≥ 90%	Staffing
Indicators checked in logs	100%	Investigate
Summaries delivered	100%	Escalate

Auditor questions to prepare

- How do you learn about threats that matter to you?
- Show a recent threat and what changed.
- Who sees it?

Frequent nonconformities

- No named source.

- No link to risk register.

Interfaces: ISMS-RSK-REGISTRE-001, ISMS-OPS-SIEM-001, ISMS-OPS-VULN-001, ISMS-CON-VEILLE-001

ISMS-ORG-ECARTS-001 — Nonconformity and corrective action

Classification C1 · INTERNAL · Format PROCEDURE · Applicability Added

Objective

Handle nonconformities and corrective actions from all sources through root-cause analysis, correction and verified closure.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Assessments and continual improvement: handling of nonconformities (chapter 1)
ISO/IEC 27001:2022	Clause 10.2 Nonconformity and corrective action; A.5.36 Compliance with policies; Clause 10.1
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
NCR-01	Nonconformities from audits, incidents, self-checks, customer complaints and monitoring shall be recorded in one register with source, severity and owner.	Register.
NCR-02	Immediate correction and containment shall be documented.	Correction notes.
NCR-03	Root-cause analysis shall be performed for severe and repeated nonconformities using a documented method.	Analysis.
NCR-04	Corrective actions shall be verified for effectiveness by an independent person.	Verification.
NCR-05	Status shall be reported monthly and overdue actions escalated.	Report.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Record	Anyone	Process owner	ISMS manager
Analyse and correct	Owners	Department heads	ISMS manager
Verify	ISMS reviewer	CISO	Owners

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Nonconformity register	Audit tool; ISMS manager	Continuous	6 years
Root-cause analyses	Audit tool; owners	Per case	6 years
Verification	Audit tool; reviewer	Per case	6 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Actions closed on time	≥ 90%	Escalate
Repeat nonconformities	0	Re-analysis
Verified closures	100%	Reopen

Auditor questions to prepare

- Show a nonconformity from record to verified closure.
- How do you spot recurring issues?
- Who verifies?

Frequent nonconformities

- Closure without verification.

- Single register missing.

Interfaces: ISMS-AUD-CLOSURE-001, ISMS-AUD-PROGRAMME-001, ISMS-INC-PROC-001

ISMS-CLI-ENGAGEMENTS-001 — Register of customer security commitments

Classification C2 · CONFIDENTIAL · Format REGISTER · Applicability Added

Objective

Keep a register of every security commitment given to customers, linked to the control and owner that fulfils it and to its evidence.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Compliance and supplier relationships: contractual commitments to customers (chapters 6 and 7)
ISO/IEC 27001:2022	A.5.31 Legal and contractual requirements; A.5.36 Compliance with policies; A.5.20
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
CEN-01	Each commitment shall be recorded with customer, source clause, deadline or frequency, owner, linked control and evidence.	Register.
CEN-02	Commitments shall be verified at least semi-annually by the owner and sampled by ISMS assurance.	Verification records.
CEN-03	Commitments that cannot be met shall be escalated to the CISO and renegotiated or accepted as exceptions.	Escalation records.
CEN-04	New or changed commitments shall be registered before signature.	Pre-signature check.
CEN-05	Registers shall be restricted to need-to-know (C2).	Access list.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Register	Contract manager	Account owner	ISMS manager
Verify	Owners	Department heads	ISMS reviewer
Escalate	ISMS manager	CISO	Legal

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Commitment register	ISMS workspace; contract manager	Continuous	Contract + 6 years
Verification records	ISMS workspace; owners	Semi-annual	3 years
Escalations	Ticket system; ISMS manager	Per case	3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Commitments with control and evidence	100%	Complete within 14 days
Commitments verified in 6 months	100%	Escalate
Unmet commitments	0	Top management

Auditor questions to prepare

- List the commitments you made to this customer and show evidence.
- What if you cannot meet one?
- Who signs them off?

Frequent nonconformities

- No owner.

- Not verified.

Interfaces: ISMS-CLI-EXIGENCES-001, ISMS-CLI-ANNEXE-001, ISMS-CON-CONTROLES-001

ISMS-ORG-CONTROLES-001 — Internal security control testing plan

Classification C2 · CONFIDENTIAL · Format STANDARD · Applicability Added

Objective

Test the design and operation of controls throughout the year, independently of the control owner, to give early warning before external assessment.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Assessments: internal control testing and independent review (chapter 1)
ISO/IEC 27001:2022	A.5.35 Independent review; A.5.36 Compliance; Clause 9.1
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
ICT-01	An annual testing plan shall cover all applicable ISA controls, with high-risk controls tested at least twice a year.	Plan.
ICT-02	Tests shall use a documented procedure, population and sample (ISMS-AUD-SAMPLE-001).	Test sheets.
ICT-03	Testers shall be independent from the control owner.	Independence record.
ICT-04	Failed tests shall create findings handled under ISMS-AUD-CLOSURE-001.	Findings.
ICT-05	Results shall feed the maturity assessment and management review.	Reports.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Plan tests	ISMS manager	CISO	Control owners
Test	ISMS reviewer	CISO	Control owners
Report	ISMS manager	CISO	Top management

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Test plan	ISMS workspace; ISMS manager	Annual	3 years
Test sheets	Audit tool; reviewers	Per test	3 years
Test report	ISMS workspace; ISMS manager	Quarterly	6 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Planned tests completed	≥ 95%	Reschedule
Tests failed	Tracked	Action
Controls tested in 12 months	100%	Escalate

Auditor questions to prepare

- Show a test you did on this control and the result.
- Who tested?
- What changed afterwards?

Frequent nonconformities

- Owner tests own control.
- Tests skipped.

Interfaces: ISMS-AUD-PROGRAMME-001, ISMS-AUD-SAMPLE-001, ISMS-AUD-MATURITY-001, ISMS-AUD-CLOSURE-001

ISMS-INC-PRESERVATION-001 — Incident evidence collection and preservation

Classification C2 · CONFIDENTIAL · Format PROCEDURE · Applicability Added

Objective

Collect and preserve digital and physical evidence of incidents in a forensically sound way, preserving admissibility and chain of custody.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Incident management: evidence collection and handling (chapter 1)
ISO/IEC 27001:2022	A.5.28 Collection of evidence; A.5.26 Response; A.8.15 Logging; A.8.17 Clock synchronisation
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
PRV-01	Evidence shall be collected by trained staff using documented methods that preserve integrity (write-blockers, hashes, memory and log capture).	Collection records with hashes.
PRV-02	Each item shall have chain of custody recording who, when, why and where it was stored.	Custody log.
PRV-03	Evidence shall be stored in a protected location with restricted access and kept until the case and legal period end.	Storage and access list.
PRV-04	Time sources shall be synchronised and offset recorded when evidence is collected (ISMS-OPS-TEMPS-001).	Time record.
PRV-05	External forensic providers shall be pre-contracted under NDA.	Retainer agreement.
PRV-06	Legal and DPO shall be consulted before collection involving personal data.	Consultation record.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Collect evidence	Forensic responder	Incident manager	Legal
Maintain custody	Evidence custodian	CISO	Incident manager
Release evidence	CISO	Managing director	Legal

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Collection and hash records	Evidence vault; responder	Per incident	Case + 6 years
Chain of custody	Evidence vault; custodian	Per item	Case + 6 years
Retainer	Contract system; legal	Annual	Contract + 6 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Items with complete custody	100%	Incident review
Forensic responders trained	100%	Train
Evidence accessed by unauthorised people	0	Incident

Auditor questions to prepare

- How would you preserve a compromised server?
- Show a custody record.
- Who may access evidence?

Frequent nonconformities

- Evidence altered by responders.
- No custody log.

Interfaces: ISMS-INC-PROC-001, ISMS-OPS-TEMPS-001, ISMS-OPS-JOURNAUX-001, ISMS-AUD-EVIDENCE-001

ISMS-RH-TIERS-001 — External workforce security management

Classification C1 · INTERNAL · Format PROCEDURE · Applicability Added

Objective

Manage the security of external workforce (contractors, interim staff, consultants) throughout engagement, with the same discipline as employees.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Human resources and supplier relationships: external personnel (chapters 2 and 6)
ISO/IEC 27001:2022	A.6.1 Screening; A.6.2 Terms; A.6.5 Responsibilities after termination; A.5.19
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
EXT-01	External workers shall be registered with sponsor, agency, access scope, start and end dates.	Register.
EXT-02	Screening proportional to access shall be completed by the agency or the organisation before access to C2/C3.	Screening evidence.
EXT-03	Security obligations shall be in contracts and NDAs, acknowledged by the individual.	Signed obligations.
EXT-04	Access shall expire with the contract and be reviewed monthly by the sponsor.	Review records.
EXT-05	Equipment shall be returned and access removed on exit with confirmation.	Exit checklist.
EXT-06	Awareness training shall be completed within 10 days.	Training records.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Register	Sponsor	Department head	HR
Provision and expire access	IAM operations	IAM owner	Sponsor
Review monthly	Sponsor	Department head	IAM owner

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
External worker register	HR / vendor system; sponsor	Continuous	Contract + 3 years
Monthly reviews	IAM tool; sponsors	Monthly	3 years
Exit checklists	Ticket system; sponsor	Per exit	3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
External workers with sponsor	100%	Assign
Accounts past contract end	0	Disable
Training completion	≥ 98%	Reminder

Auditor questions to prepare

- How many contractors have access and who sponsors each?
- Show an exit.
- How do you screen them?

Frequent nonconformities

- No sponsor.
- Access outlasting contract.

Interfaces: ISMS-RH-CHARTE-002, ISMS-RH-CYCLE-001, ISMS-IAM-TIERS-001, ISMS-RH-NDA-001

ISMS-RH-POSTES-001 — Sensitive roles and segregation of duties

Classification C2 · CONFIDENTIAL · Format PROCEDURE · Applicability Added

Objective

Identify sensitive roles, apply stronger screening and controls, and separate duties where a single person could cause serious harm.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Organisation and human resources: segregation of duties and trusted roles (chapters 1 and 2)
ISO/IEC 27001:2022	A.5.3 Segregation of duties; A.6.1 Screening; A.8.2 Privileged access rights
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
SRO-01	A list of sensitive roles (administrators, security, finance approvers, key custodians, prototype handlers) shall exist with owner.	Role list.
SRO-02	Holders shall undergo enhanced screening where lawful and acknowledge additional duties.	Screening and acknowledgements.
SRO-03	Segregation of duties matrix shall define incompatible duties and compensating controls.	Matrix.
SRO-04	Four-eyes or dual control shall apply to critical actions (key use, production release, payment, C3 export).	Workflow evidence.
SRO-05	Holders shall be reviewed annually.	Review.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Define roles	CISO	Top management	HR
Screen	HR	HR manager	CISO
Review	ISMS manager	CISO	Department heads

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Sensitive role list	ISMS workspace; ISMS manager	Annual	3 years
Screening results	HR system; HR	Per hire	Employment + 1 year
SoD matrix	IAM tool; IAM owner	Semi-annual	3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Sensitive-role holders screened	100%	Restrict
SoD conflicts uncontrolled	0	Decision
Role reviews done	100%	Escalate

Auditor questions to prepare

- Which roles are sensitive and why?
- Show a segregation conflict.
- How is dual control enforced?

Frequent nonconformities

- List incomplete.

- No review.

Interfaces: ISMS-ORG-ROLES-001, ISMS-IAM-PRIV-001, ISMS-RH-CYCLE-001

ISMS-RH-FORMATION-001 — Role-based training curriculum

Classification C1 · INTERNAL · Format STANDARD · Applicability Added

Objective

Provide role-specific security training so that people with specific responsibilities have the competence required.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Human resources: training of staff with specific responsibilities (chapter 2)
ISO/IEC 27001:2022	A.6.3 Awareness, education and training; A.5.4 Management responsibilities; Clause 7.2 Competence
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
TRN-01	A curriculum shall map each role to required modules, frequency and assessment.	Curriculum.
TRN-02	Records shall show completion and test results; incomplete training shall block privileges after 60 days.	LMS records.
TRN-03	Technical teams shall receive hands-on training at least annually.	Attendance.
TRN-04	Training content shall be updated based on incidents, audit findings and threat changes.	Update log.
TRN-05	Competence of control owners shall be assessed annually.	Assessment.
TRN-06	The role-based curriculum shall include data protection modules for roles that process personal data in volume or special categories (ISA 9.7.2), with assessment of competence.	Curriculum entries and results.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Define curriculum	ISMS manager	CISO	HR
Deliver	Trainers	HR manager	Department heads
Track	HR	HR manager	Line managers

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Curriculum	ISMS workspace; ISMS manager	Annual	3 years
Completion records	LMS; HR	Per course	3 years
Competence assessment	HR system; line managers	Annual	3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Role modules completed	≥ 95%	Escalate
Test pass rate	≥ 85%	Retrain
Content updated in 12 months	100%	Review

Auditor questions to prepare

- What training do your administrators receive?
- Show completion data.
- How is competence checked?

Frequent nonconformities

- Training generic.
- No consequence for non-completion.

Interfaces: ISMS-RH-SENSIBILISATION-001, ISMS-RH-POSTES-001, ISMS-DEV-SDLC-001

ISMS-RH-DEPLACEMENTS-001 — Travel and off-site equipment use

Classification C1 · INTERNAL · Format PROCEDURE · Applicability Added

Objective

Protect information and equipment when staff travel or work off-site, including in high-risk regions.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Human resources and physical security: mobile working and travel (chapters 2 and 3)
ISO/IEC 27001:2022	A.6.7 Remote working; A.7.9 Security of assets off-premises; A.8.1 User endpoint devices
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
TRV-01	Travel to high-risk countries shall be declared and approved; clean loan devices shall be used.	Approvals.
TRV-02	C3 information shall not be carried on travel devices without encryption and CISO approval.	Approval.
TRV-03	Devices shall never be left unattended; hotel and vehicle storage rules shall be followed.	Awareness evidence.
TRV-04	Public Wi-Fi shall only be used with VPN; screen privacy filters used on trains and planes.	Technical controls.
TRV-05	Loss or confiscation shall be reported immediately and access revoked.	Incident record.
TRV-06	Devices shall be inspected after high-risk trips.	Inspection record.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Approve travel	Line manager	Department head	CISO
Prepare devices	IT operations	IT manager	Traveller
Respond to loss	Service desk	IT manager	CISO

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Travel approvals	Ticket system; line managers	Per trip	3 years
Device preparation	ITSM; IT operations	Per trip	3 years
Post-trip inspection	ITSM; IT operations	Per trip	3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
High-risk trips approved	100%	Incident
Devices encrypted	100%	Block
Losses reported within 1 hour	100%	Review

Auditor questions to prepare

- How do you prepare a laptop for a high-risk country?
- Show an approval.
- What if a device is confiscated?

Frequent nonconformities

- No clean devices.
- No post-trip check.

Interfaces: ISMS-RH-TELETRAVAIL-001, ISMS-RH-MOBILE-001, ISMS-OPS-ENDPOINT-001

ISMS-PHY-BADGES-001 — Physical access badge management

Classification C1 · INTERNAL · Format PROCEDURE · Applicability Added

Objective

Issue, control and revoke physical access credentials so that only authorised people enter each zone.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Physical security: access credentials and zone entry (chapter 3)
ISO/IEC 27001:2022	A.7.2 Physical entry; A.7.1 Physical security perimeters; A.5.18 Access rights
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
BDG-01	Badges shall be issued after identity check and authorisation by the zone owner; badges shall be personal and non-transferable.	Issue records.
BDG-02	Lost badges shall be reported immediately and blocked within 1 hour.	Block records.
BDG-03	Zone rights shall be reviewed quarterly; leavers' badges shall be disabled at leaving time and returned.	Reviews and HR reconciliation.
BDG-04	Badge system administration shall be restricted, logged and reviewed.	Admin logs.
BDG-05	Temporary and contractor badges shall expire automatically.	Expiry data.
BDG-06	Unreturned badges shall be reported.	Sampled instances traced end to end to the record: Issue and block records.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Issue badges	Reception / security	Facility manager	Zone owner
Review rights	Zone owners	Department heads	Facility manager
Revoke	Facility management	Facility manager	HR

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Issue and block records	Access system; facility management	Continuous	12 months
Quarterly reviews	Access system; zone owners	Quarterly	3 years
Admin logs	Access system; facility management	Monthly	12 months

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Leaver badges disabled on time	100%	Incident
Lost badges blocked within 1 hour	100%	Review
Reviews completed	100%	Revoke

Auditor questions to prepare

- Show badge rights for a restricted zone and who reviewed them.
- What happens if a badge is lost?
- Who administers the system?

Frequent nonconformities

- Shared badges.

- No review.

Interfaces: ISMS-PHY-ZONES-001, ISMS-PHY-VISITEURS-001, ISMS-RH-CYCLE-001

ISMS-PHY-VISITEURS-001 — Visitor and on-site contractor procedures

Classification C1 · INTERNAL · Format PROCEDURE · Applicability Added

Objective

Control the presence of visitors and on-site contractors so that they cannot access, see or remove protected information.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Physical security: visitor and contractor handling (chapter 3)
ISO/IEC 27001:2022	A.7.2 Physical entry; A.7.6 Working in secure areas; A.7.3 Securing offices
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
VIS-01	Visitors shall be pre-announced, identified, registered, given visible badges and escorted in non-public zones.	Visitor log.
VIS-02	Visitors shall be informed of rules, including photography and device restrictions in sensitive areas.	Rules sheet and acknowledgement.
VIS-03	Contractors working on site shall have background-appropriate authorisation, time-limited access and supervision in restricted areas.	Contractor records.
VIS-04	Screens and documents containing C2/C3 shall be secured when visitors are present.	Spot-check.
VIS-05	Visitor logs shall be reviewed monthly and retained 12 months.	Review record.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Receive visitors	Reception	Facility manager	Host
Escort	Host	Department head	Security
Review logs	Security officer	CISO	Facility manager

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Visitor log	Visitor system; reception	Daily	12 months
Contractor authorisations	Facility system; facility management	Per contract	Contract + 1 year
Log reviews	ISMS workspace; security officer	Monthly	3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Visitors escorted	100%	Incident
Visitors without badge	0	Immediate
Logs reviewed monthly	100%	Escalate

Auditor questions to prepare

- What happens when a visitor arrives?
- Show last month's log review.
- How do you handle maintenance staff?

Frequent nonconformities

- Unescorted visitors.

- Paper logs unreadable.

Interfaces: ISMS-PHY-ZONES-001, ISMS-PHY-BADGES-001, ISMS-PRO-IMAGE-001

ISMS-PHY-ENV-001 — Environmental and facilities risk controls

Classification C2 · CONFIDENTIAL · Format PROCEDURE · Applicability Added

Objective

Protect facilities against environmental and infrastructure risks (fire, water, power, temperature, natural events) with tested measures.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Physical security: protection against external and environmental threats (chapter 3); availability
ISO/IEC 27001:2022	A.7.5 Protecting against physical and environmental threats; A.7.11 Supporting utilities; A.7.12 Cabling security; A.7.13 Equipment maintenance
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
ENV-01	A site risk assessment shall cover fire, flood, power loss, extreme weather, theft and nearby hazards at least every 2 years.	Assessment.
ENV-02	Fire detection and suppression shall exist in critical rooms and be inspected per law and at least annually.	Inspection certificates.
ENV-03	UPS and generator capacity shall suit RTO needs and be load-tested at least annually.	Test records.
ENV-04	Temperature and humidity in critical rooms shall be monitored with alarms and response.	Monitoring data.
ENV-05	Power and network cabling shall be protected and labelled.	Inspection.
ENV-06	Maintenance shall be done by authorised staff and recorded.	Maintenance records.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Assess	Facility manager	Site manager	CISO
Maintain	Facility management	Facility manager	IT operations
Test	Facility management	Facility manager	CISO

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Environmental assessment	Facility files; facility manager	Per 2 years	10 years
Inspection and test records	Facility files; facility management	Annual	6 years
Monitoring alarms	Monitoring tool; IT operations	Continuous	12 months

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Tests in date	100%	Schedule
Alarms handled within 30 min	≥ 95%	Review
Critical findings open > 30 days	0	CISO

Auditor questions to prepare

- When did you last test the UPS and generator?
- What happens if the server room overheats?
- Show the fire suppression certificate.

Frequent nonconformities

- Tests overdue.
- No monitoring.

Interfaces: ISMS-PHY-ZONES-001, ISMS-PRA-PCA-001, ISMS-PHY-INSPECTIONS-001

ISMS-PHY-MATERIEL-001 — Equipment maintenance, transport and removal

Classification C1 · INTERNAL · Format PROCEDURE · Applicability Added

Objective

Keep equipment secure during maintenance, transport, relocation and removal from premises.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Physical security: equipment maintenance and off-site handling (chapter 3)
ISO/IEC 27001:2022	A.7.8 Equipment siting; A.7.9 Off-premises assets; A.7.13 Equipment maintenance; A.7.14 Secure disposal
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
EQP-01	Removal of equipment from premises shall require authorisation and be logged.	Removal log.
EQP-02	Equipment sent for maintenance shall be wiped or have storage removed, unless maintained on site under supervision.	Sanitisation record.
EQP-03	Transport of C2/C3 equipment shall be in sealed containers by approved carriers with tracking.	Transport records.
EQP-04	Maintenance providers shall be bound by NDA and supervised.	NDAs and supervision logs.
EQP-05	Returned equipment shall be inspected for tampering.	Inspection.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Authorise removal	Asset owner	Department head	Facility manager
Sanitise	IT operations	IT manager	ISMS manager
Transport	Logistics	Facility manager	CISO

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Removal log	Asset tool; asset owner	Per event	3 years
Sanitisation records	ITSM; IT operations	Per event	3 years
Transport records	Logistics files; logistics	Per event	3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Removals logged	100%	Incident
Maintenance returns sanitised	100%	Investigate
Transport via approved carriers	100%	Review

Auditor questions to prepare

- How do you handle a broken disk sent to the vendor?
- Show a removal log.
- How do you guard against tampering?

Frequent nonconformities

- Equipment leaves unlogged.

- Disks sent unsanitised.

Interfaces: ISMS-PHY-SUPPORTS-001, ISMS-ACT-INVENTAIRE-001, ISMS-OPS-SUPPRESSION-001

ISMS-PHY-INSPECTIONS-001 — Periodic premises inspections

Classification C1 · INTERNAL · Format PROCEDURE · Applicability Added

Objective

Verify through regular inspections that physical security measures operate as designed.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Physical security: inspection and monitoring of premises (chapter 3)
ISO/IEC 27001:2022	A.7.4 Physical security monitoring; A.7.6; A.5.36
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
INS-01	Inspections shall be planned quarterly per site with checklist covering doors, locks, alarms, cameras, clean desk, cabinets, visitors and media.	Checklists.
INS-02	Inspections shall include out-of-hours rounds at least twice a year.	Round reports.
INS-03	Findings shall be logged and corrected within 30 days.	Findings register.
INS-04	Inspectors shall be independent of the inspected area.	Assignment record.
INS-05	Alarm and camera systems shall be tested at least every 6 months.	Test logs.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Plan inspections	Security officer	CISO	Site managers
Inspect	Inspectors	Security officer	Zone owners
Correct findings	Zone owners	Department heads	Facility management

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Inspection reports	ISMS workspace; security officer	Quarterly	3 years
Findings register	Audit tool; security officer	Continuous	3 years
Alarm tests	Facility files; facility management	Semi-annual	3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Inspections done	100%	Reschedule
Findings fixed in 30 days	≥ 90%	Escalate
Out-of-hours rounds	2/year	Do

Auditor questions to prepare

- Show your last inspection and what you fixed.
- Do you inspect outside working hours?
- How do you test alarms?

Frequent nonconformities

- Inspections cosmetic.
- Findings open.

Interfaces: ISMS-PHY-ZONES-001, ISMS-PHY-BADGES-001, ISMS-ORG-SITES-001

ISMS-IAM-PRIV-002 — Privileged access management (PAM/PIM)

Classification C2 · CONFIDENTIAL · Format PROCEDURE · Applicability Added

Objective

Operate privileged access management and just-in-time elevation technically, enforcing the policy for privileged accounts.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Identity and access management: privileged access technology and control (chapter 4)
ISO/IEC 27001:2022	A.8.2 Privileged access rights; A.8.18 Privileged utility programs; A.8.15 Logging
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
PIM-01	Privileged credentials shall be vaulted, rotated after use and never known to administrators where technically possible.	Vault configuration.
PIM-02	Elevation shall be time-limited, ticket-linked and approved for production and C3 systems.	Elevation records.
PIM-03	Sessions to critical systems shall be recorded and retained 12 months.	Recordings.
PIM-04	Standing privileges shall be removed except for break-glass.	Role analysis.
PIM-05	PAM platform administration shall use separate accounts and dual control.	Admin records.
PIM-06	Monthly sampling of sessions shall be performed.	Review notes.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Operate PAM	Security engineering	IT manager	CISO
Approve elevation	System owners	IT manager	IAM owner
Review sessions	Security officer	CISO	System owners

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Elevation records	PAM tool; security engineering	Per elevation	3 years
Session recordings	PAM tool; security engineering	Continuous	12 months
Review notes	ISMS workspace; security officer	Monthly	3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Privileged access via PAM	≥ 98%	Remediate
Standing admin accounts	Minimised	Reduce
Sessions reviewed	≥ 5%	Increase

Auditor questions to prepare

- Show a PAM elevation and its recording.
- What standing privilege remains?
- Who administers PAM?

Frequent nonconformities

- PAM bypassed.
- Recordings not reviewed.

Interfaces: ISMS-IAM-PRIV-001, ISMS-IAM-URGENCE-001, ISMS-OPS-OUTILS-001, ISMS-OPS-SECRETS-001

ISMS-IAM-SERVICE-001 — Service, API and machine identities

Classification C2 · CONFIDENTIAL · Format PROCEDURE · Applicability Added

Objective

Govern non-human identities (service accounts, API keys, workloads) so that each has an owner, minimal rights and rotated credentials.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Identity and access management: technical and service accounts (chapter 4)
ISO/IEC 27001:2022	A.5.16 Identity management; A.5.17 Authentication information; A.8.2; A.8.5
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
SVC-01	Every service, API and machine identity shall be registered with owner, purpose, scope, expiry and credential type.	Register.
SVC-02	Credentials shall be stored in a vault and rotated at least every 90 days or on staff change.	Rotation records.
SVC-03	Interactive login with service accounts shall be blocked.	Policy.
SVC-04	Rights shall be least-privilege and reviewed semi-annually by the owner.	Reviews.
SVC-05	Unused identities (90 days) shall be disabled.	Dormancy report.
SVC-06	Workload identities (managed identity, certificates) shall be preferred over static secrets.	Architecture.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Register	Technical owners	IT manager	IAM owner
Rotate	Platform engineering	IT manager	Owners
Review	Owners	Department heads	IAM owner

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Identity register	IAM tool; IAM owner	Continuous	Life + 1 year
Rotation logs	Vault; platform engineering	Per rotation	12 months
Reviews	IAM tool; owners	Semi-annual	3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Identities with owner	100%	Assign
Credentials rotated on schedule	≥ 98%	Rotate
Static secrets in code	0	Incident

Auditor questions to prepare

- How many service accounts exist and who owns them?
- Show a rotation.
- How do you find unused identities?

Frequent nonconformities

- Orphan accounts.
- Secrets never rotated.

Interfaces: ISMS-IAM-CYCLE-001, ISMS-OPS-SECRETS-001, ISMS-DEV-RELEASE-001

ISMS-IAM-TIERS-001 — Third-party and supplier access control

Classification C2 · CONFIDENTIAL · Format PROCEDURE · Applicability Added

Objective

Grant suppliers and partners only limited, supervised and time-bound access to systems and data.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Identity and access management and supplier relationships: third-party access (chapters 4 and 6)
ISO/IEC 27001:2022	A.5.19 Supplier relationships; A.5.18 Access rights; A.8.2; A.8.20
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
TPA-01	Third-party access shall be requested by an internal sponsor, approved by the data owner and limited to defined systems and times.	Request and approval.
TPA-02	Access shall use individual accounts with MFA through controlled paths (bastion, VDI); shared supplier accounts shall be prohibited.	Account list.
TPA-03	All sessions shall be logged; privileged sessions recorded.	Logs.
TPA-04	Access shall be reviewed monthly and removed at contract end or change.	Review records.
TPA-05	Suppliers shall acknowledge security obligations before access.	Acknowledgements.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Request	Sponsor	Department head	IAM owner
Provision	IAM operations	IAM owner	Data owner
Review	Sponsor	Department head	IAM owner

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Third-party access list	IAM tool; IAM owner	Monthly	3 years
Session logs	Bastion/PAM; security engineering	Continuous	12 months
Acknowledgements	Supplier files; supplier manager	Per supplier	Contract + 3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Third-party accounts with sponsor	100%	Disable
Accounts beyond contract	0	Disable
Reviews monthly	100%	Escalate

Auditor questions to prepare

- Who at suppliers can access C3 systems?
- How do you see what they do?
- How do you end access?

Frequent nonconformities

- Shared accounts.

- No logging.

Interfaces: ISMS-FOU-POLITIQUE-001, ISMS-RH-TIERS-001, ISMS-IAM-DISTANT-001, ISMS-OPS-OUTILS-001

ISMS-IAM-DISTANT-001 — Remote access and interconnections

Classification C2 · CONFIDENTIAL · Format PROCEDURE · Applicability Added

Objective

Secure remote access and interconnections so that only authenticated, compliant users and approved partner links can reach internal resources.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Identity and access management and IT security: remote access and network interconnection (chapters 4 and 5)
ISO/IEC 27001:2022	A.8.20 Network security; A.8.5 Secure authentication; A.6.7 Remote working; A.5.14
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
RMT-01	Remote access shall require MFA and compliant managed devices; access shall be restricted to needed applications.	Policy and logs.
RMT-02	VPN/ZTNA configuration shall use strong crypto and be patched; legacy protocols shall be disabled.	Configuration and scans.
RMT-03	Site-to-site and partner links shall be documented, approved, filtered and reviewed semi-annually.	Link register.
RMT-04	Remote access logs shall be monitored for anomalies such as impossible travel.	Alerts.
RMT-05	Direct exposure of administrative interfaces (RDP, SSH) to the internet shall be prohibited.	Exposure scans.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Operate access	Network engineering	IT manager	CISO
Approve partner links	Service owner	IT manager	CISO
Monitor	SOC	CISO	Network engineering

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Remote access logs	VPN/ZTNA; network engineering	Continuous	12 months
Link register	CMDB; network engineering	Semi-annual	Life + 3 years
Exposure scans	Scanner; security engineering	Weekly	12 months

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Remote users with MFA	100%	Block
Exposed admin interfaces	0	Immediate
Links reviewed	100%	Escalate

Auditor questions to prepare

- How do remote users connect and how do you verify the device?
- List partner links.
- How do you detect misuse?

Frequent nonconformities

- MFA gaps.
- Undocumented links.

Interfaces: ISMS-OPS-RESEAU-001, ISMS-IAM-AUTH-001, ISMS-IAM-TIERS-001, ISMS-OPS-EXPO-001

ISMS-IAM-URGENCE-001 — Emergency break-glass access

Classification C3 · STRICTLY CONFIDENTIAL · Format PROCEDURE · Applicability Added

Objective

Provide sealed emergency access for loss of normal authentication, with maximum control and immediate review.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Identity and access management: emergency and break-glass access (chapter 4)
ISO/IEC 27001:2022	A.8.2 Privileged access rights; A.5.15 Access control; A.8.15 Logging
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
BRK-01	Break-glass accounts shall be few, named in a register, with credentials sealed in dual-control storage.	Register and seal check.
BRK-02	Use shall require incident or approval record and shall alert the CISO immediately.	Alert and ticket.
BRK-03	Credentials shall be changed after each use and tested quarterly.	Rotation and test.
BRK-04	All activity shall be recorded and reviewed within 24 hours.	Review record.
BRK-05	Accounts shall be excluded from conditional access only where unavoidable and monitored.	Policy exclusions.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Hold seals	Custodians (two)	CISO	IT manager
Use	Authorised engineer	IT manager	CISO
Review use	Security officer	CISO	Incident manager

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Break-glass register	IAM tool; IAM owner	Quarterly	3 years
Use records and reviews	Ticket and SIEM; security officer	Per use	3 years
Quarterly tests	IAM tool; engineering	Quarterly	3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Uses reviewed within 24h	100%	Incident
Credentials changed after use	100%	Immediate
Quarterly tests done	100%	Escalate

Auditor questions to prepare

- How many break-glass accounts exist and where are they?
- Show the last use.
- How are you alerted?

Frequent nonconformities

- Shared known passwords.

- No review of use.

Interfaces: ISMS-IAM-PRIV-001, ISMS-IAM-PRIV-002, ISMS-OPS-JOURNAUX-001

ISMS-IAM-FEDERATION-001 — Single sign-on, federation and SaaS access

Classification C1 · INTERNAL · Format PROCEDURE · Applicability Added

Objective

Control single sign-on, federation and SaaS access so that identity is centrally governed across cloud and partner applications.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Identity and access management: federated identity and SaaS access (chapter 4)
ISO/IEC 27001:2022	A.5.16 Identity management; A.5.23 Cloud services; A.8.5
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
SSO-01	Business applications shall use central SSO with MFA; local accounts shall be exceptions with approval.	Application list.
SSO-02	Federation trusts shall be registered, minimal and reviewed annually.	Trust register.
SSO-03	Provisioning and deprovisioning shall be automated (SCIM) where supported.	Configuration.
SSO-04	Application owners shall review roles semi-annually.	Reviews.
SSO-05	Tokens and session lifetimes shall follow policy.	Configuration.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Operate IdP	IAM engineering	IAM owner	CISO
Onboard apps	Service owners	IT manager	IAM owner
Review trusts	IAM owner	CISO	Service owners

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Application and trust register	IdP; IAM owner	Quarterly	Life + 1 year
Provisioning logs	IdP; IAM engineering	Continuous	12 months
Role reviews	IAM tool; owners	Semi-annual	3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Apps behind SSO	≥ 95%	Plan
Local accounts without approval	0	Remove
Trusts reviewed	100%	Escalate

Auditor questions to prepare

- Which applications do not use SSO and why?
- How are leavers removed from SaaS?
- Who approves a new federation?

Frequent nonconformities

- SaaS with local logins.
- Unreviewed trusts.

Interfaces: ISMS-IAM-AUTH-001, ISMS-IAM-CYCLE-001, ISMS-OPS-CLOUD-001

ISMS-OPS-ARCHI-001 — Security architecture and technical diagrams

Classification C3 · STRICTLY CONFIDENTIAL · Format REGISTER · Applicability Added

Objective

Maintain a secure, documented architecture and accurate technical diagrams that show trust boundaries, data flows and security controls.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	IT security: network and system architecture, security requirements in new systems (chapter 5)
ISO/IEC 27001:2022	A.8.27 Secure system architecture; A.8.20; A.8.22 Segregation of networks
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
ARC-01	Reference architecture principles (defence in depth, least privilege, zero trust, segmentation, secure defaults) shall be defined and applied to new designs.	Principles document.
ARC-02	Diagrams of network, systems, cloud, identity and data flows shall be maintained for in-scope services and updated within 30 days of change.	Diagrams with version.
ARC-03	Architecture reviews shall be performed for every new or significantly changed service handling C2/C3.	Review records.
ARC-04	Single points of failure and trust boundaries shall be identified and risks recorded.	Risk records.
ARC-05	Diagrams are C3 and shall be restricted to named persons.	Access list.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Define principles	Security architect	CISO	IT manager
Maintain diagrams	Service architects	IT manager	Security architect
Review designs	Security architect	CISO	Project managers

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Principles	Document system; architect	Annual	3 years
Diagrams	Document system; architects	On change	Life + 3 years
Review records	Project portal; architect	Per review	6 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Diagrams current	≥ 95%	Update
Designs reviewed	100%	Block go-live
Diagram access violations	0	Incident

Auditor questions to prepare

- Explain how a request moves from the internet to your C3 data.
- Show last review.
- Where are your single points of failure?

Frequent nonconformities

- Outdated diagrams.
- No review.

Interfaces: ISMS-OPS-RESEAU-001, ISMS-OPS-SEGMENT-001, ISMS-ACT-FLUX-001, ISMS-PRJ-SECURITE-001

ISMS-OPS-CMDB-001 — Systems and software configuration register

Classification C2 · CONFIDENTIAL · Format REGISTER · Applicability Added

Objective

Keep an accurate register of systems, software and configurations as the single source for operations and security.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	IT security and asset management: configuration and asset information (chapters 1 and 5)
ISO/IEC 27001:2022	A.8.9 Configuration management; A.5.9 Inventory of assets
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
CMD-01	The CMDB shall record systems, software, versions, owners, dependencies, location, classification and support status.	Export.
CMD-02	Discovery shall update it automatically and discrepancies shall be reconciled monthly.	Reconciliation.
CMD-03	Changes shall update the CMDB as part of change closure.	Change linkage.
CMD-04	Data quality shall be measured and improved.	Quality report.
CMD-05	Access to the CMDB shall be role-based and logged.	Sampled instances traced end to end to the record: CMDB export.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Maintain CMDB	CMDB owner	IT manager	Service owners
Reconcile	Security engineering	CISO	CMDB owner
Improve quality	CMDB owner	IT manager	ISMS manager

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
CMDB export	CMDB; CMDB owner	Monthly	3 years
Reconciliation	CMDB; engineering	Monthly	3 years
Quality report	CMDB; owner	Quarterly	3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
CI completeness	≥ 98%	Remediate
Reconciliation gaps open > 30 days	0	CISO
Changes with CMDB update	100%	Review

Auditor questions to prepare

- How do you keep the CMDB accurate?
- Show a CI and its dependencies.
- Who owns it?

Frequent nonconformities

- Stale CIs.

- No link to changes.

Interfaces: ISMS-ACT-INVENTAIRE-001, ISMS-OPS-CHANGES-001, ISMS-OPS-VULN-001

ISMS-OPS-EOL-001 — End-of-life technologies and exceptions

Classification C1 · INTERNAL · Format PROCEDURE · Applicability Added

Objective

Identify technologies reaching end of life or support and manage replacement or isolation before they become unsupported.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	IT security: technical vulnerability management and lifecycle (chapter 5)
ISO/IEC 27001:2022	A.8.8 Management of technical vulnerabilities; A.8.9; A.5.9
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
EOL-01	Support end dates shall be recorded for all in-scope software, firmware and hardware.	CMDB data.
EOL-02	A forward-looking EOL report shall show items ending within 12 months with a replacement plan.	Report.
EOL-03	Unsupported items shall be isolated, monitored and subject to time-limited exceptions.	Exceptions.
EOL-04	No unsupported system shall hold C3 information.	Scan.
EOL-05	Vendor extended support may be used only with documented approval and cost.	Approvals.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Track EOL	CMDB owner	IT manager	Service owners
Plan replacement	Service owners	IT manager	Architect
Approve exceptions	CISO	Top management	Service owners

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
EOL report	CMDB; CMDB owner	Quarterly	3 years
Exceptions	Exception register; CISO	Per exception	Life + 3 years
Replacement plans	Project portal; service owners	Per item	3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Unsupported systems with exception	100%	Isolate
Items ending within 12 months with plan	100%	Plan
Unsupported C3 systems	0	Immediate

Auditor questions to prepare

- Which systems are end of life?
- How are they protected?
- Show a replacement plan.

Frequent nonconformities

- EOL unknown.

- Exceptions indefinite.

Interfaces: ISMS-OPS-VULN-001, ISMS-OPS-CMDB-001, ISMS-ORG-DEROGATIONS-001

ISMS-OPS-ENDPOINT-001 — Endpoint and server security baseline

Classification C2 · CONFIDENTIAL · Format PROCEDURE · Applicability Added

Objective

Secure endpoints and servers with a consistent baseline for configuration, encryption, patching and protection.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	IT security: endpoint protection and user devices (chapter 5)
ISO/IEC 27001:2022	A.8.1 User endpoint devices; A.8.7; A.8.9; A.8.24
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
EPT-01	Endpoints and servers shall be built from managed images with full-disk encryption, secure boot and local firewall.	Image and compliance reports.
EPT-02	Only managed devices shall access C2/C3 resources (conditional access).	Policy.
EPT-03	Local admin rights shall be removed for standard users.	Rights report.
EPT-04	Patch compliance shall be at least 95% within 14 days for critical.	Patch report.
EPT-05	Screen lock within 5 minutes and removable media control shall be enforced.	Policy export.
EPT-06	EDR shall run on all devices (ISMS-OPS-MALWARE-001).	Sampled instances traced end to end to the record: Compliance report.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Define baseline	Endpoint engineering	IT manager	CISO
Operate	IT operations	IT manager	Security
Measure	Security engineering	CISO	IT operations

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Compliance report	MDM / management console; engineering	Monthly	12 months
Image versions	Repository; engineering	On change	3 years
Admin rights report	IAM tool; engineering	Quarterly	3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Devices compliant	≥ 97%	Block
Encrypted devices	100%	Block
Users with local admin	< 2%	Review

Auditor questions to prepare

- How do you know laptops are encrypted?
- What happens to a non-compliant device?
- Show patch status.

Frequent nonconformities

- Unmanaged devices.
- Local admin widespread.

Interfaces: ISMS-OPS-MALWARE-001, ISMS-OPS-VULN-001, ISMS-RH-MOBILE-001, ISMS-OPS-DURCISSEMENT-001

ISMS-OPS-EMAIL-001 — Messaging and collaboration protection

Classification C1 · INTERNAL · Format PROCEDURE · Applicability Added

Objective

Protect email and collaboration tools from phishing, malware, data leakage and account takeover.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	IT security: messaging and collaboration security (chapter 5)
ISO/IEC 27001:2022	A.5.14 Information transfer; A.8.23 Web filtering; A.8.7; A.8.12 Data leakage prevention
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
EML-01	SPF, DKIM and DMARC shall be enforced with policy reject or quarantine for owned domains.	DNS records and reports.
EML-02	Inbound filtering shall include anti-phishing, malware and URL rewriting with sandboxing.	Gateway settings.
EML-03	External sharing and guest access in collaboration tools shall be restricted by classification and approved.	Tenant settings.
EML-04	Mail encryption shall be available and used for C2/C3 externally.	Encryption policy.
EML-05	Auto-forwarding to external addresses shall be blocked.	Configuration.
EML-06	Users shall be able to report phishing with one click and responses shall be tracked.	Reports.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Operate gateway	Messaging engineering	IT manager	CISO
Review sharing	ISMS manager	CISO	Owners
Handle reports	SOC	CISO	Users

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
DMARC reports	Mail platform; engineering	Monthly	12 months
Tenant configuration baseline	Admin console; engineering	Quarterly	3 years
Phish reports	SOC; SOC	Per report	12 months

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
DMARC policy enforced	100% domains	Fix
Phish reports handled in 4 hours	≥ 95%	Review
External sharing exceptions	Reviewed quarterly	Review

Auditor questions to prepare

- Show DMARC status.
- How do you stop auto-forwarding?
- How are phishing reports handled?

Frequent nonconformities

- DMARC none.
- Open guest sharing.

Interfaces: ISMS-OPS-MALWARE-001, ISMS-OPS-DLP-001, ISMS-RH-SENSIBILISATION-001

ISMS-OPS-EXPO-001 — Internet-facing service security

Classification C2 · CONFIDENTIAL · Format PROCEDURE · Applicability Added

Objective

Control and monitor all services exposed to the internet, so that the attack surface is known, minimal and hardened.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	IT security: network services and external exposure (chapter 5)
ISO/IEC 27001:2022	A.8.20; A.8.21 Security of network services; A.8.8; A.8.26
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
EXP-01	An inventory of internet-facing services, domains, IPs and certificates shall exist and be validated by external discovery at least monthly.	Inventory and scan.
EXP-02	Each exposed service shall have owner, business need, WAF or filtering where applicable and hardened configuration.	Configuration reviews.
EXP-03	Administrative interfaces shall not be internet-facing; access shall be via VPN or ZTNA.	Scan.
EXP-04	Exposed services shall be scanned weekly and tested annually by penetration test.	Reports.
EXP-05	Unknown services shall be investigated within 5 days.	Tickets.
EXP-06	Subdomain takeover and DNS hygiene shall be monitored.	Monitoring.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Maintain inventory	Security engineering	CISO	Service owners
Harden	Service owners	IT manager	Security
Monitor	SOC	CISO	Engineering

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
External inventory	Discovery tool; engineering	Monthly	12 months
Scan reports	Scanner; engineering	Weekly	12 months
Pen test	Document system; CISO	Annual	6 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Exposed services with owner	100%	Assign
Critical exposed findings	0 open > 72h	CISO
Unknown services found	Tracked	Investigate

Auditor questions to prepare

- How do you know all your internet exposure?
- Show an unknown service you found.
- Where are admin interfaces?

Frequent nonconformities

- Shadow services.

- Admin consoles exposed.

Interfaces: ISMS-OPS-RESEAU-001, ISMS-OPS-VULN-001, ISMS-OPS-PENTEST-001

ISMS-OPS-SEGMENT-001 — Network segmentation and firewall rule register

Classification C3 · STRICTLY CONFIDENTIAL · Format REGISTER · Applicability Added

Objective

Maintain the register of network segments and firewall rules so that segmentation matches design and is verified.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	IT security: network segregation and filtering (chapter 5)
ISO/IEC 27001:2022	A.8.22 Segregation of networks; A.8.20; A.8.9
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
SEG-01	A segment register shall list zones, purposes, owners, classification allowed and connected zones.	Register.
SEG-02	Every rule between zones shall have business justification, owner, request ID, creation and review dates.	Rule base export.
SEG-03	Rules shall be reviewed semi-annually and unused rules removed after 90 days of no hits.	Review records.
SEG-04	Segmentation shall be tested by technical tests at least annually.	Test report.
SEG-05	Changes shall follow change management.	Tickets.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Maintain register	Network engineering	IT manager	Security architect
Review rules	Rule owners	IT manager	CISO
Test segmentation	Security engineering	CISO	Network

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Segment register	CMDB; network engineering	On change	Life + 3 years
Rule reviews	Firewall manager; owners	Semi-annual	3 years
Segmentation tests	Document system; security engineering	Annual	6 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Rules with owner and review date	100%	Review
Any-any rules	0	Immediate
Segmentation tested	100% critical zones	Test

Auditor questions to prepare

- Show rules between user and C3 zones.
- When was it last tested?
- Who owns this rule?

Frequent nonconformities

- Rules without owner.

- Flat zones.

Interfaces: ISMS-OPS-RESEAU-001, ISMS-OPS-CHANGES-001, ISMS-OT-ZONES-001

ISMS-OPS-WIFI-001 — Wi-Fi and guest network security

Classification C1 · INTERNAL · Format PROCEDURE · Applicability Added

Objective

Secure wireless networks and guest access so they cannot be used to reach protected systems.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	IT security: wireless and guest network security (chapter 5)
ISO/IEC 27001:2022	A.8.20; A.8.22; A.7.2
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
WIF-01	Corporate Wi-Fi shall use WPA3-Enterprise or 802.1X with certificates; pre-shared keys are not allowed for staff access.	Controller configuration.
WIF-02	Guest Wi-Fi shall be isolated from internal networks, rate-limited, logged and time-limited.	Segmentation test.
WIF-03	Rogue access points shall be detected and removed.	Detection reports.
WIF-04	Wireless infrastructure shall be patched and managed from a secure network.	Compliance.
WIF-05	Access in restricted zones shall be limited or disabled.	Sampled instances traced end to end to the record: Controller config.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Operate Wi-Fi	Network engineering	IT manager	CISO
Monitor rogue APs	Security engineering	CISO	Network
Review guest access	ISMS reviewer	CISO	Facility

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Controller config	Controller; network engineering	Quarterly	3 years
Rogue AP reports	WIPS; security engineering	Weekly	12 months
Guest logs	Controller; network engineering	Continuous	6 months

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Corporate SSIDs on 802.1X	100%	Fix
Guest isolation test passed	Yes	Fix
Rogue APs open > 7 days	0	Remove

Auditor questions to prepare

- How is guest Wi-Fi separated?
- How do you detect rogue access points?
- Which Wi-Fi is allowed in the server area?

Frequent nonconformities

- PSK shared by staff.
- Guest not isolated.

Interfaces: ISMS-OPS-RESEAU-001, ISMS-OPS-SEGMENT-001, ISMS-PHY-ZONES-001

ISMS-OPS-SIEM-001 — Security detection and SOC use cases

Classification C2 · CONFIDENTIAL · Format PROCEDURE · Applicability Added

Objective

Detect and respond to security events through defined use cases, monitored sources and a documented response process.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	IT security: event monitoring and detection (chapter 5); incident reporting (chapter 1)
ISO/IEC 27001:2022	A.8.16 Monitoring activities; A.8.15 Logging; A.5.25 Assessment of events
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
SOC-01	Detection use cases shall be defined for identity abuse, malware, data exfiltration, privilege misuse, network anomalies and C3 access, mapped to threats and to MITRE ATT&CK.	Use-case catalogue.
SOC-02	Use cases shall be tested at least annually (purple team or simulation).	Test records.
SOC-03	Alerts shall be triaged within defined times; high severity within 30 minutes during operating hours and via on-call outside.	Alert metrics.
SOC-04	Coverage of log sources shall be reviewed quarterly (ISMS-OPS-JOURNAUX-001).	Review.
SOC-05	If SOC services are outsourced, the provider shall be under contract with SLAs and regular reporting.	Contract and reports.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Maintain use cases	Detection engineer	CISO	SOC
Triage alerts	SOC analysts	SOC lead	Service owners
Test detections	Security engineering	CISO	SOC

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Use-case catalogue	SIEM; detection engineer	Quarterly	3 years
Alert records	SIEM/ticket; SOC	Per alert	12 months
Detection tests	ISMS workspace; engineering	Annual	3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
High alerts triaged in 30 min	≥ 95%	Review
Use cases tested annually	100%	Plan
False-positive rate	Tracked	Tune

Auditor questions to prepare

- Show a detection from alert to response.
- How do you test rules?
- Who watches at night?

Frequent nonconformities

- No tests.
- No 24/7 coverage plan.

Interfaces: ISMS-OPS-JOURNAUX-001, ISMS-INC-PROC-001, ISMS-ORG-MENACES-001

ISMS-OPS-TEMPS-001 — Clock synchronization and forensic time quality

Classification C1 · INTERNAL · Format PROCEDURE · Applicability Added

Objective

Keep system clocks synchronised and traceable so that logs and evidence can be correlated and relied on.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	IT security: clock synchronisation for logging (chapter 5)
ISO/IEC 27001:2022	A.8.17 Clock synchronisation; A.8.15; A.5.28
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
NTP-01	All in-scope systems shall synchronise to approved internal time sources that follow at least two reliable external references.	Configuration.
NTP-02	Maximum drift shall be 1 second; deviations shall alert.	Monitoring.
NTP-03	Time source changes shall be controlled changes.	Tickets.
NTP-04	Time zone convention (UTC for logs) shall be defined.	Standard.
NTP-05	Time sources shall be secured (authenticated NTP where possible).	Sampled instances traced end to end to the record: Time configuration.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Operate time service	Infrastructure engineering	IT manager	Security
Monitor drift	Security engineering	CISO	Infrastructure
Review	ISMS reviewer	CISO	IT

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Time configuration	Config repository; infrastructure	Quarterly	3 years
Drift reports	Monitoring; security engineering	Weekly	12 months
Change records	ITSM; IT operations	Per change	3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Systems synchronised	≥ 99%	Fix
Drift over 1s	0	24h fix
Time sources documented	100%	Document

Auditor questions to prepare

- How do you ensure logs have trustworthy time?
- Show drift monitoring.
- Which sources do you use?

Frequent nonconformities

- Different time zones.
- No monitoring.

Interfaces: ISMS-OPS-JOURNAUX-001, ISMS-INC-PRESERVATION-001

ISMS-OPS-RESTORE-001 — Detailed restoration operating procedures

Classification C2 · CONFIDENTIAL · Format PROCEDURE · Applicability Added

Objective

Define and exercise the detailed procedures to restore data and systems from backups within objectives.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	IT security and continuity: restoration of data and systems (chapters 3 and 5)
ISO/IEC 27001:2022	A.8.13 Information backup; A.5.30 ICT readiness; A.8.14
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
RST-01	Restore runbooks shall exist per critical service, with prerequisites, steps, verification and owner.	Runbooks.
RST-02	Restore tests shall be performed at least quarterly for critical services and include file, database and full-system restores.	Test reports.
RST-03	Restore time and data loss shall be measured against RTO/RPO.	Metrics.
RST-04	Restores shall be verified for integrity and application consistency.	Verification.
RST-05	Restore from immutable copies shall be tested at least annually.	Test.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Maintain runbooks	Service owners	IT manager	Backup administrator
Execute tests	Backup administrator	IT manager	Service owners
Report	BCM manager	CISO	Top management

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Runbooks	Document system; service owners	Annual	3 years
Test reports	ITSM; administrator	Quarterly	3 years
Metrics	Backup tool; administrator	Per test	3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Critical services tested in quarter	100%	Test
Restore within RTO	≥ 90%	Redesign
Failed restores	0	Action

Auditor questions to prepare

- Restore this server now and show timing.
- What was the last failure?
- How do you test immutable backups?

Frequent nonconformities

- Never restored.
- Runbook outdated.

Interfaces: ISMS-OPS-SAUVEGARDE-001, ISMS-OPS-BACKUP-002, ISMS-PRA-PRA-001, ISMS-PRA-TESTS-001

ISMS-OPS-BACKUP-002 — Tamper-resistant and isolated backups

Classification C2 · CONFIDENTIAL · Format PROCEDURE · Applicability Added

Objective

Make backups resilient to ransomware and insider threat through isolation, immutability and separate credentials.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	IT security and continuity: protection of backups (chapters 3 and 5)
ISO/IEC 27001:2022	A.8.13; A.8.14; A.8.24; A.5.30
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
IMB-01	At least one backup copy shall be immutable or offline with retention lock for the defined period.	Configuration.
IMB-02	Backup infrastructure shall be separated from production domain with dedicated admin accounts and MFA.	Account lists.
IMB-03	Backups shall be encrypted with keys held outside the backup platform.	Key location.
IMB-04	Backup deletion shall require dual approval and have a time delay.	Policy.
IMB-05	Backups shall be scanned for malware before restore where feasible.	Scan records.
IMB-06	Isolation shall be tested annually by simulation.	Sampled instances traced end to end to the record: Immutability configuration.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Design backups	Backup architect	IT manager	CISO
Operate	Backup administrator	IT manager	Security
Test isolation	Security engineering	CISO	Administrator

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Immutability configuration	Backup tool; administrator	Quarterly	3 years
Isolation test	ISMS workspace; engineering	Annual	3 years
Admin account list	IAM tool; IAM owner	Quarterly	3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Critical data with immutable copy	100%	Fix
Backup admin MFA	100%	Fix
Isolation test passed	Yes	Fix

Auditor questions to prepare

- Could an attacker with domain admin delete your backups?
- Show immutable settings.
- Where are keys?

Frequent nonconformities

- Backups on domain.
- Deletion by one admin.

Interfaces: ISMS-OPS-SAUVEGARDE-001, ISMS-OPS-RESTORE-001, ISMS-IAM-PRIV-001

ISMS-OPS-SECRETS-001 — Secrets vault and key rotation

Classification C3 · STRICTLY CONFIDENTIAL · Format PROCEDURE · Applicability Added

Objective

Store, distribute and rotate secrets, keys and credentials in a vault with strict access and audit trail.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	IT security: management of secret authentication information and cryptographic keys (chapters 4 and 5)
ISO/IEC 27001:2022	A.5.17 Authentication information; A.8.24; A.8.4 Access to source code
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
SEC-01	Secrets (passwords, API keys, tokens, certificates, private keys) shall be held only in approved vaults or HSMs.	Vault inventory.
SEC-02	Secrets shall be rotated on schedule and on suspicion, with automated rotation where supported.	Rotation logs.
SEC-03	Access to the vault shall be role-based, MFA protected, and logged.	Logs.
SEC-04	Secret scanning shall run on repositories, pipelines, chat and tickets; findings shall be remediated within 24 hours.	Scan reports.
SEC-05	Vault recovery and key custody shall be tested annually.	Test.
SEC-06	Emergency access to the vault shall follow ISMS-IAM-URGENCE-001.	Sampled instances traced end to end to the record: Vault inventory.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Operate vault	Platform security	IT manager	CISO
Rotate	System owners	IT manager	Platform security
Scan	Security engineering	CISO	Developers

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Vault inventory	Vault; platform security	Quarterly	3 years
Rotation logs	Vault; platform security	Continuous	12 months
Secret scan results	Scanner; security engineering	Per scan	12 months

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Secrets in vault	≥ 98%	Migrate
Exposed secrets fixed in 24h	100%	Incident
Rotation on schedule	≥ 95%	Fix

Auditor questions to prepare

- Where are your secrets stored?
- Show a rotation.
- What if a secret appears in code?

Frequent nonconformities

- Secrets in spreadsheets.
- Rotation manual and late.

Interfaces: ISMS-IAM-AUTH-001, ISMS-IAM-SERVICE-001, ISMS-CRY-POLITIQUE-001, ISMS-DEV-RELEASE-001

ISMS-OPS-CONFIG-001 — Continuous configuration compliance

Classification C2 · CONFIDENTIAL · Format PROCEDURE · Applicability Added

Objective

Continuously verify that systems keep their approved configuration and remediate drift.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	IT security: configuration management and compliance monitoring (chapter 5)
ISO/IEC 27001:2022	A.8.9 Configuration management; A.8.32 Change management; A.8.16
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
CFG-01	Approved configuration baselines shall be machine-readable and enforced through code or compliance tooling.	Baseline repository.
CFG-02	Compliance shall be measured at least weekly for critical systems and monthly otherwise.	Reports.
CFG-03	Drift shall create tickets and be remediated by priority (critical in 7 days).	Tickets.
CFG-04	Changes shall be reconciled with change tickets; untracked changes shall be investigated.	Reconciliation.
CFG-05	Reports shall go to service owners and the CISO monthly.	Sampled instances traced end to end to the record: Compliance reports.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Maintain baselines	Platform engineering	IT manager	Security architect
Monitor	Security engineering	CISO	Platform
Remediate	System admins	Service owners	Security

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Compliance reports	Compliance tool; security engineering	Weekly / monthly	12 months
Drift tickets	ITSM; admins	Per drift	3 years
Reconciliation	ITSM; change manager	Monthly	3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Compliance rate	≥ 95%	Plan
Critical drift open > 7 days	0	CISO
Untracked changes	0	Investigate

Auditor questions to prepare

- Show drift detection and remediation.
- How are untracked changes found?
- Who receives reports?

Frequent nonconformities

- Manual checks.

- No drift tickets.

Interfaces: ISMS-OPS-DURCISSEMENT-001, ISMS-OPS-CHANGES-001, ISMS-OPS-CMDB-001

ISMS-OPS-PENTEST-001 — Penetration testing programme

Classification C2 · CONFIDENTIAL · Format STANDARD · Applicability Added

Objective

Test the resilience of systems and applications through independent, authorised penetration tests and track findings to closure.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	IT security: technical review and testing of IT systems (chapter 5)
ISO/IEC 27001:2022	A.8.8; A.8.29 Security testing in development and acceptance; A.8.34 Protection during audit testing; A.5.35
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
PEN-01	A test programme shall cover external, internal, web and mobile applications, cloud and critical APIs annually and after major change.	Programme.
PEN-02	Tests shall be performed by qualified independent testers under written rules of engagement, scope and approval.	Contract and RoE.
PEN-03	Reports shall rate findings by risk and be delivered to the CISO; critical issues shall be reported immediately.	Reports.
PEN-04	Findings shall be remediated per ISMS-OPS-VULN-001 deadlines and retested.	Retest evidence.
PEN-05	Testing of OT, production prototypes or customer systems shall need customer or plant approval.	Approvals.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Plan tests	CISO	Top management	Service owners
Perform tests	External testers	CISO	Service owners
Remediate	Service owners	IT manager	Security

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Programme	ISMS workspace; CISO	Annual	3 years
Reports	Document system; CISO	Per test	6 years
Retest evidence	ITSM; security engineering	Per finding	3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Planned tests done	100%	Escalate
Critical findings fixed within deadline	100%	Top management
Retested findings	100%	Retest

Auditor questions to prepare

- Show your last penetration test and how you closed findings.
- Who tested and how were they selected?
- How do you test C3 systems safely?

Frequent nonconformities

- No retest.
- Scope too narrow.

Interfaces: ISMS-OPS-VULN-001, ISMS-OPS-EXPO-001, ISMS-DEV-TESTS-001

ISMS-OPS-OUTILS-001 — Administrative tooling and remote maintenance security

Classification C2 · CONFIDENTIAL · Format PROCEDURE · Applicability Added

Objective

Secure administrative tools and remote maintenance channels, which provide privileged reach into systems.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	IT security and supplier relationships: administration tools and maintenance access (chapters 4, 5 and 6)
ISO/IEC 27001:2022	A.8.18 Use of privileged utility programs; A.8.2; A.5.19; A.8.20
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
ADM-01	Administration tools shall be inventoried, approved, patched and accessible only from hardened admin workstations or bastions.	Tool inventory.
ADM-02	Remote maintenance by vendors shall be enabled per session, supervised, recorded and ended afterwards.	Session records.
ADM-03	Permanent vendor remote tools shall not be installed on C3 systems.	Scan.
ADM-04	Use of unauthorised remote-control software shall be detected and blocked.	EDR/network detection.
ADM-05	Tool credentials shall be vaulted.	Vault.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Approve tools	Security architect	CISO	IT manager
Operate bastions	Platform security	IT manager	CISO
Supervise vendors	Service owners	IT manager	Security

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Tool inventory	CMDB; platform security	Quarterly	3 years
Vendor session records	Bastion/PAM; platform security	Per session	12 months
Detections	EDR; SOC	Per alert	12 months

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Admin tools inventoried	100%	Add
Vendor sessions recorded	100%	Incident
Unauthorised tools found	0	Remove

Auditor questions to prepare

- How do vendors perform remote maintenance?
- Show a recorded session.
- Which admin tools exist?

Frequent nonconformities

- Permanent remote tool.

- No recording.

Interfaces: ISMS-IAM-PRIV-002, ISMS-IAM-TIERS-001, ISMS-OT-ACCES-001

ISMS-OPS-DLP-001 — Data loss prevention and external sharing

Classification C1 · INTERNAL · Format PROCEDURE · Applicability Added

Objective

Prevent unauthorised leakage of C2/C3 information through email, web, endpoints, cloud sharing and removable media.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	IT security: protection against data leakage and information transfer (chapter 5)
ISO/IEC 27001:2022	A.8.12 Data leakage prevention; A.5.14; A.5.12; A.8.23
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
DLP-01	DLP policies shall be based on classification labels and sensitive patterns, covering email, endpoints, web uploads and cloud sharing.	Policy export.
DLP-02	Policies shall run first in monitor mode, then enforcement for C3 and high-confidence C2.	Mode records.
DLP-03	Alerts shall be triaged within 1 working day and incidents handled per procedure.	Alert tickets.
DLP-04	Exceptions shall be approved, time-limited and logged.	Exceptions.
DLP-05	Effectiveness shall be tested quarterly with test data.	Test results.
DLP-06	Employee monitoring shall respect works council and law agreements.	Agreement.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Design policies	Security engineering	CISO	DPO; works council
Triage	SOC	CISO	Data owners
Test	Security engineering	CISO	SOC

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
DLP policies	DLP console; security engineering	Quarterly	3 years
Alert records	DLP/ticket; SOC	Per alert	12 months
Test results	ISMS workspace; engineering	Quarterly	3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
C3 channels covered	100%	Extend
Alerts triaged in 1 day	≥ 95%	Review
Tests detected	≥ 95%	Tune

Auditor questions to prepare

- How do you stop a C3 file leaving by email?
- Show a DLP alert.
- How do you test DLP?

Frequent nonconformities

- Policy monitor-only forever.
- No testing.

Interfaces: ISMS-ACT-CLASSIF-001, ISMS-ACT-TRANSFERT-001, ISMS-OPS-EMAIL-001

ISMS-OPS-SUPPRESSION-001 — Secure logical data and system erasure

Classification C1 · INTERNAL · Format PROCEDURE · Applicability Added

Objective

Erase data and systems logically and securely so that information cannot be recovered after retirement, reuse or retention expiry.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Physical security and IT security: secure erasure and disposal (chapters 3 and 5)
ISO/IEC 27001:2022	A.8.10 Information deletion; A.7.14 Secure disposal; A.5.33
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
ERA-01	Erasure methods shall be defined per medium (cryptographic erase, overwrite per NIST SP 800-88, physical destruction for failed media) and per classification.	Standard.
ERA-02	Erasure shall be verified and certified for each device, cloud tenant, and virtual storage.	Certificates.
ERA-03	Cloud data deletion at exit shall be confirmed by the provider in writing.	Provider confirmation.
ERA-04	Backups containing deleted data shall expire within the defined period.	Retention records.
ERA-05	Records of erasure shall be retained 6 years.	Sampled instances traced end to end to the record: Erasure certificates.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Define standard	Security architect	CISO	IT
Erase	IT operations	IT manager	ISMS manager
Verify	ISMS reviewer	CISO	IT

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Erasure certificates	ITSM; IT operations	Per event	6 years
Provider confirmations	Supplier files; supplier manager	Per exit	6 years
Verification samples	ISMS workspace; reviewer	Quarterly	3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Retired devices with certificate	100%	Hold device
Cloud exits confirmed	100%	Request
Samples verified	100%	Re-erase

Auditor questions to prepare

- How do you erase a server disk?
- Show a certificate.
- How do you confirm cloud deletion?

Frequent nonconformities

- No verification.

- Provider unconfirmed.

Interfaces: ISMS-PHY-SUPPORTS-001, ISMS-ACT-CONSERVATION-001, ISMS-FOU-SORTIE-001

ISMS-OPS-CLOUD-002 — Cloud posture review and service exit

Classification C2 · CONFIDENTIAL · Format PROCEDURE · Applicability Added

Objective

Review cloud posture and service exits periodically to keep cloud risk understood and reversible.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	IT security and supplier relationships: cloud service review and exit (chapters 5 and 6)
ISO/IEC 27001:2022	A.5.23 Cloud services; A.5.22 Monitoring and review of supplier services; A.5.30
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
CPR-01	Each cloud service shall be reviewed at least annually for posture, provider assurance, location, subprocessors and incidents.	Review record.
CPR-02	Exit plans shall define data export formats, timelines, deletion confirmation and alternatives.	Exit plan.
CPR-03	Exit plans for critical services shall be tested or walked through every 2 years.	Test record.
CPR-04	Provider changes in terms or region shall be assessed within 30 days.	Assessment.
CPR-05	Concentration risk shall be evaluated.	Sampled instances traced end to end to the record: Cloud reviews.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Review cloud services	Cloud owner	IT manager	CISO
Plan exit	Service owners	IT manager	Procurement
Test exit	Service owners	IT manager	ISMS manager

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Cloud reviews	Supplier files; cloud owner	Annual	3 years
Exit plans	Document system; service owners	Annual	Life + 3 years
Exit tests	ISMS workspace; owners	Biennial	3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Cloud reviews in 12 months	100%	Overdue
Exit plans for critical services	100%	Create
Provider changes assessed in 30 days	100%	Escalate

Auditor questions to prepare

- How would you leave this provider?
- Show your latest review.
- What if the provider fails?

Frequent nonconformities

- No exit plan.

- Reviews skipped.

Interfaces: ISMS-OPS-CLOUD-001, ISMS-FOU-SORTIE-001, ISMS-FOU-SUIVI-001

ISMS-DEV-RELEASE-001 — Secure releases and CI/CD

Classification C1 · INTERNAL · Format PROCEDURE · Applicability Added

Objective

Release software through a controlled, secure and traceable pipeline with approvals and integrity guarantees.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	IT security: secure development, release and deployment (chapter 5)
ISO/IEC 27001:2022	A.8.32 Change management; A.8.25; A.8.28; A.8.31
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
REL-01	Releases shall be built from version-controlled source by a controlled CI/CD pipeline; manual production builds are prohibited.	Pipeline configuration.
REL-02	Pipeline definitions and secrets shall be protected, with restricted access and logging.	Access list.
REL-03	Artefacts shall be signed and stored in a protected registry; deployment shall verify signatures.	Signature checks.
REL-04	Production deployment shall require approval by someone other than the author and pass automated security gates.	Approvals.
REL-05	Rollback shall be tested.	Test.
REL-06	Release records shall link to changes.	Sampled instances traced end to end to the record: Release records.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Operate pipeline	Platform engineering	Engineering manager	CISO
Approve release	Release manager	Service owner	Security
Review pipeline security	Security engineering	CISO	Platform

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Release records	CI/CD; release manager	Per release	3 years
Approvals	CI/CD; release manager	Per release	3 years
Pipeline access review	IAM tool; platform	Quarterly	3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Releases through pipeline	100%	Incident
Releases with independent approval	100%	Review
Unsigned artefacts deployed	0	Block

Auditor questions to prepare

- Walk me from commit to production.
- Who can change the pipeline?
- How do you roll back?

Frequent nonconformities

- Manual hotfixes.

- Author approves own release.

Interfaces: ISMS-DEV-SDLC-001, ISMS-DEV-TESTS-001, ISMS-OPS-CHANGES-001, ISMS-OPS-SECRETS-001

ISMS-DEV-TESTS-001 — Application security verification

Classification C2 · CONFIDENTIAL · Format PROCEDURE · Applicability Added

Objective

Verify application security by testing during development and before release, and track defects to closure.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	IT security: security testing in development and acceptance (chapter 5)
ISO/IEC 27001:2022	A.8.29 Security testing; A.8.28 Secure coding; A.8.33 Test information
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
AVT-01	A test strategy shall define SAST, SCA, DAST, secret scanning and manual review by risk and technology.	Strategy.
AVT-02	Security tests shall run in pipeline on each merge or release; high severity findings shall block release unless an exception is approved.	Pipeline results.
AVT-03	Authorisation, input validation, session handling and API access controls shall be tested for apps handling C2/C3.	Test cases.
AVT-04	Production data shall not be used for testing without masking.	Data controls.
AVT-05	Findings shall be tracked to closure with deadlines in line with ISMS-OPS-VULN-001.	Tickets.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Define strategy	Security architect	CISO	Engineering manager
Run tests	Developers / security	Engineering manager	Security
Triage	Security engineering	CISO	Developers

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Test results	CI/CD; engineering	Per build	12 months
Findings	Tracker; security engineering	Per finding	3 years
Exceptions	Exception register; CISO	Per exception	Life + 3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Releases with passed gates	100%	Block
High findings open > 14 days	0	CISO
Test coverage of critical apps	100%	Extend

Auditor questions to prepare

- What do you test before release?
- Show a blocked release.
- How do you test authorisation?

Frequent nonconformities

- Gates not enforced.
- Findings left open.

Interfaces: ISMS-DEV-SDLC-001, ISMS-DEV-RELEASE-001, ISMS-OPS-PENTEST-001

ISMS-DEV-EXTERNE-001 — Third-party software and solution acquisition

Classification C1 · INTERNAL · Format PROCEDURE · Applicability Added

Objective

Acquire and integrate third-party software and external development safely, with security requirements, assurance and ongoing supply-chain management.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	IT security and supplier relationships: outsourced development and acquisition (chapters 5 and 6)
ISO/IEC 27001:2022	A.8.30 Outsourced development; A.5.21 ICT supply chain; A.8.25
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
ACQ-01	Security requirements shall be included in tender documents and contracts, including secure development, vulnerability handling and code access.	Contract clauses.
ACQ-02	Suppliers shall provide evidence of secure development, tests and SBOM before acceptance.	Evidence.
ACQ-03	Acceptance tests (security and functional) shall be performed before go-live.	Acceptance record.
ACQ-04	Source code escrow or access shall be considered for critical software.	Decision.
ACQ-05	Updates shall follow patch management and supplier vulnerability notifications shall be tracked.	Notification log.
ACQ-06	Licences and open-source obligations shall be verified.	Sampled instances traced end to end to the record: Requirements in contracts.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Define requirements	Security architect	CISO	Procurement
Assess supplier	Supplier manager	CISO	Service owner
Accept software	Service owner	IT manager	Security

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Requirements in contracts	Contract system; procurement	Per contract	Contract + 10 years
Evidence and SBOM	Supplier files; supplier manager	Per release	Product life + 3 years
Acceptance records	Project portal; service owner	Per delivery	6 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Software acquisitions with security clauses	100%	Block
Suppliers with SBOM	≥ 90%	Request
Acceptance tests done	100%	Block

Auditor questions to prepare

- How do you assure software you buy?
- Show security clauses.

- How do you learn of supplier vulnerabilities?

Frequent nonconformities

- No acceptance test.
- No SBOM.

Interfaces: ISMS-DEV-SDLC-001, ISMS-FOU-POLITIQUE-001, ISMS-FOU-EVALUATION-001

ISMS-FOU-REGISTRE-001 — Supplier register and criticality

Classification C2 · CONFIDENTIAL · Format REGISTER · Applicability Added

Objective

Maintain a complete register of suppliers with criticality, data access and assurance status as the foundation of supplier management.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Supplier relationships: inventory and classification of suppliers (chapter 6)
ISO/IEC 27001:2022	A.5.19; A.5.21 ICT supply chain; A.5.9
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
SRG-01	Every supplier with access to C2/C3 information, systems or premises shall be registered with contact, service, data classes, locations, subcontractors and contract dates.	Register.
SRG-02	Criticality tier shall be assigned by documented criteria and reviewed annually.	Tier criteria and reviews.
SRG-03	Procurement shall not onboard a supplier without register entry.	Procurement gate.
SRG-04	The register shall be reconciled with accounts payable and IAM third-party accounts semi-annually.	Reconciliation.
SRG-05	Changes (merger, subcontractor, location) shall update the register within 30 days.	Sampled instances traced end to end to the record: Supplier register.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Maintain register	Procurement	Procurement manager	Supplier manager
Tier suppliers	Supplier manager	CISO	Service owners
Reconcile	ISMS reviewer	CISO	Finance; IAM

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Supplier register	Procurement system; procurement	Continuous	Contract + 6 years
Tier reviews	Supplier files; supplier manager	Annual	3 years
Reconciliation	ISMS workspace; reviewer	Semi-annual	3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Suppliers with tier and owner	100%	Assign
Reconciliation gaps	0	Resolve in 30 days
Tier reviews in 12 months	100%	Escalate

Auditor questions to prepare

- Show your critical suppliers and why they are critical.
- How do you know the register is complete?
- What changed this year?

Frequent nonconformities

- Register incomplete.
- No tier criteria.

Interfaces: ISMS-FOU-POLITIQUE-001, ISMS-FOU-EVALUATION-001, ISMS-IAM-TIERS-001

ISMS-FOU-EVALUATION-001 — Supplier security due diligence

Classification C1 · INTERNAL · Format PROCEDURE · Applicability Added

Objective

Perform proportionate due diligence on suppliers before contract to understand and treat security risk.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Supplier relationships: selection and assessment (chapter 6)
ISO/IEC 27001:2022	A.5.19; A.5.21; A.5.22
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
SDD-01	Due diligence shall be performed before contract signature, proportionate to tier, using questionnaire, certificates, TISAX labels, reports and, for high tier, audits.	Due-diligence file.
SDD-02	Findings shall be rated and treated by corrective plan or risk acceptance before data is shared.	Plans and acceptances.
SDD-03	TISAX label scope, level and validity shall be checked on the ENX platform when the supplier claims it.	Label check.
SDD-04	Financial and geopolitical risks shall be considered for critical suppliers.	Assessment.
SDD-05	Results shall be reviewed by CISO for high tier.	Sampled instances traced end to end to the record: Due-diligence files.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Assess supplier	Supplier manager	Procurement manager	CISO
Approve	CISO	Top management	Service owner
Record	Procurement	Procurement manager	Supplier manager

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Due-diligence files	Supplier repository; supplier manager	Per supplier	Contract + 6 years
Label checks	ENX portal; supplier manager	Per supplier	Contract + 3 years
Approvals	Document system; CISO	Per supplier	Contract + 6 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Suppliers assessed before data sharing	100%	Block
High-tier files reviewed by CISO	100%	Review
Open critical gaps at contract	0	Do not sign

Auditor questions to prepare

- Show due diligence done before contract.
- How do you check a supplier's TISAX label?
- What did you do about gaps?

Frequent nonconformities

- Assessment after contract.

- Label scope unchecked.

Interfaces: ISMS-FOU-POLITIQUE-001, ISMS-FOU-REGISTRE-001, ISMS-CLI-SECURITE-002

ISMS-FOU-SUIVI-001 — Ongoing supplier security assurance

Classification C1 · INTERNAL · Format PROCEDURE · Applicability Added

Objective

Monitor supplier security performance and assurance over the contract life, not only at onboarding.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Supplier relationships: monitoring and review of supplier services (chapter 6)
ISO/IEC 27001:2022	A.5.22 Monitoring, review and change management of supplier services; A.5.21
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
SMO-01	High-tier suppliers shall have an annual security review and quarterly service meeting covering incidents, changes, audit results and SLA performance.	Meeting records.
SMO-02	Certificates, labels and assurance reports shall be tracked for expiry.	Expiry tracker.
SMO-03	Supplier incidents and changes of sub-suppliers shall be notified and assessed.	Notifications.
SMO-04	Issues shall be tracked in a corrective plan.	Plan.
SMO-05	Review outcomes shall inform tiering and renewal decisions.	Sampled instances traced end to end to the record: Review records.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Run reviews	Supplier manager	CISO	Service owner
Track expiry	Supplier manager	Procurement manager	CISO
Decide renewal	Service owner	Department head	CISO

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Review records	Supplier files; supplier manager	Annual / quarterly	Contract + 3 years
Expiry tracker	Supplier files; supplier manager	Quarterly	Until superseded
Corrective plans	Supplier files; supplier manager	Per issue	Contract + 3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
High-tier reviews in 12 months	100%	Escalate
Expired assurance	0	Request in 14 days
Plans closed on time	≥ 90%	Escalate

Auditor questions to prepare

- What did you learn from the last supplier review?
- How do you know a supplier's label is still valid?
- Show a corrective plan.

Frequent nonconformities

- No monitoring.

- Expired labels.

Interfaces: ISMS-FOU-ASSURANCE-002, ISMS-FOU-EVALUATION-001, ISMS-FOU-INCIDENT-001

ISMS-FOU-SOUS-TRAITANCE-001 — Subcontractor chain and external information flows

Classification C1 · INTERNAL · Format PROCEDURE · Applicability Added

Objective

Know and control the chain of subcontractors and the information flows to them so that obligations are preserved down the chain.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Supplier relationships: subcontractors and flow-down (chapter 6)
ISO/IEC 27001:2022	A.5.19; A.5.20; A.5.21
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
SUB-01	Suppliers shall declare subcontractors involved in services touching our or customer information, with location and role.	Declarations.
SUB-02	Contracts shall require flow-down of security obligations and prior approval of subcontractor changes.	Clauses.
SUB-03	The subcontractor chain and flows shall be mapped for high-tier suppliers.	Chain map.
SUB-04	Customer restrictions on subcontracting shall be honoured and notified.	Customer check.
SUB-05	Changes shall be reviewed within 30 days.	Sampled instances traced end to end to the record: Declarations.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Collect declarations	Supplier manager	Procurement manager	Legal
Map chain	Supplier manager	CISO	Service owner
Approve changes	CISO	Top management	Customers

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Declarations	Supplier files; supplier manager	Annual	Contract + 3 years
Chain maps	Supplier files; supplier manager	Annual	Contract + 3 years
Approvals	Document system; CISO	Per change	Contract + 6 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
High-tier suppliers with chain map	100%	Complete
Subcontractor changes approved before start	100%	Incident
Declarations current	100%	Request

Auditor questions to prepare

- Who are your suppliers' subcontractors?
- How do customers approve them?
- Show a change.

Frequent nonconformities

- Chain unknown.

- No flow-down.

Interfaces: ISMS-FOU-POLITIQUE-001, ISMS-CLI-EXIGENCES-001, ISMS-RGP-DPA-001

ISMS-FOU-SORTIE-001 — Supplier exit and reversibility

Classification C1 · INTERNAL · Format PROCEDURE · Applicability Added

Objective

Terminate supplier relationships securely by recovering information, removing access and confirming deletion.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Supplier relationships: termination and reversibility (chapter 6)
ISO/IEC 27001:2022	A.5.20; A.5.11 Return of assets; A.8.10
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
SXT-01	Contracts shall define exit assistance, data return formats, deletion and timelines.	Clauses.
SXT-02	An exit checklist shall cover access removal, asset return, data return, deletion certificate and knowledge transfer.	Checklist.
SXT-03	Access shall be removed on or before the end date.	IAM evidence.
SXT-04	Deletion shall be confirmed in writing, including backups within the agreed period.	Confirmation.
SXT-05	Exit shall be recorded and lessons used for future contracts.	Sampled instances traced end to end to the record: Exit checklists.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Plan exit	Service owner	Department head	Procurement
Execute	Supplier manager	CISO	IAM; IT
Confirm deletion	Supplier manager	CISO	Supplier

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Exit checklists	Supplier files; service owner	Per exit	6 years
Deletion confirmations	Supplier files; supplier manager	Per exit	6 years
IAM removals	IAM tool; IAM owner	Per exit	3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Exits with checklist	100%	Review
Deletion confirmed	100%	Escalate
Access removed on time	100%	Incident

Auditor questions to prepare

- Show an exit and deletion proof.
- How do you get your data back?
- Who removes access?

Frequent nonconformities

- No deletion proof.
- Access lingers.

Interfaces: ISMS-FOU-POLITIQUE-001, ISMS-OPS-CLOUD-002, ISMS-OPS-SUPPRESSION-001

ISMS-FOU-INCIDENT-001 — Supplier alerts and incident management

Classification C1 · INTERNAL · Format PROCEDURE · Applicability Added

Objective

Receive, assess and act on supplier alerts and incidents that may affect our information, and notify suppliers of ours.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Supplier relationships: incident management with suppliers (chapters 1 and 6)
ISO/IEC 27001:2022	A.5.24; A.5.26; A.5.19; A.5.22
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
SIN-01	Contracts shall require suppliers to notify incidents within 24 hours (shorter if customers require) to a named contact.	Clauses.
SIN-02	A supplier incident shall be logged and classified using ISMS-INC-PROC-001 within 4 hours.	Incident ticket.
SIN-03	Impact assessment shall include customer data, access and downstream notifications.	Impact assessment.
SIN-04	Supplier shall provide root-cause and corrective actions, tracked to closure.	Reports.
SIN-05	Contact lists shall be verified semi-annually.	Sampled instances traced end to end to the record: Supplier incident tickets.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Receive alert	Service desk / SOC	Incident manager	Supplier manager
Assess impact	Incident manager	CISO	Service owner
Follow up supplier	Supplier manager	CISO	Supplier

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Supplier incident tickets	Incident system; incident manager	Per incident	6 years
Reports from suppliers	Supplier files; supplier manager	Per incident	6 years
Contact verification	Supplier files; supplier manager	Semi-annual	3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Notifications within 24h	≥ 95%	Contract action
Actions closed on time	≥ 90%	Escalate
Contacts verified	100%	Update

Auditor questions to prepare

- What happens when a supplier reports a breach?
- Show last case.
- Do your contracts set notification times?

Frequent nonconformities

- No clause.
- No follow-up.

Interfaces: ISMS-INC-PROC-001, ISMS-CLI-INCIDENT-001, ISMS-FOU-SUIVI-001

ISMS-CON-VEILLE-001 — Legal and standards watch

Classification C1 · INTERNAL · Format STANDARD · Applicability Added

Objective

Monitor changes in laws, standards and customer requirements and convert them into timely decisions and actions.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Compliance: monitoring of legal and standard changes (chapter 7); ISA edition changes
ISO/IEC 27001:2022	A.5.31 Legal, statutory, regulatory and contractual requirements; A.5.6 Contact with special interest groups; A.5.7
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
WAT-01	Named sources (ENX/VDA, ISO, data protection authorities, customers, legal counsel) and responsible persons shall be defined.	Source list.
WAT-02	Changes shall be assessed for relevance within 30 days and logged with decision and action.	Watch log.
WAT-03	ISA catalogue version changes shall trigger impact analysis of the ISMS and ISMS-ORG-ISA-001.	Analysis.
WAT-04	Actions shall be planned and tracked; relevant changes shall be reported to the steering committee.	Reports.
WAT-05	Effective dates shall be tracked.	Sampled instances traced end to end to the record: Watch log.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Monitor sources	Compliance officer	CISO	Legal
Assess changes	ISMS manager	CISO	Owners
Report	CISO	Top management	Steering committee

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Watch log	ISMS workspace; compliance officer	Continuous	6 years
Impact analyses	ISMS workspace; ISMS manager	Per change	6 years
Reports	Document system; CISO	Quarterly	6 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Changes assessed within 30 days	100%	Escalate
Actions on time	≥ 90%	Review
Sources reviewed in 12 months	100%	Update

Auditor questions to prepare

- How do you hear about ISA changes?
- Show a change you assessed.
- Who is responsible?

Frequent nonconformities

- No source list.

- Changes unassessed.

Interfaces: ISMS-CON-CONFORMITE-001, ISMS-ORG-ISA-001, ISMS-ORG-GOUVERNANCE-001

ISMS-CON-DONNEES-001 — Confidentiality obligations management

Classification C2 · CONFIDENTIAL · Format PROCEDURE · Applicability Added

Objective

Manage confidentiality obligations to customers, partners and law so that people know what is confidential and for how long.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Compliance: confidentiality and protection of customer information (chapter 7)
ISO/IEC 27001:2022	A.6.6 Confidentiality agreements; A.5.34; A.5.12
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
CON-01	A register shall list confidentiality obligations by customer and partner, scope, duration and handling rules.	Register.
CON-02	Staff and suppliers with access shall be briefed and bound.	Briefing records.
CON-03	Obligations shall be reflected in classification and access (named lists for C3).	Mapping.
CON-04	Expiry and end-of-contract duties (return, destruction) shall be tracked.	Calendar.
CON-05	Breaches shall be handled as incidents with customer notification.	Sampled instances traced end to end to the record: Obligations register.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Maintain register	Compliance officer	CISO	Legal
Brief staff	Line managers	Department heads	HR
Track expiry	Contract manager	Legal	Owners

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Obligations register	ISMS workspace; compliance officer	Quarterly	Contract + 6 years
Briefing records	HR system; managers	Per project	3 years
Return and destruction records	Document system; owners	Per contract	6 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Obligations with owner	100%	Assign
Briefings on time	100%	Escalate
Expired obligations handled	100%	Act

Auditor questions to prepare

- What are you obliged to keep confidential and for whom?
- How do staff know?
- Show a return or destruction.

Frequent nonconformities

- Obligations unknown to staff.

- No end-of-contract action.

Interfaces: ISMS-RH-NDA-001, ISMS-ACT-CLASSIF-001, ISMS-CLI-ENGAGEMENTS-001

ISMS-CON-RETENTION-001 — Audit record retention and archiving

Classification C1 · INTERNAL · Format PROCEDURE · Applicability Added

Objective

Retain ISMS and audit records for the periods required for proof, law and contract, and archive them securely.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Compliance: protection of records and audit evidence (chapter 7)
ISO/IEC 27001:2022	A.5.33 Protection of records; Clause 7.5.3 Control of documented information
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
ARK-01	Retention periods for ISMS records (audit, risk, incident, access reviews, training) shall be defined (minimum three years or the assessment cycle plus current period).	Schedule.
ARK-02	Archives shall be protected against loss and alteration, with access control and integrity checks.	Archive configuration.
ARK-03	Retrieval shall be tested semi-annually.	Retrieval test.
ARK-04	Disposal after retention shall be authorised and recorded.	Disposal record.
ARK-05	Legal holds shall prevail.	Sampled instances traced end to end to the record: Schedule.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Maintain schedule	ISMS manager	CISO	Legal
Operate archive	IT operations	IT manager	ISMS manager
Test retrieval	ISMS reviewer	CISO	IT

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Schedule	Document system; ISMS manager	Annual	6 years
Retrieval tests	ISMS workspace; reviewer	Semi-annual	3 years
Disposal records	ITSM; IT operations	Per event	6 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Records retrievable	100%	Fix
Retention breaches	0	Correct
Tests done	100%	Escalate

Auditor questions to prepare

- Retrieve audit records for last year.
- How do you protect archives?
- How long do you keep incident records?

Frequent nonconformities

- Records lost.

- No test.

Interfaces: ISMS-ACT-CONSERVATION-001, ISMS-AUD-EVIDENCE-001, ISMS-ORG-DOC-001

ISMS-CON-CONTROLES-001 — Contractual compliance testing

Classification C1 · INTERNAL · Format STANDARD · Applicability Added

Objective

Test compliance with contractual and customer-specific security requirements and report to the customer where required.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Compliance: verification of contractual security requirements (chapter 7)
ISO/IEC 27001:2022	A.5.36 Compliance with policies; A.5.31; A.5.35
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
CCT-01	Every contractual requirement in ISMS-CLI-ENGAGEMENTS-001 shall be tested at least annually.	Test plan.
CCT-02	Tests shall be performed independently of owners and results documented.	Results.
CCT-03	Failures shall be reported to the CISO and, where the contract requires, to the customer.	Escalation.
CCT-04	Customer audit requests shall be handled per agreement.	Audit handling log.
CCT-05	Test results shall be reported to the steering committee at least annually with the share of contractual requirements met and open gaps.	Management report.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Plan tests	ISMS manager	CISO	Contract manager
Test	ISMS reviewer	CISO	Owners
Handle customer audits	CISO	Top management	Account owner

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Test plan and results	ISMS workspace; reviewer	Annual	Contract + 6 years
Escalations	Ticket system; ISMS manager	Per failure	6 years
Customer audit log	ISMS workspace; CISO	Per audit	Contract + 6 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Requirements tested	100%	Reschedule
Failures reported on time	100%	Escalate
Customer audits managed	100%	Review

Auditor questions to prepare

- How do you check you meet this customer clause?
- Show a failed test.
- How do you host a customer audit?

Frequent nonconformities

- No tests.

- Failures hidden.

Interfaces: ISMS-CLI-ENGAGEMENTS-001, ISMS-CLI-EXIGENCES-001, ISMS-ORG-CONTROLES-001

ISMS-ORG-AI-001 — AI services and sensitive-information security handling

Classification C1 · INTERNAL · Format PROCEDURE · Applicability Risk-based recommendation — not a standalone blanket TISAX obligation

Objective

Govern the use of AI services, so that sensitive information is not exposed and use is controlled.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Organisation and IT security: use of external services and information handling (chapters 1 and 5); not an ISA control by name — risk-based recommendation
ISO/IEC 27001:2022	A.5.10 Acceptable use; A.5.23 Cloud services; A.8.12 Data leakage prevention; A.5.34
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
AIU-01	An approved list of AI services shall exist with permitted data classes; C3 and customer data shall not go to unapproved services.	Approved list.
AIU-02	Each AI service shall be assessed (data retention, training use, location, subprocessors, terms) before approval.	Assessment.
AIU-03	Use shall be via company accounts with SSO and logging; personal accounts are prohibited for company data.	Configuration.
AIU-04	Outputs shall be reviewed by humans before use in decisions or customer deliverables.	Policy.
AIU-05	Staff shall be trained on acceptable use.	Training.
AIU-06	DLP shall monitor uploads to unapproved AI services.	DLP rules.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Assess services	Security architect	CISO	Legal; DPO
Operate controls	IT operations	IT manager	CISO
Train	ISMS manager	CISO	HR

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Approved list and assessments	ISMS workspace; architect	Per service	Life + 3 years
Usage logs	Platform; IT operations	Continuous	12 months
Training	LMS; HR	Annual	3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
AI services assessed	100%	Block
Uploads of C3 to unapproved AI	0	Incident
Staff trained	≥ 95%	Reminder

Auditor questions to prepare

- Which AI tools are allowed and why?
- How do you prevent C3 uploads?
- Show an assessment.

Frequent nonconformities

- No list.
- Personal accounts.

Interfaces: ISMS-RH-CHARTE-001, ISMS-OPS-DLP-001, ISMS-OPS-CLOUD-001

ISMS-PRO-GOUV-001 — Prototype security governance and customer requirements

Classification C3 · STRICTLY CONFIDENTIAL · Format STANDARD · Applicability Conditional

Objective

Govern the protection of prototypes (vehicles, components, parts and related media) through clear responsibility, customer requirement mapping and approval of who may handle what.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Prototype protection module: organisation, requirements and responsibilities (prototype chapter)
ISO/IEC 27001:2022	A.5.2; A.5.31; A.5.19; A.7.1
Target maturity	Level 3 minimum for all applicable prototype protection requirements; the module applies only where the assessment objective 'Prototype protection' is in scope

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
PGV-01	A prototype protection manager shall be appointed in writing with deputy and direct access to top management.	Appointment.
PGV-02	Customer prototype requirements (security level, zones, transport, photography, events, return) shall be registered and mapped to controls and owners.	Requirements register.
PGV-03	Only persons authorised by name and need (access list) shall handle, view or enter prototype areas; each shall be briefed and sign obligations.	Access list, briefings.
PGV-04	Prototype projects shall be registered with owner, location, customer, dates and applicable restrictions before receipt.	Project register.
PGV-05	Deviations from customer requirements shall need customer approval.	Approvals.
PGV-06	Prototype security incidents shall be reported to the customer within contract time.	Sampled instances traced end to end to the record: Requirements register.
PGV-07	Presentations, exhibitions and events involving prototypes (ISA 8.5.1) shall be approved by the customer and the prototype manager in advance, with a written security concept covering the closed location, access list, camouflage, no-photography rules, supervision, transport and a debrief after the event.	Event approval, security concept and debrief record.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Appoint manager	Top management	Managing director	CISO
Maintain requirements	Prototype manager	CISO	Customers
Authorise personnel	Prototype manager	Department head	HR

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Requirements register	ISMS workspace; prototype manager	Per project	Contract + 6 years
Authorised-persons list	Access system; prototype manager	Monthly	Project + 3 years
Briefing records	HR system; prototype manager	Per person	Project + 3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Authorised persons briefed	100%	Remove access
Projects registered before receipt	100%	Stop receipt
Deviations approved	100%	Incident

Auditor questions to prepare

- Who is responsible for prototype protection?
- Show the list of authorised persons for this project.
- How did you translate the customer requirements?

Frequent nonconformities

- Informal access list.
- Receipt before registration.

Interfaces: ISMS-PRO-ZONES-001, ISMS-PRO-TRACABILITE-001, ISMS-CLI-EXIGENCES-001, ISMS-PRO-RECON-001

ISMS-PRO-ZONES-001 — Prototype facilities and restricted zones

Classification C3 · STRICTLY CONFIDENTIAL · Format PROCEDURE · Applicability Conditional

Objective

Protect prototypes with physical facilities and zones that prevent unauthorised access, viewing and photography.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Prototype protection module: physical and environmental security of prototype facilities (prototype chapter)
ISO/IEC 27001:2022	A.7.1; A.7.2; A.7.3; A.7.4; A.7.6
Target maturity	Level 3 minimum for all applicable prototype protection requirements; the module applies only where the assessment objective 'Prototype protection' is in scope

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
PZN-01	Prototype areas shall be enclosed, with opaque walls and shielded openings, preventing observation from outside, including by drones and long lenses.	Site inspection.
PZN-02	Entry shall use individual credentials with access control and intrusion detection, 24/7 alarm to a staffed receiver, and video monitoring with 90 days retention where lawful.	System exports.
PZN-03	Visitors shall be excluded or escorted with approval from the prototype manager; the visitor log shall name the prototype area.	Visitor log.
PZN-04	Mobile phones, cameras and recording devices shall be prohibited unless approved, with lockers and signage.	Policy and checks.
PZN-05	Prototypes shall be covered or stored in locked rooms when not in use.	Spot checks.
PZN-06	Zone reviews shall be done quarterly.	Sampled instances traced end to end to the record: Access and alarm logs.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Operate zone	Facility management	Prototype manager	CISO
Review access	Prototype manager	CISO	Facility
Inspect	Security officer	CISO	Prototype manager

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Access and alarm logs	Access system; facility	Continuous	12 months
Quarterly reviews	ISMS workspace; prototype manager	Quarterly	3 years
Inspection reports	ISMS workspace; security officer	Quarterly	3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Reviews done	100%	Revoke
Alarm response test	Passed twice a year	Fix
Unauthorised devices found	0	Incident

Auditor questions to prepare

- Take us to the prototype area: who can enter?

- How do you prevent photography from outside?
- Test an alarm.

Frequent nonconformities

- Windows unshielded.
- Shared codes.

Interfaces: ISMS-PHY-ZONES-001, ISMS-PRO-IMAGE-001, ISMS-PHY-BADGES-001

ISMS-PRO-TRACABILITE-001 — Prototype lifecycle traceability

Classification C3 · STRICTLY CONFIDENTIAL · Format PROCEDURE · Applicability Conditional

Objective

Track every prototype item from receipt to return or destruction so that location, custodian and status are always known.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Prototype protection module: inventory, tracking and traceability of prototype parts (prototype chapter)
ISO/IEC 27001:2022	A.5.9; A.5.11; A.7.9
Target maturity	Level 3 minimum for all applicable prototype protection requirements; the module applies only where the assessment objective 'Prototype protection' is in scope

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
PTR-01	Each prototype, part or sample shall have a unique identifier, owner, location, custodian, classification and status.	Register.
PTR-02	Every movement (receipt, transfer, test, storage, shipment, return) shall be recorded in real time or within the same day with signature of custodian.	Movement log.
PTR-03	Physical inventory shall be reconciled to the register at least monthly (weekly for critical items).	Reconciliation.
PTR-04	Missing items shall trigger ISMS-PRO-RECON-001 immediately.	Incident record.
PTR-05	Records shall be retained for the contract life plus period required by customer.	Sampled instances traced end to end to the record: Prototype register.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Maintain register	Prototype custodian	Prototype manager	Customer
Reconcile	Prototype custodian	Prototype manager	ISMS reviewer
Report discrepancies	Prototype manager	CISO	Customer

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Prototype register	Tracking system; custodian	Continuous	Contract + 6 years
Movement logs	Tracking system; custodian	Per movement	Contract + 6 years
Reconciliations	ISMS workspace; custodian	Monthly	3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Items with complete record	100%	Fix
Reconciliation done	100%	Escalate
Discrepancies open > 24h	0	CISO

Auditor questions to prepare

- Where is part X now and who has it?
- Show a reconciliation.
- What happens when something is missing?

Frequent nonconformities

- Spreadsheet unsynced.
- Movements unrecorded.

Interfaces: ISMS-PRO-RECON-001, ISMS-PRO-TRANSPORT-001, ISMS-PRO-DESTRUCTION-001

ISMS-PRO-TRANSPORT-001 — Prototype secure transport and storage

Classification C3 · STRICTLY CONFIDENTIAL · Format PROCEDURE · Applicability Conditional

Objective

Transport and temporarily store prototypes so that they are never exposed to unauthorised observation or access.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Prototype protection module: transport, shipment and storage (prototype chapter)
ISO/IEC 27001:2022	A.7.9; A.7.10; A.5.14
Target maturity	Level 3 minimum for all applicable prototype protection requirements; the module applies only where the assessment objective 'Prototype protection' is in scope

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
PTS-01	Transport shall use approved carriers under contract with security obligations, in closed, covered or sealed vehicles or containers with tracking.	Contracts and tracking logs.
PTS-02	Routes, stops and handovers shall be planned and approved; overnight stops shall be in secured locations.	Transport plan.
PTS-03	Handover shall be recorded with signatures and seal numbers verified.	Handover records.
PTS-04	Drivers and escorts shall be briefed and bound to confidentiality.	Briefings.
PTS-05	Incidents during transport shall be reported immediately.	Incident log.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Plan transport	Logistics	Prototype manager	CISO
Execute	Carrier	Logistics	Prototype manager
Verify handover	Custodians	Prototype manager	Customer

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Transport plans	Logistics system; logistics	Per shipment	Contract + 3 years
Tracking and seal logs	Carrier; logistics	Per shipment	Contract + 3 years
Handover records	Tracking system; custodians	Per shipment	Contract + 6 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Shipments with approved plan	100%	Stop
Seals verified	100%	Incident
Tracking gaps	0	Investigate

Auditor questions to prepare

- Show a recent shipment's plan and handover.
- How are carriers vetted?
- What if a stop is unplanned?

Frequent nonconformities

- Open vehicles.

- No seals.

Interfaces: ISMS-PRO-TRACABILITE-001, ISMS-PRO-VEHICULES-001, ISMS-FOU-POLITIQUE-001

ISMS-PRO-IMAGE-001 — Prototype photography and media handling

Classification C3 · STRICTLY CONFIDENTIAL · Format PROCEDURE · Applicability Conditional

Objective

Prevent unauthorised photography, filming and image sharing of prototypes and related material.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Prototype protection module: photography, filming and media handling (prototype chapter)
ISO/IEC 27001:2022	A.7.6; A.5.10; A.5.12
Target maturity	Level 3 minimum for all applicable prototype protection requirements; the module applies only where the assessment objective 'Prototype protection' is in scope

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
PIG-01	Photography and video of prototypes shall be forbidden unless approved in writing by the prototype manager and, where required, the customer.	Approval records.
PIG-02	Approved images shall be taken with company devices, classified C3, stored in the protected repository and never on personal or cloud accounts.	Storage evidence.
PIG-03	Devices with cameras shall be restricted in prototype zones by policy and signage.	Policy.
PIG-04	Images shall be logged with who took them, when, purpose and destination.	Image log.
PIG-05	Publication of any image shall require customer approval.	Approvals.
PIG-06	Film and photo shootings involving prototypes (ISA 8.5.2) shall follow a customer-approved security plan: closed or shielded location, only authorised crew bound by NDA, supervised handling, image review before release, and secure deletion of unapproved material.	Shooting plan, crew NDAs, review and deletion records.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Approve photography	Prototype manager	CISO	Customer
Handle images	Authorised photographer	Prototype manager	ISMS manager
Monitor	Security officer	CISO	Prototype manager

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Approvals	ISMS workspace; prototype manager	Per request	Project + 3 years
Image log	Protected repository; photographer	Per image	Project + 3 years
Checks	ISMS workspace; security officer	Quarterly	3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Images with approval	100%	Incident
Images on unapproved storage	0	Delete and investigate
Checks done	100%	Escalate

Auditor questions to prepare

- Who can take pictures and where do they go?
- Show approval.

- What stops staff from using a phone?

Frequent nonconformities

- Photos in personal cloud.
- No approval.

Interfaces: ISMS-PRO-ZONES-001, ISMS-PHY-VISITEURS-001, ISMS-ACT-CLASSIF-001

ISMS-PRO-DESTRUCTION-001 — Prototype return, destruction and recycling

Classification C3 · STRICTLY CONFIDENTIAL · Format PROCEDURE · Applicability Conditional

Objective

Return, destroy or recycle prototypes and parts securely at end of use, with customer-verifiable proof.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Prototype protection module: return, destruction and recycling (prototype chapter)
ISO/IEC 27001:2022	A.7.14; A.5.11; A.8.10
Target maturity	Level 3 minimum for all applicable prototype protection requirements; the module applies only where the assessment objective 'Prototype protection' is in scope

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
PDS-01	Disposition (return, destroy, recycle) shall follow the customer instruction and be recorded per item.	Disposition record.
PDS-02	Destruction shall render parts unusable and unidentifiable and shall be witnessed by two authorised persons or a certified provider.	Witness records.
PDS-03	Certificates of destruction with item IDs, date, method and witnesses shall be issued and sent to the customer.	Certificates.
PDS-04	Recycling providers shall be contractually bound and audited.	Contracts and audits.
PDS-05	Registers shall be closed only after reconciliation.	Sampled instances traced end to end to the record: Disposition records.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Decide disposition	Prototype manager	CISO	Customer
Destroy	Authorised staff/provider	Prototype manager	Witnesses
Certify	Prototype manager	CISO	Customer

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Disposition records	Tracking system; prototype manager	Per item	Contract + 6 years
Destruction certificates	Document system; prototype manager	Per batch	Contract + 6 years
Provider audits	Supplier files; supplier manager	Annual	3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Items with certificate	100%	Hold
Providers audited	100%	Audit
Registers closed after reconciliation	100%	Reopen

Auditor questions to prepare

- Show a destruction certificate and how it ties to items.
- Who witnessed?
- What if the customer wants a return?

Frequent nonconformities

- Certificates generic.

- No witness.

Interfaces: ISMS-PRO-TRACABILITE-001, ISMS-PHY-SUPPORTS-001, ISMS-FOU-POLITIQUE-001

ISMS-PRO-VEHICULES-001 — Protected test vehicles and trials

Classification C3 · STRICTLY CONFIDENTIAL · Format PROCEDURE · Applicability Conditional

Objective

Protect test vehicles and trials against observation and unauthorised access on test tracks and public roads.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Prototype protection module: trial and test vehicles (prototype chapter)
ISO/IEC 27001:2022	A.7.9; A.5.19; A.7.6
Target maturity	Level 3 minimum for all applicable prototype protection requirements; the module applies only where the assessment objective 'Prototype protection' is in scope

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
PVE-01	Trial vehicles shall be camouflaged or covered as required by the customer, with approval of the prototype manager.	Camouflage plan.
PVE-02	Trial plans (routes, times, locations) shall be approved, shared only with those needing them, and varied where required.	Trial plans.
PVE-03	Vehicles shall never be left unattended in public; overnight parking shall be in secured, monitored sites.	Parking records.
PVE-04	Drivers shall be trained and bound; use of personal phones for photos shall be prohibited.	Briefings.
PVE-05	Incidents (accidents, theft, observation) shall be reported at once to the prototype manager and customer.	Incident log.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Plan trials	Trial manager	Prototype manager	Customer
Drive	Authorised drivers	Trial manager	Prototype manager
Report incidents	Driver	Trial manager	CISO

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Trial plans	Project portal; trial manager	Per trial	Contract + 3 years
Parking and custody log	Tracking system; trial manager	Per trial	Contract + 3 years
Briefings	HR system; trial manager	Per driver	Project + 3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Trials with approved plan	100%	Stop
Overnight parking secured	100%	Incident
Drivers briefed	100%	Remove

Auditor questions to prepare

- How do you protect a vehicle on the road?
- Show a trial plan.
- What if it is photographed?

Frequent nonconformities

- Unsecured parking.
- Plans widely shared.

Interfaces: ISMS-PRO-TRANSPORT-001, ISMS-PRO-IMAGE-001, ISMS-PRO-GOUV-001

ISMS-PRO-RECON-001 — Prototype inventory reconciliation and missing-item response

Classification C3 · STRICTLY CONFIDENTIAL · Format PROCEDURE · Applicability Conditional — prototype protection

Objective

Detect and respond to missing or unaccounted prototype items through reconciliation and an immediate response process.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Prototype protection module: inventory reconciliation and loss response (prototype chapter)
ISO/IEC 27001:2022	A.5.9; A.5.24; A.7.9
Target maturity	Level 3 minimum for all applicable prototype protection requirements; the module applies only where the assessment objective 'Prototype protection' is in scope

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
PRC-01	Reconciliation of physical items to the register shall be done at least monthly and after every movement batch, by a person independent of the custodian.	Reconciliation records.
PRC-02	A missing item shall be searched for within 2 hours, then reported to the prototype manager, CISO and customer within contractual time (maximum 24 hours).	Timeline records.
PRC-03	Response shall include lock-down, access log analysis, camera review and interviews, handled as a security incident.	Incident file.
PRC-04	Root cause and corrective actions shall be recorded and shared with the customer.	Report.
PRC-05	Repeated discrepancies shall trigger an audit of the area.	Sampled instances traced end to end to the record: Reconciliation records.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Reconcile	Independent reviewer	Prototype manager	Custodian
Respond	Incident manager	CISO	Prototype manager
Notify customer	CISO	Top management	Account manager

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Reconciliation records	Tracking system; reviewer	Monthly	Contract + 6 years
Incident files	Incident system; incident manager	Per case	Contract + 6 years
Customer notifications	Document system; CISO	Per case	Contract + 6 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Reconciliations on time	100%	Escalate
Missing items open > 24h	0	Top management
Customer notified in time	100%	Review

Auditor questions to prepare

- What do you do in the first hour after finding an item missing?
- Show a reconciliation by someone other than the custodian.
- How do you inform customers?

Frequent nonconformities

- Custodian reconciles own stock.
- Slow response.

Interfaces: ISMS-PRO-TRACABILITE-001, ISMS-INC-PROC-001, ISMS-CLI-INCIDENT-001

ISMS-RGP-REGISTRE-001 — Personal data processing records

Classification C2 · CONFIDENTIAL · Format PROCEDURE · Applicability Conditional

Objective

Keep the record of processing activities complete and current as the basis of all data protection controls.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Data protection module: records of processing activities (data protection module; chapter 7)
ISO/IEC 27001:2022	A.5.34 Privacy and protection of PII; A.5.31; GDPR Article 30
Target maturity	Level 3 minimum where the data protection module applies; legal conformity under GDPR is a separate responsibility of the controller and the DPO

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
ROP-01	Every processing activity shall be recorded with purpose, legal basis, data categories, subjects, recipients, transfers, retention, security measures and owner.	Register.
ROP-02	The register shall be reviewed at least annually and on change by process owners.	Review log.
ROP-03	Processor activities shall be recorded where the organisation acts as processor.	Processor records.
ROP-04	The register shall be available to the supervisory authority on request.	Availability.
ROP-05	New processing shall be registered before start.	Sampled instances traced end to end to the record: Processing register.
ROP-06	A data protection officer or a named person responsible for data protection (ISA 9.2.1) shall be appointed in writing with defined tasks, independence from conflicting duties, a direct reporting line to top management and published contact details.	Appointment letter, task description and reporting records.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Maintain register	DPO	Managing director	Process owners
Review	Process owners	Department heads	DPO
Provide to authority	DPO	Managing director	Legal

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Processing register	Privacy tool; DPO	Continuous	Life + 3 years
Review log	Privacy tool; DPO	Annual	3 years
Processor records	Privacy tool; DPO	Continuous	Life + 3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Processing with owner and basis	100%	Complete
Reviewed in 12 months	100%	Escalate
New processing registered before start	100%	Block

Auditor questions to prepare

- Show a record and its legal basis.
- How do you capture new processing?

- Who is the DPO?

Frequent nonconformities

- Register outdated.
- No legal basis.

Interfaces: ISMS-RGP-PIA-001, ISMS-RGP-RETENTION-001, ISMS-RGP-DPA-001

ISMS-RGP-PIA-001 — Data protection impact assessment (DPIA)

Classification C2 · CONFIDENTIAL · Format PROCEDURE · Applicability Conditional

Objective

Assess privacy risk of high-risk processing before launch and treat it.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Data protection module: data protection impact assessment (data protection module)
ISO/IEC 27001:2022	A.5.34; A.5.8; GDPR Article 35
Target maturity	Level 3 minimum where the data protection module applies; legal conformity under GDPR is a separate responsibility of the controller and the DPO

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
DPI-01	A screening shall decide for each new or changed processing whether a DPIA is required using documented criteria.	Screening records.
DPI-02	A DPIA shall describe the processing, necessity, risks to individuals and measures, with DPO advice and, where necessary, consultation with the authority.	DPIA.
DPI-03	Residual risk shall be accepted by the controller's top management.	Approval.
DPI-04	DPIAs shall be reviewed when risks change or every 3 years.	Review.
DPI-05	Results shall feed the risk register.	Sampled instances traced end to end to the record: Screenings.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Screen	Project manager	Process owner	DPO
Conduct DPIA	Process owner	Department head	DPO; CISO
Approve	Top management	Managing director	DPO

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Screenings	Privacy tool; DPO	Per project	Processing life + 3 years
DPIAs	Privacy tool; DPO	Per processing	Processing life + 3 years
Approvals	Document system; top management	Per DPIA	Processing life + 3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
New processing screened	100%	Block
DPIA completed before start	100%	Stop
DPIAs reviewed on time	100%	Escalate

Auditor questions to prepare

- Show a DPIA and the decision.
- How do you decide a DPIA is needed?
- Who accepted residual risk?

Frequent nonconformities

- DPIA after launch.
- No approval.

Interfaces: ISMS-RGP-REGISTRE-001, ISMS-RSK-METHODE-001, ISMS-PRJ-SECURITE-001

ISMS-RGP-DROITS-001 — Data-subject rights procedure

Classification C1 · INTERNAL · Format PROCEDURE · Applicability Conditional

Objective

Respond to data subject requests within legal deadlines with verified identity and full records.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Data protection module: data subject rights (data protection module)
ISO/IEC 27001:2022	A.5.34; GDPR Articles 12 to 22
Target maturity	Level 3 minimum where the data protection module applies; legal conformity under GDPR is a separate responsibility of the controller and the DPO

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
DSR-01	Requests shall be received through named channels and logged on receipt.	Request log.
DSR-02	Identity of the requester shall be verified proportionately.	Verification.
DSR-03	Responses shall be sent within one month (extendable by two months with reasons).	Response timing.
DSR-04	All systems and processors holding the data shall be searched and acted on.	Search evidence.
DSR-05	Refusals shall be reasoned and informed with remedies.	Refusals.
DSR-06	Metrics shall be reported annually.	Sampled instances traced end to end to the record: Request log.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Receive and log	Privacy desk	DPO	Customer service
Collect data	System owners	IT manager	DPO
Respond	DPO	Managing director	Legal

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Request log	Privacy tool; DPO	Per request	3 years
Response records	Privacy tool; DPO	Per request	3 years
Annual report	Document system; DPO	Annual	3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Requests answered in time	100%	Escalate
Identity checked	100%	Review
Searches complete	100%	Fix

Auditor questions to prepare

- Show a request and your response timeline.
- How do you search all systems?
- What if you refuse?

Frequent nonconformities

- Late responses.

- Incomplete search.

Interfaces: ISMS-RGP-REGISTRE-001, ISMS-RGP-RETENTION-001, ISMS-ACT-FLUX-001

ISMS-RGP-VIOLATION-001 — Personal data breach response

Classification C2 · CONFIDENTIAL · Format PROCEDURE · Applicability Conditional

Objective

Detect, assess and notify personal data breaches within legal deadlines.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Data protection module: personal data breach response (data protection module; chapter 1)
ISO/IEC 27001:2022	A.5.24; A.5.26; A.5.34; GDPR Articles 33 and 34
Target maturity	Level 3 minimum where the data protection module applies; legal conformity under GDPR is a separate responsibility of the controller and the DPO

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
PDB-01	Suspected breaches shall be reported immediately to the incident process and DPO.	Reports.
PDB-02	The DPO shall assess risk to individuals within 24 hours and decide on notification.	Assessment.
PDB-03	Notification to the supervisory authority shall occur within 72 hours of awareness if required; affected individuals shall be informed without undue delay where high risk.	Notifications.
PDB-04	Customers for whom the organisation is processor shall be notified per DPA, at the latest within 24 hours.	Customer notices.
PDB-05	All breaches shall be recorded in a register with facts, effects and measures.	Breach register.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Detect and report	All staff	Incident manager	DPO
Assess	DPO	Managing director	CISO; legal
Notify	DPO	Managing director	Communications

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Breach register	Privacy tool; DPO	Per breach	6 years
Notifications	Document system; DPO	Per breach	6 years
Assessments	Privacy tool; DPO	Per breach	6 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Assessments within 24h	100%	Escalate
Notifications in 72h	100%	Top management
Breaches recorded	100%	Review

Auditor questions to prepare

- Walk me through a breach from discovery to notification.
- How do you decide notification?
- Show the register.

Frequent nonconformities

- 72-hour clock missed.
- Register incomplete.

Interfaces: ISMS-INC-PROC-001, ISMS-CLI-INCIDENT-001, ISMS-RGP-DPA-001

ISMS-RGP-TRANSFERTS-001 — International personal data transfers

Classification C1 · INTERNAL · Format PROCEDURE · Applicability Conditional

Objective

Ensure international transfers of personal data rely on valid mechanisms and safeguards.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Data protection module: international transfers (data protection module)
ISO/IEC 27001:2022	A.5.34; A.5.14; GDPR Chapter V
Target maturity	Level 3 minimum where the data protection module applies; legal conformity under GDPR is a separate responsibility of the controller and the DPO

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
ITR-01	Transfers of personal data outside the EEA shall be identified, including remote access from third countries.	Transfer register.
ITR-02	A valid mechanism (adequacy, standard contractual clauses, binding corporate rules) shall be in place with a transfer impact assessment where needed.	Mechanism and assessment.
ITR-03	Supplementary technical measures (encryption, key control, pseudonymisation) shall be applied as assessed.	Measures.
ITR-04	Customers shall be informed of transfers per contract.	Notifications.
ITR-05	The register shall be reviewed annually.	Sampled instances traced end to end to the record: Transfer register.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Identify transfers	DPO	Managing director	IT; procurement
Assess	DPO	Managing director	Legal
Apply measures	IT operations	IT manager	CISO

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Transfer register	Privacy tool; DPO	Quarterly	Life + 3 years
Assessments	Privacy tool; DPO	Per transfer	Life + 3 years
Measure evidence	Config; IT operations	Annual	3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Transfers with mechanism	100%	Suspend
Assessments current	100%	Update
Register reviewed	100%	Escalate

Auditor questions to prepare

- Where does personal data go?
- Show a transfer assessment.
- How do you handle support access from abroad?

Frequent nonconformities

- Unknown transfers.
- Outdated clauses.

Interfaces: ISMS-INF-HEB-002, ISMS-RGP-DPA-001, ISMS-OPS-CLOUD-001

ISMS-RGP-RETENTION-001 — Personal data retention and disposal

Classification C1 · INTERNAL · Format PROCEDURE · Applicability Conditional

Objective

Retain personal data only as long as necessary and delete or anonymise it afterwards.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Data protection module: storage limitation and disposal (data protection module)
ISO/IEC 27001:2022	A.5.34; A.8.10; GDPR Article 5(1)(e)
Target maturity	Level 3 minimum where the data protection module applies; legal conformity under GDPR is a separate responsibility of the controller and the DPO

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
PRT-01	A retention period per processing shall be defined with justification and implemented technically.	Retention schedule and configuration.
PRT-02	Deletion jobs shall run automatically with logs and exceptions approved.	Job logs.
PRT-03	Backups shall expire within a defined period after deletion.	Backup policy.
PRT-04	Requests to erase shall follow ISMS-RGP-DROITS-001.	Link.
PRT-05	Deletion shall be verified by sampling quarterly.	Sampled instances traced end to end to the record: Retention schedule.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Define periods	DPO	Managing director	Process owners
Operate deletion	IT operations	IT manager	DPO
Verify	ISMS reviewer	CISO	DPO

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Retention schedule	Privacy tool; DPO	Annual	3 years
Deletion logs	Systems; IT operations	Per run	12 months
Verification	ISMS workspace; reviewer	Quarterly	3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Systems with automated deletion	≥ 90%	Plan
Data beyond retention	0	Delete
Samples verified	100%	Fix

Auditor questions to prepare

- How long do you keep this data?
- Show a deletion log.
- What about backups?

Frequent nonconformities

- Indefinite storage.
- No verification.

Interfaces: ISMS-RGP-REGISTRE-001, ISMS-ACT-CONSERVATION-001, ISMS-RGP-DROITS-001

ISMS-OT-INVENTAIRE-001 — OT and industrial asset inventory

Classification C2 · CONFIDENTIAL · Format REGISTER · Applicability Conditional

Objective

Maintain an accurate inventory of industrial assets and their network context to enable protection and change control.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Asset management and IT security applied to production environments (chapters 1 and 5); availability objective
ISO/IEC 27001:2022	A.5.9; A.8.9; IEC 62443-2-1 asset inventory
Target maturity	Applicable where production or OT environments are in the assessment scope (availability objective, customer requirement); references IEC 62443 as a complementary framework, not a TISAX requirement

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
OTI-01	The OT inventory shall list controllers, HMIs, servers, network devices, firmware versions, vendors, locations, criticality and support status.	Inventory.
OTI-02	Passive discovery shall be used to find unknown devices; intrusive scans only with plant approval.	Discovery records.
OTI-03	Inventory shall be reconciled with the IT CMDB and zone documentation semi-annually.	Reconciliation.
OTI-04	Each asset shall have a plant owner and a cybersecurity owner.	Owner fields.
OTI-05	Unsupported devices shall be flagged with compensating controls.	Sampled instances traced end to end to the record: OT inventory.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Maintain inventory	OT engineering	Plant manager	CISO
Discover	OT security engineer	CISO	Plant
Reconcile	ISMS reviewer	CISO	OT engineering

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
OT inventory	OT asset tool; OT engineering	Continuous	Life + 3 years
Discovery reports	OT monitoring; OT security	Monthly	12 months
Reconciliation	ISMS workspace; reviewer	Semi-annual	3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
OT assets with owner and criticality	100%	Assign
Unknown devices open > 14 days	0	CISO
Reconciliation done	100%	Escalate

Auditor questions to prepare

- How do you know all OT devices?
- Show an unsupported controller and compensation.
- Who owns it?

Frequent nonconformities

- Inventory from vendor drawings only.
- No owner.

Interfaces: ISMS-OT-ZONES-001, ISMS-OT-CORRECTIFS-001, ISMS-ACT-INVENTAIRE-001

ISMS-OT-ZONES-001 — Industrial zones and conduits architecture

Classification C3 · STRICTLY CONFIDENTIAL · Format PROCEDURE · Applicability Conditional

Objective

Segment the industrial network into zones and conduits aligned with criticality, controlling all traffic between IT and OT.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	IT security: network segregation applied to industrial environments (chapter 5)
ISO/IEC 27001:2022	A.8.22; A.8.20; IEC 62443-3-2 zones and conduits
Target maturity	Applicable where production or OT environments are in the assessment scope (availability objective, customer requirement); references IEC 62443 as a complementary framework, not a TISAX requirement

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
OTZ-01	Zones and conduits shall be defined with security level targets and documented in diagrams.	Diagrams.
OTZ-02	IT-OT traffic shall pass a DMZ with deny-by-default firewalls and allowed protocols documented.	Rules.
OTZ-03	Direct internet access from OT zones shall be prohibited.	Test.
OTZ-04	Segmentation shall be validated annually by technical test.	Test report.
OTZ-05	Changes shall follow ISMS-OT-CHANGES-001.	Sampled instances traced end to end to the record: Zone and conduit documents.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Design zones	OT architect	CISO	Plant
Operate firewalls	Network engineering	IT manager	OT
Test	Security engineering	CISO	OT

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Zone and conduit documents	Document system; OT architect	On change	Life + 3 years
Firewall rule reviews	Firewall manager; network	Semi-annual	3 years
Segmentation tests	Document system; security engineering	Annual	6 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Conduits documented	100%	Document
Any-any rules in OT	0	Immediate
Tests done	100%	Test

Auditor questions to prepare

- Show how IT reaches OT.
- Prove the zone separation.
- Can OT reach the internet?

Frequent nonconformities

- Flat OT network.
- Undocumented conduits.

Interfaces: ISMS-OPS-SEGMENT-001, ISMS-OT-ACCES-001, ISMS-OT-INVENTAIRE-001

ISMS-OT-ACCES-001 — Secure industrial remote maintenance

Classification C2 · CONFIDENTIAL · Format PROCEDURE · Applicability Conditional

Objective

Allow remote maintenance of industrial systems only through controlled, supervised and time-limited sessions.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Identity and access management applied to industrial remote maintenance (chapters 4 and 5)
ISO/IEC 27001:2022	A.8.2; A.5.19; A.8.20; IEC 62443-2-4 service provider requirements
Target maturity	Applicable where production or OT environments are in the assessment scope (availability objective, customer requirement); references IEC 62443 as a complementary framework, not a TISAX requirement

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
OTA-01	Remote access shall pass an access gateway with MFA, individual accounts and session recording.	Gateway logs.
OTA-02	Each session shall be requested, approved by the plant owner, time-limited and ended afterwards.	Session approvals.
OTA-03	Vendors shall be under contract with security clauses and trained personnel.	Contracts.
OTA-04	Remote tools installed permanently shall be disabled unless approved.	Scan.
OTA-05	Sessions shall be reviewed monthly (ISMS-OT-SESSION-002).	Sampled instances traced end to end to the record: Session approvals.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Request session	Vendor / OT engineer	Plant manager	CISO
Approve	Plant owner	Plant manager	CISO
Review	OT security	CISO	Plant

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Session approvals	Ticket system; plant owner	Per session	3 years
Session recordings	Gateway; OT security	Per session	12 months
Contracts	Supplier files; supplier manager	Per vendor	Contract + 6 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Sessions with approval	100%	Incident
Sessions recorded	100%	Investigate
Permanent vendor access	0	Disable

Auditor questions to prepare

- How do vendors reach your PLCs?
- Show a recording.
- Who approves?

Frequent nonconformities

- Permanent VPN for vendor.
- No recording.

Interfaces: ISMS-OT-SESSION-002, ISMS-IAM-TIERS-001, ISMS-OPS-OUTILS-001

ISMS-OT-CORRECTIFS-001 — OT vulnerability and patch management

Classification C2 · CONFIDENTIAL · Format PROCEDURE · Applicability Conditional

Objective

Manage OT vulnerabilities and patching with safety and availability priorities and compensating controls.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	IT security: vulnerability management adapted to industrial systems (chapter 5)
ISO/IEC 27001:2022	A.8.8; A.8.9; IEC 62443-2-3 patch management
Target maturity	Applicable where production or OT environments are in the assessment scope (availability objective, customer requirement); references IEC 62443 as a complementary framework, not a TISAX requirement

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
OTP-01	Vulnerability information shall be monitored for installed OT products and assessed with plant engineering within 14 days.	Assessment log.
OTP-02	Patches shall be tested on a representative system and applied in agreed maintenance windows after vendor approval.	Test and window records.
OTP-03	Where patching is impossible, compensating controls (segmentation, monitoring, virtual patching) shall be applied and risk accepted with expiry.	Exceptions.
OTP-04	Patch status shall be reported quarterly to the plant manager and CISO.	Report.
OTP-05	Emergency patches shall follow ISMS-OT-CHANGES-001.	Sampled instances traced end to end to the record: Assessment log.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Assess vulnerabilities	OT security engineer	CISO	Plant engineering
Patch	OT engineering	Plant manager	Vendor
Accept risk	Plant manager	Top management	CISO

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Assessment log	OT tool; OT security	Continuous	3 years
Patch records	Change system; OT engineering	Per patch	3 years
Exceptions	Exception register; CISO	Per exception	Life + 3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Assessments within 14 days	≥ 90%	Escalate
Exceptions with controls	100%	Review
Patch report delivered	100%	Escalate

Auditor questions to prepare

- How do you patch a PLC?
- Show an exception.
- Who decides on downtime?

Frequent nonconformities

- IT patch windows imposed on OT.
- No compensation.

Interfaces: ISMS-OPS-VULN-001, ISMS-OT-CHANGES-001, ISMS-OT-INVENTAIRE-001

ISMS-OT-CHANGES-001 — Industrial change management

Classification C2 · CONFIDENTIAL · Format PROCEDURE · Applicability Conditional

Objective

Control changes to industrial systems to protect safety, quality and availability.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	IT security: change management in industrial environments (chapter 5)
ISO/IEC 27001:2022	A.8.32; A.8.9; IEC 62443-2-1
Target maturity	Applicable where production or OT environments are in the assessment scope (availability objective, customer requirement); references IEC 62443 as a complementary framework, not a TISAX requirement

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
OTC-01	Every change to control logic, configuration or firmware shall have an approved request with safety and quality impact assessment.	Change records.
OTC-02	Backups of configurations and programs shall be taken before the change and after.	Backup records.
OTC-03	Changes shall be tested in simulation or non-production where possible and have a rollback plan.	Test records.
OTC-04	Approval shall involve plant engineering, safety and security.	Approvals.
OTC-05	Unauthorised changes shall be detected by configuration comparison.	Sampled instances traced end to end to the record: Change records.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Request	OT engineer	Plant manager	Safety
Approve	Change board	Plant manager	CISO
Detect	OT security	CISO	Plant

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Change records	OT change system; OT engineering	Per change	6 years
Configuration backups	OT repository; OT engineering	Per change	Life + 3 years
Comparison reports	OT tool; OT security	Monthly	12 months

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Changes approved	100%	Incident
Backups before change	100%	Stop
Unauthorised changes	0	Investigate

Auditor questions to prepare

- Show a PLC program change.
- How do you detect a rogue change?
- Who approves safety impact?

Frequent nonconformities

- Direct changes by vendor.
- No backup.

Interfaces: ISMS-OPS-CHANGES-001, ISMS-OT-CORRECTIFS-001, ISMS-OT-ACCES-001

ISMS-OT-PRA-001 — Production continuity and OT recovery

Classification C2 · CONFIDENTIAL · Format STANDARD · Applicability Conditional

Objective

Recover production and OT systems within objectives after cyber or technical incidents.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Business continuity and IT security applied to production (chapters 3 and 5); availability objective
ISO/IEC 27001:2022	A.5.30; A.8.13; A.8.14; IEC 62443-2-1
Target maturity	Applicable where production or OT environments are in the assessment scope (availability objective, customer requirement); references IEC 62443 as a complementary framework, not a TISAX requirement

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
OTR-01	Recovery objectives (RTO/RPO) shall be defined per line or cell from the BIA.	Objectives.
OTR-02	Offline copies of controller programs, SCADA configurations, images and licences shall be stored securely and be restorable.	Backup inventory.
OTR-03	Manual or degraded operation procedures shall exist for critical processes.	Procedures.
OTR-04	Recovery shall be tested at least annually for the most critical line.	Test report.
OTR-05	Spare parts and vendor support contracts shall match RTO.	Contracts.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Plan recovery	OT engineering	Plant manager	BCM manager
Test	OT engineering	Plant manager	CISO
Maintain spares	Maintenance	Plant manager	Procurement

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
OT backup inventory	OT repository; OT engineering	Quarterly	Life + 3 years
Test reports	BCM workspace; OT engineering	Annual	6 years
Degraded procedures	Document system; plant manager	Annual	3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Critical lines tested	100%	Plan
Recovery within RTO	≥ 90%	Redesign
Backups restorable	100%	Fix

Auditor questions to prepare

- How fast can you restart this line after ransomware?
- Show a restore test.
- What do you do manually?

Frequent nonconformities

- Never restored.

- Backups not offline.

Interfaces: ISMS-PRA-PRA-001, ISMS-OT-INVENTAIRE-001, ISMS-OPS-RESTORE-001

ISMS-OT-FOURNISSEURS-001 — OT integrator and manufacturer security

Classification C2 · CONFIDENTIAL · Format PROCEDURE · Applicability Conditional

Objective

Require integrators and equipment manufacturers to meet security expectations through contract and verification.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Supplier relationships applied to OT integrators and manufacturers (chapter 6)
ISO/IEC 27001:2022	A.5.19; A.5.21; A.8.30; IEC 62443-2-4 and 4-1
Target maturity	Applicable where production or OT environments are in the assessment scope (availability objective, customer requirement); references IEC 62443 as a complementary framework, not a TISAX requirement

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
OTS-01	Contracts with integrators and OEMs shall include security requirements (secure development, vulnerability disclosure, default credentials removal, documentation, support period).	Clauses.
OTS-02	Evidence of conformance (for example IEC 62443 certifications) shall be requested and checked for scope.	Evidence.
OTS-03	Acceptance tests shall check security configuration before handover.	Acceptance records.
OTS-04	Support and patch commitments shall be recorded with end dates.	Records.
OTS-05	Maintenance personnel shall be authorised and supervised.	Sampled instances traced end to end to the record: Contract clauses.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Define requirements	OT architect	CISO	Procurement
Assess	Supplier manager	CISO	Plant
Accept	Plant owner	Plant manager	Security

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Contract clauses	Contract system; procurement	Per contract	Contract + 10 years
Evidence	Supplier files; supplier manager	Per supplier	Contract + 6 years
Acceptance	Project portal; plant owner	Per delivery	Life + 3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Contracts with security clauses	100%	Block
Evidence checked	100%	Request
Acceptance tests	100%	Block handover

Auditor questions to prepare

- How do you secure what an integrator delivers?
- Show clauses.
- How long will the vendor patch?

Frequent nonconformities

- No clauses.
- Default passwords left.

Interfaces: ISMS-FOU-POLITIQUE-001, ISMS-DEV-EXTERNE-001, ISMS-OT-ACCES-001

ISMS-OT-IEC62443-001 — IEC 62443 applicability and gap review

Classification C2 · CONFIDENTIAL · Format PROCEDURE · Applicability Conditional

Objective

Assess applicability of IEC 62443 and track gaps as complementary evidence for OT protection.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Complementary framework for industrial environments; not part of the VDA ISA
ISO/IEC 27001:2022	IEC 62443-2-1; IEC 62443-3-3; A.5.31
Target maturity	Applicable where production or OT environments are in the assessment scope (availability objective, customer requirement); references IEC 62443 as a complementary framework, not a TISAX requirement

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
OTG-01	Applicability of IEC 62443 shall be decided by top management based on customers, plant risk and law and recorded with rationale.	Decision.
OTG-02	A gap assessment against selected parts (2-1 programme, 3-2 zones, 3-3 system requirements) shall be done and tracked.	Gap register.
OTG-03	Target security levels per zone shall be defined and linked to risk.	Target levels.
OTG-04	Gaps shall have actions and owners and be reviewed annually.	Action log.
OTG-05	The relation to TISAX scope shall be documented to avoid inconsistent claims.	Sampled instances traced end to end to the record: Applicability decision.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Decide applicability	Top management	Managing director	CISO
Assess	OT architect	CISO	Plant
Track gaps	OT security	CISO	Plant manager

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Applicability decision	Document system; CISO	Annual	6 years
Gap register	ISMS workspace; OT architect	Annual	3 years
Action log	Ticket system; OT security	Per gap	3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Gaps with action	100%	Plan
Actions on time	≥ 85%	Escalate
Decision reviewed	100%	Escalate

Auditor questions to prepare

- Do you apply IEC 62443 and why?
- Show your gap register.
- How does it relate to TISAX?

Frequent nonconformities

- Claim without assessment.

- No linkage to risk.

Interfaces: ISMS-OT-ZONES-001, ISMS-OT-INVENTAIRE-001, ISMS-ORG-SOA-001

ISMS-OT-SESSION-002 — OT privileged remote session release and forensic record

Classification C2 · CONFIDENTIAL · Format PROCEDURE · Applicability Conditional — OT operations

Objective

Release privileged remote OT sessions only under supervised, recorded and time-bound conditions that preserve a forensic record.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	Identity and access management: privileged remote sessions in industrial environments (chapter 4)
ISO/IEC 27001:2022	A.8.2; A.8.15; A.5.28; IEC 62443-2-4
Target maturity	Applicable where production or OT environments are in the assessment scope (availability objective, customer requirement); references IEC 62443 as a complementary framework, not a TISAX requirement

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
OTE-01	Each privileged session shall be requested with ticket, scope, duration and approver; release shall be performed by a different person.	Release record.
OTE-02	Sessions shall be mediated by a gateway with MFA and recorded (video and command logs) with integrity protection.	Recordings.
OTE-03	Recordings and logs shall be retained 12 months and reviewed monthly by sample.	Review notes.
OTE-04	Post-session checks shall confirm that access was closed and configuration matches the approved change.	Post-check.
OTE-05	Anomalies shall trigger incident handling.	Sampled instances traced end to end to the record: Release records.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Request	Vendor / engineer	Plant manager	CISO
Release	Security operator	CISO	Plant owner
Review	OT security	CISO	Plant manager

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Release records	Ticket; security operator	Per session	3 years
Recordings	Gateway; OT security	Per session	12 months
Review notes	ISMS workspace; OT security	Monthly	3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Sessions released by second person	100%	Incident
Sessions recorded	100%	Investigate
Monthly review done	100%	Escalate

Auditor questions to prepare

- Who may release an OT session and how is it recorded?
- Show a recording.
- What happens after the session?

Frequent nonconformities

- Self-release.
- Recordings not kept.

Interfaces: ISMS-OT-ACCES-001, ISMS-IAM-PRIV-002, ISMS-INC-PRESERVATION-001

ISMS-ORG-CONTEXTE-001 — Organisational context and interested parties

Classification C1 · INTERNAL · Format REGISTER · Applicability Core supporting control

Objective

Understand the context of the organisation and the requirements of interested parties so that scope, risks and objectives reflect reality.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	
ISO/IEC 27001:2022	Clause 4.1 Understanding the organisation and its context; Clause 4.2 Understanding the needs and expectations of interested parties; Clause 4.3 Scope
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
CTX-01	Internal and external issues relevant to information security shall be identified and recorded with source and date.	Issues register.
CTX-02	All interested parties with security requirements shall be listed with an owner, including customers, regulators, suppliers, staff representatives and the TISAX exchange platform.	Party register.
CTX-03	Requirements of each party shall be recorded with reference to the contract, law or standard clause.	Source references.
CTX-04	The register shall feed scope, risk assessment, objectives and the requirements register, with documented links.	Traceability links.
CTX-05	The register shall be reviewed at least annually and after acquisitions, new customers, relocations, major incidents or legal change.	Review record.
CTX-06	Changes shall be reported to the steering committee and top management.	Committee minutes.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Maintain register	ISMS manager	CISO	Account managers; legal
Validate requirements	Party owners	Department heads	ISMS manager
Review and approve	CISO	Top management	Steering committee

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Context and interested-party register	ISMS workspace; ISMS manager	Annual / on change	6 years
Review minutes	Document system; CISO	Annual	6 years
Traceability links	ISMS workspace; ISMS manager	Annual	3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Interested parties with owner and requirements	100%	Complete within 14 days
Register reviewed within 12 months	100%	Escalate to top management
Requirements without linked control	0	Assign control or exception

Auditor questions to prepare

- Who are your interested parties and what do they require?

- How did the context influence your scope and risks?
- What changed since the last assessment?

Frequent nonconformities

- Register not maintained after creation.
- No link to risks or scope.

Interfaces: ISMS-ORG-PERIMETRE-001, ISMS-RSK-METHODE-001, ISMS-CLI-EXIGENCES-001, ISMS-ORG-GOUVERNANCE-001

ISMS-RH-DISCIPLINE-001 — Disciplinary procedure for security breaches

Classification C1 · INTERNAL · Format PROCEDURE · Applicability Core supporting control

Objective

Provide a lawful, consistent and documented disciplinary process so that obligations in contracts and the acceptable use charter are enforceable.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	
ISO/IEC 27001:2022	A.6.4 Disciplinary process; A.6.2 Terms and conditions of employment; A.5.10 Acceptable use
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
DSC-01	A formal disciplinary process for information security breaches shall exist, be communicated to staff and be consistent with employment law and works agreements.	Procedure and communication evidence.
DSC-02	Breaches shall be classified by severity and each class shall have a range of proportionate measures.	Classification table.
DSC-03	Investigations shall be conducted by HR with legal and CISO, respecting data protection and employee rights.	Case file.
DSC-04	The person concerned shall be heard and decisions shall be reasoned, dated and signed by an authorised manager.	Hearing and decision records.
DSC-05	Measures involving contractors shall follow the contract and be notified to the contracting company.	Contractor case records.
DSC-06	Case statistics (anonymised) shall be reported to the steering committee at least annually.	Anonymised report.
DSC-07	Disciplinary records shall be retained only for the period allowed by law.	Retention record.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Investigate	HR	HR manager	Legal; CISO
Decide measure	Authorised line manager	Department head	HR; legal
Report statistics	CISO	Top management	HR

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Disciplinary case files	HR case system; HR	Per case	As law allows
Decision records	HR case system; line managers	Per case	As law allows
Anonymised annual report	Document system; CISO	Annual	3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Breach cases closed within 30 days	≥ 90%	HR manager review
Cases with documented hearing	100%	Reopen
Staff aware of the process	≥ 95% in awareness check	Awareness action

Auditor questions to prepare

- What happens when someone breaches the acceptable use rules?

- Show an anonymised case and how proportionality was assessed.
- How are works council and law respected?

Frequent nonconformities

- Sanctions applied without a documented process.
- Contractors outside the process.

Interfaces: ISMS-RH-CHARTE-001, ISMS-RH-CHARTE-002, ISMS-RH-CYCLE-001, ISMS-INC-PROC-001, ISMS-INC-PRESERVATION-001

ISMS-RH-ANTECEDENTS-001 — Background verification and screening

Classification C1 · INTERNAL · Format PROCEDURE · Applicability Core supporting control

Objective

Reduce insider and impersonation risk by verifying trustworthiness before granting access to protected information.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	
ISO/IEC 27001:2022	A.6.1 Screening; A.6.2 Terms and conditions of employment; A.5.34 Privacy and protection of PII
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
SCR-01	Screening levels shall be defined per role and classification (basic, enhanced, customer-specific), approved by HR, legal and the CISO.	Level matrix.
SCR-02	Screening shall be completed before access to C2/C3 information or to prototype areas is granted.	Dates versus access grant dates.
SCR-03	Checks shall respect local law, proportionality and consent; results shall be held by HR and not copied into IT or line records.	Privacy assessment and storage controls.
SCR-04	Customer-required clearances shall be recorded and tracked until expiry.	Clearance register.
SCR-05	Adverse findings shall be reviewed by two persons and decisions documented.	Decision records.
SCR-06	Enhanced screening shall be repeated at least every 3 years or on role change.	Re-screening schedule.
SCR-07	Agencies and suppliers providing personnel shall contractually guarantee equivalent screening and prove it on request.	Contract clause and evidence.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Define levels	HR	HR manager	Legal; CISO
Perform checks	HR / screening provider	HR manager	Line manager
Decide on adverse findings	HR manager	Top management	Legal; CISO

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Screening level matrix	Document system; HR	Annual	3 years
Screening outcomes	HR system; HR	Per person	Employment + 1 year
Clearance register	HR system; HR	Continuous	Clearance + 1 year

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Sensitive-role holders screened before access	100%	Restrict access
Re-screening due dates met	100%	HR escalation
External personnel with screening evidence	100%	Block access

Auditor questions to prepare

- How do you screen people with access to strictly confidential information?
- Show evidence that screening preceded access for a recent hire.

- How do you handle customer clearance requirements?

Frequent nonconformities

- Screening after access was granted.
- Results stored in line manager files.

Interfaces: ISMS-RH-CYCLE-001, ISMS-RH-POSTES-001, ISMS-RH-TIERS-001, ISMS-RH-NDA-001, ISMS-PRO-GOUV-001

ISMS-OPS-LOGICIELS-001 — Software installation and approval

Classification C1 · INTERNAL · Format PROCEDURE · Applicability Core supporting control

Objective

Ensure only evaluated, approved and supported software processes the organisation's information.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	
ISO/IEC 27001:2022	A.8.19 Installation of software on operational systems; A.8.9 Configuration management; A.5.32 Intellectual property rights; A.8.7 Protection against malware
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
SWA-01	An approved software catalogue shall exist with version, owner, licence status, support end date and permitted data classes.	Catalogue export.
SWA-02	Software shall be requested through a ticket and assessed for security, privacy and licence before first use, including SaaS and browser extensions.	Assessment records.
SWA-03	Standard users shall not install software; installation shall use managed deployment tools or application control.	Technical settings.
SWA-04	Unapproved software found by discovery shall be removed or assessed within 10 working days.	Discovery findings and tickets.
SWA-05	Open-source and third-party components in used software shall be checked for known vulnerabilities and licence terms.	Check record.
SWA-06	The catalogue shall be reviewed at least annually and unsupported software handled via ISMS-OPS-EOL-001.	Review record.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Assess requests	Security analyst	CISO	Software owner; legal
Maintain catalogue	IT operations	IT manager	Security
Run discovery	Security engineering	CISO	IT operations

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Software catalogue	CMDB; IT operations	Continuous	Life + 3 years
Request and assessment tickets	ITSM; security analyst	Per request	3 years
Discovery reports	Endpoint tool; engineering	Monthly	12 months

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Installed software in catalogue	≥ 98%	Remove or approve within 10 days
Requests assessed in 10 working days	≥ 90%	Staffing review
Unsupported software without exception	0	CISO

Auditor questions to prepare

- How do you ensure only approved software runs?
- Show a software request and its assessment.

- How do you find unapproved software?

Frequent nonconformities

- Admin rights for all users.
- No catalogue or discovery.

Interfaces: ISMS-OPS-ENDPOINT-001, ISMS-OPS-EOL-001, ISMS-OPS-CMDB-001, ISMS-DEV-EXTERNE-001, ISMS-ORG-AI-001

ISMS-OPS-ENVIRONNEMENTS-001 — Environment separation and test data

Classification C1 · INTERNAL · Format PROCEDURE · Applicability Core supporting control

Objective

Prevent unauthorised access and unintended changes to production by separating environments and protecting test data.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	
ISO/IEC 27001:2022	A.8.31 Separation of development, test and production environments; A.8.33 Test information; A.8.32 Change management
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
SEP-01	Development, test and production shall use separate networks or tenants, accounts, credentials and secrets.	Architecture and configuration.
SEP-02	Developers shall not have standing write access to production; access shall be granted just in time and logged.	Access lists and logs.
SEP-03	Test data shall be synthetic or irreversibly masked; production data in tests shall be approved, time-limited, protected as production and deleted afterwards.	Masking and approvals.
SEP-04	Promotion between environments shall use controlled pipelines with approvals (ISMS-DEV-RELEASE-001).	Pipeline records.
SEP-05	Environments shall be inventoried with owners and reviewed quarterly.	Register and review.
SEP-06	Test environments reachable from the internet shall be treated as production for security controls.	Exposure review.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Maintain environments	Platform engineering	IT manager	Security architect
Approve production data in tests	Data owner	Department head	CISO; DPO
Verify separation	Security engineering	CISO	Platform

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Environment register	CMDB; platform engineering	Quarterly	Life + 3 years
Test data approvals	Ticket system; data owners	Per request	3 years
Separation tests	ISMS workspace; security engineering	Annual	3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Environments with owner and separation evidence	100%	Fix within 14 days
Test datasets containing unmasked personal data	0	Incident
Developers with standing production access	0	Remove

Auditor questions to prepare

- How are development and production separated?
- Show an approval to use production data in a test.

- Who can write to production?

Frequent nonconformities

- Shared credentials across environments.
- Production copies in test.

Interfaces: ISMS-DEV-SDLC-001, ISMS-DEV-RELEASE-001, ISMS-DEV-TESTS-001, ISMS-OPS-CHANGES-001, ISMS-RGP-RETENTION-001

ISMS-PHY-BUREAU-001 — Clean desk and screen lock

Classification C1 · INTERNAL · Format PROCEDURE · Applicability Core supporting control

Objective

Reduce the risk of unauthorised viewing, copying or removal of information at unattended workplaces.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	
ISO/IEC 27001:2022	A.7.7 Clear desk and clear screen; A.7.6 Working in secure areas; A.8.1 User endpoint devices
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
CDK-01	Screens shall lock automatically within 5 minutes and users shall lock manually when leaving the workplace.	MDM or group policy export.
CDK-02	C2 and C3 documents and media shall be locked away when unattended and at the end of the day.	Spot checks.
CDK-03	Secure print release shall be enforced for C2/C3 and unclaimed printouts shall be collected and destroyed daily.	Printer configuration and logs.
CDK-04	Meeting rooms and whiteboards shall be cleared after use and shared spaces checked daily by the user.	Room checks.
CDK-05	Staff working at home or in shared spaces shall apply the same rules and use privacy screens where visible to others.	Remote work declaration and awareness.
CDK-06	Spot checks shall be performed at least quarterly per site with findings corrected in 14 days.	Spot-check reports and tickets.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Apply the rules	All staff	Department heads	Security officer
Perform spot checks	Security officer	CISO	Site managers
Correct findings	Department heads	Site manager	ISMS manager

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Spot-check reports	ISMS workspace; security officer	Quarterly	3 years
Printer and lock policy exports	Device console; IT operations	Quarterly	3 years
Corrective tickets	Ticket system; department heads	Per finding	3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Spot checks without C2/C3 left unattended	≥ 95%	Awareness action
Findings corrected in 14 days	≥ 90%	Escalate
Devices with 5-minute lock	100%	Fix within 7 days

Auditor questions to prepare

- Show your clean desk rules and the last spot check.
- What stops someone reading an unattended screen?
- How do you handle printouts?

Frequent nonconformities

- Papers with C3 data on desks.
- Lock timeout over 15 minutes.

Interfaces: ISMS-PHY-ZONES-001, ISMS-PHY-INSPECTIONS-001, ISMS-RH-TELETRAVAIL-001, ISMS-PHY-SUPPORTS-001, ISMS-RH-SENSIBILISATION-001

ISMS-OPS-PURVIEW-001 — Microsoft Purview labelling and DLP configuration register

Classification C2 · CONFIDENTIAL · Format REGISTER · Applicability Core supporting control

Objective

Provide verifiable evidence that classification labels and data loss prevention are configured and enforced as designed.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	
ISO/IEC 27001:2022	A.5.12 Classification of information; A.5.13 Labelling of information; A.8.12 Data leakage prevention; A.8.9 Configuration management
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
PUR-01	The four classification levels shall exist as sensitivity labels with encryption for C2 (where specified) and C3, with marking in header, footer and watermark as required by ISMS-ACT-CLASSIF-001.	Label configuration export.
PUR-02	Label policies shall apply to all in-scope users; default labelling shall be C1 and mandatory labelling shall apply to documents and email.	Policy export.
PUR-03	Auto-labelling shall detect defined sensitive information types and customer markings and shall never downgrade a customer label.	Rule export and tests.
PUR-04	DLP policies shall cover email, collaboration, endpoint, cloud storage and web upload for C2/C3, with documented actions and user override rules.	DLP export.
PUR-05	Every policy shall be tested (simulation) before enforcement and retested after changes.	Test records.
PUR-06	Configuration shall be exported at least quarterly and compared with the register; differences shall be explained by change tickets.	Export and comparison.
PUR-07	Administration of Purview shall be restricted to named roles with MFA and logged.	Role membership and logs.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Maintain configuration	Security engineering	CISO	IT operations
Approve label design	CISO	Top management	Legal; DPO
Review exports	ISMS reviewer	CISO	Security engineering

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Configuration exports	Tenant export; security engineering	Quarterly	3 years
Policy test records	ISMS workspace; security engineering	Per change	3 years
Change tickets	ITSM; security engineering	Per change	3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Register matches tenant export	100%	Correct within 5 days
Policies in enforce mode for C3	100%	CISO
Sampled documents with correct label	≥ 95%	Policy tuning

Auditor questions to prepare

- Show me your label configuration and how it matches the classification policy.
- How did you test the DLP policy before enforcement?
- Who can change labels?

Frequent nonconformities

- Register typed from memory and not matching the tenant.
- DLP only in monitor mode.

Interfaces: ISMS-ACT-CLASSIF-001, ISMS-OPS-DLP-001, ISMS-OPS-EMAIL-001, ISMS-OPS-CHANGES-001, ISMS-ORG-AI-001

ISMS-ORG-AUTORITES-001 — Contacts with authorities and special interest groups

Classification C1 · INTERNAL · Format REGISTER · Applicability Core supporting control

Objective

Ensure the right external parties can be reached quickly and appropriately during incidents and compliance events.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	
ISO/IEC 27001:2022	A.5.5 Contact with authorities; A.5.6 Contact with special interest groups; A.5.24 Incident management planning
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
AUT-01	A contact register shall list authorities, CERTs, regulators, key customers' security contacts, ENX, insurers and forensic and legal advisers with channel and availability.	Register.
AUT-02	Criteria and authority for contacting each party shall be defined, including legal notification duties and deadlines.	Decision matrix.
AUT-03	Contact data shall be verified at least twice a year with a test contact.	Verification records.
AUT-04	The register shall be accessible offline to the crisis team and incident manager.	Offline copy check.
AUT-05	All real contacts shall be logged in the case file with time, person and content summary.	Case files.
AUT-06	Participation in at least one threat-sharing or professional group shall be maintained and benefits reported annually.	Membership and report.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Maintain register	ISMS manager	CISO	Legal; communications
Decide on contact	CISO	Managing director	Legal
Verify contacts	ISMS manager	CISO	Incident manager

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Contact register	Document system; ISMS manager	Semi-annual	3 years
Verification records	ISMS workspace; ISMS manager	Semi-annual	3 years
Case contact logs	Incident system; incident manager	Per incident	6 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Contacts verified in 6 months	100%	Update within 5 days
Register available offline	100%	Fix
Notification deadlines met	100%	Top management

Auditor questions to prepare

- Who would you call at the national CERT and when?
- When did you last verify these contacts?

- Show a real contact with an authority.

Frequent nonconformities

- Contact numbers outdated.
- Nobody authorised to notify.

Interfaces: ISMS-INC-PROC-001, ISMS-INC-CRISE-001, ISMS-CLI-INCIDENT-001, ISMS-RGP-VIOLATION-001, ISMS-CON-VEILLE-001

ISMS-ORG-COMMUNICATION-001 — Information security communication plan

Classification C1 · INTERNAL · Format PROCEDURE · Applicability Core supporting control

Objective

Make sure the right information security messages reach the right audiences reliably, both inside and outside the organisation.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	
ISO/IEC 27001:2022	Clause 7.4 Communication; A.6.3 Awareness, education and training; A.5.2 Roles and responsibilities; A.5.5 Contact with authorities
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
COM-01	A communication matrix shall define audience, topic, owner, channel, frequency, approver and language for security communications.	Matrix.
COM-02	Policy changes, security alerts, incident notices and awareness campaigns shall use approved channels and templates.	Samples.
COM-03	Crisis and incident communications shall follow ISMS-INC-CRISE-001 with approved spokespersons only.	Crisis plan link.
COM-04	Staff shall have a documented way to ask questions and report concerns and receive an answer within 3 working days.	Question log.
COM-05	Reach and effectiveness shall be measured and reported quarterly.	Metrics report.
COM-06	Messages sent to customers about security shall be consistent with the approved fact sheet and approved by the CISO.	Approvals.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Maintain plan	ISMS manager	CISO	Communications; HR
Approve messages	CISO	Top management	Legal
Deliver communications	Communications / HR	Department heads	ISMS manager

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Communication matrix	Document system; ISMS manager	Annual	3 years
Distribution logs	Intranet and mail system; communications	Per message	12 months
Metrics reports	ISMS workspace; ISMS manager	Quarterly	3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Mandatory messages read within 5 working days	≥ 90%	Reminder and line manager follow-up
Questions answered in 3 days	≥ 95%	Staffing review
Plan reviewed in 12 months	100%	Escalate

Auditor questions to prepare

- How do staff learn about a change of security policy?
- Show a recent security communication and its reach.

- Who may speak to customers about a security incident?

Frequent nonconformities

- Ad hoc communications with no owner.
- No measurement.

Interfaces: ISMS-RH-SENSIBILISATION-001, ISMS-INC-CRISE-001, ISMS-CLI-FICHE-001, ISMS-ORG-GOUVERNANCE-001, ISMS-ORG-AUTORITES-001

ISMS-OPS-CAPACITES-001 — Capacity and availability management

Classification C1 · INTERNAL · Format PROCEDURE · Applicability Core supporting control

Objective

Prevent availability incidents caused by lack of capacity through monitoring, forecasting and timely adjustment.

Framework mapping

FRAMEWORK	REFERENCE
VDA ISA 6 (topic level)	
ISO/IEC 27001:2022	A.8.6 Capacity management; A.8.14 Redundancy of information processing facilities; A.5.30 ICT readiness for business continuity
Target maturity	Level 3 minimum for all applicable controls

Mandatory requirements

ID	REQUIREMENT (SHALL)	VERIFICATION AT AL3
CAP-01	Capacity indicators and thresholds shall be defined for each critical service and aligned with RTO and RPO.	Indicator list.
CAP-02	Monitoring shall alert the owner at warning and critical thresholds 24/7 for critical services.	Alert configuration and tickets.
CAP-03	A capacity forecast shall be produced at least quarterly and reviewed with service owners.	Forecast reports.
CAP-04	Capacity changes shall follow change management and shall be completed before critical thresholds are reached.	Change records.
CAP-05	Cloud quotas, licences and certificates affecting availability shall be tracked and renewed in advance.	Tracking register.
CAP-06	Load or failover tests shall be performed at least annually for critical services.	Test reports.

Activities and accountability

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED / INFORMED
Monitor capacity	IT operations	IT manager	Service owners
Forecast and plan	Service owners	IT manager	Finance
Approve changes	Change authority	IT manager	CISO

Records and evidence

RECORD	SYSTEM OF RECORD / OWNER	FREQUENCY	RETENTION
Capacity indicators and thresholds	Monitoring tool; IT operations	Annual	3 years
Capacity forecasts	ISMS workspace; service owners	Quarterly	3 years
Capacity incidents and reviews	ITSM; IT operations	Per incident	3 years

Indicators and escalation

INDICATOR	BASELINE TARGET	ESCALATION TRIGGER
Critical services below critical threshold	100%	Immediate action
Capacity incidents	0 critical	Root-cause review
Forecasts delivered quarterly	100%	Escalate

Auditor questions to prepare

- How do you know when a critical system will run out of capacity?
- Show a forecast and the action taken.

- What happens at the critical threshold?

Frequent nonconformities

- No monitoring of storage.
- Forecast absent.

Interfaces: ISMS-PRA-PCA-001, ISMS-PRA-PRA-001, ISMS-OPS-CHANGES-001, ISMS-OPS-JOURNAUX-001, ISMS-OPS-CLOUD-001

4 Evidence master index

Every record that an AL3 auditor can ask for, with its system of record, owner, frequency and retention.

DOCUMENT	RECORD	SYSTEM / OWNER	FREQUENCY	RETENTION
ISMS-OPS-VULN-001	Asset-to-scanner reconciliation	CMDB and scanner export; IT Operations	Monthly	3 years
ISMS-OPS-VULN-001	Scan results and job history	Scanner platform; security engineering	Weekly / monthly	3 years
ISMS-OPS-VULN-001	Triage and priority record	Ticketing system; vulnerability analyst	Per finding	3 years
ISMS-OPS-VULN-001	Patch deployment and change record	Change system; service owner	Per change	3 years
ISMS-OPS-VULN-001	Independent closure evidence	Ticket plus rescan ID; ISMS reviewer	Per finding	3 years
ISMS-OPS-VULN-001	Risk acceptance and EOL exceptions	Exception register; CISO	Per exception	Exception life + 3 years
ISMS-OPS-VULN-001	Penetration test reports and retest	Document store; CISO	Annual	6 years
ISMS-CRY-POLITIQUE-001	Cryptographic standard	Document system; architect	Annual	3 years
ISMS-CRY-POLITIQUE-001	Key inventory and lifecycle log	KMS/HSM; platform engineering	Continuous	Key life + 3 years
ISMS-CRY-POLITIQUE-001	Certificate inventory	CLM or CMDB; platform engineering	Continuous	Cert life + 1 year
ISMS-CRY-POLITIQUE-001	Encryption and TLS compliance scans	Scanner; security engineering	Quarterly	3 years
ISMS-OPS-CHANGES-001	Change tickets	ITSM; change manager	Per change	3 years
ISMS-OPS-CHANGES-001	CAB minutes	ITSM; change manager	Weekly	3 years
ISMS-OPS-CHANGES-001	Emergency reviews	ITSM; change manager	Per emergency	3 years
ISMS-OPS-DURCISSEMENT-001	Baseline catalogue	Repository; platform engineering	Annual	3 years
ISMS-OPS-DURCISSEMENT-001	Compliance scan results	Compliance tool; security engineering	Monthly	3 years
ISMS-OPS-DURCISSEMENT-001	Deviation approvals	Exception register; CISO	Per exception	Life + 3 years
ISMS-OPS-MALWARE-001	Coverage and health reports	EDR console; security engineering	Weekly	12 months
ISMS-OPS-MALWARE-001	Detection tickets	Ticket/SIEM; analyst	Per alert	3 years
ISMS-OPS-MALWARE-001	Exceptions	Exception register; CISO	Per exception	Life + 3 years
ISMS-OPS-JOURNAUX-001	Logging standard	Document system; architect	Annual	3 years
ISMS-OPS-JOURNAUX-001	Source coverage reconciliation	SIEM; security engineering	Quarterly	3 years
ISMS-OPS-JOURNAUX-001	Alert handling tickets	SIEM / ticket; SOC	Per alert	3 years
ISMS-OPS-JOURNAUX-001	Log archives	Log platform; security engineering	Continuous	12 months minimum
ISMS-OPS-SAUVEGARDE-001	Backup job reports	Backup tool; administrator	Daily	12 months
ISMS-OPS-SAUVEGARDE-001	Restore test results	ITSM; administrator	Quarterly	3 years

DOCUMENT	RECORD	SYSTEM / OWNER	FREQUENCY	RETENTION
ISMS-OPS-SAUVEGARDE-001	Backup matrix	Document system; IT manager	Annual	3 years
ISMS-OPS-RESEAU-001	Network and data-flow diagrams	Document system; network engineering	On change	Life + 3 years
ISMS-OPS-RESEAU-001	Firewall rule reviews	Firewall manager; network engineering	Semi-annual	3 years
ISMS-OPS-RESEAU-001	Remote access reports	VPN/ZTNA; network engineering	Monthly	12 months
ISMS-OPS-CLOUD-001	Cloud service register	CMDB; cloud owner	Quarterly	Life + 3 years
ISMS-OPS-CLOUD-001	Onboarding assessments	Supplier files; supplier manager	Per service	Contract life + 3 years
ISMS-OPS-CLOUD-001	Posture reports	CSPM; cloud engineering	Weekly	12 months
ISMS-OPS-CLOUD-001	Provider assurance reports	Supplier files; supplier manager	Annual	3 years
ISMS-DEV-SDLC-001	Requirements and threat models	Repository; architect	Per project	Product life + 3 years
ISMS-DEV-SDLC-001	Pipeline security results	CI/CD; engineering	Per build	12 months
ISMS-DEV-SDLC-001	Penetration tests	Document system; CISO	Per release / annual	6 years
ISMS-DEV-SDLC-001	SBOM	Repository; engineering	Per release	Product life + 3 years
ISMS-POL-SSI-002	Approved policy with version history	Document management system; CISO	On change / annual	Superseded versions kept 6 years
ISMS-POL-SSI-002	Acknowledgement records	HR system or LMS; HR	Joining and on change	Employment + 3 years
ISMS-POL-SSI-002	Annual policy review record	Management review minutes; CISO	Annual	6 years
ISMS-POL-SSI-002	Policy exception register	Exception register; CISO	Continuous	Exception life + 3 years
ISMS-POL-SSI-001	Release approval	Document system; CISO	Per version	6 years
ISMS-POL-SSI-001	Consistency check	ISMS workspace; ISMS manager	Per version	6 years
ISMS-POL-SSI-001	Distribution log	Customer register; account owner	Per release	3 years
ISMS-ORG-PERIMETRE-001	Scope register and boundary diagram	ISMS workspace; ISMS manager	Annual / on change	6 years
ISMS-ORG-PERIMETRE-001	Exclusion approvals	Document system; CISO	Per exclusion	6 years
ISMS-ORG-PERIMETRE-001	ENX portal scope extract	ENX portal; ISMS manager	Per assessment	6 years
ISMS-ORG-PERIMETRE-001	Interface register	ISMS workspace; ISMS manager	Quarterly	3 years
ISMS-ORG-ROLES-001	Appointment letters	HR system; HR	On change	Employment + 6 years
ISMS-ORG-ROLES-001	RACI matrix	ISMS workspace; ISMS manager	Annual	3 years
ISMS-ORG-ROLES-001	Segregation of duties analysis	IAM tooling; IAM owner	Semi-annual	3 years
ISMS-ORG-DEROGATIONS-001	Exception requests and approvals	Exception register; CISO	Per exception	Life + 3 years
ISMS-ORG-DEROGATIONS-001	Monthly register review	Meeting minutes; CISO	Monthly	3 years
ISMS-ORG-DEROGATIONS-001	Expiry and closure evidence	Ticket system; ISMS manager	Per exception	Life + 3 years
ISMS-ACT-CLASSIF-001	Classification scheme and mapping	Document system; CISO	Annual	3 years
ISMS-ACT-CLASSIF-001	Asset classifications	Asset register; asset owners	Annual	3 years
ISMS-ACT-CLASSIF-001	Label and DLP configuration	Security console; IT operations	Quarterly	3 years

DOCUMENT	RECORD	SYSTEM / OWNER	FREQUENCY	RETENTION
ISMS-ACT-CLASSIF-001	Labelling sample results	ISMS workspace; reviewer	Semi-annual	3 years
ISMS-ACT-INVENTAIRE-001	Asset inventory with attributes	CMDB; CMDB owner	Continuous	Life + 3 years
ISMS-ACT-INVENTAIRE-001	Reconciliation reports	CMDB and scanners; engineering	Monthly	3 years
ISMS-ACT-INVENTAIRE-001	Disposal certificates	Procurement files; IT operations	Per disposal	6 years
ISMS-ACT-INVENTAIRE-001	Ownership confirmation	Asset register; asset owners	Annual	3 years
ISMS-RSK-METHODE-001	Risk methodology	Document system; CISO	Annual	3 years
ISMS-RSK-METHODE-001	Risk assessment reports	Risk tool; risk coordinator	Annual / on change	6 years
ISMS-RSK-METHODE-001	Risk register	Risk tool; ISMS manager	Continuous	6 years
ISMS-RSK-METHODE-001	Residual-risk acceptances	Document system; top management	Per decision	6 years
ISMS-PRJ-SECURITE-001	Security screening	Project portal; project manager	Per project	6 years
ISMS-PRJ-SECURITE-001	Security requirements and approvals	Project portal; architect	Per project	6 years
ISMS-PRJ-SECURITE-001	Gate and go-live approvals	Change system; CISO delegate	Per gate	6 years
ISMS-AUD-PROGRAMME-001	Audit programme and plans	Audit tool; ISMS manager	Annual	6 years
ISMS-AUD-PROGRAMME-001	Audit reports and evidence	Audit tool; auditors	Per audit	6 years
ISMS-AUD-PROGRAMME-001	Management review minutes	Document system; CISO	Annual	6 years
ISMS-AUD-PROGRAMME-001	Findings register	Audit tool; ISMS manager	Continuous	6 years
ISMS-INC-PROC-001	Incident tickets and timeline	Ticket system; incident manager	Per incident	6 years
ISMS-INC-PROC-001	Notification records	Document system; CISO	Per incident	6 years
ISMS-INC-PROC-001	Post-incident review	ISMS workspace; ISMS manager	Per major incident	6 years
ISMS-INC-PROC-001	Evidence log	Evidence vault; incident manager	Per incident	Per legal need
ISMS-INC-CRISE-001	Crisis plan and roster	Document system; CISO	Semi-annual	3 years
ISMS-INC-CRISE-001	Crisis log	Crisis log tool; secretary	Per crisis	6 years
ISMS-INC-CRISE-001	Exercise report	ISMS workspace; ISMS manager	Annual	3 years
ISMS-CLI-EXIGENCES-001	Customer requirements register	ISMS workspace; ISMS manager	Per contract / semi-annual	Contract life + 6 years
ISMS-CLI-EXIGENCES-001	Conflict decisions	Document system; CISO	Per conflict	Contract life + 6 years
ISMS-RH-CYCLE-001	Screening results (minimal)	HR system; HR	Per hire	Employment + 1 year or as law allows
ISMS-RH-CYCLE-001	Signed obligations	HR system; HR	Per hire	Employment + 6 years
ISMS-RH-CYCLE-001	Joiner/mover/leaver tickets	Ticket system; service desk	Per event	3 years
ISMS-RH-CYCLE-001	Exit checklist and asset return	HR system; line manager	Per leaver	3 years
ISMS-RH-SENSIBILISATION-001	Training completion	LMS; HR	Per course	3 years
ISMS-RH-SENSIBILISATION-001	Simulation results	Phishing platform; engineering	Semi-annual	3 years

DOCUMENT	RECORD	SYSTEM / OWNER	FREQUENCY	RETENTION
ISMS-RH-SENSIBILISATION-001	Programme review	ISMS workspace; ISMS manager	Annual	3 years
ISMS-RH-CHARTE-001	Signed charter acceptance	HR system; HR	Joining / on change	Employment + 3 years
ISMS-RH-CHARTE-001	Breach cases	HR case system; HR	Per case	As law allows
ISMS-RH-TELETRAVAIL-001	Remote-work declaration	HR system; HR	Joining / annual	Employment + 3 years
ISMS-RH-TELETRAVAIL-001	MDM compliance report	MDM; IT operations	Monthly	3 years
ISMS-RH-TELETRAVAIL-001	Foreign-working approvals	Ticket system; line managers	Per case	3 years
ISMS-RH-MOBILE-001	Enrolment and compliance report	MDM; IT operations	Monthly	3 years
ISMS-RH-MOBILE-001	Wipe actions	MDM and ticket; service desk	Per event	3 years
ISMS-RH-MOBILE-001	BYOD approvals	Ticket system; line manager	Per device	Device life + 1 year
ISMS-PHY-ZONES-001	Zone register and plans	ISMS workspace; facility manager	Annual / on change	3 years
ISMS-PHY-ZONES-001	Access-control logs and reviews	Access system; facility management	Quarterly review	12 months logs; 3 years reviews
ISMS-PHY-ZONES-001	Visitor log	Visitor system; reception	Daily	12 months
ISMS-PHY-ZONES-001	Fire, UPS and climate test records	Facility files; facility manager	Annual	6 years
ISMS-PHY-ZONES-001	Spot-check results	ISMS workspace; reviewer	Quarterly	3 years
ISMS-PHY-SUPPORTS-001	Media register	Asset tool; IT operations	Per media	Life + 3 years
ISMS-PHY-SUPPORTS-001	Destruction certificates	Procurement files; facility manager	Per batch	6 years
ISMS-PHY-SUPPORTS-001	C3 copy register	Document control; document owners	Per copy	6 years
ISMS-PRA-PCA-001	BIA and RTO/RPO table	BCM workspace; BCM manager	Annual	6 years
ISMS-PRA-PCA-001	Continuity plans	Document system; BCM manager	Annual	6 years
ISMS-PRA-PCA-001	Review and update log	BCM workspace; BCM manager	Annual	3 years
ISMS-PRA-PRA-001	DR runbooks	Document system; service owners	Annual	3 years
ISMS-PRA-PRA-001	DR test reports	BCM workspace; IT manager	Annual	6 years
ISMS-PRA-PRA-001	Corrective actions	Ticket system; IT manager	Per test	3 years
ISMS-PRA-TESTS-001	Test plan	BCM workspace; BCM manager	Annual	3 years
ISMS-PRA-TESTS-001	Test reports	BCM workspace; BCM manager	Per test	6 years
ISMS-PRA-TESTS-001	Corrective actions	Ticket system; owners	Per test	3 years
ISMS-IAM-POLITIQUE-001	Role catalogue	IAM tool; IAM owner	Semi-annual	3 years
ISMS-IAM-POLITIQUE-001	Access approvals	Ticket / IAM system; data owners	Per request	3 years
ISMS-IAM-POLITIQUE-001	Account inventory with exceptions	IAM tool; IAM owner	Monthly	3 years
ISMS-IAM-CYCLE-001	Account tickets	Ticket system; service desk	Per event	3 years
ISMS-IAM-CYCLE-001	Service account register	IAM tool; technical owners	Quarterly	Life + 1 year
ISMS-IAM-CYCLE-001	Dormancy report	IAM tool; IAM engineering	Monthly	3 years
ISMS-IAM-CYCLE-001	Break-glass reviews	SIEM and ticket; CISO	Per use	3 years

DOCUMENT	RECORD	SYSTEM / OWNER	FREQUENCY	RETENTION
ISMS-IAM-AUTH-001	Authentication policy configuration	IdP console; IAM engineering	Quarterly	3 years
ISMS-IAM-AUTH-001	MFA coverage report	IdP; IAM engineering	Monthly	3 years
ISMS-IAM-AUTH-001	Reset requests	Ticket system; service desk	Per event	1 year
ISMS-IAM-PRIV-001	Privileged account inventory	PAM/IAM tool; IAM engineering	Monthly	3 years
ISMS-IAM-PRIV-001	Session recordings and reviews	PAM tool; security officer	Monthly	12 months recordings; 3 years reviews
ISMS-IAM-PRIV-001	Recertification	IAM tool; system owners	Quarterly	3 years
ISMS-IAM-REVUE-001	Review campaigns	IAM tool; IAM owner	Quarterly / semi-annual	3 years
ISMS-IAM-REVUE-001	Revocation tickets	Ticket system; service desk	Per removal	3 years
ISMS-IAM-REVUE-001	Population reconciliation	IAM tool; IAM engineering	Per campaign	3 years
ISMS-FOU-POLITIQUE-001	Supplier register	Procurement system; procurement	Continuous	Contract + 6 years
ISMS-FOU-POLITIQUE-001	Due-diligence files	Supplier repository; supplier manager	Annual	Contract + 6 years
ISMS-FOU-POLITIQUE-001	Contracts and clauses	Contract system; legal	Per contract	Contract + 10 years
ISMS-FOU-POLITIQUE-001	Exit evidence	Supplier files; service owner	Per exit	6 years
ISMS-CON-CONFORMITE-001	Legal and contractual register	Compliance tool; compliance officer	Annual	6 years
ISMS-CON-CONFORMITE-001	Compliance assessments	Compliance workspace; officer	Annual	6 years
ISMS-CON-CONFORMITE-001	Licence register	Asset tool; IT	Quarterly	Life + 3 years
ISMS-CLI-FICHE-001	Approved fact sheet	Document system; CISO	Per version	6 years
ISMS-CLI-FICHE-001	Evidence index	ISMS workspace; ISMS manager	Per version	6 years
ISMS-CLI-FICHE-001	Distribution log	CRM; account manager	Per release	3 years
ISMS-CLI-QUESTIONNAIRE-001	Answer base	ISMS workspace; ISMS manager	Annual	3 years
ISMS-CLI-QUESTIONNAIRE-001	Response log	CRM; account manager	Per response	6 years
ISMS-CLI-QUESTIONNAIRE-001	Approvals	Document system; CISO	Per response	6 years
ISMS-CLI-ANNEXE-001	Standard annex	Contract system; legal	Annual	Contract + 10 years
ISMS-CLI-ANNEXE-001	Signed annexes	Contract system; legal	Per contract	Contract + 10 years
ISMS-CLI-ANNEXE-001	Deviations	Contract system; legal	Per contract	Contract + 10 years
ISMS-CLI-INCIDENT-001	Notification matrix	Document system; ISMS manager	Semi-annual	3 years
ISMS-CLI-INCIDENT-001	Notifications sent	Incident system; incident manager	Per incident	Contract + 6 years
ISMS-CLI-INCIDENT-001	Final reports	Incident system; CISO	Per incident	Contract + 6 years
ISMS-INF-HEB-002	Data location register	CMDB; cloud owner	Semi-annual	Life + 3 years
ISMS-INF-HEB-002	Verification results	Cloud console; engineering	Semi-annual	3 years
ISMS-INF-HEB-002	Customer notifications	CRM; account manager	Per change	Contract + 3 years
ISMS-FOU-CHARTE-001	Requirements document	Document system; ISMS manager	Annual	6 years

DOCUMENT	RECORD	SYSTEM / OWNER	FREQUENCY	RETENTION
ISMS-FOU-CHARTE-001	Declarations	Supplier files; supplier manager	Annual	Contract + 6 years
ISMS-FOU-CHARTE-001	Corrective plans	Supplier files; supplier manager	Per case	Contract + 3 years
ISMS-RGP-DPA-001	DPA template	Contract system; DPO	Annual	Contract + 10 years
ISMS-RGP-DPA-001	Signed DPAs	Contract system; legal	Per contract	Contract + 10 years
ISMS-RGP-DPA-001	TOMs annex	ISMS workspace; ISMS manager	Annual	Contract + 6 years
ISMS-RH-NDA-001	NDA register	Contract system; legal	Continuous	Expiry + 6 years
ISMS-RH-NDA-001	Signed NDAs	Contract system; legal	Per NDA	Expiry + 6 years
ISMS-RH-CHARTE-002	Signed charters	HR/contract system; sponsor	Per contractor	Contract + 3 years
ISMS-RH-CHARTE-002	Contractor access list	IAM tool; IAM owner	Monthly	3 years
ISMS-PUB-CONFIANCE-001	Claim-evidence table	ISMS workspace; ISMS manager	Quarterly	3 years
ISMS-PUB-CONFIANCE-001	Publication approvals	Document system; CISO	Per change	3 years
ISMS-AUD-FIELDWORK-001	Readiness plan	ISMS workspace; ISMS manager	Per assessment	6 years
ISMS-AUD-FIELDWORK-001	Interview schedule and briefings	ISMS workspace; ISMS manager	Per assessment	3 years
ISMS-AUD-FIELDWORK-001	Request log	Audit portal; point of contact	Daily during fieldwork	6 years
ISMS-AUD-FIELDWORK-001	Walk-through report	ISMS workspace; ISMS manager	Per site	3 years
ISMS-AUD-SAMPLE-001	Population register	ISMS workspace; ISMS manager	Per cycle	3 years
ISMS-AUD-SAMPLE-001	Sample selection and test sheets	Audit tool; reviewers	Per test	3 years
ISMS-AUD-SAMPLE-001	Deviation analysis	Audit tool; ISMS manager	Per test	3 years
ISMS-AUD-MATURITY-001	Maturity scoring sheet	ISMS workspace; ISMS manager	Annual	3 years
ISMS-AUD-MATURITY-001	Challenge notes	ISMS workspace; reviewer	Annual	3 years
ISMS-AUD-MATURITY-001	Operating-cycle evidence	Per control system	Per cycle	3 years
ISMS-AUD-CLOSURE-001	Finding register	Audit tool; ISMS manager	Continuous	6 years
ISMS-AUD-CLOSURE-001	Root-cause analyses	Audit tool; owners	Per finding	6 years
ISMS-AUD-CLOSURE-001	Verification evidence	Audit tool; reviewer	Per finding	6 years
ISMS-AUD-CLOSURE-001	Escalation log	ISMS workspace; ISMS manager	Weekly	3 years
ISMS-ORG-SOA-001	Statement of applicability	ISMS workspace; ISMS manager	Annual / on change	6 years
ISMS-ORG-SOA-001	Exclusion approvals	Document system; top management	Per exclusion	6 years
ISMS-ORG-SOA-001	Edition and order record	ENX portal; ISMS manager	Per assessment	6 years
ISMS-ORG-INTERFACES-001	Interface register	ISMS workspace; ISMS manager	Quarterly	3 years
ISMS-ORG-INTERFACES-001	Validation evidence	Supplier files; supplier manager	Annual	3 years

DOCUMENT	RECORD	SYSTEM / OWNER	FREQUENCY	RETENTION
ISMS-ORG-INTERFACES-001	Walk-through reports	ISMS workspace; reviewer	Annual	3 years
ISMS-ORG-ATTEST-001	Attestations	ISMS workspace; control owners	Semi-annual	3 years
ISMS-ORG-ATTEST-001	Challenge tests	Audit tool; reviewer	Semi-annual	3 years
ISMS-ORG-ATTEST-001	Summary	Management review; CISO	Semi-annual	6 years
ISMS-FOU-ASSURANCE-002	Supplier dossiers	Supplier repository; supplier manager	Annual	Contract + 6 years
ISMS-FOU-ASSURANCE-002	Validity checks	Supplier repository; supplier manager	Quarterly	3 years
ISMS-FOU-ASSURANCE-002	Supplier audits	Audit tool; reviewer	Per audit	Contract + 6 years
ISMS-INC-EXERCISE-001	Exercise plan and scripts	ISMS workspace; ISMS manager	Annual	3 years
ISMS-INC-EXERCISE-001	After-action reports	ISMS workspace; facilitator	Per exercise	6 years
ISMS-INC-EXERCISE-001	Action log	Ticket system; ISMS manager	Per exercise	3 years
ISMS-AUD-EVIDENCE-001	Evidence register	ISMS workspace; ISMS manager	Per item	6 years
ISMS-AUD-EVIDENCE-001	Data-room access logs	Data-room platform; ISMS manager	Continuous	12 months
ISMS-AUD-EVIDENCE-001	Redaction approvals	Document system; DPO	Per release	6 years
ISMS-CLI-DIFFUSION-001	Disclosure log	CRM; account manager	Per request	3 years
ISMS-CLI-DIFFUSION-001	Approvals and NDAs	Document system; CISO	Per release	6 years
ISMS-CLI-DIFFUSION-001	Data-room access logs	Data-room platform; ISMS manager	Continuous	12 months
ISMS-CLI-TISAX-001	Portal extract and review	ENX portal; ISMS manager	Quarterly	6 years
ISMS-CLI-TISAX-001	Sharing log	ENX portal and CRM; ISMS manager	Per share	6 years
ISMS-CLI-TISAX-001	Label expiry calendar	ISMS workspace; ISMS manager	Quarterly	Until superseded + 3 years
ISMS-CLI-SECURITE-002	Questionnaire and score	Supplier repository; supplier manager	Per supplier	Contract + 6 years
ISMS-CLI-SECURITE-002	Evidence copies	Supplier repository; supplier manager	Per supplier	Contract + 6 years
ISMS-CLI-SECURITE-002	Corrective plans	Supplier repository; supplier manager	Per gap	Contract + 3 years
ISMS-ORG-DOC-001	Document register	Document system; ISMS manager	Continuous	Life + 6 years
ISMS-ORG-DOC-001	Approval records	Document system; approvers	Per version	6 years
ISMS-ORG-DOC-001	Overdue review report	ISMS workspace; ISMS manager	Monthly	3 years
ISMS-ORG-OBJECTIFS-001	Objectives register	ISMS workspace; ISMS manager	Annual	6 years
ISMS-ORG-OBJECTIFS-001	Quarterly results	ISMS dashboard; ISMS manager	Quarterly	3 years
ISMS-ORG-OBJECTIFS-001	Actions	Ticket system; owners	Per miss	3 years
ISMS-ORG-GOUVERNANCE-001	Minutes	Document system; ISMS manager	Quarterly	6 years
ISMS-ORG-GOUVERNANCE-001	Decision log	ISMS workspace; ISMS manager	Quarterly	6 years
ISMS-ORG-GOUVERNANCE-001	Attendance	Minutes; ISMS manager	Quarterly	3 years

DOCUMENT	RECORD	SYSTEM / OWNER	FREQUENCY	RETENTION
ISMS-ORG-SITES-001	Site assessments	ISMS workspace; reviewer	Annual	3 years
ISMS-ORG-SITES-001	Quarterly reports	ISMS workspace; contacts	Quarterly	3 years
ISMS-ORG-SITES-001	Site contact list	Document system; ISMS manager	Semi-annual	3 years
ISMS-ORG-ISA-001	ISA matrix	ISMS workspace; ISMS manager	Quarterly	6 years
ISMS-ORG-ISA-001	Reconciliation record	ISMS workspace; reviewer	Annual	3 years
ISMS-ORG-ISA-001	ISA change log	ISMS workspace; ISMS manager	Per change	3 years
ISMS-RSK-REGISTRE-001	Risk register	Risk tool; risk coordinator	Quarterly	6 years
ISMS-RSK-REGISTRE-001	Acceptances	Document system; top management	Per decision	6 years
ISMS-RSK-REGISTRE-001	Review minutes	Meeting minutes; coordinator	Quarterly	3 years
ISMS-RSK-TRAITEMENT-001	Treatment plan	Risk tool; ISMS manager	Monthly	6 years
ISMS-RSK-TRAITEMENT-001	Verification notes	Risk tool; reviewer	Per action	6 years
ISMS-RSK-TRAITEMENT-001	Approval	Document system; top management	Annual	6 years
ISMS-ACT-FLUX-001	Data-flow maps	Document system; architect	On change / annual	Life + 3 years
ISMS-ACT-FLUX-001	Flow register	CMDB; architect	Quarterly	Life + 3 years
ISMS-ACT-FLUX-001	Validation	ISMS workspace; engineering	Annual	3 years
ISMS-ACT-TRANSFERT-001	Channel matrix	Document system; architect	Annual	3 years
ISMS-ACT-TRANSFERT-001	Transfer logs	MFT/DLP; IT operations	Continuous	12 months
ISMS-ACT-TRANSFERT-001	Misdirection incidents	Incident system; analyst	Per event	3 years
ISMS-ACT-CONSERVATION-001	Retention schedule	Document system; compliance officer	Annual	6 years
ISMS-ACT-CONSERVATION-001	Destruction records	ITSM; IT operations	Per event	6 years
ISMS-ACT-CONSERVATION-001	Legal holds	Legal files; legal	Per hold	Hold + 6 years
ISMS-ORG-MENACES-001	Threat log	ISMS workspace; analyst	Weekly	3 years
ISMS-ORG-MENACES-001	Assessments	Ticket system; analyst	Per item	3 years
ISMS-ORG-MENACES-001	Quarterly summary	Document system; CISO	Quarterly	3 years
ISMS-ORG-ECARTS-001	Nonconformity register	Audit tool; ISMS manager	Continuous	6 years
ISMS-ORG-ECARTS-001	Root-cause analyses	Audit tool; owners	Per case	6 years
ISMS-ORG-ECARTS-001	Verification	Audit tool; reviewer	Per case	6 years
ISMS-CLI-ENGAGEMENTS-001	Commitment register	ISMS workspace; contract manager	Continuous	Contract + 6 years
ISMS-CLI-ENGAGEMENTS-001	Verification records	ISMS workspace; owners	Semi-annual	3 years
ISMS-CLI-ENGAGEMENTS-001	Escalations	Ticket system; ISMS manager	Per case	3 years
ISMS-ORG-CONTROLES-001	Test plan	ISMS workspace; ISMS manager	Annual	3 years
ISMS-ORG-CONTROLES-001	Test sheets	Audit tool; reviewers	Per test	3 years

DOCUMENT	RECORD	SYSTEM / OWNER	FREQUENCY	RETENTION
ISMS-ORG-CONTROLES-001	Test report	ISMS workspace; ISMS manager	Quarterly	6 years
ISMS-INC-PRESERVATION-001	Collection and hash records	Evidence vault; responder	Per incident	Case + 6 years
ISMS-INC-PRESERVATION-001	Chain of custody	Evidence vault; custodian	Per item	Case + 6 years
ISMS-INC-PRESERVATION-001	Retainer	Contract system; legal	Annual	Contract + 6 years
ISMS-RH-TIERS-001	External worker register	HR / vendor system; sponsor	Continuous	Contract + 3 years
ISMS-RH-TIERS-001	Monthly reviews	IAM tool; sponsors	Monthly	3 years
ISMS-RH-TIERS-001	Exit checklists	Ticket system; sponsor	Per exit	3 years
ISMS-RH-POSTES-001	Sensitive role list	ISMS workspace; ISMS manager	Annual	3 years
ISMS-RH-POSTES-001	Screening results	HR system; HR	Per hire	Employment + 1 year
ISMS-RH-POSTES-001	SoD matrix	IAM tool; IAM owner	Semi-annual	3 years
ISMS-RH-FORMATION-001	Curriculum	ISMS workspace; ISMS manager	Annual	3 years
ISMS-RH-FORMATION-001	Completion records	LMS; HR	Per course	3 years
ISMS-RH-FORMATION-001	Competence assessment	HR system; line managers	Annual	3 years
ISMS-RH-DEPLACEMENTS-001	Travel approvals	Ticket system; line managers	Per trip	3 years
ISMS-RH-DEPLACEMENTS-001	Device preparation	ITSM; IT operations	Per trip	3 years
ISMS-RH-DEPLACEMENTS-001	Post-trip inspection	ITSM; IT operations	Per trip	3 years
ISMS-PHY-BADGES-001	Issue and block records	Access system; facility management	Continuous	12 months
ISMS-PHY-BADGES-001	Quarterly reviews	Access system; zone owners	Quarterly	3 years
ISMS-PHY-BADGES-001	Admin logs	Access system; facility management	Monthly	12 months
ISMS-PHY-VISITEURS-001	Visitor log	Visitor system; reception	Daily	12 months
ISMS-PHY-VISITEURS-001	Contractor authorisations	Facility system; facility management	Per contract	Contract + 1 year
ISMS-PHY-VISITEURS-001	Log reviews	ISMS workspace; security officer	Monthly	3 years
ISMS-PHY-ENV-001	Environmental assessment	Facility files; facility manager	Per 2 years	10 years
ISMS-PHY-ENV-001	Inspection and test records	Facility files; facility management	Annual	6 years
ISMS-PHY-ENV-001	Monitoring alarms	Monitoring tool; IT operations	Continuous	12 months
ISMS-PHY-MATERIEL-001	Removal log	Asset tool; asset owner	Per event	3 years
ISMS-PHY-MATERIEL-001	Sanitisation records	ITSM; IT operations	Per event	3 years
ISMS-PHY-MATERIEL-001	Transport records	Logistics files; logistics	Per event	3 years
ISMS-PHY-INSPECTIONS-001	Inspection reports	ISMS workspace; security officer	Quarterly	3 years
ISMS-PHY-INSPECTIONS-001	Findings register	Audit tool; security officer	Continuous	3 years
ISMS-PHY-INSPECTIONS-001	Alarm tests	Facility files; facility management	Semi-annual	3 years

DOCUMENT	RECORD	SYSTEM / OWNER	FREQUENCY	RETENTION
ISMS-IAM-PRIV-002	Elevation records	PAM tool; security engineering	Per elevation	3 years
ISMS-IAM-PRIV-002	Session recordings	PAM tool; security engineering	Continuous	12 months
ISMS-IAM-PRIV-002	Review notes	ISMS workspace; security officer	Monthly	3 years
ISMS-IAM-SERVICE-001	Identity register	IAM tool; IAM owner	Continuous	Life + 1 year
ISMS-IAM-SERVICE-001	Rotation logs	Vault; platform engineering	Per rotation	12 months
ISMS-IAM-SERVICE-001	Reviews	IAM tool; owners	Semi-annual	3 years
ISMS-IAM-TIERS-001	Third-party access list	IAM tool; IAM owner	Monthly	3 years
ISMS-IAM-TIERS-001	Session logs	Bastion/PAM; security engineering	Continuous	12 months
ISMS-IAM-TIERS-001	Acknowledgements	Supplier files; supplier manager	Per supplier	Contract + 3 years
ISMS-IAM-DISTANT-001	Remote access logs	VPN/ZTNA; network engineering	Continuous	12 months
ISMS-IAM-DISTANT-001	Link register	CMDB; network engineering	Semi-annual	Life + 3 years
ISMS-IAM-DISTANT-001	Exposure scans	Scanner; security engineering	Weekly	12 months
ISMS-IAM-URGENCE-001	Break-glass register	IAM tool; IAM owner	Quarterly	3 years
ISMS-IAM-URGENCE-001	Use records and reviews	Ticket and SIEM; security officer	Per use	3 years
ISMS-IAM-URGENCE-001	Quarterly tests	IAM tool; engineering	Quarterly	3 years
ISMS-IAM-FEDERATION-001	Application and trust register	IdP; IAM owner	Quarterly	Life + 1 year
ISMS-IAM-FEDERATION-001	Provisioning logs	IdP; IAM engineering	Continuous	12 months
ISMS-IAM-FEDERATION-001	Role reviews	IAM tool; owners	Semi-annual	3 years
ISMS-OPS-ARCHI-001	Principles	Document system; architect	Annual	3 years
ISMS-OPS-ARCHI-001	Diagrams	Document system; architects	On change	Life + 3 years
ISMS-OPS-ARCHI-001	Review records	Project portal; architect	Per review	6 years
ISMS-OPS-CMDB-001	CMDB export	CMDB; CMDB owner	Monthly	3 years
ISMS-OPS-CMDB-001	Reconciliation	CMDB; engineering	Monthly	3 years
ISMS-OPS-CMDB-001	Quality report	CMDB; owner	Quarterly	3 years
ISMS-OPS-EOL-001	EOL report	CMDB; CMDB owner	Quarterly	3 years
ISMS-OPS-EOL-001	Exceptions	Exception register; CISO	Per exception	Life + 3 years
ISMS-OPS-EOL-001	Replacement plans	Project portal; service owners	Per item	3 years
ISMS-OPS-ENDPOINT-001	Compliance report	MDM / management console; engineering	Monthly	12 months
ISMS-OPS-ENDPOINT-001	Image versions	Repository; engineering	On change	3 years
ISMS-OPS-ENDPOINT-001	Admin rights report	IAM tool; engineering	Quarterly	3 years
ISMS-OPS-EMAIL-001	DMARC reports	Mail platform; engineering	Monthly	12 months
ISMS-OPS-EMAIL-001	Tenant configuration baseline	Admin console; engineering	Quarterly	3 years
ISMS-OPS-EMAIL-001	Phish reports	SOC; SOC	Per report	12 months
ISMS-OPS-EXPO-001	External inventory	Discovery tool; engineering	Monthly	12 months
ISMS-OPS-EXPO-001	Scan reports	Scanner; engineering	Weekly	12 months
ISMS-OPS-EXPO-001	Pen test	Document system; CISO	Annual	6 years
ISMS-OPS-SEGMENT-001	Segment register	CMDB; network engineering	On change	Life + 3 years
ISMS-OPS-SEGMENT-001	Rule reviews	Firewall manager; owners	Semi-annual	3 years
ISMS-OPS-SEGMENT-001	Segmentation tests	Document system; security engineering	Annual	6 years

DOCUMENT	RECORD	SYSTEM / OWNER	FREQUENCY	RETENTION
ISMS-OPS-WIFI-001	Controller config	Controller; network engineering	Quarterly	3 years
ISMS-OPS-WIFI-001	Rogue AP reports	WIPS; security engineering	Weekly	12 months
ISMS-OPS-WIFI-001	Guest logs	Controller; network engineering	Continuous	6 months
ISMS-OPS-SIEM-001	Use-case catalogue	SIEM; detection engineer	Quarterly	3 years
ISMS-OPS-SIEM-001	Alert records	SIEM/ticket; SOC	Per alert	12 months
ISMS-OPS-SIEM-001	Detection tests	ISMS workspace; engineering	Annual	3 years
ISMS-OPS-TEMPS-001	Time configuration	Config repository; infrastructure	Quarterly	3 years
ISMS-OPS-TEMPS-001	Drift reports	Monitoring; security engineering	Weekly	12 months
ISMS-OPS-TEMPS-001	Change records	ITSM; IT operations	Per change	3 years
ISMS-OPS-RESTORE-001	Runbooks	Document system; service owners	Annual	3 years
ISMS-OPS-RESTORE-001	Test reports	ITSM; administrator	Quarterly	3 years
ISMS-OPS-RESTORE-001	Metrics	Backup tool; administrator	Per test	3 years
ISMS-OPS-BACKUP-002	Immutability configuration	Backup tool; administrator	Quarterly	3 years
ISMS-OPS-BACKUP-002	Isolation test	ISMS workspace; engineering	Annual	3 years
ISMS-OPS-BACKUP-002	Admin account list	IAM tool; IAM owner	Quarterly	3 years
ISMS-OPS-SECRETS-001	Vault inventory	Vault; platform security	Quarterly	3 years
ISMS-OPS-SECRETS-001	Rotation logs	Vault; platform security	Continuous	12 months
ISMS-OPS-SECRETS-001	Secret scan results	Scanner; security engineering	Per scan	12 months
ISMS-OPS-CONFIG-001	Compliance reports	Compliance tool; security engineering	Weekly / monthly	12 months
ISMS-OPS-CONFIG-001	Drift tickets	ITSM; admins	Per drift	3 years
ISMS-OPS-CONFIG-001	Reconciliation	ITSM; change manager	Monthly	3 years
ISMS-OPS-PENTEST-001	Programme	ISMS workspace; CISO	Annual	3 years
ISMS-OPS-PENTEST-001	Reports	Document system; CISO	Per test	6 years
ISMS-OPS-PENTEST-001	Retest evidence	ITSM; security engineering	Per finding	3 years
ISMS-OPS-OUTILS-001	Tool inventory	CMDB; platform security	Quarterly	3 years
ISMS-OPS-OUTILS-001	Vendor session records	Bastion/PAM; platform security	Per session	12 months
ISMS-OPS-OUTILS-001	Detections	EDR; SOC	Per alert	12 months
ISMS-OPS-DLP-001	DLP policies	DLP console; security engineering	Quarterly	3 years
ISMS-OPS-DLP-001	Alert records	DLP/ticket; SOC	Per alert	12 months
ISMS-OPS-DLP-001	Test results	ISMS workspace; engineering	Quarterly	3 years
ISMS-OPS-SUPPRESSION-001	Erasure certificates	ITSM; IT operations	Per event	6 years
ISMS-OPS-SUPPRESSION-001	Provider confirmations	Supplier files; supplier manager	Per exit	6 years
ISMS-OPS-SUPPRESSION-001	Verification samples	ISMS workspace; reviewer	Quarterly	3 years
ISMS-OPS-CLOUD-002	Cloud reviews	Supplier files; cloud owner	Annual	3 years
ISMS-OPS-CLOUD-002	Exit plans	Document system; service owners	Annual	Life + 3 years
ISMS-OPS-CLOUD-002	Exit tests	ISMS workspace; owners	Biennial	3 years
ISMS-DEV-RELEASE-001	Release records	CI/CD; release manager	Per release	3 years
ISMS-DEV-RELEASE-001	Approvals	CI/CD; release manager	Per release	3 years
ISMS-DEV-RELEASE-001	Pipeline access review	IAM tool; platform	Quarterly	3 years
ISMS-DEV-TESTS-001	Test results	CI/CD; engineering	Per build	12 months
ISMS-DEV-TESTS-001	Findings	Tracker; security engineering	Per finding	3 years

DOCUMENT	RECORD	SYSTEM / OWNER	FREQUENCY	RETENTION
ISMS-DEV-TESTS-001	Exceptions	Exception register; CISO	Per exception	Life + 3 years
ISMS-DEV-EXTERNE-001	Requirements in contracts	Contract system; procurement	Per contract	Contract + 10 years
ISMS-DEV-EXTERNE-001	Evidence and SBOM	Supplier files; supplier manager	Per release	Product life + 3 years
ISMS-DEV-EXTERNE-001	Acceptance records	Project portal; service owner	Per delivery	6 years
ISMS-FOU-REGISTRE-001	Supplier register	Procurement system; procurement	Continuous	Contract + 6 years
ISMS-FOU-REGISTRE-001	Tier reviews	Supplier files; supplier manager	Annual	3 years
ISMS-FOU-REGISTRE-001	Reconciliation	ISMS workspace; reviewer	Semi-annual	3 years
ISMS-FOU-EVALUATION-001	Due-diligence files	Supplier repository; supplier manager	Per supplier	Contract + 6 years
ISMS-FOU-EVALUATION-001	Label checks	ENX portal; supplier manager	Per supplier	Contract + 3 years
ISMS-FOU-EVALUATION-001	Approvals	Document system; CISO	Per supplier	Contract + 6 years
ISMS-FOU-SUIVI-001	Review records	Supplier files; supplier manager	Annual / quarterly	Contract + 3 years
ISMS-FOU-SUIVI-001	Expiry tracker	Supplier files; supplier manager	Quarterly	Until superseded
ISMS-FOU-SUIVI-001	Corrective plans	Supplier files; supplier manager	Per issue	Contract + 3 years
ISMS-FOU-SOUS-TRAITANCE-001	Declarations	Supplier files; supplier manager	Annual	Contract + 3 years
ISMS-FOU-SOUS-TRAITANCE-001	Chain maps	Supplier files; supplier manager	Annual	Contract + 3 years
ISMS-FOU-SOUS-TRAITANCE-001	Approvals	Document system; CISO	Per change	Contract + 6 years
ISMS-FOU-SORTIE-001	Exit checklists	Supplier files; service owner	Per exit	6 years
ISMS-FOU-SORTIE-001	Deletion confirmations	Supplier files; supplier manager	Per exit	6 years
ISMS-FOU-SORTIE-001	IAM removals	IAM tool; IAM owner	Per exit	3 years
ISMS-FOU-INCIDENT-001	Supplier incident tickets	Incident system; incident manager	Per incident	6 years
ISMS-FOU-INCIDENT-001	Reports from suppliers	Supplier files; supplier manager	Per incident	6 years
ISMS-FOU-INCIDENT-001	Contact verification	Supplier files; supplier manager	Semi-annual	3 years
ISMS-CON-VEILLE-001	Watch log	ISMS workspace; compliance officer	Continuous	6 years
ISMS-CON-VEILLE-001	Impact analyses	ISMS workspace; ISMS manager	Per change	6 years
ISMS-CON-VEILLE-001	Reports	Document system; CISO	Quarterly	6 years
ISMS-CON-DONNEES-001	Obligations register	ISMS workspace; compliance officer	Quarterly	Contract + 6 years
ISMS-CON-DONNEES-001	Briefing records	HR system; managers	Per project	3 years
ISMS-CON-DONNEES-001	Return and destruction records	Document system; owners	Per contract	6 years
ISMS-CON-RETENTION-001	Schedule	Document system; ISMS manager	Annual	6 years
ISMS-CON-RETENTION-001	Retrieval tests	ISMS workspace; reviewer	Semi-annual	3 years
ISMS-CON-RETENTION-001	Disposal records	ITSM; IT operations	Per event	6 years

DOCUMENT	RECORD	SYSTEM / OWNER	FREQUENCY	RETENTION
ISMS-CON-CONTROLES-001	Test plan and results	ISMS workspace; reviewer	Annual	Contract + 6 years
ISMS-CON-CONTROLES-001	Escalations	Ticket system; ISMS manager	Per failure	6 years
ISMS-CON-CONTROLES-001	Customer audit log	ISMS workspace; CISO	Per audit	Contract + 6 years
ISMS-ORG-AI-001	Approved list and assessments	ISMS workspace; architect	Per service	Life + 3 years
ISMS-ORG-AI-001	Usage logs	Platform; IT operations	Continuous	12 months
ISMS-ORG-AI-001	Training	LMS; HR	Annual	3 years
ISMS-PRO-GOUV-001	Requirements register	ISMS workspace; prototype manager	Per project	Contract + 6 years
ISMS-PRO-GOUV-001	Authorised-persons list	Access system; prototype manager	Monthly	Project + 3 years
ISMS-PRO-GOUV-001	Briefing records	HR system; prototype manager	Per person	Project + 3 years
ISMS-PRO-ZONES-001	Access and alarm logs	Access system; facility	Continuous	12 months
ISMS-PRO-ZONES-001	Quarterly reviews	ISMS workspace; prototype manager	Quarterly	3 years
ISMS-PRO-ZONES-001	Inspection reports	ISMS workspace; security officer	Quarterly	3 years
ISMS-PRO-TRACABILITE-001	Prototype register	Tracking system; custodian	Continuous	Contract + 6 years
ISMS-PRO-TRACABILITE-001	Movement logs	Tracking system; custodian	Per movement	Contract + 6 years
ISMS-PRO-TRACABILITE-001	Reconciliations	ISMS workspace; custodian	Monthly	3 years
ISMS-PRO-TRANSPORT-001	Transport plans	Logistics system; logistics	Per shipment	Contract + 3 years
ISMS-PRO-TRANSPORT-001	Tracking and seal logs	Carrier; logistics	Per shipment	Contract + 3 years
ISMS-PRO-TRANSPORT-001	Handover records	Tracking system; custodians	Per shipment	Contract + 6 years
ISMS-PRO-IMAGE-001	Approvals	ISMS workspace; prototype manager	Per request	Project + 3 years
ISMS-PRO-IMAGE-001	Image log	Protected repository; photographer	Per image	Project + 3 years
ISMS-PRO-IMAGE-001	Checks	ISMS workspace; security officer	Quarterly	3 years
ISMS-PRO-DESTRUCTION-001	Disposition records	Tracking system; prototype manager	Per item	Contract + 6 years
ISMS-PRO-DESTRUCTION-001	Destruction certificates	Document system; prototype manager	Per batch	Contract + 6 years
ISMS-PRO-DESTRUCTION-001	Provider audits	Supplier files; supplier manager	Annual	3 years
ISMS-PRO-VEHICULES-001	Trial plans	Project portal; trial manager	Per trial	Contract + 3 years
ISMS-PRO-VEHICULES-001	Parking and custody log	Tracking system; trial manager	Per trial	Contract + 3 years
ISMS-PRO-VEHICULES-001	Briefings	HR system; trial manager	Per driver	Project + 3 years
ISMS-PRO-RECON-001	Reconciliation records	Tracking system; reviewer	Monthly	Contract + 6 years
ISMS-PRO-RECON-001	Incident files	Incident system; incident manager	Per case	Contract + 6 years
ISMS-PRO-RECON-001	Customer notifications	Document system; CISO	Per case	Contract + 6 years

DOCUMENT	RECORD	SYSTEM / OWNER	FREQUENCY	RETENTION
ISMS-RGP-REGISTRE-001	Processing register	Privacy tool; DPO	Continuous	Life + 3 years
ISMS-RGP-REGISTRE-001	Review log	Privacy tool; DPO	Annual	3 years
ISMS-RGP-REGISTRE-001	Processor records	Privacy tool; DPO	Continuous	Life + 3 years
ISMS-RGP-PIA-001	Screenings	Privacy tool; DPO	Per project	Processing life + 3 years
ISMS-RGP-PIA-001	DPIAs	Privacy tool; DPO	Per processing	Processing life + 3 years
ISMS-RGP-PIA-001	Approvals	Document system; top management	Per DPIA	Processing life + 3 years
ISMS-RGP-DROITS-001	Request log	Privacy tool; DPO	Per request	3 years
ISMS-RGP-DROITS-001	Response records	Privacy tool; DPO	Per request	3 years
ISMS-RGP-DROITS-001	Annual report	Document system; DPO	Annual	3 years
ISMS-RGP-VIOLATION-001	Breach register	Privacy tool; DPO	Per breach	6 years
ISMS-RGP-VIOLATION-001	Notifications	Document system; DPO	Per breach	6 years
ISMS-RGP-VIOLATION-001	Assessments	Privacy tool; DPO	Per breach	6 years
ISMS-RGP-TRANSFERTS-001	Transfer register	Privacy tool; DPO	Quarterly	Life + 3 years
ISMS-RGP-TRANSFERTS-001	Assessments	Privacy tool; DPO	Per transfer	Life + 3 years
ISMS-RGP-TRANSFERTS-001	Measure evidence	Config; IT operations	Annual	3 years
ISMS-RGP-RETENTION-001	Retention schedule	Privacy tool; DPO	Annual	3 years
ISMS-RGP-RETENTION-001	Deletion logs	Systems; IT operations	Per run	12 months
ISMS-RGP-RETENTION-001	Verification	ISMS workspace; reviewer	Quarterly	3 years
ISMS-OT-INVENTAIRE-001	OT inventory	OT asset tool; OT engineering	Continuous	Life + 3 years
ISMS-OT-INVENTAIRE-001	Discovery reports	OT monitoring; OT security	Monthly	12 months
ISMS-OT-INVENTAIRE-001	Reconciliation	ISMS workspace; reviewer	Semi-annual	3 years
ISMS-OT-ZONES-001	Zone and conduit documents	Document system; OT architect	On change	Life + 3 years
ISMS-OT-ZONES-001	Firewall rule reviews	Firewall manager; network	Semi-annual	3 years
ISMS-OT-ZONES-001	Segmentation tests	Document system; security engineering	Annual	6 years
ISMS-OT-ACCES-001	Session approvals	Ticket system; plant owner	Per session	3 years
ISMS-OT-ACCES-001	Session recordings	Gateway; OT security	Per session	12 months
ISMS-OT-ACCES-001	Contracts	Supplier files; supplier manager	Per vendor	Contract + 6 years
ISMS-OT-CORRECTIFS-001	Assessment log	OT tool; OT security	Continuous	3 years
ISMS-OT-CORRECTIFS-001	Patch records	Change system; OT engineering	Per patch	3 years
ISMS-OT-CORRECTIFS-001	Exceptions	Exception register; CISO	Per exception	Life + 3 years
ISMS-OT-CHANGES-001	Change records	OT change system; OT engineering	Per change	6 years

DOCUMENT	RECORD	SYSTEM / OWNER	FREQUENCY	RETENTION
ISMS-OT-CHANGES-001	Configuration backups	OT repository; OT engineering	Per change	Life + 3 years
ISMS-OT-CHANGES-001	Comparison reports	OT tool; OT security	Monthly	12 months
ISMS-OT-PRA-001	OT backup inventory	OT repository; OT engineering	Quarterly	Life + 3 years
ISMS-OT-PRA-001	Test reports	BCM workspace; OT engineering	Annual	6 years
ISMS-OT-PRA-001	Degraded procedures	Document system; plant manager	Annual	3 years
ISMS-OT-FOURNISSEURS-001	Contract clauses	Contract system; procurement	Per contract	Contract + 10 years
ISMS-OT-FOURNISSEURS-001	Evidence	Supplier files; supplier manager	Per supplier	Contract + 6 years
ISMS-OT-FOURNISSEURS-001	Acceptance	Project portal; plant owner	Per delivery	Life + 3 years
ISMS-OT-IEC62443-001	Applicability decision	Document system; CISO	Annual	6 years
ISMS-OT-IEC62443-001	Gap register	ISMS workspace; OT architect	Annual	3 years
ISMS-OT-IEC62443-001	Action log	Ticket system; OT security	Per gap	3 years
ISMS-OT-SESSION-002	Release records	Ticket; security operator	Per session	3 years
ISMS-OT-SESSION-002	Recordings	Gateway; OT security	Per session	12 months
ISMS-OT-SESSION-002	Review notes	ISMS workspace; OT security	Monthly	3 years
ISMS-ORG-CONTEXTE-001	Context and interested-party register	ISMS workspace; ISMS manager	Annual / on change	6 years
ISMS-ORG-CONTEXTE-001	Review minutes	Document system; CISO	Annual	6 years
ISMS-ORG-CONTEXTE-001	Traceability links	ISMS workspace; ISMS manager	Annual	3 years
ISMS-RH-DISCIPLINE-001	Disciplinary case files	HR case system; HR	Per case	As law allows
ISMS-RH-DISCIPLINE-001	Decision records	HR case system; line managers	Per case	As law allows
ISMS-RH-DISCIPLINE-001	Anonymised annual report	Document system; CISO	Annual	3 years
ISMS-RH-ANTECEDENTS-001	Screening level matrix	Document system; HR	Annual	3 years
ISMS-RH-ANTECEDENTS-001	Screening outcomes	HR system; HR	Per person	Employment + 1 year
ISMS-RH-ANTECEDENTS-001	Clearance register	HR system; HR	Continuous	Clearance + 1 year
ISMS-OPS-LOGICIELS-001	Software catalogue	CMDB; IT operations	Continuous	Life + 3 years
ISMS-OPS-LOGICIELS-001	Request and assessment tickets	ITSM; security analyst	Per request	3 years
ISMS-OPS-LOGICIELS-001	Discovery reports	Endpoint tool; engineering	Monthly	12 months
ISMS-OPS-ENVIRONNEMENTS-001	Environment register	CMDB; platform engineering	Quarterly	Life + 3 years
ISMS-OPS-ENVIRONNEMENTS-001	Test data approvals	Ticket system; data owners	Per request	3 years
ISMS-OPS-ENVIRONNEMENTS-001	Separation tests	ISMS workspace; security engineering	Annual	3 years
ISMS-PHY-BUREAU-001	Spot-check reports	ISMS workspace; security officer	Quarterly	3 years
ISMS-PHY-BUREAU-001	Printer and lock policy exports	Device console; IT operations	Quarterly	3 years
ISMS-PHY-BUREAU-001	Corrective tickets	Ticket system; department heads	Per finding	3 years
ISMS-OPS-PURVIEW-001	Configuration exports	Tenant export; security engineering	Quarterly	3 years

DOCUMENT	RECORD	SYSTEM / OWNER	FREQUENCY	RETENTION
ISMS-OPS-PURVIEW-001	Policy test records	ISMS workspace; security engineering	Per change	3 years
ISMS-OPS-PURVIEW-001	Change tickets	ITSM; security engineering	Per change	3 years
ISMS-ORG-AUTORITES-001	Contact register	Document system; ISMS manager	Semi-annual	3 years
ISMS-ORG-AUTORITES-001	Verification records	ISMS workspace; ISMS manager	Semi-annual	3 years
ISMS-ORG-AUTORITES-001	Case contact logs	Incident system; incident manager	Per incident	6 years
ISMS-ORG-COMMUNICATION-001	Communication matrix	Document system; ISMS manager	Annual	3 years
ISMS-ORG-COMMUNICATION-001	Distribution logs	Intranet and mail system; communications	Per message	12 months
ISMS-ORG-COMMUNICATION-001	Metrics reports	ISMS workspace; ISMS manager	Quarterly	3 years
ISMS-OPS-CAPACITES-001	Capacity indicators and thresholds	Monitoring tool; IT operations	Annual	3 years
ISMS-OPS-CAPACITES-001	Capacity forecasts	ISMS workspace; service owners	Quarterly	3 years
ISMS-OPS-CAPACITES-001	Capacity incidents and reviews	ITSM; IT operations	Per incident	3 years

5 Auditor question bank

Prepare a primary and a deputy interviewee per question; both must give the same account.

ISMS-OPS-VULN-001 — Vulnerability and patch management

- Show me how you know the scanner sees every in-scope asset. Who reconciles it and when was the last time something was found missing?
- Pick a critical finding from the last quarter: when was it detected, who triaged it, when was it fixed and who verified it?
- How do you handle a vulnerability that cannot be patched? Show me the register and one example with its compensating control.
- Which systems are end-of-life today and how are they isolated?
- How do you test systems you must not scan, such as OT or prototype equipment?
- What happened the last time a critical advisory was published for software you run?

ISMS-CRY-POLITIQUE-001 — Cryptography, keys and certificates

- How are your keys protected and who can access them?
- Show me the certificate inventory and next expiries.
- What encryption protects backups?

ISMS-OPS-CHANGES-001 — IT change management

- Pick a recent change: show request, test, approval, implementation, review.
- How do you detect unauthorised changes?
- How do you separate test and production data?

ISMS-OPS-DURCISSEMENT-001 — Secure configuration and hardening

- Which benchmark do you use and how do you measure compliance?
- Show me a deviation and how it was approved.
- How do you build a new server?

ISMS-OPS-MALWARE-001 — Malware protection

- How do you know every server has protection?
- Show me the last malware detection and response.
- How are non-agent systems protected?

ISMS-OPS-JOURNAUX-001 — Security logging and monitoring

- Show me what you log for privileged access and where it is stored.
- What happens if someone deletes a log?
- Show me a detection and how you followed it.

ISMS-OPS-SAUVEGARDE-001 — Backup and restoration policy

- Show me a restore test and how long it took.
- What protects your backups from ransomware?
- How are backups encrypted?

ISMS-OPS-RESEAU-001 — Network security policy

- Explain how the prototype or customer segment is separated.
- Show me the last firewall rule review.
- How is remote access secured?

ISMS-OPS-CLOUD-001 — Cloud services security policy

- Where does C3 data reside in the cloud and who can access it?
- Show me how you assessed your last cloud provider.
- What is your exit plan?

ISMS-DEV-SDLC-001 — Secure procurement and development lifecycle

- Show me how a security requirement flows into tests.
- What blocks a release with a critical vulnerability?
- How do you handle secrets in code?

ISMS-POL-SSI-002 — Full information security policy

- Where is your current approved policy and who approved it?
- How do you know every employee has read it? Show me the data.
- How does top management steer the ISMS beyond signing the policy?
- Show me one change to the policy and how it was communicated.

ISMS-POL-SSI-001 — Shareable information security policy

- Is this the same policy you work to internally?
- Who approved it for external publication?
- How do you ensure customers get the current version?

ISMS-ORG-PERIMETRE-001 — ISMS scope and boundaries

- Walk me through your scope. What is explicitly outside and why?
- Where does your data leave the scope and who protects it there?
- Show that every site in the ENX portal is in your register.
- What changed since the last assessment?

ISMS-ORG-ROLES-001 — Information security roles and RACI

- Who is accountable for information security at top-management level?
- Who stands in when the CISO is absent?
- Show me a segregation-of-duties conflict and how you handled it.

ISMS-ORG-DEROGATIONS-001 — Security exceptions management

- How many exceptions are active? Show me the register.
- Show an exception that expired. What happened?
- Who may approve a high-risk exception?

ISMS-ACT-CLASSIF-001 — Information classification and handling

- Show me a C3 document and tell me who can read it and how that is enforced.
- How do you handle a customer's own marking?
- How do you detect mislabelled data?

ISMS-ACT-INVENTAIRE-001 — Asset management and inventory

- How do you know your inventory is complete?
- Pick a server and show me owner, classification and patch state.
- How are cloud and personal devices captured?

ISMS-RSK-METHODE-001 — Information security risk methodology

- How did you decide which risks to accept?
- Show me how a new threat entered the register.
- Who is the risk owner for your prototype data?

ISMS-PRJ-SECURITE-001 — Security in projects

- Show me a recent project and its security approvals.
- How are security requirements derived?
- What happens if a project wants to go live without approval?

ISMS-AUD-PROGRAMME-001 — Internal audit, self-assessment and management review

- Show me last year's audit programme and what was actually audited.
- Who audits the ISMS manager's work?
- Which decision did management take from the last review?

ISMS-INC-PROC-001 — Information security incident management

- Walk me through your last incident from detection to review.
- How do staff know how to report?
- How did you decide whether to notify the customer?
- When did you last exercise this?

ISMS-INC-CRISE-001 — Crisis management and communications

- Who can declare a crisis and how fast can the team assemble?

- How would you communicate if email was down?
- Show me what you learned from your last exercise.

ISMS-CLI-EXIGENCES-001 — Customer information security requirements

- How do you know what your customers require?
- Show me one customer requirement and the control that meets it.
- How do you flow requirements to suppliers?

ISMS-RH-CYCLE-001 — Employee joiner-mover-leaver lifecycle

- Pick three leavers: show the leaving date, account disable time and asset return.
- How do you screen people who handle prototypes?
- How do you detect that a person changed role and kept old access?

ISMS-RH-SENSIBILISATION-001 — Security awareness and training programme

- Show completion rates for the last cycle and what you did about laggards.
- What training do your administrators get?
- Ask any employee: how do you report an incident?

ISMS-RH-CHARTE-001 — Employee IT acceptable-use charter

- Show me an employee's acceptance record.
- What may staff not do with customer data?
- How are breaches handled?

ISMS-RH-TELETRAVAIL-001 — Remote and mobile work policy

- How do you protect a laptop with C3 data lost in a train?
- How do you know staff at home use a secure network?
- Can someone work from abroad? Show me an approval.

ISMS-RH-MOBILE-001 — Mobile device and BYOD controls

- How do you stop an unmanaged phone from reading mail?
- Show me a non-compliant device and what happened.
- What may BYOD users store?

ISMS-PHY-ZONES-001 — Physical security zones and premises

- Walk us to the server room: who can enter and how do you know who entered last week?
- Show the zone plan and what is allowed in each zone.
- How do you handle a visitor who needs to enter a restricted area?
- Show the last UPS and fire test.

ISMS-PHY-SUPPORTS-001 — Physical media handling and disposal

- Show me the destruction certificate for the last retired disk.
- How do you transport backup media?
- How do you stop USB data copying?

ISMS-PRA-PCA-001 — Business impact analysis and continuity plan

- What is the maximum downtime of your most critical process and who agreed it?
- Where is the plan if systems are down?
- How are customers' availability needs considered?

ISMS-PRA-PRA-001 — IT disaster recovery plan

- Show me the last DR test and recovery time against RTO.
- What if your cloud region fails?
- What are your single points of failure?

ISMS-PRA-TESTS-001 — Business continuity, recovery and restore tests

- Which tests did you run last year and what failed?
- How do you know your backups can be restored?
- Show me the corrective action from the last test.

ISMS-IAM-POLITIQUE-001 — Identity and access management policy

- Pick a user and tell me who approved each of their rights.

- Do you have shared accounts? Show the register.
- How do you manage external users?

ISMS-IAM-CYCLE-001 — User account lifecycle management

- Show me service accounts and their owners.
- How many dormant accounts do you have?
- How is break-glass use monitored?

ISMS-IAM-AUTH-001 — Authentication and multi-factor authentication

- Show me MFA coverage: who is exempt and why?
- How do you verify the user for a password reset?
- Which legacy protocols remain enabled?

ISMS-IAM-PRIV-001 — Privileged and administrative access

- How many administrators do you have and who reviews their activity?
- Show me one privileged session and its review.
- How do you protect admin workstations?

ISMS-IAM-REVUE-001 — Periodic access certification

- Show last campaign and the number of rights removed.
- Who reviews privileged access?
- How do you ensure the review list was complete?

ISMS-FOU-POLITIQUE-001 — Supplier security management policy

- Which of your suppliers can see C3 data and how did you assess them?
- Show me a supplier whose assessment found gaps.
- How do you check a supplier's TISAX label?

ISMS-CON-CONFORMITE-001 — Legal, regulatory and contractual compliance

- How do you know which laws apply to you?
- Show me how a new regulation was handled.
- How do you manage open-source licences?

ISMS-CLI-FICHE-001 — Customer security fact sheet

- Where does each statement come from?
- How do you keep it aligned with the TISAX portal?
- Who approved it?

ISMS-CLI-QUESTIONNAIRE-001 — Approved customer security responses

- How do you ensure answers are accurate?
- Show me an answer and its evidence.
- Who may sign a questionnaire?

ISMS-CLI-ANNEXE-001 — Customer contractual security annex

- Which obligations do you owe a given customer and who is responsible?
- How are deviations approved?
- Where are signed annexes stored?

ISMS-CLI-INCIDENT-001 — Customer incident notification procedure

- What is the shortest notification duty you have and how do you meet it?
- Show a notification you sent.
- Who decides to notify?

ISMS-INF-HEB-002 — Customer-facing data-location statement

- Prove that data stays in the stated region.
- Who can access from outside?
- How do you notify location changes?

ISMS-FOU-CHARTE-001 — Supplier security requirements

- How do you ensure suppliers know your requirements?
- Show a declaration.

- What happens when a supplier fails?

ISMS-RGP-DPA-001 — Data processing agreement template

- Show me the TOMs and the controls behind them.
- How do you handle a subprocessor change?
- Which processors do you use?

ISMS-RH-NDA-001 — Confidentiality agreement template

- Show an NDA signed before a disclosure.
- How do you track expiry?
- Who can sign?

ISMS-RH-CHARTE-002 — IT acceptable-use charter for contractors

- Who sponsors each contractor?
- How is access ended?
- Which devices do contractors use?

ISMS-PUB-CONFIANCE-001 — Public security trust page

- Which claims on your page can you prove?
- Who approves changes?
- How does it match the portal?

ISMS-AUD-FIELDWORK-001 — AL3 assessment fieldwork and on-site readiness plan

- Who will we speak to for each control and are they available?
- Show the staged evidence for a control we pick.
- Take us to the server room and one restricted area now.

ISMS-AUD-SAMPLE-001 — Audit evidence population and sampling standard

- How did you select this sample and how do you know the population was complete?
- Show a deviation you found yourselves.
- Can I extract the list from the system myself?

ISMS-AUD-MATURITY-001 — ISA maturity assessment and sustained-operation test

- How did you score this control and who challenged it?
- What proves that it has run for more than one cycle?
- What did you do about controls scoring below 3?

ISMS-AUD-CLOSURE-001 — Assessment finding remediation and independent closure testing

- Show a finding from last year and its closure evidence.
- Who verified closure?
- How do you stop recurrence?

ISMS-ORG-SOA-001 — Control applicability and documented rationale statement

- Why is this control not applicable?
- Show where this control is implemented.
- Which ISA edition applies to your order?

ISMS-ORG-INTERFACES-001 — Cross-site shared control and handoff assurance

- Who is responsible for this control at the other site?
- How do you know the provider performs it?
- Show me a handoff test.

ISMS-ORG-ATTEST-001 — Control owner attestation and independent challenge

- Who attests that this control works and what do they base it on?
- Show a challenged attestation.
- What happens if the attestation is wrong?

ISMS-FOU-ASSURANCE-002 — High-risk supplier assurance dossier and evidence validity

- Show evidence that this supplier's TISAX label covers the service you use.
- What is the validity of that evidence?
- What did your last supplier audit find?

ISMS-INC-EXERCISE-001 — Cyber crisis tabletop and decision exercise programme

- What scenario did you exercise and what changed afterwards?
- Who participated?
- How were notification decisions tested?

ISMS-AUD-EVIDENCE-001 — Evidence chain of custody, minimisation and secure disclosure

- How do you ensure what you gave us is authentic?
- Who saw this evidence?
- How do you protect customer data in evidence?

ISMS-CLI-DIFFUSION-001 — Security-evidence disclosure procedure

- How do you decide what a customer may see?
- Show the log for the last disclosure.
- How do you retract access afterwards?

ISMS-CLI-TISAX-001 — TISAX assessment-result sharing procedure

- How is your portal scope kept consistent with reality?
- Who may share your result?
- When does your label expire and what is the plan?

ISMS-CLI-SECURITE-002 — Supplier qualification questionnaire

- How do you tier suppliers and what do you ask each tier?
- Show a scored questionnaire and what you did with the gaps.
- How do you verify answers?

ISMS-ORG-DOC-001 — ISMS document control

- How do you know staff use the current version?
- Show a document change and who approved it.
- Where are drafts kept?

ISMS-ORG-OBJECTIFS-001 — Security objectives and metrics

- Which objectives did you set and how did you perform?
- Show a missed objective and the action.
- Who sees these results?

ISMS-ORG-GOUVERNANCE-001 — Security steering committee and decisions

- Show recent minutes and decisions.
- How does top management steer security?
- How are decisions followed up?

ISMS-ORG-SITES-001 — Multi-site security operating model

- How do you ensure every site follows the same rules?
- Show a site assessment.
- Who is responsible locally?

ISMS-ORG-ISA-001 — VDA ISA coverage and applicability matrix

- How do you know all ISA controls are covered?
- Show the evidence behind one control.
- Which ISA version do you use?

ISMS-RSK-REGISTRE-001 — Information security risk register

- Show your top five risks and treatment.
- How did a recent incident change the register?
- Who accepted this risk?

ISMS-RSK-TRAITEMENT-001 — Risk treatment plan

- Show a risk you treated and how you verified it.
- Who approved the plan?
- What is overdue?

ISMS-ACT-FLUX-001 — Information-flow and data-flow maps

- Show where customer data flows from receipt to deletion.
- How do you detect an undocumented flow?
- Who approves an external flow?

ISMS-ACT-TRANSFERT-001 — Secure information exchange and transfer

- How do you send C3 files to a customer?
- Show a transfer log.
- What if the wrong person received data?

ISMS-ACT-CONSERVATION-001 — Information retention and destruction

- How do you delete data after a contract ends?
- Show a destruction record.
- How do you handle legal holds?

ISMS-ORG-MENACES-001 — Threat intelligence and risk context

- How do you learn about threats that matter to you?
- Show a recent threat and what changed.
- Who sees it?

ISMS-ORG-ECARTS-001 — Nonconformity and corrective action

- Show a nonconformity from record to verified closure.
- How do you spot recurring issues?
- Who verifies?

ISMS-CLI-ENGAGEMENTS-001 — Register of customer security commitments

- List the commitments you made to this customer and show evidence.
- What if you cannot meet one?
- Who signs them off?

ISMS-ORG-CONTROLES-001 — Internal security control testing plan

- Show a test you did on this control and the result.
- Who tested?
- What changed afterwards?

ISMS-INC-PRESERVATION-001 — Incident evidence collection and preservation

- How would you preserve a compromised server?
- Show a custody record.
- Who may access evidence?

ISMS-RH-TIERS-001 — External workforce security management

- How many contractors have access and who sponsors each?
- Show an exit.
- How do you screen them?

ISMS-RH-POSTES-001 — Sensitive roles and segregation of duties

- Which roles are sensitive and why?
- Show a segregation conflict.
- How is dual control enforced?

ISMS-RH-FORMATION-001 — Role-based training curriculum

- What training do your administrators receive?
- Show completion data.
- How is competence checked?

ISMS-RH-DEPLACEMENTS-001 — Travel and off-site equipment use

- How do you prepare a laptop for a high-risk country?
- Show an approval.
- What if a device is confiscated?

ISMS-PHY-BADGES-001 — Physical access badge management

- Show badge rights for a restricted zone and who reviewed them.
- What happens if a badge is lost?
- Who administers the system?

ISMS-PHY-VISITEURS-001 — Visitor and on-site contractor procedures

- What happens when a visitor arrives?
- Show last month's log review.
- How do you handle maintenance staff?

ISMS-PHY-ENV-001 — Environmental and facilities risk controls

- When did you last test the UPS and generator?
- What happens if the server room overheats?
- Show the fire suppression certificate.

ISMS-PHY-MATERIEL-001 — Equipment maintenance, transport and removal

- How do you handle a broken disk sent to the vendor?
- Show a removal log.
- How do you guard against tampering?

ISMS-PHY-INSPECTIONS-001 — Periodic premises inspections

- Show your last inspection and what you fixed.
- Do you inspect outside working hours?
- How do you test alarms?

ISMS-IAM-PRIV-002 — Privileged access management (PAM/PIM)

- Show a PAM elevation and its recording.
- What standing privilege remains?
- Who administers PAM?

ISMS-IAM-SERVICE-001 — Service, API and machine identities

- How many service accounts exist and who owns them?
- Show a rotation.
- How do you find unused identities?

ISMS-IAM-TIERS-001 — Third-party and supplier access control

- Who at suppliers can access C3 systems?
- How do you see what they do?
- How do you end access?

ISMS-IAM-DISTANT-001 — Remote access and interconnections

- How do remote users connect and how do you verify the device?
- List partner links.
- How do you detect misuse?

ISMS-IAM-URGENCE-001 — Emergency break-glass access

- How many break-glass accounts exist and where are they?
- Show the last use.
- How are you alerted?

ISMS-IAM-FEDERATION-001 — Single sign-on, federation and SaaS access

- Which applications do not use SSO and why?
- How are leavers removed from SaaS?
- Who approves a new federation?

ISMS-OPS-ARCHI-001 — Security architecture and technical diagrams

- Explain how a request moves from the internet to your C3 data.
- Show last review.
- Where are your single points of failure?

ISMS-OPS-CMDB-001 — Systems and software configuration register

- How do you keep the CMDB accurate?
- Show a CI and its dependencies.
- Who owns it?

ISMS-OPS-EOL-001 — End-of-life technologies and exceptions

- Which systems are end of life?
- How are they protected?
- Show a replacement plan.

ISMS-OPS-ENDPOINT-001 — Endpoint and server security baseline

- How do you know laptops are encrypted?
- What happens to a non-compliant device?
- Show patch status.

ISMS-OPS-EMAIL-001 — Messaging and collaboration protection

- Show DMARC status.
- How do you stop auto-forwarding?
- How are phishing reports handled?

ISMS-OPS-EXPO-001 — Internet-facing service security

- How do you know all your internet exposure?
- Show an unknown service you found.
- Where are admin interfaces?

ISMS-OPS-SEGMENT-001 — Network segmentation and firewall rule register

- Show rules between user and C3 zones.
- When was it last tested?
- Who owns this rule?

ISMS-OPS-WIFI-001 — Wi-Fi and guest network security

- How is guest Wi-Fi separated?
- How do you detect rogue access points?
- Which Wi-Fi is allowed in the server area?

ISMS-OPS-SIEM-001 — Security detection and SOC use cases

- Show a detection from alert to response.
- How do you test rules?
- Who watches at night?

ISMS-OPS-TEMPS-001 — Clock synchronization and forensic time quality

- How do you ensure logs have trustworthy time?
- Show drift monitoring.
- Which sources do you use?

ISMS-OPS-RESTORE-001 — Detailed restoration operating procedures

- Restore this server now and show timing.
- What was the last failure?
- How do you test immutable backups?

ISMS-OPS-BACKUP-002 — Tamper-resistant and isolated backups

- Could an attacker with domain admin delete your backups?
- Show immutable settings.
- Where are keys?

ISMS-OPS-SECRETS-001 — Secrets vault and key rotation

- Where are your secrets stored?
- Show a rotation.
- What if a secret appears in code?

ISMS-OPS-CONFIG-001 — Continuous configuration compliance

- Show drift detection and remediation.
- How are untracked changes found?
- Who receives reports?

ISMS-OPS-PENTEST-001 — Penetration testing programme

- Show your last penetration test and how you closed findings.
- Who tested and how were they selected?
- How do you test C3 systems safely?

ISMS-OPS-OUTILS-001 — Administrative tooling and remote maintenance security

- How do vendors perform remote maintenance?
- Show a recorded session.
- Which admin tools exist?

ISMS-OPS-DLP-001 — Data loss prevention and external sharing

- How do you stop a C3 file leaving by email?
- Show a DLP alert.
- How do you test DLP?

ISMS-OPS-SUPPRESSION-001 — Secure logical data and system erasure

- How do you erase a server disk?
- Show a certificate.
- How do you confirm cloud deletion?

ISMS-OPS-CLOUD-002 — Cloud posture review and service exit

- How would you leave this provider?
- Show your latest review.
- What if the provider fails?

ISMS-DEV-RELEASE-001 — Secure releases and CI/CD

- Walk me from commit to production.
- Who can change the pipeline?
- How do you roll back?

ISMS-DEV-TESTS-001 — Application security verification

- What do you test before release?
- Show a blocked release.
- How do you test authorisation?

ISMS-DEV-EXTERNE-001 — Third-party software and solution acquisition

- How do you assure software you buy?
- Show security clauses.
- How do you learn of supplier vulnerabilities?

ISMS-FOU-REGISTRE-001 — Supplier register and criticality

- Show your critical suppliers and why they are critical.
- How do you know the register is complete?
- What changed this year?

ISMS-FOU-EVALUATION-001 — Supplier security due diligence

- Show due diligence done before contract.
- How do you check a supplier's TISAX label?
- What did you do about gaps?

ISMS-FOU-SUIVI-001 — Ongoing supplier security assurance

- What did you learn from the last supplier review?
- How do you know a supplier's label is still valid?
- Show a corrective plan.

ISMS-FOU-SOUS-TRAITANCE-001 — Subcontractor chain and external information flows

- Who are your suppliers' subcontractors?
- How do customers approve them?
- Show a change.

ISMS-FOU-SORTIE-001 — Supplier exit and reversibility

- Show an exit and deletion proof.
- How do you get your data back?
- Who removes access?

ISMS-FOU-INCIDENT-001 — Supplier alerts and incident management

- What happens when a supplier reports a breach?
- Show last case.
- Do your contracts set notification times?

ISMS-CON-VEILLE-001 — Legal and standards watch

- How do you hear about ISA changes?
- Show a change you assessed.
- Who is responsible?

ISMS-CON-DONNEES-001 — Confidentiality obligations management

- What are you obliged to keep confidential and for whom?
- How do staff know?
- Show a return or destruction.

ISMS-CON-RETENTION-001 — Audit record retention and archiving

- Retrieve audit records for last year.
- How do you protect archives?
- How long do you keep incident records?

ISMS-CON-CONTROLES-001 — Contractual compliance testing

- How do you check you meet this customer clause?
- Show a failed test.
- How do you host a customer audit?

ISMS-ORG-AI-001 — AI services and sensitive-information security handling

- Which AI tools are allowed and why?
- How do you prevent C3 uploads?
- Show an assessment.

ISMS-PRO-GOUV-001 — Prototype security governance and customer requirements

- Who is responsible for prototype protection?
- Show the list of authorised persons for this project.
- How did you translate the customer requirements?

ISMS-PRO-ZONES-001 — Prototype facilities and restricted zones

- Take us to the prototype area: who can enter?
- How do you prevent photography from outside?
- Test an alarm.

ISMS-PRO-TRACABILITE-001 — Prototype lifecycle traceability

- Where is part X now and who has it?
- Show a reconciliation.
- What happens when something is missing?

ISMS-PRO-TRANSPORT-001 — Prototype secure transport and storage

- Show a recent shipment's plan and handover.
- How are carriers vetted?
- What if a stop is unplanned?

ISMS-PRO-IMAGE-001 — Prototype photography and media handling

- Who can take pictures and where do they go?
- Show approval.
- What stops staff from using a phone?

ISMS-PRO-DESTRUCTION-001 — Prototype return, destruction and recycling

- Show a destruction certificate and how it ties to items.
- Who witnessed?
- What if the customer wants a return?

ISMS-PRO-VEHICULES-001 — Protected test vehicles and trials

- How do you protect a vehicle on the road?
- Show a trial plan.
- What if it is photographed?

ISMS-PRO-RECON-001 — Prototype inventory reconciliation and missing-item response

- What do you do in the first hour after finding an item missing?
- Show a reconciliation by someone other than the custodian.
- How do you inform customers?

ISMS-RGP-REGISTRE-001 — Personal data processing records

- Show a record and its legal basis.
- How do you capture new processing?
- Who is the DPO?

ISMS-RGP-PIA-001 — Data protection impact assessment (DPIA)

- Show a DPIA and the decision.
- How do you decide a DPIA is needed?
- Who accepted residual risk?

ISMS-RGP-DROITS-001 — Data-subject rights procedure

- Show a request and your response timeline.
- How do you search all systems?
- What if you refuse?

ISMS-RGP-VIOLATION-001 — Personal data breach response

- Walk me through a breach from discovery to notification.
- How do you decide notification?
- Show the register.

ISMS-RGP-TRANSFERTS-001 — International personal data transfers

- Where does personal data go?
- Show a transfer assessment.
- How do you handle support access from abroad?

ISMS-RGP-RETENTION-001 — Personal data retention and disposal

- How long do you keep this data?
- Show a deletion log.
- What about backups?

ISMS-OT-INVENTAIRE-001 — OT and industrial asset inventory

- How do you know all OT devices?
- Show an unsupported controller and compensation.
- Who owns it?

ISMS-OT-ZONES-001 — Industrial zones and conduits architecture

- Show how IT reaches OT.
- Prove the zone separation.
- Can OT reach the internet?

ISMS-OT-ACCES-001 — Secure industrial remote maintenance

- How do vendors reach your PLCs?
- Show a recording.
- Who approves?

ISMS-OT-CORRECTIFS-001 — OT vulnerability and patch management

- How do you patch a PLC?
- Show an exception.
- Who decides on downtime?

ISMS-OT-CHANGES-001 — Industrial change management

- Show a PLC program change.
- How do you detect a rogue change?
- Who approves safety impact?

ISMS-OT-PRA-001 — Production continuity and OT recovery

- How fast can you restart this line after ransomware?
- Show a restore test.
- What do you do manually?

ISMS-OT-FOURNISSEURS-001 — OT integrator and manufacturer security

- How do you secure what an integrator delivers?
- Show clauses.
- How long will the vendor patch?

ISMS-OT-IEC62443-001 — IEC 62443 applicability and gap review

- Do you apply IEC 62443 and why?
- Show your gap register.
- How does it relate to TISAX?

ISMS-OT-SESSION-002 — OT privileged remote session release and forensic record

- Who may release an OT session and how is it recorded?
- Show a recording.
- What happens after the session?

ISMS-ORG-CONTEXTE-001 — Organisational context and interested parties

- Who are your interested parties and what do they require?
- How did the context influence your scope and risks?
- What changed since the last assessment?

ISMS-RH-DISCIPLINE-001 — Disciplinary procedure for security breaches

- What happens when someone breaches the acceptable use rules?
- Show an anonymised case and how proportionality was assessed.
- How are works council and law respected?

ISMS-RH-ANTECEDENTS-001 — Background verification and screening

- How do you screen people with access to strictly confidential information?
- Show evidence that screening preceded access for a recent hire.
- How do you handle customer clearance requirements?

ISMS-OPS-LOGICIELS-001 — Software installation and approval

- How do you ensure only approved software runs?
- Show a software request and its assessment.
- How do you find unapproved software?

ISMS-OPS-ENVIRONNEMENTS-001 — Environment separation and test data

- How are development and production separated?
- Show an approval to use production data in a test.
- Who can write to production?

ISMS-PHY-BUREAU-001 — Clean desk and screen lock

- Show your clean desk rules and the last spot check.
- What stops someone reading an unattended screen?
- How do you handle printouts?

ISMS-OPS-PURVIEW-001 — Microsoft Purview labelling and DLP configuration register

- Show me your label configuration and how it matches the classification policy.
- How did you test the DLP policy before enforcement?
- Who can change labels?

ISMS-ORG-AUTORITES-001 — Contacts with authorities and special interest groups

- Who would you call at the national CERT and when?
- When did you last verify these contacts?
- Show a real contact with an authority.

ISMS-ORG-COMMUNICATION-001 — Information security communication plan

- How do staff learn about a change of security policy?
- Show a recent security communication and its reach.
- Who may speak to customers about a security incident?

ISMS-OPS-CAPACITES-001 — Capacity and availability management

- How do you know when a critical system will run out of capacity?
- Show a forecast and the action taken.
- What happens at the critical threshold?

6 Indicator dashboard definition

Indicators to report to the ISMS meeting and management review.

DOCUMENT	INDICATOR	TARGET	ESCALATION
ISMS-OPS-VULN-001	Critical/high findings closed within deadline	≥ 95% each quarter	< 90% in a quarter: root-cause review at ISMS meeting
ISMS-OPS-VULN-001	Mean age of open critical findings	≤ 7 days	Any critical finding open beyond 30 days goes to CISO
ISMS-OPS-VULN-001	Asset coverage by authenticated scan	≥ 98% of in-scope assets	< 95%: coverage remediation plan within 14 days
ISMS-OPS-VULN-001	Open risk acceptances past expiry	0	Any expired acceptance escalates to top management
ISMS-OPS-VULN-001	Sampled closures verified independently	100% of sample	Any miss reopens the finding and the sample doubles
ISMS-CRY-POLITIQUE-001	Certificates expired in production	0	Incident
ISMS-CRY-POLITIQUE-001	C2/C3 stores encrypted	100%	Any exception via exception procedure
ISMS-CRY-POLITIQUE-001	Deprecated algorithms in use	0	Remediation plan within 30 days
ISMS-OPS-CHANGES-001	Changes with approval before implementation	100%	Any miss is an incident review
ISMS-OPS-CHANGES-001	Failed or rolled-back changes	≤ 5%	> 10%: root cause
ISMS-OPS-CHANGES-001	Emergency changes share	≤ 5%	Rising trend reviewed
ISMS-OPS-DURCISSEMENT-001	Systems compliant with baseline	≥ 95%	< 90%: remediation plan
ISMS-OPS-DURCISSEMENT-001	Critical deviations open > 30 days	0	CISO
ISMS-OPS-DURCISSEMENT-001	Systems built from approved images	100%	Rebuild
ISMS-OPS-MALWARE-001	Endpoints with healthy agent	≥ 99%	< 97%: remediation within 7 days
ISMS-OPS-MALWARE-001	High alerts triaged within 1 hour	≥ 95%	Staffing review
ISMS-OPS-MALWARE-001	Signature age > 48h	0	Investigate
ISMS-OPS-JOURNAUX-001	In-scope systems sending logs	≥ 98%	Remediate within 14 days
ISMS-OPS-JOURNAUX-001	Critical alerts handled within target	≥ 95%	Review
ISMS-OPS-JOURNAUX-001	Time drift above 1 second	0	Fix within 24 hours
ISMS-OPS-SAUVEGARDE-001	Successful backup jobs	≥ 99%	< 97%: review
ISMS-OPS-SAUVEGARDE-001	Critical systems with successful restore test in last quarter	100%	Immediate test
ISMS-OPS-SAUVEGARDE-001	Immutable copies available	100% of critical data	Remediation
ISMS-OPS-RESEAU-001	Rules with owner and review date	100%	Review within 14 days
ISMS-OPS-RESEAU-001	Overly permissive (any-any) rules	0	Immediate
ISMS-OPS-RESEAU-001	Diagrams older than 12 months	0	Update
ISMS-OPS-CLOUD-001	Cloud services registered and assessed	100%	Unregistered service blocked or assessed within 30 days
ISMS-OPS-CLOUD-001	Critical posture findings open > 14 days	0	CISO

DOCUMENT	INDICATOR	TARGET	ESCALATION
ISMS-OPS-CLOUD-001	Provider certificates in date	100%	Request evidence
ISMS-DEV-SDLC-001	Releases with completed security gates	100%	Block
ISMS-DEV-SDLC-001	Critical dependency vulnerabilities open > 14 days	0	Escalation
ISMS-DEV-SDLC-001	Developers trained in last 12 months	≥ 95%	Plan
ISMS-POL-SSI-002	Policy reviewed within 12 months	100%	Overdue by > 30 days: CISO to top management
ISMS-POL-SSI-002	Staff acknowledgement of current version	≥ 98% within 30 days of release	< 90%: HR reminder campaign
ISMS-POL-SSI-002	Objectives with measured result	100%	Unmeasured objective is a management review item
ISMS-POL-SSI-001	Channels carrying the current version	100%	Any stale copy removed within 5 working days
ISMS-POL-SSI-001	Review on time	100%	Overdue: CISO notified
ISMS-ORG-PERIMETRE-001	Scope elements with named owner	100%	Orphan element assigned within 10 days
ISMS-ORG-PERIMETRE-001	Scope review on time	100%	Overdue: CISO escalates
ISMS-ORG-PERIMETRE-001	Unreconciled assets between scope and CMDB	0	Any gap raised as ISMS action
ISMS-ORG-ROLES-001	Roles with named holder and deputy	100%	Vacancy filled or covered within 30 days
ISMS-ORG-ROLES-001	SoD conflicts without compensating control	0	CISO decision within 10 days
ISMS-ORG-DEROGATIONS-001	Expired exceptions still active	0	Immediate CISO escalation
ISMS-ORG-DEROGATIONS-001	Exceptions older than 12 months	0	Top management review
ISMS-ORG-DEROGATIONS-001	Exceptions with compensating controls tested	100%	Untested control reopens exception
ISMS-ACT-CLASSIF-001	Sampled documents correctly labelled	≥ 95%	< 90%: awareness action
ISMS-ACT-CLASSIF-001	Assets with owner-assigned classification	100%	Unclassified assets closed within 30 days
ISMS-ACT-CLASSIF-001	C3 information accessed outside named list	0	Incident procedure
ISMS-ACT-INVENTAIRE-001	Assets with complete mandatory attributes	≥ 98%	< 95%: data quality plan
ISMS-ACT-INVENTAIRE-001	Discovery exceptions open > 5 days	0	CISO notified
ISMS-ACT-INVENTAIRE-001	Assets without owner	0	Assign within 10 days
ISMS-RSK-METHODE-001	Risks with owner and treatment date	100%	Unassigned risks escalated at next meeting
ISMS-RSK-METHODE-001	High risks overdue for treatment	0	Top management review
ISMS-RSK-METHODE-001	Risk assessment within 12 months	100%	Triggers audit finding
ISMS-PRJ-SECURITE-001	Projects with completed screening	100%	Stop-work for missing screening
ISMS-PRJ-SECURITE-001	Go-lives with security approval	100%	Emergency path only with CISO sign-off
ISMS-PRJ-SECURITE-001	Security defects open at go-live	0 high	Waiver via exception procedure
ISMS-AUD-PROGRAMME-001	Planned audits delivered	100%	Slippage explained to top management
ISMS-AUD-PROGRAMME-001	Findings closed on time	≥ 90%	< 80%: management review item

DOCUMENT	INDICATOR	TARGET	ESCALATION
ISMS-AUD-PROGRAMME-001	Repeat findings	0	Root-cause analysis required
ISMS-INC-PROC-001	Events classified within 4 hours	≥ 95%	< 90%: staffing review
ISMS-INC-PROC-001	Customer notifications within contract time	100%	Any miss reported to top management
ISMS-INC-PROC-001	Post-incident reviews within 10 days	≥ 90%	Overdue list at ISMS meeting
ISMS-INC-CRISE-001	Crisis roster verified	Twice yearly	Unreachable members replaced within 5 days
ISMS-INC-CRISE-001	Exercise performed	Annual	Missed exercise is an audit finding
ISMS-CLI-EXIGENCES-001	Contracts reviewed within 10 days	100%	Escalate delay to CISO
ISMS-CLI-EXIGENCES-001	Requirements without mapped control	0	Mapped within 10 days
ISMS-RH-CYCLE-001	Leaver accounts disabled on last day	100%	Any miss is an incident review
ISMS-RH-CYCLE-001	Joiners with completed screening before access	100%	Stop access until completed
ISMS-RH-CYCLE-001	Orphan accounts found per month	0	Root-cause analysis
ISMS-RH-SENSIBILISATION-001	Annual training completion	≥ 98%	< 95%: top management notice
ISMS-RH-SENSIBILISATION-001	Phishing simulation report rate	≥ 60%	< 40%: targeted campaign
ISMS-RH-SENSIBILISATION-001	Click rate	≤ 5%	> 10%: remedial training
ISMS-RH-CHARTE-001	Staff with current acceptance	100%	Access reviewed for missing acceptance
ISMS-RH-CHARTE-001	Review on time	100%	CISO notified
ISMS-RH-TELETRAVAIL-001	Remote devices compliant with policy	≥ 98%	< 95%: access conditional block
ISMS-RH-TELETRAVAIL-001	Lost devices wiped within 4 hours of report	100%	Incident review
ISMS-RH-MOBILE-001	Mobile devices compliant	≥ 98%	< 95%: access restriction
ISMS-RH-MOBILE-001	Wipe completed within 4 hours	100%	Incident review
ISMS-PHY-ZONES-001	Restricted-zone access reviews on time	100%	Overdue review: facility manager escalation
ISMS-PHY-ZONES-001	Unescorted visitors found	0	Incident
ISMS-PHY-ZONES-001	Environmental tests in date	100%	Overdue test is a finding
ISMS-PHY-SUPPORTS-001	Media with destruction certificate	100%	Missing certificate is an incident
ISMS-PHY-SUPPORTS-001	Unauthorised removable media events	0	Investigation
ISMS-PRA-PCA-001	Critical processes with approved RTO/RPO	100%	Gaps added to risk register
ISMS-PRA-PCA-001	Plans reviewed within 12 months	100%	Overdue: CISO
ISMS-PRA-PCA-001	RTO targets supported by tested capability	≥ 90%	Gap treatment plan
ISMS-PRA-PRA-001	Critical services DR-tested in last 12 months	100%	Untested service is a finding
ISMS-PRA-PRA-001	Measured recovery time within RTO	≥ 90% of tests	Failure triggers redesign
ISMS-PRA-TESTS-001	Planned tests performed	100%	Missed test escalated
ISMS-PRA-TESTS-001	Test findings closed on time	≥ 90%	Escalation
ISMS-IAM-POLITIQUE-001	Shared accounts without exception	0	Immediate remediation

DOCUMENT	INDICATOR	TARGET	ESCALATION
ISMS-IAM-POLITIQUE-001	Access requests with documented approval	100%	Review of approver
ISMS-IAM-POLITIQUE-001	External accounts without expiry	0	Disable within 5 days
ISMS-IAM-CYCLE-001	Dormant accounts older than 90 days	0	Disable within 5 days
ISMS-IAM-CYCLE-001	Service accounts with owner	100%	Assign within 10 days
ISMS-IAM-CYCLE-001	Break-glass uses reviewed	100%	Incident
ISMS-IAM-AUTH-001	Users covered by MFA	100% in scope	Any gap blocked within 5 days
ISMS-IAM-AUTH-001	Admins with phishing-resistant MFA	≥ 90%	Plan to 100%
ISMS-IAM-AUTH-001	Legacy protocol logins	0	Investigate
ISMS-IAM-PRIV-001	Admins using separate accounts	100%	Remediation within 10 days
ISMS-IAM-PRIV-001	Privileged accounts recertified in quarter	100%	Disable unconfirmed
ISMS-IAM-PRIV-001	Standing global admins above target	0	Reduce within 14 days
ISMS-IAM-REVUE-001	Reviews completed on time	100%	Revoke unconfirmed rights
ISMS-IAM-REVUE-001	Rights removed within 5 days	100%	Escalation
ISMS-IAM-REVUE-001	Share of rights revoked per campaign	Tracked	Very low rate triggers review quality check
ISMS-FOU-POLITIQUE-001	High-tier suppliers assessed in last 12 months	100%	Overdue triggers CISO decision
ISMS-FOU-POLITIQUE-001	Suppliers with data access and signed security terms	100%	Block access
ISMS-FOU-POLITIQUE-001	Expired labels or certificates	0	Remediation request within 5 days
ISMS-CON-CONFORMITE-001	Register reviewed in 12 months	100%	Overdue: top management
ISMS-CON-CONFORMITE-001	New requirements assessed within 30 days	100%	Escalation
ISMS-CLI-FICHE-001	Statements with evidence	100%	Remove unsupported statement
ISMS-CLI-FICHE-001	Fact sheet current within 30 days of change	100%	Escalation
ISMS-CLI-QUESTIONNAIRE-001	Answers with evidence and date	100%	Remove
ISMS-CLI-QUESTIONNAIRE-001	Responses approved before release	100%	Incident
ISMS-CLI-ANNEXE-001	Signed annexes mapped to controls	100%	Mapping before delivery
ISMS-CLI-ANNEXE-001	Annex reviewed in 12 months	100%	Escalation
ISMS-CLI-INCIDENT-001	Notifications within contractual time	100%	Top management
ISMS-CLI-INCIDENT-001	Matrix contacts verified	Twice yearly	Update within 5 days
ISMS-INF-HEB-002	Statements verified in 6 months	100%	Correct
ISMS-INF-HEB-002	Unauthorised location events	0	Incident
ISMS-FOU-CHARTE-001	Suppliers with declaration in 12 months	100% of tiered	Block
ISMS-FOU-CHARTE-001	Corrective plans closed on time	≥ 90%	Escalation
ISMS-RGP-DPA-001	Processors with signed DPA	100%	Block processing
ISMS-RGP-DPA-001	TOMs updated in 12 months	100%	Escalation
ISMS-RH-NDA-001	Disclosures preceded by NDA	100%	Incident
ISMS-RH-NDA-001	NDAs expiring without review	0	Legal
ISMS-RH-CHARTE-002	Contractors with acceptance and sponsor	100%	Block access
ISMS-RH-CHARTE-002	Contractor accounts past contract end	0	Disable
ISMS-PUB-CONFIANCE-001	Claims with evidence	100%	Remove

DOCUMENT	INDICATOR	TARGET	ESCALATION
ISMS-PUB-CONFIANCE-001	Page reviewed in 90 days	100%	Escalation
ISMS-AUD-FIELDWORK-001	Controls at maturity ≥ 3 in self-assessment	100% before fieldwork	Gap plan with dates
ISMS-AUD-FIELDWORK-001	Evidence requests answered within 4 working hours	≥ 90%	Resource increase
ISMS-AUD-FIELDWORK-001	Sites walked through before assessment	100%	Do not start fieldwork
ISMS-AUD-SAMPLE-001	Controls with population defined	100%	Define before test
ISMS-AUD-SAMPLE-001	Samples with complete evidence	≥ 95%	Root-cause analysis
ISMS-AUD-SAMPLE-001	Sample deviation rate	≤ 5%	Extended sample and action
ISMS-AUD-MATURITY-001	Applicable controls scoring ≥ 3	100%	Corrective plan
ISMS-AUD-MATURITY-001	Score challenged independently	100%	Rescore
ISMS-AUD-MATURITY-001	Controls with sustained records	≥ 95%	Plan
ISMS-AUD-CLOSURE-001	Actions closed by due date	≥ 90%	< 80%: management review
ISMS-AUD-CLOSURE-001	Closures independently verified	100%	Reopen
ISMS-AUD-CLOSURE-001	Reopened findings	0	Root cause
ISMS-ORG-SOA-001	Applicable controls mapped to evidence	100%	Gap plan
ISMS-ORG-SOA-001	Exclusions approved and justified	100%	Reassess
ISMS-ORG-INTERFACES-001	Interfaces with named parties and evidence	100%	Complete in 14 days
ISMS-ORG-INTERFACES-001	Validations in date	100%	Request evidence
ISMS-ORG-ATTEST-001	Attestations received on time	100%	Escalation
ISMS-ORG-ATTEST-001	Challenged attestations confirmed	≥ 90%	Root-cause
ISMS-FOU-ASSURANCE-002	High-risk dossiers complete and valid	100%	Action in 14 days
ISMS-FOU-ASSURANCE-002	Supplier findings closed on time	≥ 90%	Escalation
ISMS-INC-EXERCISE-001	Planned exercises held	100%	Escalation
ISMS-INC-EXERCISE-001	Actions closed on time	≥ 90%	Review
ISMS-AUD-EVIDENCE-001	Evidence items in register	100%	Add
ISMS-AUD-EVIDENCE-001	Items with redaction check	100%	Incident
ISMS-AUD-EVIDENCE-001	Sharing spaces withdrawn on time	100%	Immediate
ISMS-CLI-DIFFUSION-001	Disclosures with approval before release	100%	Incident
ISMS-CLI-DIFFUSION-001	Shared spaces withdrawn on time	100%	Immediate removal
ISMS-CLI-DIFFUSION-001	Unredacted personal data findings	0	Incident review
ISMS-CLI-TISAX-001	Portal data correct at review	100%	Correct within 5 days
ISMS-CLI-TISAX-001	Reassessment ordered ≥ 6 months before expiry	100%	Top management
ISMS-CLI-TISAX-001	Result shares with CISO approval	100%	Incident

DOCUMENT	INDICATOR	TARGET	ESCALATION
ISMS-CLI-SECURITE-002	Tiered suppliers with current questionnaire	100%	Block new data sharing
ISMS-CLI-SECURITE-002	High-tier answers evidenced	100%	Reopen
ISMS-CLI-SECURITE-002	Plans closed on time	≥ 90%	Escalate
ISMS-ORG-DOC-001	Documents approved and in date	≥ 98%	Overdue list to CISO
ISMS-ORG-DOC-001	Drafts in operational use	0	Withdraw
ISMS-ORG-DOC-001	Marking errors in sample	≤ 5%	Awareness action
ISMS-ORG-OBJECTIFS-001	Objectives measured on schedule	100%	Escalate
ISMS-ORG-OBJECTIFS-001	Objectives met	≥ 80%	Analysis
ISMS-ORG-OBJECTIFS-001	Objectives with named owner	100%	Assign
ISMS-ORG-GOUVERNANCE-001	Meetings held as planned	100%	Reschedule within 14 days
ISMS-ORG-GOUVERNANCE-001	Decisions closed on time	≥ 85%	Escalate
ISMS-ORG-GOUVERNANCE-001	Top management attendance	≥ 80%	Discuss
ISMS-ORG-SITES-001	Sites assessed in 12 months	100%	Immediate plan
ISMS-ORG-SITES-001	Open site findings > 60 days	0	CISO
ISMS-ORG-SITES-001	Sites with named contact	100%	Appoint
ISMS-ORG-ISA-001	Applicable controls with evidence	100%	Plan
ISMS-ORG-ISA-001	Controls below maturity 3	0 at assessment	Corrective plan
ISMS-ORG-ISA-001	Matrix reviewed in quarter	100%	Escalate
ISMS-RSK-REGISTRE-001	Risks with owner and date	100%	Assign
ISMS-RSK-REGISTRE-001	High risks over treatment date	0	Top management
ISMS-RSK-REGISTRE-001	Register reviewed in quarter	100%	Escalate
ISMS-RSK-TRAITEMENT-001	Actions on time	≥ 85%	Escalate
ISMS-RSK-TRAITEMENT-001	Treatments verified	100%	Reopen
ISMS-RSK-TRAITEMENT-001	Overdue high-risk actions	0	Top management
ISMS-ACT-FLUX-001	C2/C3 flows mapped	100%	Map within 30 days
ISMS-ACT-FLUX-001	Unknown flows open > 5 days	0	CISO
ISMS-ACT-FLUX-001	Maps validated in 12 months	100%	Escalate
ISMS-ACT-TRANSFERT-001	Transfers via approved channels	≥ 98%	DLP follow-up
ISMS-ACT-TRANSFERT-001	Misdirected transfers	0	Incident
ISMS-ACT-TRANSFERT-001	C3 transfers logged	100%	Investigate
ISMS-ACT-CONSERVATION-001	Records beyond retention	0	Delete within 30 days
ISMS-ACT-CONSERVATION-001	Destruction certified	100%	Incident
ISMS-ACT-CONSERVATION-001	Schedule reviewed	100%	Escalate

DOCUMENT	INDICATOR	TARGET	ESCALATION
ISMS-ORG-MENACES-001	Relevant threats assessed within 5 days	≥ 90%	Staffing
ISMS-ORG-MENACES-001	Indicators checked in logs	100%	Investigate
ISMS-ORG-MENACES-001	Summaries delivered	100%	Escalate
ISMS-ORG-ECARTS-001	Actions closed on time	≥ 90%	Escalate
ISMS-ORG-ECARTS-001	Repeat nonconformities	0	Re-analysis
ISMS-ORG-ECARTS-001	Verified closures	100%	Reopen
ISMS-CLI-ENGAGEMENTS-001	Commitments with control and evidence	100%	Complete within 14 days
ISMS-CLI-ENGAGEMENTS-001	Commitments verified in 6 months	100%	Escalate
ISMS-CLI-ENGAGEMENTS-001	Unmet commitments	0	Top management
ISMS-ORG-CONTROLES-001	Planned tests completed	≥ 95%	Reschedule
ISMS-ORG-CONTROLES-001	Tests failed	Tracked	Action
ISMS-ORG-CONTROLES-001	Controls tested in 12 months	100%	Escalate
ISMS-INC-PRESERVATION-001	Items with complete custody	100%	Incident review
ISMS-INC-PRESERVATION-001	Forensic responders trained	100%	Train
ISMS-INC-PRESERVATION-001	Evidence accessed by unauthorised people	0	Incident
ISMS-RH-TIERS-001	External workers with sponsor	100%	Assign
ISMS-RH-TIERS-001	Accounts past contract end	0	Disable
ISMS-RH-TIERS-001	Training completion	≥ 98%	Reminder
ISMS-RH-POSTES-001	Sensitive-role holders screened	100%	Restrict
ISMS-RH-POSTES-001	SoD conflicts uncontrolled	0	Decision
ISMS-RH-POSTES-001	Role reviews done	100%	Escalate
ISMS-RH-FORMATION-001	Role modules completed	≥ 95%	Escalate
ISMS-RH-FORMATION-001	Test pass rate	≥ 85%	Retrain
ISMS-RH-FORMATION-001	Content updated in 12 months	100%	Review
ISMS-RH-DEPLACEMENTS-001	High-risk trips approved	100%	Incident
ISMS-RH-DEPLACEMENTS-001	Devices encrypted	100%	Block
ISMS-RH-DEPLACEMENTS-001	Losses reported within 1 hour	100%	Review
ISMS-PHY-BADGES-001	Leaver badges disabled on time	100%	Incident
ISMS-PHY-BADGES-001	Lost badges blocked within 1 hour	100%	Review
ISMS-PHY-BADGES-001	Reviews completed	100%	Revoke
ISMS-PHY-VISITEURS-001	Visitors escorted	100%	Incident
ISMS-PHY-VISITEURS-001	Visitors without badge	0	Immediate
ISMS-PHY-VISITEURS-001	Logs reviewed monthly	100%	Escalate

DOCUMENT	INDICATOR	TARGET	ESCALATION
ISMS-PHY-ENV-001	Tests in date	100%	Schedule
ISMS-PHY-ENV-001	Alarms handled within 30 min	≥ 95%	Review
ISMS-PHY-ENV-001	Critical findings open > 30 days	0	CISO
ISMS-PHY-MATERIEL-001	Removals logged	100%	Incident
ISMS-PHY-MATERIEL-001	Maintenance returns sanitised	100%	Investigate
ISMS-PHY-MATERIEL-001	Transport via approved carriers	100%	Review
ISMS-PHY-INSPECTIONS-001	Inspections done	100%	Reschedule
ISMS-PHY-INSPECTIONS-001	Findings fixed in 30 days	≥ 90%	Escalate
ISMS-PHY-INSPECTIONS-001	Out-of-hours rounds	2/year	Do
ISMS-IAM-PRIV-002	Privileged access via PAM	≥ 98%	Remediate
ISMS-IAM-PRIV-002	Standing admin accounts	Minimised	Reduce
ISMS-IAM-PRIV-002	Sessions reviewed	≥ 5%	Increase
ISMS-IAM-SERVICE-001	Identities with owner	100%	Assign
ISMS-IAM-SERVICE-001	Credentials rotated on schedule	≥ 98%	Rotate
ISMS-IAM-SERVICE-001	Static secrets in code	0	Incident
ISMS-IAM-TIERS-001	Third-party accounts with sponsor	100%	Disable
ISMS-IAM-TIERS-001	Accounts beyond contract	0	Disable
ISMS-IAM-TIERS-001	Reviews monthly	100%	Escalate
ISMS-IAM-DISTANT-001	Remote users with MFA	100%	Block
ISMS-IAM-DISTANT-001	Exposed admin interfaces	0	Immediate
ISMS-IAM-DISTANT-001	Links reviewed	100%	Escalate
ISMS-IAM-URGENCE-001	Uses reviewed within 24h	100%	Incident
ISMS-IAM-URGENCE-001	Credentials changed after use	100%	Immediate
ISMS-IAM-URGENCE-001	Quarterly tests done	100%	Escalate
ISMS-IAM-FEDERATION-001	Apps behind SSO	≥ 95%	Plan
ISMS-IAM-FEDERATION-001	Local accounts without approval	0	Remove
ISMS-IAM-FEDERATION-001	Trusts reviewed	100%	Escalate
ISMS-OPS-ARCHI-001	Diagrams current	≥ 95%	Update
ISMS-OPS-ARCHI-001	Designs reviewed	100%	Block go-live
ISMS-OPS-ARCHI-001	Diagram access violations	0	Incident
ISMS-OPS-CMDB-001	CI completeness	≥ 98%	Remediate
ISMS-OPS-CMDB-001	Reconciliation gaps open > 30 days	0	CISO
ISMS-OPS-CMDB-001	Changes with CMDB update	100%	Review
ISMS-OPS-EOL-001	Unsupported systems with exception	100%	Isolate
ISMS-OPS-EOL-001	Items ending within 12 months with plan	100%	Plan
ISMS-OPS-EOL-001	Unsupported C3 systems	0	Immediate
ISMS-OPS-ENDPOINT-001	Devices compliant	≥ 97%	Block
ISMS-OPS-ENDPOINT-001	Encrypted devices	100%	Block

DOCUMENT	INDICATOR	TARGET	ESCALATION
ISMS-OPS-ENDPOINT-001	Users with local admin	< 2%	Review
ISMS-OPS-EMAIL-001	DMARC policy enforced	100% domains	Fix
ISMS-OPS-EMAIL-001	Phish reports handled in 4 hours	≥ 95%	Review
ISMS-OPS-EMAIL-001	External sharing exceptions	Reviewed quarterly	Review
ISMS-OPS-EXPO-001	Exposed services with owner	100%	Assign
ISMS-OPS-EXPO-001	Critical exposed findings	0 open > 72h	CISO
ISMS-OPS-EXPO-001	Unknown services found	Tracked	Investigate
ISMS-OPS-SEGMENT-001	Rules with owner and review date	100%	Review
ISMS-OPS-SEGMENT-001	Any-any rules	0	Immediate
ISMS-OPS-SEGMENT-001	Segmentation tested	100% critical zones	Test
ISMS-OPS-WIFI-001	Corporate SSIDs on 802.1X	100%	Fix
ISMS-OPS-WIFI-001	Guest isolation test passed	Yes	Fix
ISMS-OPS-WIFI-001	Rogue APs open > 7 days	0	Remove
ISMS-OPS-SIEM-001	High alerts triaged in 30 min	≥ 95%	Review
ISMS-OPS-SIEM-001	Use cases tested annually	100%	Plan
ISMS-OPS-SIEM-001	False-positive rate	Tracked	Tune
ISMS-OPS-TEMPS-001	Systems synchronised	≥ 99%	Fix
ISMS-OPS-TEMPS-001	Drift over 1s	0	24h fix
ISMS-OPS-TEMPS-001	Time sources documented	100%	Document
ISMS-OPS-RESTORE-001	Critical services tested in quarter	100%	Test
ISMS-OPS-RESTORE-001	Restore within RTO	≥ 90%	Redesign
ISMS-OPS-RESTORE-001	Failed restores	0	Action
ISMS-OPS-BACKUP-002	Critical data with immutable copy	100%	Fix
ISMS-OPS-BACKUP-002	Backup admin MFA	100%	Fix
ISMS-OPS-BACKUP-002	Isolation test passed	Yes	Fix
ISMS-OPS-SECRETS-001	Secrets in vault	≥ 98%	Migrate
ISMS-OPS-SECRETS-001	Exposed secrets fixed in 24h	100%	Incident
ISMS-OPS-SECRETS-001	Rotation on schedule	≥ 95%	Fix
ISMS-OPS-CONFIG-001	Compliance rate	≥ 95%	Plan
ISMS-OPS-CONFIG-001	Critical drift open > 7 days	0	CISO
ISMS-OPS-CONFIG-001	Untracked changes	0	Investigate
ISMS-OPS-PENTEST-001	Planned tests done	100%	Escalate
ISMS-OPS-PENTEST-001	Critical findings fixed within deadline	100%	Top management
ISMS-OPS-PENTEST-001	Retested findings	100%	Retest
ISMS-OPS-OUTILS-001	Admin tools inventoried	100%	Add
ISMS-OPS-OUTILS-001	Vendor sessions recorded	100%	Incident
ISMS-OPS-OUTILS-001	Unauthorised tools found	0	Remove
ISMS-OPS-DLP-001	C3 channels covered	100%	Extend
ISMS-OPS-DLP-001	Alerts triaged in 1 day	≥ 95%	Review
ISMS-OPS-DLP-001	Tests detected	≥ 95%	Tune
ISMS-OPS-SUPPRESSION-001	Retired devices with certificate	100%	Hold device
ISMS-OPS-SUPPRESSION-001	Cloud exits confirmed	100%	Request

DOCUMENT	INDICATOR	TARGET	ESCALATION
ISMS-OPS-SUPPRESSION-001	Samples verified	100%	Re-erase
ISMS-OPS-CLOUD-002	Cloud reviews in 12 months	100%	Overdue
ISMS-OPS-CLOUD-002	Exit plans for critical services	100%	Create
ISMS-OPS-CLOUD-002	Provider changes assessed in 30 days	100%	Escalate
ISMS-DEV-RELEASE-001	Releases through pipeline	100%	Incident
ISMS-DEV-RELEASE-001	Releases with independent approval	100%	Review
ISMS-DEV-RELEASE-001	Unsigned artefacts deployed	0	Block
ISMS-DEV-TESTS-001	Releases with passed gates	100%	Block
ISMS-DEV-TESTS-001	High findings open > 14 days	0	CISO
ISMS-DEV-TESTS-001	Test coverage of critical apps	100%	Extend
ISMS-DEV-EXTERNE-001	Software acquisitions with security clauses	100%	Block
ISMS-DEV-EXTERNE-001	Suppliers with SBOM	≥ 90%	Request
ISMS-DEV-EXTERNE-001	Acceptance tests done	100%	Block
ISMS-FOU-REGISTRE-001	Suppliers with tier and owner	100%	Assign
ISMS-FOU-REGISTRE-001	Reconciliation gaps	0	Resolve in 30 days
ISMS-FOU-REGISTRE-001	Tier reviews in 12 months	100%	Escalate
ISMS-FOU-EVALUATION-001	Suppliers assessed before data sharing	100%	Block
ISMS-FOU-EVALUATION-001	High-tier files reviewed by CISO	100%	Review
ISMS-FOU-EVALUATION-001	Open critical gaps at contract	0	Do not sign
ISMS-FOU-SUIVI-001	High-tier reviews in 12 months	100%	Escalate
ISMS-FOU-SUIVI-001	Expired assurance	0	Request in 14 days
ISMS-FOU-SUIVI-001	Plans closed on time	≥ 90%	Escalate
ISMS-FOU-SOUS-TRAITANCE-001	High-tier suppliers with chain map	100%	Complete
ISMS-FOU-SOUS-TRAITANCE-001	Subcontractor changes approved before start	100%	Incident
ISMS-FOU-SOUS-TRAITANCE-001	Declarations current	100%	Request
ISMS-FOU-SORTIE-001	Exits with checklist	100%	Review
ISMS-FOU-SORTIE-001	Deletion confirmed	100%	Escalate
ISMS-FOU-SORTIE-001	Access removed on time	100%	Incident
ISMS-FOU-INCIDENT-001	Notifications within 24h	≥ 95%	Contract action
ISMS-FOU-INCIDENT-001	Actions closed on time	≥ 90%	Escalate
ISMS-FOU-INCIDENT-001	Contacts verified	100%	Update
ISMS-CON-VEILLE-001	Changes assessed within 30 days	100%	Escalate
ISMS-CON-VEILLE-001	Actions on time	≥ 90%	Review
ISMS-CON-VEILLE-001	Sources reviewed in 12 months	100%	Update
ISMS-CON-DONNEES-001	Obligations with owner	100%	Assign
ISMS-CON-DONNEES-001	Briefings on time	100%	Escalate

DOCUMENT	INDICATOR	TARGET	ESCALATION
ISMS-CON-DONNEES-001	Expired obligations handled	100%	Act
ISMS-CON-RETENTION-001	Records retrievable	100%	Fix
ISMS-CON-RETENTION-001	Retention breaches	0	Correct
ISMS-CON-RETENTION-001	Tests done	100%	Escalate
ISMS-CON-CONTROLES-001	Requirements tested	100%	Reschedule
ISMS-CON-CONTROLES-001	Failures reported on time	100%	Escalate
ISMS-CON-CONTROLES-001	Customer audits managed	100%	Review
ISMS-ORG-AI-001	AI services assessed	100%	Block
ISMS-ORG-AI-001	Uploads of C3 to unapproved AI	0	Incident
ISMS-ORG-AI-001	Staff trained	≥ 95%	Reminder
ISMS-PRO-GOUV-001	Authorised persons briefed	100%	Remove access
ISMS-PRO-GOUV-001	Projects registered before receipt	100%	Stop receipt
ISMS-PRO-GOUV-001	Deviations approved	100%	Incident
ISMS-PRO-ZONES-001	Reviews done	100%	Revoke
ISMS-PRO-ZONES-001	Alarm response test	Passed twice a year	Fix
ISMS-PRO-ZONES-001	Unauthorised devices found	0	Incident
ISMS-PRO-TRACABILITE-001	Items with complete record	100%	Fix
ISMS-PRO-TRACABILITE-001	Reconciliation done	100%	Escalate
ISMS-PRO-TRACABILITE-001	Discrepancies open > 24h	0	CISO
ISMS-PRO-TRANSPORT-001	Shipments with approved plan	100%	Stop
ISMS-PRO-TRANSPORT-001	Seals verified	100%	Incident
ISMS-PRO-TRANSPORT-001	Tracking gaps	0	Investigate
ISMS-PRO-IMAGE-001	Images with approval	100%	Incident
ISMS-PRO-IMAGE-001	Images on unapproved storage	0	Delete and investigate
ISMS-PRO-IMAGE-001	Checks done	100%	Escalate
ISMS-PRO-DESTRUCTION-001	Items with certificate	100%	Hold
ISMS-PRO-DESTRUCTION-001	Providers audited	100%	Audit
ISMS-PRO-DESTRUCTION-001	Registers closed after reconciliation	100%	Reopen
ISMS-PRO-VEHICULES-001	Trials with approved plan	100%	Stop
ISMS-PRO-VEHICULES-001	Overnight parking secured	100%	Incident
ISMS-PRO-VEHICULES-001	Drivers briefed	100%	Remove
ISMS-PRO-RECON-001	Reconciliations on time	100%	Escalate
ISMS-PRO-RECON-001	Missing items open > 24h	0	Top management
ISMS-PRO-RECON-001	Customer notified in time	100%	Review

DOCUMENT	INDICATOR	TARGET	ESCALATION
ISMS-RGP-REGISTRE-001	Processing with owner and basis	100%	Complete
ISMS-RGP-REGISTRE-001	Reviewed in 12 months	100%	Escalate
ISMS-RGP-REGISTRE-001	New processing registered before start	100%	Block
ISMS-RGP-PIA-001	New processing screened	100%	Block
ISMS-RGP-PIA-001	DPIA completed before start	100%	Stop
ISMS-RGP-PIA-001	DPIAs reviewed on time	100%	Escalate
ISMS-RGP-DROITS-001	Requests answered in time	100%	Escalate
ISMS-RGP-DROITS-001	Identity checked	100%	Review
ISMS-RGP-DROITS-001	Searches complete	100%	Fix
ISMS-RGP-VIOLATION-001	Assessments within 24h	100%	Escalate
ISMS-RGP-VIOLATION-001	Notifications in 72h	100%	Top management
ISMS-RGP-VIOLATION-001	Breaches recorded	100%	Review
ISMS-RGP-TRANSFERTS-001	Transfers with mechanism	100%	Suspend
ISMS-RGP-TRANSFERTS-001	Assessments current	100%	Update
ISMS-RGP-TRANSFERTS-001	Register reviewed	100%	Escalate
ISMS-RGP-RETENTION-001	Systems with automated deletion	≥ 90%	Plan
ISMS-RGP-RETENTION-001	Data beyond retention	0	Delete
ISMS-RGP-RETENTION-001	Samples verified	100%	Fix
ISMS-OT-INVENTAIRE-001	OT assets with owner and criticality	100%	Assign
ISMS-OT-INVENTAIRE-001	Unknown devices open > 14 days	0	CISO
ISMS-OT-INVENTAIRE-001	Reconciliation done	100%	Escalate
ISMS-OT-ZONES-001	Conduits documented	100%	Document
ISMS-OT-ZONES-001	Any-any rules in OT	0	Immediate
ISMS-OT-ZONES-001	Tests done	100%	Test
ISMS-OT-ACCES-001	Sessions with approval	100%	Incident
ISMS-OT-ACCES-001	Sessions recorded	100%	Investigate
ISMS-OT-ACCES-001	Permanent vendor access	0	Disable
ISMS-OT-CORRECTIFS-001	Assessments within 14 days	≥ 90%	Escalate
ISMS-OT-CORRECTIFS-001	Exceptions with controls	100%	Review
ISMS-OT-CORRECTIFS-001	Patch report delivered	100%	Escalate
ISMS-OT-CHANGES-001	Changes approved	100%	Incident
ISMS-OT-CHANGES-001	Backups before change	100%	Stop
ISMS-OT-CHANGES-001	Unauthorised changes	0	Investigate
ISMS-OT-PRA-001	Critical lines tested	100%	Plan

DOCUMENT	INDICATOR	TARGET	ESCALATION
ISMS-OT-PRA-001	Recovery within RTO	≥ 90%	Redesign
ISMS-OT-PRA-001	Backups restorable	100%	Fix
ISMS-OT-FOURNISSEURS-001	Contracts with security clauses	100%	Block
ISMS-OT-FOURNISSEURS-001	Evidence checked	100%	Request
ISMS-OT-FOURNISSEURS-001	Acceptance tests	100%	Block handover
ISMS-OT-IEC62443-001	Gaps with action	100%	Plan
ISMS-OT-IEC62443-001	Actions on time	≥ 85%	Escalate
ISMS-OT-IEC62443-001	Decision reviewed	100%	Escalate
ISMS-OT-SESSION-002	Sessions released by second person	100%	Incident
ISMS-OT-SESSION-002	Sessions recorded	100%	Investigate
ISMS-OT-SESSION-002	Monthly review done	100%	Escalate
ISMS-ORG-CONTEXTE-001	Interested parties with owner and requirements	100%	Complete within 14 days
ISMS-ORG-CONTEXTE-001	Register reviewed within 12 months	100%	Escalate to top management
ISMS-ORG-CONTEXTE-001	Requirements without linked control	0	Assign control or exception
ISMS-RH-DISCIPLINE-001	Breach cases closed within 30 days	≥ 90%	HR manager review
ISMS-RH-DISCIPLINE-001	Cases with documented hearing	100%	Reopen
ISMS-RH-DISCIPLINE-001	Staff aware of the process	≥ 95% in awareness check	Awareness action
ISMS-RH-ANTECEDENTS-001	Sensitive-role holders screened before access	100%	Restrict access
ISMS-RH-ANTECEDENTS-001	Re-screening due dates met	100%	HR escalation
ISMS-RH-ANTECEDENTS-001	External personnel with screening evidence	100%	Block access
ISMS-OPS-LOGICIELS-001	Installed software in catalogue	≥ 98%	Remove or approve within 10 days
ISMS-OPS-LOGICIELS-001	Requests assessed in 10 working days	≥ 90%	Staffing review
ISMS-OPS-LOGICIELS-001	Unsupported software without exception	0	CISO
ISMS-OPS-ENVIRONNEMENTS-001	Environments with owner and separation evidence	100%	Fix within 14 days
ISMS-OPS-ENVIRONNEMENTS-001	Test datasets containing unmasked personal data	0	Incident
ISMS-OPS-ENVIRONNEMENTS-001	Developers with standing production access	0	Remove
ISMS-PHY-BUREAU-001	Spot checks without C2/C3 left unattended	≥ 95%	Awareness action
ISMS-PHY-BUREAU-001	Findings corrected in 14 days	≥ 90%	Escalate
ISMS-PHY-BUREAU-001	Devices with 5-minute lock	100%	Fix within 7 days
ISMS-OPS-PURVIEW-001	Register matches tenant export	100%	Correct within 5 days
ISMS-OPS-PURVIEW-001	Policies in enforce mode for C3	100%	CISO
ISMS-OPS-PURVIEW-001	Sampled documents with correct label	≥ 95%	Policy tuning
ISMS-ORG-AUTORITES-001	Contacts verified in 6 months	100%	Update within 5 days

DOCUMENT	INDICATOR	TARGET	ESCALATION
ISMS-ORG-AUTORITES-001	Register available offline	100%	Fix
ISMS-ORG-AUTORITES-001	Notification deadlines met	100%	Top management
ISMS-ORG-COMMUNICATION-001	Mandatory messages read within 5 working days	≥ 90%	Reminder and line manager follow-up
ISMS-ORG-COMMUNICATION-001	Questions answered in 3 days	≥ 95%	Staffing review
ISMS-ORG-COMMUNICATION-001	Plan reviewed in 12 months	100%	Escalate
ISMS-OPS-CAPACITES-001	Critical services below critical threshold	100%	Immediate action
ISMS-OPS-CAPACITES-001	Capacity incidents	0 critical	Root-cause review
ISMS-OPS-CAPACITES-001	Forecasts delivered quarterly	100%	Escalate

7 Baseline parameter register (ISMS-ORG-PARAMETRES-001)

Baseline values proposed in the annexes. They become binding when approved by top management in the parameter register.

ID	PARAMETER	BASELINE	SOURCE
P-GOV-01	Policy review cycle	At least every 12 months and on significant change	ISMS-POL-SSI-002
P-GOV-02	Steering committee frequency	At least quarterly	ISMS-ORG-GOUVERNANCE-001
P-GOV-03	Management review frequency	At least annually	ISMS-AUD-PROGRAMME-001
P-GOV-04	Exception maximum duration	12 months (90 days for vulnerabilities)	ISMS-ORG-DEROGATIONS-001
P-GOV-05	Customer contract security review	Within 10 working days of receipt	ISMS-CLI-EXIGENCES-001
P-GOV-06	Risk assessment cycle	At least annually and on significant change	ISMS-RSK-METHODE-001
P-GOV-07	Self-assessment before TISAX assessment	Within 6 months before fieldwork	ISMS-AUD-FIELDWORK-001
P-GOV-08	Sample size	25 items or all if fewer; 10% above 250 items (minimum 25)	ISMS-AUD-SAMPLE-001
P-GOV-09	Sample deviation rate triggering extended testing	Above 5%	ISMS-AUD-SAMPLE-001
P-INC-01	Event classification	Within 4 hours of receipt	ISMS-INC-PROC-001
P-INC-02	Customer notification (no contractual period)	Within 24 hours of confirmation	ISMS-CLI-INCIDENT-001
P-INC-03	Personal data breach notification to authority	Within 72 hours of awareness	ISMS-RGP-VIOLATION-001
P-INC-04	Post-incident review	Within 10 working days	ISMS-INC-PROC-001
P-INC-05	Supplier incident notification	Within 24 hours	ISMS-FOU-INCIDENT-001
P-HR-01	Leaver account disabling	End of last working day (immediately for dismissal for cause)	ISMS-RH-CYCLE-001
P-HR-02	Role change access re-evaluation	Within 5 working days	ISMS-RH-CYCLE-001
P-HR-03	Induction security training	Within 10 working days of joining	ISMS-RH-SENSIBILISATION-001
P-HR-04	Refresher training	At least annually	ISMS-RH-SENSIBILISATION-001
P-HR-05	Phishing simulation	At least twice a year	ISMS-RH-SENSIBILISATION-001
P-HR-06	Screen lock	5 minutes	ISMS-RH-TELETRAVAIL-001
P-PHY-01	Restricted-zone access review	Quarterly	ISMS-PHY-ZONES-001
P-PHY-02	Visitor log retention	12 months	ISMS-PHY-ZONES-001
P-PHY-03	Lost badge blocking	Within 1 hour	ISMS-PHY-BADGES-001
P-PHY-04	UPS, fire and climate tests	At least annually	ISMS-PHY-ZONES-001
P-PHY-05	Premises inspections	Quarterly, with two out-of-hours rounds a year	ISMS-PHY-INSPECTIONS-001
P-BCM-01	Business impact analysis	At least annually	ISMS-PRA-PCA-001
P-BCM-02	Disaster recovery test	At least annually per critical service	ISMS-PRA-PRA-001
P-BCM-03	Restore test (critical systems)	Quarterly	ISMS-OPS-SAUVEGARDE-001
P-IAM-01	Access review (C2/C3 applications)	Semi-annual; privileged and C3 access quarterly	ISMS-IAM-REVUE-001
P-IAM-02	Unconfirmed access after review	Revoked after 14 days	ISMS-IAM-REVUE-001
P-IAM-03	Dormant accounts	Disabled at 90 days, removed at 180 days	ISMS-IAM-CYCLE-001
P-IAM-04	Password length	14 characters or passphrase, no forced periodic change	ISMS-IAM-AUTH-001
P-IAM-05	Service credential rotation	At least every 90 days	ISMS-IAM-SERVICE-001
P-IAM-06	Break-glass use review	Within 24 hours	ISMS-IAM-URGENCE-001

ID	PARAMETER	BASELINE	SOURCE
P-OPS-01	Vulnerability triage	Within 2 working days	ISMS-OPS-VULN-001
P-OPS-02	Remediation: exploited or critical on exposed system	72 hours	ISMS-OPS-VULN-001
P-OPS-03	Remediation: critical or high	14 days	ISMS-OPS-VULN-001
P-OPS-04	Remediation: medium	60 days	ISMS-OPS-VULN-001
P-OPS-05	Remediation: low	120 days or next planned release	ISMS-OPS-VULN-001
P-OPS-06	Authenticated scan frequency	Weekly (internet-facing), monthly (internal)	ISMS-OPS-VULN-001
P-OPS-07	Penetration test	At least annually and after major change	ISMS-OPS-PENTEST-001
P-OPS-08	Log retention	At least 12 months, 3 months immediately available	ISMS-OPS-JOURNAUX-001
P-OPS-09	Maximum clock drift	1 second	ISMS-OPS-TEMPS-001
P-OPS-10	Firewall rule review	Semi-annual; unused rules removed after 90 days without hits	ISMS-OPS-SEGMENT-001
P-OPS-11	Emergency change retrospective approval	Within 2 working days	ISMS-OPS-CHANGES-001
P-OPS-12	Certificate renewal start	At least 30 days before expiry	ISMS-CRY-POLITIQUE-001
P-OPS-13	Exposed secret remediation	Within 24 hours	ISMS-OPS-SECRETS-001
P-OPS-14	Minimum TLS version	TLS 1.2 (1.3 where supported)	ISMS-CRY-POLITIQUE-001
P-SUP-01	High-tier supplier assessment	Annually	ISMS-FOU-POLITIQUE-001
P-SUP-02	Standard-tier questionnaire	Every 24 months	ISMS-CLI-SECURITE-002
P-SUP-03	Expired supplier evidence action	Within 14 days	ISMS-FOU-ASSURANCE-002
P-SUP-04	Subcontractor change review	Within 30 days	ISMS-FOU-SOUS-TRAITANCE-001
P-CMP-01	Legal register review	At least annually	ISMS-CON-CONFORMITE-001
P-CMP-02	Law or standard change assessment	Within 30 days	ISMS-CON-VEILLE-001
P-CMP-03	Audit record retention	Minimum three years (assessment cycle plus current period)	ISMS-CON-RETENTION-001
P-PRO-01	Prototype reconciliation	Monthly (weekly for critical items)	ISMS-PRO-TRACABILITE-001
P-PRO-02	Missing prototype search before escalation	2 hours; customer notified within 24 hours at most	ISMS-PRO-RECON-001
P-PRO-03	Video retention in prototype areas	90 days where lawful	ISMS-PRO-ZONES-001
P-DP-01	Data subject request response	One month (extendable by two months with reasons)	ISMS-RGP-DROITS-001
P-OT-01	OT vulnerability assessment	Within 14 days	ISMS-OT-CORRECTIFS-001
P-OT-02	OT recovery test	At least annually for the most critical line	ISMS-OT-PRA-001

8 AL3 readiness checklist

WHEN	READINESS CONDITION
T-90 days	Scope, objectives, ISA edition and participant data confirmed in the ENX portal; assessment order placed; provider and dates fixed.
T-90	Self-assessment complete with maturity score and independent challenge for every applicable control.
T-60	All controls below level 3 have corrective plans and have started; recurring controls show at least two cycles or three months of records.
T-45	Evidence repository staged and indexed; populations defined and extractable; redaction done.
T-30	Policy set approved and current; no draft documents in use; acknowledgement and training rates meet targets.
T-30	Interviewees nominated, briefed and available with deputies; walk-through route agreed.
T-28	Site walk-through completed: zones, server room, clean desk, delivery, visitors, media.
T-14	Technical demonstrations rehearsed: scan trace, patch compliance, access review, log retrieval, restore result.
T-7	Open exceptions reviewed and approved; supplier dossiers valid; customer requirements register current.
T-1	Auditor room, access, contacts and request log ready; point of contact and deputy confirmed.
During	Daily review of provisional findings; clarify facts; no records created retrospectively.
T+10 days	Corrective action plan with owners, dates and acceptance criteria submitted (ISMS-AUD-CLOSURE-001).