ISO/IEC TS 27022

ISO/IEC 27000
ISO/IEC 27001
ISO/IEC 27002
ISO/IEC 27003
ISO/IEC 27004
ISO/IEC 27005
ISO/IEC 27006
ISO/IEC 27007
ISO/IEC TS 27008
ISO/IEC 27010
ISO/IEC 27011
ISO/IEC 27013
ISO/IEC 27014
ISO/IEC TR 27016
ISO/IEC 27017
ISO/IEC 27018
ISO/IEC 27019
ISO/IEC 27021
ISO/IEC TS 27022
ISO/IEC TR 27024
ISO/IEC TS 27028
ISO/IEC TR 27029
ISO/IEC 27031
ISO/IEC 27032
ISO/IEC 27033
ISO/IEC 27034
ISO/IEC 27035

< Previous standard ^ Up a level ^ Next standard >

ISO/IEC TS 27022:2021 — Information technology — **Guidance on information security management system processes** *(first edition)*

Abstract

"[ISO/IEC TS 27022] defines a process reference model (PRM) for the domain of information security management, which is meeting the criteria defined in ISO/IEC 33004 for process reference models (see Annex A). It is intended to guide users of ISO/IEC 27001 to: incorporate the process approach as described by ISO/IEC 27000:2018, 4.3, within the ISMS; be aligned to all the work done within other standards of the ISO/IEC 27000 family from the perspective of the operation of ISMS processes; support users in the operation of an ISMS. [ISO/IEC TS 27022] is complementing the requirements-oriented perspective of ISO/IEC 27003 with an operational, process-oriented point of view."

[Source: ISO/IEC TS 27022:2021]

Introduction

The standard (a **T**echnical **S**pecification) "provides a process reference model (PRM) for information security management, which differentiates between ISMS processes and measures/controls initiated by them ... [and] describes the ISMS processes implied by ISO/IEC 27001."

The standard is based on a PhD thesis.

Scope

According to the scope, the standard "*is intended to guide users of ISO/IEC 27001 to:*

- *incorporate the process approach as described by ISO/IEC 27000:2018 clause 4.3 within the ISMS*
- *be aligned to all the work done within other standards of the ISO/IEC 27000 family from the perspective of the operation of ISMS processes*
- *support users in the operation of an ISMS – the document will complement the requirements oriented perspective of ISO/IEC 27003 with an operational, process oriented point of view."*

The standard does not define any new ISMS requirements, beyond those already defined in ISO/IEC 27001. In other words, it is advisory rather than mandatory.

Purpose and justification

The standard lays out, in some detail, a **P**rocess **R**eference **M**odel comprising a generic suite of ISMS processes that organisations *may* wish to use as a basis for designing custom processes within their own ISMS.

ISO/IEC 27036
ISO/IEC 27037
ISO/IEC 27038
ISO/IEC 27039
ISO/IEC 27040
ISO/IEC 27041
ISO/IEC 27042
ISO/IEC 27043
ISO/IEC 27045
ISO/IEC 27046
ISO/IEC 27050
ISO/IEC 27070
ISO/IEC 27071
ISO/IEC 27090
ISO/IEC 27091
ISO/IEC 27099
ISO/IEC TS 27100
ISO/IEC 27102
ISO/IEC TR 27103
ISO/IEC TR 27109
ISO/IEC TS 27110
ISO/IEC TS 27115
ISO/IEC 27116
ISO/IEC 27400
ISO/IEC 27402
ISO/IEC 27403
ISO/IEC 27404
ISO/IEC TR 27550
ISO/IEC 27551
ISO/IEC 27553
ISO/IEC 27554
ISO/IEC 27555
ISO/IEC 27556
ISO/IEC 27557
ISO/IEC 27559
ISO/IEC TS 27560

Structure and content

The ISMS processes described fall into 3 “categories” (types or groups) *i.e.*:

- **Governance activities** (confusingly titled ‘management processes’) - direction and oversight for the ISMS;
- **Core operations** *e.g.* information risk and security management, policy management, incident management, internal audits ...; and
- **Support** *e.g.* records management, communicating with interested parties about the ISMS, managing relationships with ISMS ‘customers’ ...

The processes are each laid out in an Appendix, first as a table specifying:

- Process “category” denoting the type of process
- A brief description
- Objective/purposes
- Input[s] and Output[s]
- Activities/functions *i.e.* a few words for each of the main steps in the process
- Informative references.

The table is followed by a flowchart summarising the process on one side or less.

Status

The *first* edition was published in **2021**.

An *amendment* updating references to ISO/IEC 27001:2022 and other ISO27k standards was in preparation in **2024**. A proposal to revise the standard was dropped due to lack of expert support.

Personal comments

Mature organisations may already have processes for:

1. Asset management;
2. Audit management, both internal and external;
3. Business continuity management (see ISO 22301);
4. Change management plus configuration management and version control;
5. Continuous improvement and maturity management;
6. Database [security] management;
7. Exemption management (management-approved nonconformity with policies);
8. Facilities management including power and other services for the computer room;
9. Identity, access rights and user account management;
10. Incident management including incident investigation and forensics;
11. Information management in general;
12. Information [security] risk management (partly covered by ISO/IEC 27005);
13. Information security management (covered by ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27003 and others);
14. IT!
15. Internal audits and certification audits;
16. Key management, plus the rest of cryptography;
17. Log management, plus alarms and alerts;
18. Metrics and management information management (partly covered by ISO/IEC 27004);
19. Monitoring and oversight of the risk management and security arrangements;
20. Patching, including emergency arrangements for urgent fixes;

ISO/IEC 27561
ISO/IEC 27562
ISO/IEC TR 27563
ISO/IEC 27564
ISO/IEC 27565
ISO/IEC 27566
ISO/IEC 27568
ISO/IEC 27569
ISO/IEC TS 27570
ISO/IEC 27573
ISO/IEC 27701
ISO/IEC 27706
ISO 27799

21. Performance and capacity management;
22. Personnel/HR management including “onboarding” and “offboarding” (nasty neologisms!);
23. Preventive and corrective actions;
24. Quality management, especially quality assurance;
25. Service management [organisations that are heavily process-oriented may be using ITIL/ISO 20000, in which case ISO/IEC 27013 is applicable];
26. Supplier/vendor relationship management, including telecomms, Internet and cloud services, outsourced development, contract security guards, maintenance/servicing, professional services (consulting, contracting, accounting, tax advising) *etc.*;
27. System and network [security] management;
28. System/software development and testing ...

... and more.

Providing generally-applicable advice without imposing further constraints is challenging. The processes need to be described without losing the flexibility to cater for myriad differences between organisations. In particular, the processes need to be valuable (cost-effective) in practice to justify their existence, for instance by:

- Removing unnecessary bureaucracy, rationalising and justifying whatever remains;
- Facilitating or encouraging process automation and innovation where applicable;
- Facilitating or encouraging use of existing processes, adapting them where necessary;
- Perhaps re-using effective ISMS processes elsewhere in the organisation;
- Managing the processes themselves *e.g.* management processes for monitoring, reviewing, evaluating and maintaining the ISMS processes, responding to changes, identifying and exploiting improvement opportunities *etc*.

It would be unfortunate if ISMS processes were perceived as distinct from normal operations, rather than being integral to the organisation’s routine activities. The process for managing an information security or privacy incident, for example, is essentially the same as that for managing any other incident, hence it is generally unnecessary to create an alternative incident management process if the existing one (perhaps with a few tweaks) is effective.

< Previous standard ^ Up a level ^ Next standard >