C1 · INTERNAL

# TISAX / ISMS DOCUMENTATION LIBRARY V6.1

Release, information-classification and deployment guide for the editable ISMS working library — with the labelling scheme applied to every document and the open gaps that remain before an AL3 assessment.

| 149 | 4 | 11 | 33 |
|---|---|---|---|
| WORD TEMPLATES | CLASSIFICATION LEVELS | MISSING DOCUMENTS | TRACKED GAPS |

**VERSION 6.1 · 01 NOVEMBER 2026**

Aurélien Husson · Chief Information Security Officer
contact@aurelson.com

**C1 · INTERNAL — Staff and authorised contractors under confidentiality undertaking**

01 / WHAT CHANGED IN V6.1

# Labelled, traceable, honest

V6.1 adds a complete information-classification scheme and applies it to every file in the pack. The V5 wording, caveats and working-draft status are preserved, except the classification procedure, which is rewritten in full.

01 / WORD

### 149 documents marked

Classification label in the header and footer of every page, a classification block on page 1, distribution and handling rules, revision history and custom document properties.

02 / CLASSIFICATION

### ISMS-ACT-CLASSIF-001 rewritten

Four levels C0–C3, decision rules, marking per medium, handling matrix, Microsoft Purview label design and customer-marking equivalence.

03 / WORKBOOK

### 14 tracking sheets

New Classification Scheme, Missing Documents and Content QA sheets; classification, review dates and QA flags in the register; dashboard KPIs.

04 / INTEGRITY

### Valid Office files

All Word files now pass OOXML schema validation; metadata cleaned; registers, README and SHA-256 manifest regenerated.

RELEASE PRINCIPLE

Better presentation and labelling are not evidence of conformance. No source record, signed management approval, complete ISA question mapping or AL3 outcome is implied by this release. 87 documents still rely mostly on generic control wording and need a subject-matter rewrite (page 08).

| Item | V6.0 | V6.1 |
|---|---|---|
| Classification scheme | Not defined (procedure named no levels) | C0 Public · C1 Internal · C2 Confidential · C3 Strictly Confidential |
| Marking on documents | None | Header + footer on every page, page-1 block, document properties |
| Version control | Version only; 13 docs showed 5.0 under a 6.0 cover | Revision history table; versions aligned to 6.1 |
| Evidence Index labels | Ad-hoc: Limited / Confidential / Restricted | Restricted to the C0–C3 list by data validation |
| Page numbering | PAGE only | Page X / Y |


© 2026 Aurélien Husson · CISO · contact@aurelson.com · Guide V6.1

02 / FOUR LEVELS

# One label, read the same way everywhere

The level is always written as code + English label — for example C2 · CONFIDENTIAL — so that people, DLP rules and Microsoft Purview labels recognise it. Colour supports the text; it never replaces it.

## C0
**PUBLIC**

2 DOCUMENTS IN LIBRARY

**Approved for release to the public. Disclosure causes no harm.**

**Protection need:** None (approved for publication)

**Distribution:** Unrestricted once release is approved; INTERNAL until then

**Examples:** Trust page, approved shareable policy

**Purview label:** Public

## C1
**INTERNAL**
INTERNE

75 DOCUMENTS IN LIBRARY

**Default for business information not meant for the public. Limited harm if disclosed.**

**Protection need:** Normal (Normal protection need)

**Distribution:** Staff and authorised contractors under confidentiality undertaking

**Examples:** Policies, procedures, training, blank templates

**Purview label:** Internal

## C2
**CONFIDENTIAL**
CONFIDENTIEL

59 DOCUMENTS IN LIBRARY

**Need-to-know group. Significant financial, contractual, legal or reputational damage if disclosed.**

**Protection need:** High (High protection need (Info high))

**Distribution:** Need-to-know: document owner and roles named in section 2

**Examples:** Risk register, incidents, audit findings, configurations, contracts, personal data

**Purview label:** Confidential

## C3
**STRICTLY CONFIDENTIAL**
STRICTEMENT CONFIDENTIEL

13 DOCUMENTS IN LIBRARY

**Named individuals only. Severe damage, breach of customer secrecy or direct path to compromise.**

**Protection need:** Very high (Very high protection need (Info very high / prototype))

**Distribution:** Named individuals only; access list kept by document owner

**Examples:** Prototypes, secrets and keys, break-glass, network/OT architecture, special-category data

**Purview label:** Strictly Confidential

**Rules that settle most disputes.** Apply the highest level that results from customer marking, prototype status, personal data, impact and aggregation. Unlabelled internal information = C1; unlabelled customer information = C2 until confirmed. Customer markings are never removed. Only the owner may lower a level.


© 2026 Aurélien Husson · CISO · contact@aurelson.com · Guide V6.1

03 / HANDLING MATRIX

# What each level allows

Minimum rules. Stricter customer, legal or contractual requirements prevail. Bracketed values are local parameters to confirm in the ISMS parameter register.

| Activity | C0 · PUBLIC | C1 · INTERNAL | C2 · CONFIDENTIAL | C3 · STRICTLY CONFIDENTIAL |
|---|---|---|---|---|
| Access | Anyone | Staff and authorised contractors | Need-to-know group set by owner | Named list approved by owner |
| Storage | Any | Company-managed systems | Encrypted, access-controlled | Rights-managed repository; no unmanaged sync |
| External transfer | Free | Owner approval | NDA + encrypted channel | Owner + customer written approval; logged |
| BYOD | Allowed | Managed apps only | No download to unmanaged devices | Not permitted |
| Cloud / AI | Allowed | Approved tenants | Enterprise services only; no public AI | Prohibited unless CISO (and customer) approve |
| Printing | Allowed | Allowed | Secure print release | Owner consent; numbered copies |
| Disposal | Normal | Standard deletion | Shredding [P-4] / secure deletion | [P-5+] or certified destruction |
| If mishandled | — | Tell line manager | Security incident | Immediate incident + customer notification check |

04 / MARKING ON A DOCUMENT PAGE




**Header label.** Right-aligned chip in the level colour on every page.

**Classification block.** Level, protection need, distribution and handling rules on page 1, repeated in the approval table.

**Document properties.** Classification, ClassificationCode, Distribution, DocumentID, DocumentVersion, SensitivityLabel — ready for Purview or DMS mapping.

**Footer label.** Level in EN and FR plus a short distribution phrase; page X / Y; document ID and version.


© 2026 Aurélien Husson · CISO · contact@aurelson.com · Guide V6.1

05 / SENSITIVITY LABELS

# Microsoft Purview target design

Label names and visual-marking text must match the scheme exactly. Validate against tenant licences and pilot with one team before tenant-wide publication.

| Level | Purview label | Protection | Content marking | Policy |
|---|---|---|---|---|
| C0 · PUBLIC | Public | None | None | Manual |
| C1 · INTERNAL | Internal | No encryption | Footer | Default label for documents and e-mail |
| C2 · CONFIDENTIAL | Confidential (+ customer sub-labels if contracts require) | Encryption: employees + named partner groups | Header + footer | Auto-labelling recommendations; DLP blocks unencrypted external sharing |
| C3 · STRICTLY CONFIDENTIAL | Strictly Confidential | Named permissions; Do Not Forward; limited offline | Header + footer + watermark | Manual; private teams without guests |

Tenant-wide: mandatory labelling, justification to lower or remove a label, attachments inherit the e-mail label, label activity retained for audit.

06 / CUSTOMER AND THIRD-PARTY MARKINGS

| External marking | Internal equivalent | Rule |
|---|---|---|
| Public / Öffentlich | C0 · PUBLIC | — |
| Internal / Intern | C1 · INTERNAL | No forwarding outside the receiving organisation without sender approval |
| Confidential / Vertraulich / Confidentiel | C2 · CONFIDENTIAL | Project team named in the contract only |
| Strictly confidential / Streng vertraulich / Secret / Geheim | C3 · STRICTLY CONFIDENTIAL | Named recipients; customer approval for onward sharing |
| Prototype-protected / secrecy agreement | C3 · STRICTLY CONFIDENTIAL | Prototype protection rules (ISMS-PRO-*) also apply |
| Unmarked, received from a customer | C2 · CONFIDENTIAL (provisional) | Ask the sender; record the answer |

**TISAX LINK**

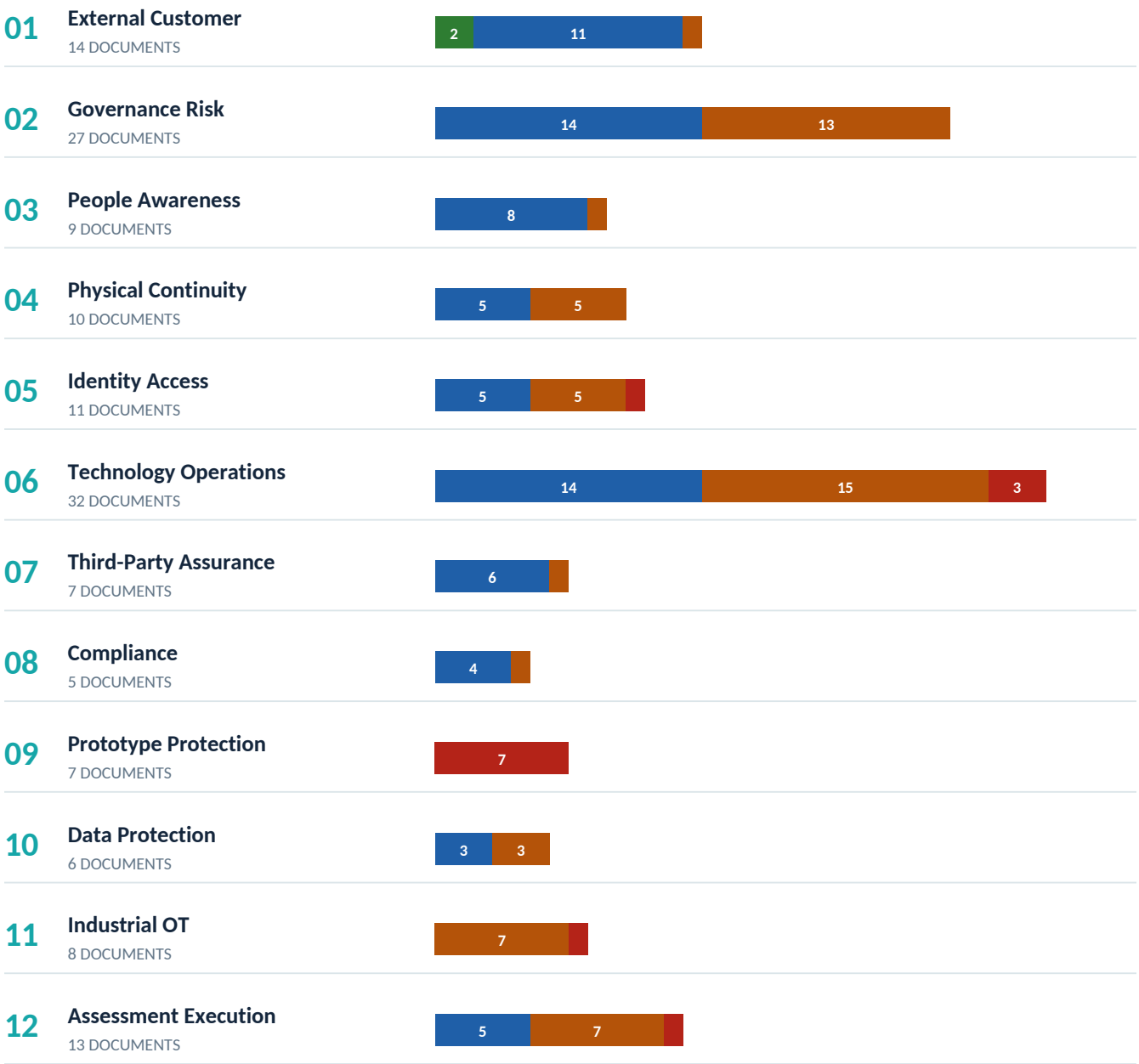
C2 corresponds to a high protection need (assessment objective “Info high”, AL2); C3 to a very high protection need (“Info very high”, AL3) and to prototype objectives. Confirm wording against the ISA edition of your assessment order — ISA2027 applies to assessments ordered from 1 January 2027.


© 2026 Aurélien Husson · CISO · contact@aurelson.com · Guide V6.1

07 / LIBRARY MAP

# Where the sensitive material sits

Document identifiers are unchanged across all twelve folders. Each bar shows how many documents of the folder reach each level once completed.




| C0 · PUBLIC | C1 · INTERNAL | C2 · CONFIDENTIAL | C3 · STRICTLY CONFIDENTIAL | TOTAL 149 EDITABLE DOCUMENTS |
|---|---|---|---|---|
| 2 | 75 | 59 | 13 | |


© 2026 Aurélien Husson · CISO · contact@aurelson.com · Guide V6.1

08 / COVERAGE REVIEW

# Documents the library still needs

Topics checked against ISO/IEC 27001:2022 clauses and Annex A and the VDA ISA chapters. Each item is also in the workbook (Missing Documents and Gap Register G19–G32).

| Proposed ID | Title | Requirement | Level | Priority |
|---|---|---|---|---|
| ISMS-ORG-PARAMETRES-001 | ISMS parameter register | Internal policy decision | C1 · INTERNAL | High |
| ISMS-ORG-CONTEXTE-001 | Context of the organisation and interested parties | ISO 27001 cl. 4.1, 4.2 | C1 · INTERNAL | High |
| ISMS-RH-SANCTIONS-001 | Disciplinary process for security violations | ISO 27001 A.6.4 | C1 · INTERNAL | High |
| ISMS-RH-SCREENING-001 | Personnel screening and background verification | ISO 27001 A.6.1; VDA ISA HR | C2 · CONFIDENTIAL | High |
| ISMS-OPS-LOGICIELS-001 | Approved software and installation control | ISO 27001 A.8.19; VDA ISA software approval | C1 · INTERNAL | High |
| ISMS-DEV-ENVIRONNEMENTS-001 | Environment separation, test data and data masking | ISO 27001 A.8.31, A.8.33, A.8.11 | C1 · INTERNAL | High |
| ISMS-PHY-BUREAU-001 | Clear desk and clear screen | ISO 27001 A.7.7 | C1 · INTERNAL | Medium |
| ISMS-ACT-LABELS-001 | Sensitivity label and DLP configuration record | ISO 27001 A.5.13; implements ISMS-ACT-CLASSIF-001 | C2 · CONFIDENTIAL | Medium |
| ISMS-ORG-CONTACTS-001 | Authorities and special-interest group contacts | ISO 27001 A.5.5, A.5.6 | C1 · INTERNAL | Medium |
| ISMS-ORG-COMMUNICATION-001 | ISMS communication plan | ISO 27001 cl. 7.4 | C1 · INTERNAL | Medium |
| ISMS-OPS-CAPACITE-001 | Capacity management | ISO 27001 A.8.6 | C1 · INTERNAL | Low |

## ALSO OPEN AT LIBRARY LEVEL

• **ISA edition not chosen.** ISA 6 for assessments ordered before 1 January 2027, ISA2027 afterwards. No official question IDs are mapped yet (G01, G21).

• **Owners, approvals and evidence.** All 149 documents are still working drafts with placeholder owners; no operating evidence is recorded (G02–G15).

• **Microsoft Purview not yet configured.** The label design exists on paper only; record the configuration in ISMS-ACT-LABELS-001 once deployed (G32).


© 2026 Aurélien Husson · CISO · contact@aurelson.com · Guide V6.1

09 / CONTENT QUALITY

# Generic wording is the biggest remaining risk

An AL3 assessor interviews owners and tests operation against what the document says. Text that could fit any subject will not survive that test.

**544**
control requirements

**135**
distinct operating actions behind them

**87**
documents ≥ 75 % generic

**31**
documents sharing one worked example

| Pattern found | Example | Fix |
|---|---|---|
| Operating action does not match the requirement | POL-SSI-001 §3.2 “Keep network diagrams out of the shareable edition” → action “Maintain an attributable version trail” | Write the concrete step that delivers the requirement |
| Worked example unrelated to the subject | ACT-CLASSIF-001 (V6.0) illustrated with a risk-register row; a TLS-certificate row reused in 31 documents | One realistic example per document, from its own process |
| Same assurance text in every document | “Select independent samples, challenge evidence sufficiency…” repeated for every reviewer role | Name the sample, population and frequency for this control |
| Version inconsistencies | 13 assessment templates showed version 5.0 inside a V6 cover | Fixed in V6.1; keep the revision history up to date |

**Where to start.** The workbook sheet *Content QA* scores every document; 87 are “High” priority. Rewrite the C2/C3 technical procedures and the documents an assessor will request first (scope, risk, SoA, incident, access, backup, supplier, prototype) before the AL3 fieldwork. ISMS-ACT-CLASSIF-001 shows the target level of specificity.


© 2026 Aurélien Husson · CISO · contact@aurelson.com · Guide V6.1

10 / DEPLOYMENT SEQUENCE

# From labelled template to operating control

A document becomes auditable through ownership, approval, implementation and records of real operation.

**01** **FIX ASSESSMENT SCOPE**
Entities, sites, contractual expectations, objectives and ISA edition (ISA 6 or ISA2027 by order date).

**02** **CONFIRM APPLICABILITY**
Decide conditional topics: prototype, OT, data protection, AI.

**03** **ASSIGN OWNERS**
Process owner, operating owner, release authority, reviewer.

**04** **CONFIRM CLASSIFICATION**
Check each target level in the register; deploy Purview labels; train staff on the four levels.

**05** **PARAMETERISE AND REWRITE**
Fill thresholds, systems and escalation paths; rewrite High-priority generic sections; create missing documents.

**06** **APPROVE AND PUBLISH**
Signatures, effective date, revision history, label applied on publication.

**07** **OPERATE, TEST, CLOSE**
Native-source records, sampled tests, preserved failures, independent closure.

| Release check | Result for V6.1 |
|---|---|
| Document integrity | 149 Word files, 149 unique IDs, all pass OOXML schema validation, all rendered and checked page by page for header and footer labels |
| Classification consistency | Label in each file = Document Register = workbook (C0: 2 · C1: 75 · C2: 59 · C3: 13) |
| Workbook | 0 formula errors after recalculation; no pre-approved evidence or readiness scores |
| Assessment limitation | Only the official VDA ISA workbook supports question-level mapping; this library is not an ENX evaluation and claims no TISAX label |


© 2026 Aurélien Husson · CISO · contact@aurelson.com · Guide V6.1