anchor@anchor-cyber:~$ man iso-27001-2022

ANCHOR CYBER SECURITY LLC

# ISO/IEC 27001:2022 — Field Reference

Structure only — clause numbers, Annex A themes, and a CSF crosswalk. Not a substitute for the licensed standard.

**WHY THIS CARD IS THIN ON DETAIL**

ISO/IEC 27001 is a copyrighted, licensed standard — unlike NIST's public-domain work, its actual clause and control requirement text can't be reproduced here. This card indexes structure (numbers, theme names, counts) so you can navigate a real engagement; for the actual requirement wording, use Anchor's purchased copy of the standard.

## The ISMS Clauses / 4 – 10, the mandatory requirements

| | | |
|---|---|---|
| 4 | **Context** | Understand the organization, interested parties, and what's actually inside the ISMS boundary. |
| 5 | **Leadership** | Top management commits, sets policy, and assigns roles/authorities — same spirit as CSF's GV.RR. |
| 6 | **Planning** | Risk assessment and treatment plan; security objectives. The engine room of the whole ISMS. |
| 7 | **Support** | Resources, competence, awareness, communication, and documented information. |
| 8 | **Operation** | Actually execute the risk treatment plan and run the controls day to day. |
| 9 | **Evaluation** | Internal audit and management review — is the ISMS actually working. |
| 10 | **Improvement** | Nonconformity handling and continual improvement — closes the loop back to Clause 6. |

$ iso27001 --annex-a

## Annex A — Four Themes / 93 controls total

### A.5
**Organizational**

Policy, roles, supplier relationships, incident management, business continuity, compliance.

controls **37** (A.5.1 - A.5.37)

### A.6
**People**

Screening, terms of employment, awareness/training, disciplinary process, remote working.

controls **8** (A.6.1 - A.6.8)

### A.7
**Physical**

Secure areas, equipment, media handling, clear desk/clear screen, physical monitoring.

controls **14** (A.7.1 - A.7.14)

### A.8
**Technological**

Access control, cryptography, ops security, network security, secure development.

controls **34** (A.8.1 - A.8.34)

$ iso27001 --diff 2013 2022

## The 11 Controls New in 2022

| CODE | TITLE |
|---|---|
| **5.7** | Threat intelligence |
| **5.23** | Information security for use of cloud services |
| **5.30** | ICT readiness for business continuity |
| **7.4** | Physical security monitoring |
| **8.9** | Configuration management |
| **8.10** | Information deletion |
| **8.11** | Data masking |
| **8.12** | Data leakage prevention |
| **8.16** | Monitoring activities |
| **8.23** | Web filtering |
| **8.28** | Secure coding |

$ iso27001 --crosswalk csf-2.0

## Rough CSF 2.0 Crosswalk

/ our own read, not an official NIST or ISO mapping

| ANNEX A THEME | NEAREST CSF FUNCTIONS | WHY |
|---|---|---|
| A.5 Organizational | GV, ID | Policy, roles, supplier/incident management overlap heavily with GOVERN and IDENTIFY. |
| A.6 People | PR.AT | Screening, training, and disciplinary process map onto Awareness and Training almost directly. |
| A.7 Physical | PR.PS, PR.IR | Facilities and equipment controls sit under Platform/Infrastructure resilience. |
| A.8 Technological | PR.AA, PR.DS, DE.CM | Access control, crypto, and monitoring split across Protect and Detect. |

src: ISO/IEC 27001:2022 (structure only — full text is ISO's licensed content) exit 0