

Specimen: five rows of the attribute register

ISO/IEC 27028, Edition 1, stage 60.00 under publication, 20 October 2026. The standard is guidance, not a certifiable requirement. The five attribute values come from ISO/IEC 27002:2022 clause 4.2 and Annex A Table A.1. The publication window of 8 December 2026 is our arithmetic from ISO’s seven-week production statement, not an announced date.

What this is. This is a labelled specimen: the first five rows of the register, the column order and the plan. It is not a client record. 93 controls and 16 structural units, with the evidence an auditor asks for and the common gaps. It does not reproduce the ISO text and it does not certify.

The dated plan

Date	Action	What it covers	Evidence to keep
2026-10-27	Decide and record	Decide whether to adopt the attribute view this cycle, defer it or decline it. Record the decision, the owner and the reason in the change statement.	A one-page decision record with owner and date.
2026-11-10	Add the five columns	Add one column per attribute beside the control code and name in the controlled Statement of Applicability. Leave the inclusion decisions and justifications unchanged. Record a version and an approver.	A versioned SoA with the new columns.
2026-11-17	Spot-check three controls	Pick three controls you know well. Compare your values with Table A.1, check the evidence behind each, and record any divergence and its reason.	Three checked controls with a source line and an evidence pointer.
2026-11-24	Ask the certification body	Ask in writing how the next audit will treat the attribute view, and record the answer in the audit file.	A dated question and answer.
2026-12-01	Name an owner and a due date	Put an owner and a due date on every attribute row. A blank owner is the first thing an auditor reads as incomplete.	A register with no blank owner.
2026-12-08	Publication check	Check the ISO record for stage 60.60 or a change to the window. The date is our arithmetic from the seven-week production statement, not an announced date.	A dated stage note.
2026-12-15	Read the published text	Read the published standard and check the five definitions and any additional attributes against this register. Update the values if a definition changed.	A dated reading note and a new register version if needed.
2027-01-15	Brief the control owners	Brief the people who supply the evidence on the five attributes in plain words. Add the attribute columns to the internal audit checklist.	A briefing record and a checklist version.
2027-02-15	Rehearse the audit question	Run one internal review of the attribute columns against the evidence list. Keep the findings separate from the incident and risk registers.	A review note and one corrective action if needed.
After publication	Reissue the register	Kit buyers receive the register rebuilt against the published text at no extra charge. Check the ISO record for a correction or amendment.	The published record, the reissued files and a change log row.

Change statement (one page)

We reviewed the Statement of Applicability against the public ISO/IEC 27028 record on _____. The review covered the five attribute columns, the comparison with Table A.1, the owner and review date on every row, and the question to the certification body. The decision was _____. The owner is _____. The next review is due _____. ISO/IEC 27028 is guidance and this statement does not certify anything.

Item	Decision	Owner	Date	Reason
Adopt the five attribute columns this cycle				
Define an attribute of our own				
Keep the published value beside a local value				
Ask the certification body				
Review the register with the risk treatment plan				

The register

Ref	Code	Type	Theme	Control	Control type	Properties	Concepts	Capability	Domain	Your value	Why	Evidence
ISO27028-5.1	5.1	Control	Organizational controls	Policies for information security	Preventive	Confidentiality; Integrity; Availability	Identify	Governance	Governance and ecosystem; Resilience			The top-level information security policy with top management approval, covering the definition, objectives or objective-setting framework, principles, commitments to requirements and continual improvement, role assignments and the exceptions procedure; The register of topic-specific policies with an owner, approving manager and version for each; Review records showing the planned interval met and ad hoc reviews after changes in strategy, technology, regulation, risk, threats or incidents, with management review and audit results as inputs; Acknowledgement records from personnel and relevant external parties that they understand and will comply; Change log showing top management approval of every change to the top-level policy; Evidence that externally distributed policy versions were checked for confidential content
ISO27028-5.10	5.10	Control	Organizational controls	Acceptable use of information and other associated assets	Preventive	Confidentiality; Integrity; Availability	Protect	Asset management; Information protection	Governance and ecosystem; Protection			The acceptable use topic-specific policy stating expected and prohibited behaviour, permitted and forbidden uses, and the monitoring the organization performs; Evidence the policy was communicated to and accepted by personnel and external users; Handling procedures per classification level covering access, copies, storage, media marking and disposal; Records of authorized users for sensitive information and assets; Disposal authorizations with the deletion method used; Agreements governing use of third-party assets such as public cloud services and collaboration platforms

Ref	Code	Type	Theme	Control	Control type	Properties	Concepts	Capability	Domain	Your value	Why	Evidence
ISO27028-5.11	5.11	Control	Organizational controls	Return of assets	Preventive	Confidentiality; Integrity; Availability	Protect	Asset management	Protection			The leaver and mover procedure with an asset return step and a checklist of assets issued to each person; Signed asset return records reconciled against the asset inventory; Records of information transferred from and securely wiped on personally owned or purchased devices; Knowledge transfer or handover documentation for departing staff holding operationally important knowledge; Evidence of monitoring or technical restrictions on copying data during notice periods; Return records for authentication hardware such as keys, tokens and smartcards
ISO27028-5.12	5.12	Control	Organizational controls	Classification of information	Preventive	Confidentiality; Integrity; Availability	Identify	Information protection	Protection; Defence			The topic-specific classification policy with named levels, criteria based on impact, and conventions covering confidentiality, integrity and availability; Evidence the scheme was communicated to relevant interested parties and built into procedures; Classification records in the asset inventory or labels showing owner-assigned classifications; Records of classification reviews and reclassification when sensitivity or criticality changed; Information-sharing agreements that map the other party's classification levels to the organization's own; Alignment between the classification scheme and the access control policy
ISO27028-5.13	5.13	Control	Organizational controls	Labelling of information	Preventive	Confidentiality; Integrity; Availability	Protect	Information protection	Defence; Protection			Labelling procedures covering all formats, with rules on placement, exemptions and cases where labelling is not possible; Examples of labelled documents, emails, reports and media showing the chosen techniques such as headers, watermarks or metadata; Configuration of labelling or data classification tooling that applies metadata and enforces handling decisions; Evidence that sensitive system outputs such as reports and exports carry classification labels; Training records for personnel on labelling and handling; Documented handling for systems that protect at the highest level and label on export

Not legal advice; does not certify. Source record: 5284b5a388b9941a. Retrieved 2026-10-20. The full evidence list and extension worksheet are in the CSV and XLSX.