SRIDA IT PROFESSIONAL REFERENCE PUBLICATION

ISO/IEC 27028

Using Information Security Control Attributes · 2026 edition

Implementation Guidance & Assurance Testing Procedures

DOCUMENT ID	VERSION	STATUS
SRIDA-ATTR-27028-RTP-001	1.0	Final — Approved for Publication

Rajendra Bodda
Chief Information Security Officer (CISO)
Srida IT · 2026

Independent professional guidance.
Not an ISO publication.

Free sample pages · The complete manual is available at sridait.com/manuals/rtp-iso27028 · © 2026 Srida IT

ISO/IEC 27028:2026 — Using Information Security Control Attributes

Implementation Guidance & Assurance Testing Procedures

SAMPLE

Prepared by

Rajendra Bodda

Chief Information Security Officer (CISO)

Published by Srida IT

SRIDA-ATTR-27028-RTP-001 · Version 1.0 · November 2026

This publication is an independently developed professional guidance document prepared by Srida IT. It is not a publication of ISO or IEC, does not reproduce the text of ISO/IEC 27028, 27002 or 27001, and does not confer any certification: ISO/IEC 27028 is guidance and is not certifiable. Readers should obtain the published standards from ISO, IEC or their national standards body; only those texts are authoritative.

Free sample pages · The complete manual is available at sridait.com/manuals/rtp-iso27028 · © 2026 Srida IT

Document Information and Control

Field	Value
Document title	ISO/IEC 27028:2026 — Using Information Security Control Attributes
Subtitle	Implementation Guidance & Assurance Testing Procedures
Document identifier	SRIDA-ATTR-27028-RTP-001
Version	1.0
Status	Final — Approved for Publication
Classification	Srida IT Professional Reference Publication
Author	Rajendra Bodda, Chief Information Security Officer (CISO)
Publisher	Srida IT
Publication year	2026
Issue date	November 2026
Reference document	ISO/IEC 27028:2026, Information security, cybersecurity and privacy protection — Guidance on using information security control attributes (published November 2026)
Related documents	ISO/IEC 27001:2022; ISO/IEC 27002:2022; ISO/IEC 27005:2022; ISO/IEC 27701:2025; NIST CSF 2.0 (CSWP 29); CIS Critical Security Controls v8
Companion publications	SRIDA-ISMS-27001-RTP-001; SRIDA-NIST-CSF-RTP-001; SRIDA-PIMS-27701-RTP-001; SRIDA-AIS-27090-RTP-001
Next review	On a new edition of ISO/IEC 27028 or ISO/IEC 27002, and at least annually

Version history

Version	Date	Author	Description of change
1.0	November 2026	Rajendra Bodda	First published edition, approved for publication.

Approval

Role	Name	Date
Approved for publication	Rajendra Bodda, Chief Information Security Officer (CISO)	19 November 2026

Distribution

Released for publication by Srida IT. Distribution and use are subject to the permitted-use terms in the Copyright, Legal and Usage Notices.

SAMPLE

Free sample pages · The complete manual is available at sridait.com/manuals/rtp-iso27028 · © 2026 Srida IT

Table of Contents

Part I Foundations 18

Chapter 1 Introduction to ISO/IEC 27028:2026 19
Chapter 2 Control Attributes in ISO/IEC 27002:2022 23
Chapter 3 Why Attributes Matter: Risk Treatment and Control Determination 27
Chapter 4 Attributes and Related Frameworks 31
Chapter 5 Terminology and Abbreviations 35
Chapter 6 How to Use This Manual 38

Part II The Attribute Framework 41

Chapter 7 Attribute Types of ISO/IEC 27002:2022 42
AT-01 Control type 43
AT-02 Information security properties 49
AT-03 Cybersecurity concepts 55
AT-04 Operational capabilities 61
AT-05 Security domains 68
Chapter 8 Extended Control Attributes 74
AT-06 Assurance 75
AT-07 Complexity 81
AT-08 Contextual fit 86
AT-09 Control environment and dependencies 91
AT-10 Failure modes 96
AT-11 Formality 102
AT-12 Integration 107
AT-13 Maturity of the control 112
AT-14 Measurability 117
AT-15 Multi-functionality 123
AT-16 Origin and sourcing 129
AT-17 Regulation 135
AT-18 Strength 141
AT-19 Risk reduction focus 147
AT-20 Transparency 153
AT-21 Cost and value 159
Chapter 9 Organisation-Specific Attributes 164
AT-22 Organisation-specific attributes 165

Part III Controls Through the Attribute Lens 172

Chapter 10 Organizational Controls (5.1–5.37) 173
5.1 Policies for information security 175
5.2 Information security roles and responsibilities 178
5.3 Segregation of duties 181
5.4 Management responsibilities 184
5.5 Contact with authorities 186
5.6 Contact with special interest groups 188
5.7 Threat intelligence 190
5.8 Information security in project management 193
5.9 Inventory of information and other associated assets 195
5.10 Acceptable use of information and other associated assets 198
5.11 Return of assets 200

SAMPLE

Free sample pages · The complete manual is available at sridait.com/manuals/rtp-iso27028 · © 2026 Srida IT

5.12 Classification of information 202
5.13 Labelling of information 205
5.14 Information transfer 207
5.15 Access control 209
5.16 Identity management 211
5.17 Authentication information 213
5.18 Access rights 215
5.19 Information security in supplier relationships 217
5.20 Addressing information security within supplier agreements 220
5.21 Managing information security in the ICT supply chain 223
5.22 Monitoring, review and change management of supplier services 226
5.23 Information security for use of cloud services 229
5.24 Information security incident management planning and preparation 232
5.25 Assessment and decision on information security events 235
5.26 Response to information security incidents 237
5.27 Learning from information security incidents 240
5.28 Collection of evidence 242
5.29 Information security during disruption 245
5.30 ICT readiness for business continuity 247
5.31 Legal, statutory, regulatory and contractual requirements 249
5.32 Intellectual property rights 251
5.33 Protection of records 253
5.34 Privacy and protection of PII 255
5.35 Independent review of information security 258
5.36 Compliance with policies, rules and standards for information security 261
5.37 Documented operating procedures 264

Chapter 11 People Controls (6.1–6.8) 267
6.1 Screening 268
6.2 Terms and conditions of employment 271
6.3 Information security awareness, education and training 274
6.4 Disciplinary process 277
6.5 Responsibilities after termination or change of employment 279
6.6 Confidentiality or non-disclosure agreements 281
6.7 Remote working 284
6.8 Information security event reporting 287

Chapter 12 Physical Controls (7.1–7.14) 289
7.1 Physical security perimeters 290
7.2 Physical entry 293
7.3 Securing offices, rooms and facilities 296
7.4 Physical security monitoring 298
7.5 Protecting against physical and environmental threats 301
7.6 Working in secure areas 304
7.7 Clear desk and clear screen 307
7.8 Equipment siting and protection 309
7.9 Security of assets off-premises 311
7.10 Storage media 313
7.11 Supporting utilities 315
7.12 Cabling security 318
7.13 Equipment maintenance 320
7.14 Secure disposal or re-use of equipment 323

Chapter 13 Technological Controls (8.1–8.34) 326
8.1 User end point devices 328
8.2 Privileged access rights 331

SAMPLE

Free sample pages · The complete manual is available at sridait.com/manuals/rtp-iso27028 · © 2026 Srida IT

CHAPTER 1

Introduction to ISO/IEC 27028:2026

Most information security programmes have, at some point, built a spreadsheet of controls and then added columns to it: who owns the control, which regulation asks for it, whether it stops an incident or only notices one, which system it lives in. Those extra columns are control attributes in all but name. ISO/IEC 27002:2022 gave the idea a formal shape by tagging each of its 93 controls with five attribute types. ISO/IEC 27028:2026 takes the next step: it is a guidance document on how organisations can use control attributes, the five that ISO/IEC 27002 supplies and others they design for themselves, to make better decisions about controls.

This chapter explains what ISO/IEC 27028 is, how it reached publication, what kind of document it is, who it is likely to help, and, just as importantly, what this manual can and cannot say about it. Readers should take the last point seriously. This manual was written without access to the licensed text of ISO/IEC 27028. Everything it says about that standard comes from public secondary sources, and it is marked accordingly.

1.1 What ISO/IEC 27028 is

ISO/IEC 27028:2026 belongs to the ISO/IEC 27000 family, developed by the joint technical committee of ISO and IEC that is responsible for information security, cybersecurity and privacy protection (ISO/IEC JTC 1/SC 27). Its published title, as recorded in a national standards catalogue, is “Information security, cybersecurity and privacy protection — Guidance on using information security control attributes”. The same catalogue gives an issue date of 11 November 2026.

The subject is narrow and practical. A control attribute is a property of a control that lets it be classified, filtered and compared. ISO/IEC 27002:2022 introduced five attribute types (control type, information security properties, cybersecurity concepts, operational capabilities and security domains) and stated that organisations could create attributes of their own. It did not, however, say very much about how to design additional attributes, how to assign values consistently, or how to put the resulting data to work. ISO/IEC 27028 is understood to address that gap.

Public commentary on the draft and published versions describes the scope as guidance on the use of control attributes, written generically so that it applies to organisations of any type, size or nature. The same commentary reports that the document discusses examples of additional attributes beyond the five in ISO/IEC 27002, such as assurance, complexity, failure modes, measurability, origin and cost, and that it treats custom attributes and custom attribute values as feasible. These reported examples come from a single secondary source. This manual treats them as useful ideas worth exploring, not as confirmed content of the standard.

1.2 The journey from Technical Specification to International Standard

The project's history, as far as it can be reconstructed from public records, explains some of the uncertainty around it.

- **Early working title.** A draft-for-comment record at the British Standards Institution carried the title "Guidance on ISO/IEC 27002 attributes". That framing tied the work closely to the five attribute types in ISO/IEC 27002:2022.
- **Technical Specification.** The project began as a Technical Specification, designated ISO/IEC TS 27028. A Technical Specification is normally used where the subject is still developing or where there is not yet consensus for a full International Standard.
- **Progression to International Standard.** The work was later progressed as an International Standard. At Draft International Standard (DIS) stage the title was reported as "Guideline on using information security control attributes". The title moved away from "ISO/IEC 27002 attributes" towards "information security control attributes", which signals a broader scope: attributes are not limited to the 27002 catalogue.
- **Ballots.** The DIS ballot is reported to have run from about December 2025 to February 2026, with a Final Draft International Standard (FDIS) stage around August 2026.
- **Publication.** Publication as ISO/IEC 27028:2026 followed, with the catalogue issue date noted above.

Neither the edition number, the page count nor the clause and annex titles of the published standard could be confirmed from public sources. For that reason this manual never cites an ISO/IEC 27028 clause number or title. Where it refers to the standard, it refers to it as a whole.

SAMPLE

Free sample pages · The complete manual is available at sridait.com/manuals/rtp-iso27028 · © 2026 Srida IT

1.3 A guidance standard, not a requirements standard

The ISO/IEC 27000 family contains two broad kinds of document. Requirements standards, of which ISO/IEC 27001 is the best known, use "shall" statements against which an organisation can be audited and certified. Guidance standards, such as ISO/IEC 27002, ISO/IEC 27005 and ISO/IEC 27028, explain how something can be done; they use "should" and "can" and are not certifiable on their own.

Several consequences follow for practitioners.

- **There is no ISO/IEC 27028 certificate.** No accredited certification scheme exists for it, and none is likely, because the document contains no requirements to certify against. Any offer to certify an organisation against ISO/IEC 27028 should be treated with suspicion.
- **Adoption is voluntary and selective.** An organisation may take the ideas it finds useful and leave the rest. It does not need to adopt every example attribute, and it does not need to justify leaving one out.
- **The anchor remains ISO/IEC 27001.** In an ISO/IEC 27001 information security management system (ISMS), attributes are a tool for carrying out risk treatment (clause 6.1.3) and for maintaining the Statement of Applicability. A certification auditor will assess those clauses against ISO/IEC 27001. Attribute work can make the evidence clearer, but it does not create a separate audit criterion.
- **Attributes do not replace risk assessment.** A filter that returns "all detective controls supporting availability" is a convenient starting list. It is not a decision. Controls are still selected because identified risks call for them.

> **Srida IT position.** Throughout this manual, statements that an organisation "should" do something reflect good practice as Srida IT understands it. They are not requirements of ISO/IEC 27028, and failing to follow them is not a nonconformity against any standard.

1.4 Why attributes deserve a standard of their own

The older ISO/IEC 27002:2013 structure placed each control in exactly one clause, under one control objective. That was tidy but rigid. A control that served access control, logging and supplier management at once had to live in one place, and anyone looking at the catalogue from a different angle had to build their own cross-reference.

Attributes solve this by allowing many views of the same catalogue. A risk owner can ask for preventive controls protecting confidentiality. A security operations lead can ask for everything tagged with the Detect concept. A board committee can ask how the control set is spread across the four security domains. A compliance team can add a regulation attribute and ask which controls carry obligations under the CERT-In Directions or the RBI IT governance framework. The catalogue is the same; the questions differ.

The difficulty is that attribute data is only as good as the discipline behind it. Two teams tagging the same control can reach different answers. An attribute defined loosely ("complexity: high") means little unless there is a rule for when a control is high. And attributes multiply: once an organisation starts, it is tempting to add a dozen more columns that nobody maintains. Guidance on designing, assigning, governing and using attributes therefore has real value, and that is the territory ISO/IEC 27028 occupies.

1.5 Who ISO/IEC 27028 and this manual help

Table 1-1. Audiences and what they can take from attribute-based practice

Audience	Typical use of control attributes
CISOs and ISMS managers	Structuring the control catalogue, preparing the Statement of Applicability, explaining coverage to management in terms other than a list of 93 numbers.
Risk managers	Building candidate control lists during risk treatment, checking that treatment plans balance preventive, detective and corrective measures.
Security architects and engineers	Checking fit with the architecture, finding single points of failure, understanding dependencies and failure behaviour.
Compliance and privacy teams	Mapping controls to regulatory drivers and to frameworks such as NIST CSF 2.0, CIS Controls v8 and ISO/IEC 27701.
Internal and external auditors	Targeting samples, testing whether attribute data is accurate, and judging whether attribute-based decisions are traceable to risk.

SAMPLE

Free sample pages · The complete manual is available at sridait.com/manuals/rtp-iso27028 · © 2026 Srida IT

AT-06 · EXTENDED ATTRIBUTE

Assurance

Srida IT value set | WP-AT-06

A Definition and Source Status

Assurance

The **Assurance** attribute records how much justified confidence an organisation can have that a control is designed suitably and is operating as intended, based on the kind, quality and independence of the evidence the control produces. It describes the control's evidential position, not its importance and not its strength: a strong control that leaves no reliable trace may still rate Low on assurance, and a simple control with complete, system-generated records may rate High.

*Assurance is one of the example additional attributes reported in connection with ISO/IEC 27028:2026 by a single secondary source (iso27001security.com); the licensed text was not available, so the link to ISO/IEC 27028 is. It is not one of the five ISO/IEC 27002:2022 attribute types. The value set (Low / Medium / High), the meanings, the decision rules and the examples below are **Srida IT practice**, not text from any ISO standard.*

B Values and Decision Rules

Table 8-2. Values of AT-06 Assurance

Value	Meaning	Decision rule	Examples
Low	Srida IT practice: the control's operation can be shown only through assertion, recollection or occasional, informal records. Evidence is incomplete, created after the event, or produced by the same person who operates the control.	Assign Low when an assessor could not re-perform or independently corroborate the control for a sampled period without relying mainly on interviews, or when more than one in five sampled occurrences lack contemporaneous records.	• 6.4 Disciplinary process: often invoked rarely and recorded inconsistently, so operating evidence is thin. • 7.7 Clear desk and clear screen: evidence is usually a point-in-time walk-round, not continuous. • 5.6 Contact with special interest groups: membership exists but the value of the contact is hard to evidence.
Medium	Srida IT practice: the control produces documented, dated records for most occurrences, but they are manual, partially complete, or reviewed only by the control operator's own line.	Assign Medium when records exist for the population and an assessor can sample and corroborate them, but completeness depends on people remembering to record, or the review is not independent of the operator.	• 5.18 Access rights: periodic access reviews are documented, but sign-offs are often bulk approvals by the same managers. • 6.3 Information security awareness, education and training: completion is recorded, effect on behaviour is not. • 5.27 Learning from information security incidents: post-incident reviews exist but follow-through is tracked manually.
High	Srida IT practice: the control produces complete, tamper-evident, system-generated evidence for the whole population, and the evidence is reviewed or tested by someone independent of the operator.	Assign High only when all three conditions hold: (a) evidence is generated automatically or as an unavoidable by-product of the process; (b) the full population can be extracted and reconciled; (c) there is independent review, testing or monitoring of the evidence at a defined frequency.	• 8.13 Information backup: job logs plus scheduled, documented restore tests give strong operating evidence. • 8.15 Logging: centrally collected, integrity-protected logs are themselves the evidence. • 8.32 Change management: a ticketing workflow with enforced approvals leaves a complete, reconcilable trail.

Value set, meanings and decision rules are Srida IT practice; organisations may define their own.

SAMPLE

Free sample pages · The complete manual is available at sridait.com/manuals/rtp-iso27028 · © 2026 Srida IT

C Objective

Tagging controls with an Assurance value lets the organisation see, before an audit rather than during it, which parts of its control set it can actually prove. It supports the ISO/IEC 27001 clause 9.1 and 9.2 requirements to evaluate performance and to audit the ISMS by directing monitoring and internal audit effort towards controls whose evidence is weakest, and it helps the risk owner judge whether residual risk calculated on the assumption that a control works is credible. Used well, the attribute turns a vague sense that some controls are hard to evidence into a short, prioritised list of evidence improvements.

D Interpretation

Assurance is a property of the control as implemented in a particular organisation, not of the ISO/IEC 27002 control in the abstract. The same control, 5.18 Access rights for example, can be High in a firm with an identity governance platform that records every certification decision and Low in a firm that reviews access by e-mail. Srida IT therefore treats any pre-filled assurance value from a template as a starting hypothesis to be confirmed against real evidence.

A common pitfall is to confuse assurance with effectiveness. A control can be operating perfectly and still rate Low because nobody can show it; equally, a control can rate High on assurance and be ineffective, because the evidence clearly shows it failing. The attribute answers the question “how well can we know?”, and the testing procedures elsewhere in this manual answer “does it work?”. Keeping the two separate stops teams from upgrading assurance simply because no incidents have occurred.

Smaller organisations, such as a Bengaluru SaaS start-up with forty staff, will legitimately have more Medium values because they lack independent second-line functions. That is acceptable where the risk is proportionate; the aim is not to drive every control to High but to make sure that high-risk controls are not left at Low. Regulated entities, for example a Pune fintech NBFC subject to RBI IT governance expectations, will usually need High assurance on access, logging, change and backup controls because supervisors and statutory auditors routinely sample them.

Assurance also decays. A control rated High last year can drift to Medium when a tool licence lapses, a log source stops forwarding or the independent reviewer leaves. Srida IT practice is to re-confirm Assurance values at least annually and whenever the evidence-producing system changes.

E Use Cases

- Control selection: when two candidate controls treat the same risk, prefer the one capable of High assurance where the risk is rated high or where a regulator expects evidence.
- Statement of Applicability: add an assurance column so that the SoA shows not only that a control is implemented but how well its operation can be demonstrated.
- Gap analysis: list controls that treat high-rated risks yet sit at Low assurance; these are evidence gaps even when no design gap exists.
- Internal audit planning: weight audit coverage and sample sizes towards Low and Medium controls, and rely more on continuous monitoring for High controls.
- Reporting: show the board the share of high-risk controls at each assurance level as a simple indicator of how defensible the ISMS is.
- Budgeting: justify investment in automation or tooling by the number of controls it would move from Low or Medium to High.
- Third-party reliance: decide whether a supplier's SOC 2 or ISO/IEC 27001 report gives enough assurance for supplier-operated controls, or whether additional evidence is needed.

F How to Assign Values

1. Confirm the scope: list the controls in the SoA and the systems, sites and processes in which each operates.
2. For each control, identify what evidence it produces in normal operation, who produces it and where it is stored.
3. Test the three Srida IT conditions for High (automatic evidence, complete population, independent review); if any one fails, consider Medium.
4. Check whether a sample of recent occurrences can be corroborated from records alone; if not, the value is Low.
5. Record the value with a one-line justification and the evidence source, and note any scope parts that differ (for example a branch office with weaker evidence).
6. Where the control is applied differently across scopes, record the lowest value as the control value and note the variation, rather than averaging.
7. Have the assignment reviewed by someone outside the control owner's line, normally the ISMS manager or internal audit.
8. Re-confirm the value after material changes to tooling, staffing or process, and at least annually.

SAMPLE

Free sample pages · The complete manual is available at sridait.com/manuals/rtp-iso27028 · © 2026 Srida IT

ISO/IEC 27002:2022 CONTROL 5.15 · ORGANIZATIONAL CONTROL

Access control

Attribute profile · Srida IT assignment

A Purpose

This control has the organisation set rules for controlling physical and logical access to information and associated assets, based on business and security needs. Access is granted on a need-to-know and need-to-use basis, and the rules are the reference for the identity, authentication and access-rights controls that follow.

Described in Srida IT's own words; see ISO/IEC 27002:2022 for the control and its guidance.

B Attribute Profile

Table 10-30. Attribute profile, control 5.15

Attribute type	Values
Control type (AT-01)	#Preventive
Information security properties (AT-02)	#Confidentiality #Integrity #Availability
Cybersecurity concepts (AT-03)	#Protect
Operational capabilities (AT-04)	#Identity_and_access_management
Security domains (AT-05)	#Protection

This control, and the three that follow it, share a compact profile: Preventive, Protect, Identity_and_access_management, Protection. Srida IT treats 5.15 as the policy layer of access control and 5.16 to 5.18 as its operational layers. Some organisations add Physical_security because the rules cover physical access as well; that is a sensible re-tag if the organisation does not rely on 7.2 for that. Others add Governance because access policy is approved at governance level. Srida IT suggests keeping the core tag and showing the physical and governance links through the 'related' field rather than diluting attribute queries.

Srida IT assignment informed by ISO/IEC 27002:2022; compare with the licensed attribute table and tag to your own context.

SAMPLE

C Extended Attribute Profile

Extended attribute	Value	Why
Assurance (AT-06)	**Medium**	The access policy is easy to inspect; its effect is evidenced through 5.16 to 5.18 and 8.2 to 8.5.
Complexity (AT-07)	**Medium**	Defining roles and need-to-know rules across many systems and data sets takes effort.
Failure modes (AT-10)	**Fail-open**	Where rules are unclear, administrators tend to grant broad access to avoid blocking work.
Measurability (AT-14)	**Periodic manual**	Rule compliance is checked through periodic access reviews and audits.
Origin and sourcing (AT-16)	**In-house**	Access rules are organisation-specific.
Cost and value (AT-21)	**Low**	Rule definition is mostly staff time; enforcement costs fall under related technical controls.

Indicative Srida IT values for a typical mid-size organisation; your values depend on how the control is implemented.

D Selection Guidance

- Selected universally; exclusion is almost never justified.
- Strong cue where many users share systems containing data of different sensitivity, as in a hospital information system used by clinicians, billing and administration.
- Attribute query `capabilities = Identity_and_access_management` returns 5.15 to 5.18 and several 8.x controls; Srida IT recommends confirming 5.15 first, as it sets the criteria they are tested against.
- Zero-trust or cloud-first strategies are a cue to revisit the access rules rather than only the technology.

© 2026 Srida IT · Version 1.0 · Independent guidance, not an ISO publication

Free sample pages · The complete manual is available at sridait.com/manuals/rtp-iso27028 · © 2026 Srida IT

E Implementation

1. Write access control rules covering principles (least privilege, need-to-know, deny by default), roles, approval and review.
2. Define role models or access profiles for main job families and key systems.
3. Link rules to classification so that more sensitive information requires stronger approval.
4. Cover physical access, remote access, privileged access and third-party access explicitly.
5. Review the rules annually and when the operating model changes.

F Attribute Views

- In an identity-and-access view, 5.15 heads the cluster; Srida IT shows it as the parent node in access-control dashboards.
- In a Fail-open filter it appears with 5.3, 5.11, 5.18 and 8.2, which together indicate how gracefully access breaks.

G NIST CSF 2.0 Link

- PR.AA-05
- GV.PO-01

H Assurance Testing Procedures

Table 10-31. Assurance testing procedures, control 5.15

Test ID	Method	Testing procedure	Result
TP-5.15-01	**EXAMINE**	Examine the access control policy or rules and confirm least privilege, need-to-know, approval, review, privileged and third-party access are addressed.	☐ Effective ☐ Partial ☐ Not effective ☐ N/A
TP-5.15-02	**INSPECT**	Inspect role definitions for two critical systems and confirm they reflect documented job needs and classification-based rules.	☐ Effective ☐ Partial ☐ Not effective ☐ N/A
TP-5.15-03	**SAMPLE**	Sample 15 users across two systems and compare their actual access with the role definition for their job; record excess rights.	☐ Effective ☐ Partial ☐ Not effective ☐ N/A
TP-5.15-04	**INTERVIEW**	Interview two system owners and ask how they decide whether a request meets the access rules.	☐ Effective ☐ Partial ☐ Not effective ☐ N/A

I Expected Evidence

- Access control policy or rules
- Role or profile definitions
- Access comparison results
- Approval workflow configuration
- Policy review records

J Common Gaps

- No role model exists, so access is cloned from colleagues and accumulates far beyond need.
- The rules do not cover third-party and vendor access, which is granted informally by project teams.

K Related Controls

- 5.16
- 5.17
- 5.18
- 5.3
- 8.2
- 8.3
- 8.5
- 7.2

© 2026 Srida IT · Version 1.0 · Independent guidance, not an ISO publication

Free sample pages · The complete manual is available at sridait.com/manuals/rtp-iso27028 · © 2026 Srida IT

APPENDIX A

Control Attribute Matrix

All 93 ISO/IEC 27002:2022 controls with the Srida IT attribute profile used in Part III. This is a Srida IT assignment informed by ISO/IEC 27002:2022, not a reproduction of its attribute tables; compare it with the licensed standard and adjust it to your own implementation.

Table A-1. Control attribute matrix

Control	Title	Control type	Properties	Concepts	Operational capabilities	Security domains
5.1	Policies for information security	Preventive	Confidentiality, Integrity, Availability	Identify	Governance	Governance and Ecosystem, Resilience
5.2	Information security roles and responsibilities	Preventive	Confidentiality, Integrity, Availability	Identify	Governance	Governance and Ecosystem, Protection, Resilience
5.3	Segregation of duties	Preventive	Confidentiality, Integrity, Availability	Protect	Governance, Identity and access management	Governance and Ecosystem
5.4	Management responsibilities	Preventive	Confidentiality, Integrity, Availability	Identify	Governance	Governance and Ecosystem
5.5	Contact with authorities	Preventive, Corrective	Confidentiality, Integrity, Availability	Identify, Protect, Respond, Recover	Governance	Defence, Resilience
5.6	Contact with special interest groups	Preventive, Corrective	Confidentiality, Integrity, Availability	Protect, Respond, Recover	Governance	Defence
5.7	Threat intelligence	Preventive, Detective, Corrective	Confidentiality, Integrity, Availability	Identify, Detect, Respond	Threat and vulnerability management	Defence, Resilience
5.8	Information security in project management	Preventive	Confidentiality, Integrity, Availability	Identify, Protect	Governance	Governance and Ecosystem, Protection
5.9	Inventory of information and other associated assets	Preventive	Confidentiality, Integrity, Availability	Identify	Asset management	Governance and Ecosystem, Protection
5.10	Acceptable use of information and other associated assets	Preventive	Confidentiality, Integrity, Availability	Protect	Asset management, Information protection	Governance and Ecosystem, Protection
5.11	Return of assets	Preventive	Confidentiality, Integrity, Availability	Protect	Asset management	Protection
5.12	Classification of information	Preventive	Confidentiality, Integrity, Availability	Identify	Information protection	Protection, Defence
5.13	Labelling of information	Preventive	Confidentiality, Integrity, Availability	Protect	Information protection	Defence, Protection
5.14	Information transfer	Preventive	Confidentiality, Integrity, Availability	Protect	Asset management, Information protection	Protection
5.15	Access control	Preventive	Confidentiality, Integrity, Availability	Protect	Identity and access management	Protection

SAMPLE

Free sample pages · The complete manual is available at sridait.com/manuals/rtp-iso27028 · © 2026 Srida IT