**ISO 27002: 2022**

[**https://www.isms.online/iso-27002/**](https://www.isms.online/iso-27002/)

[**https://www.urmconsulting.com/blog/**](https://www.urmconsulting.com/blog/)

**About:D**

It is an information security standard published by ISO/IEC. It has a close association with ISO 27001.

It provides guidance on how to implement ISO 27001 ISMS security controls listed in Annexure A (93 controls)

The 2022 versions includes new controls reflecting **threat intelligence and cloud security.**

ISO 27002 is not a certifiable standard.

However compliance with its information security, physical security, cyber security, privacy management guidelines brings the organisation a step closer in meeting ISO 27001 certification requirements.

It helps to enhance an organisation’s security posture, manage risks, align with best practices in information security management.

It is a **guidance standard**, not a requirement standard

It provides a reference set of information security, cyber security and privacy protection controls.

It is designed in such a way that it is applicable to all organisations

Helps organisations identify which controls are applicable to them by dividing them into themes

**Importance:**

Organisations collect, use and process all sorts of data including PII. With every plus point comes a minus point which is that, there is always risks and threats to watch out for.

An effective **ISMS** system is required to maintain the CIA triad within the organisation. It has a broad scope which may cause as a challenge.

**Benefits:**

An assurance to the organisation that the assets are protected.

It is an ever evolving, updating working framework

It reflects itself as a compliant and reliable organisation to clients and business partners, hence forming a good reputation for themselves.

These requirements are internationally recognised.

Increases overall productivity.

ISO compliant organisation will have advantage in contract negotiations and participation in global business opportunities.

One can benefit from lower insurance premiums from providers

**Why was it revised? :**

New version was published on **15th February 2022**

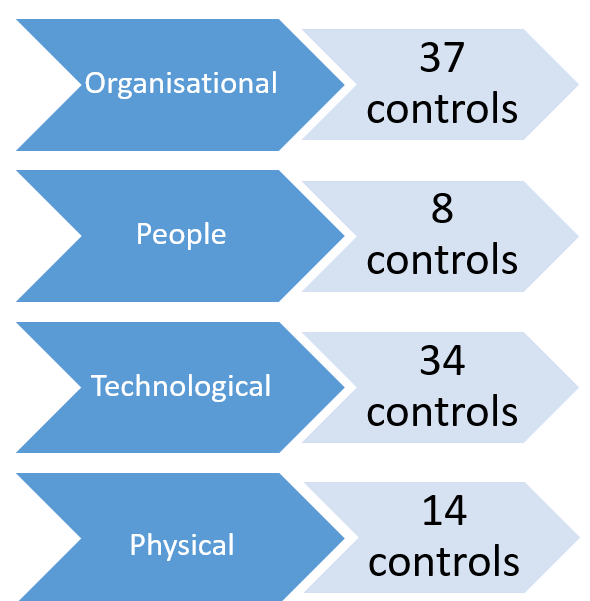
In order to update information security controls to reflect developments and current information security practices in various sectors.

**Changes made:**

To retrieve focus from Code of Practice and positioning it as an information security control

It serves as a more straightforward structure that can be applied.

It is capable to manage a broader risk profile.



**Change of name/ title:**

**Before:** ISO 27002:2013 was titled :-

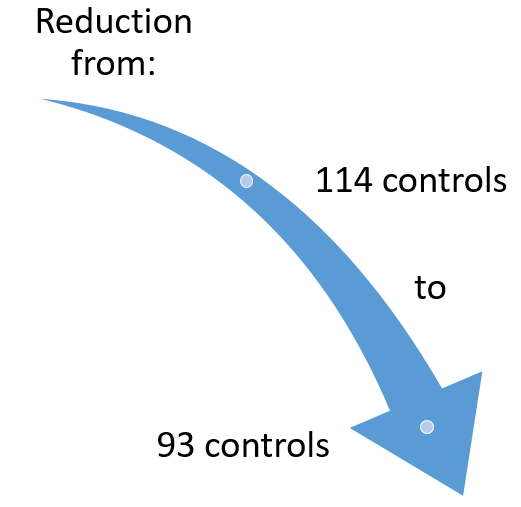
Information technology – Security techniques – Code of practice for information security controls

**After:** ISO 27001: 2022 :-

Information security, Cybersecurity and privacy protection – Information security controls

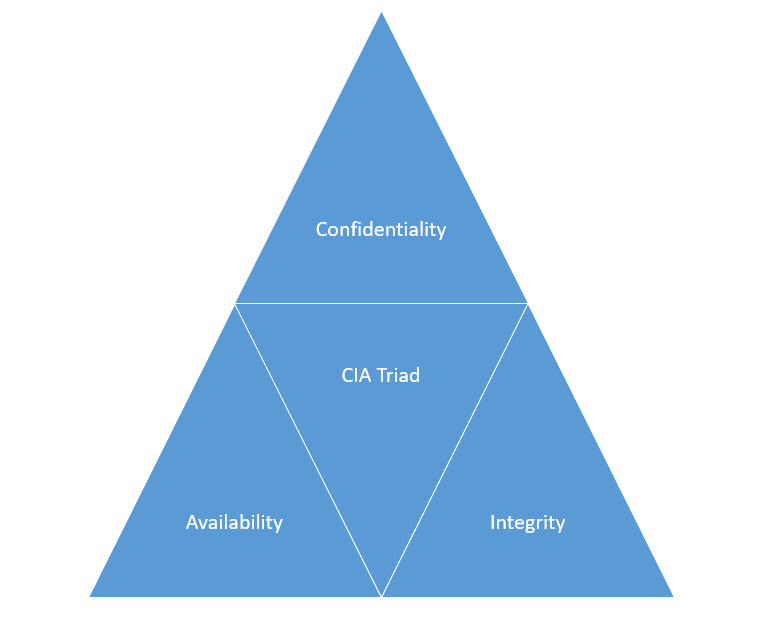
**Reason for change:**

Evolving business continuity, cyber risks needs an information security control objective and broadened scope for use in context specific scenarios



* A total of 24 controls were merged from few security controls from 2013 version
* 58 controls have been reviewed and revised to align with current environment
* Robust language utilisation
* Controls equipped with **Purpose** and **Attributes** statement

**Information Security Properties:**



**NIST Cybersecurity Framework Model Concepts:**

1. **Identify**: To look for or make out the discrepancies in security and to check for security risks
2. **Protect**: To protect the identified information from risks
3. **Detect:** To detect occurrence of a cyber security event
4. **Respond:** To take necessary action against detected cyber security events
5. **Recover:** To help the organisation restore back after the event of an attack. It is the most necessary step.

**Operational Capability:**

View Controls from practitioner’s perspective of information security capabilities

**Security Domains:**

View controls from perspective of 4 security domains:

1. Governance and Ecosystem
2. Information system security governance
3. Risk Management
4. Ecosystem cyber security management

* Control have various applications
* Several controls are required in a given situation
* The controls have minor elements

**Annex A:**

The table demonstrates use of attributes giving examples of how to assign attributes to controls

*New Controls:*

|  |  |
| --- | --- |
| **ISO 27002: 2022 New Control** | **Control Name** |
| 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 |

5 organisational and 1 people’s control describe the measures needed for organisations to prevent, detect, report and correct information security incidents:

*Incident Management Controls*

* **A.5.24 – Information security incident management planning and preparation**
* **A.5.25 – Assessment and decision on information security events**
* **A.5.26 – Response to information security incidents**
* **A.5.27 – Learning from information security incidents**
* **A.5.28 – Collection of evidence**
* **A.6.8 – Information security event reporting.**

**Why are they necessary?**

Organisation will have to respond to security incidents.

ISO 27002: 2022 defines information security incidents as one or multiple related and identified information security events that can harm an organisation’s assets or compromise its operations’.

**Types of incident management controls:**

* Preventive: - Stop in incident from occurring / reduce the likelihood of an incident
* Corrective:- Resolve an already occurred issue
* Detective:- Detect incidents as and when it occurs

**Implementing Annex A incident management controls:**

**A.5.24 – Information security incident management planning and preparation:-**

Define and document organisation’s approach to handling security incidents. This is achieved by documented incident management policy or procedure. It must cover entire incident lifecycle.

It also needs to describe who within the organisation is responsible for responding to incidents along with appropriate contact.

It must need to define the responsibilities of all members of staff in scenario of incident management.

* Notifying individual immediately after occurrence of incident
* To provide accurate testimonies during investigation
* Cooperating with incident management team during response phase

The document needs to be communicated to all members of staff.

**A.5.25 – Assessment and decision on information security events**

Organisation must clearly be able to distinguish between infosec events and incidents.

For better understanding it is advisable for users to have a documented list of types of incidents which makes it easier for the staff to distinguish and understand the criteria for types.

Examples: A phishing email, business secrets leaks

Organisation must also provide criteria for weakness or flaws that could lead to an incident in the future.

Examples: Unpatched software, Poor encryption

An individual such as a CISO must be held responsible for the declaration and communication of the incident.

**A.5.26 – Response to information security incidents**

Response with due procedures. All staff members must read, acknowledge the policy and ensure they are fully aware of their responsibilities.

Recording of all steps followed during investigation in an incident log / report. It would be part of a review or management meeting.

Implement documented response plans for incident types, prioritise based on results of risk assessments which enables organisation to respond more consistently.

**A.5.27 – Learning from information security incidents**

How and what triggered assets to be compromised. It helps us to understand which threat routes are taken.

Organisation must regularly use information about incidents faced to determine new controls or upgrade existing controls

This information can be captured in an incident report or in the log.

What to document? :

* What has occurred
* How it occurred
* What the response was
* How infosec controls can be improved to reduce impact or likelihood of events in the future

It is a good practice to take recordings of discussions as evidence

**A.5.28 – Collection of evidence**

Considered whether to take legal or disciplinary action

It depends on the type of incident that has occurred along with the necessary evidence collected

This control ensures that evidence has been identified, collected, acquired, preserved. It also helps understand what types are needed, how it is collected, stored and the methodology of chain of custody being established.

Focus on if it is recovering from an incident or identifying threat actors behind it.

Helps in making a radicalised proportionate choice while collecting evidence.

**A.6.8 – Information security event reporting.**

Organisation must provide a way to report any events. A common practice is to document the organisation’s point of contact within incident management policy.

Its updation must be done at a regular basis to the personnel of the organisation, including contractors.

The faster the reporting the better the handling of the impact.

Incident reporting channels must also be secure.

Examples are dedicated email address, incident chats on Microsoft teams, incident forms, online reporting pages, service desk tickets.

**ISO 27001 VS ISO 27002:**

|  |  |
| --- | --- |
| **ISO 27001** | **ISO 27002** |
| Management standard defining how to build an infosec system | When implementation specific security controls needed to safeguard ISMS |
| Scope, design to build a compliant ISMS | Set of guidelines and techniques for implementing security controls |
| We can certify to it | We cannot certify to it |
| Specify risk assessment by organisation | Does not specify it |
| Standard for when in the initial process of starting | Must be referred to once controls have been identified which must be implemented |
| Certifiable standard that sets requirements for an ISMS | Supplementary standard providing detailed guidelines |
| Set Requirements | Detailed guidance |
| Focus on ISMS framework | Guidance on implementing the security controls |
| Has mandatory clauses 4-10 that must be complied with for certification | Are not mandatory and can be adapted to the organisation's specific needs |

**How does it affect the organisation? :**

In a certain period organisations are required to adopt to the revised versions of the ISO 27001 for their certification audits.

This provides them ample time to make changes and must not significantly impact the ISMS ability to sustain compliance.

When converting to a new standard organisations need to reassess how their frameworks, controls, policies align with the new structure and updated controls.

**Who all will the revision affect? :**

* If already ISO 27001: 2013 certified
* Are in between mid certification
* About to re certify

🡪 **The revised standard will be applicable upon renewal / re certification**

**Hence, all certified organisations would have to prepare for the revised standard upon re-certification or if adopting new sets of controls**

**How will it affect re certification? :**

* They would be expected to revisit their Risk assessment
* Identify new controls
* Revise their Statement of Applicability by comparing revised Annex A controls

**Compliance must also include:**

* Update to risk treatment process along with updated controls
* Update to Statement of Applicability
* Update current policies and procedures along with guidance against each control where necessary

Until a new standard is published the current schemes will continue

**Which new standards would be affected?**

Management standards and frameworks related to ISO 27002:2013 version will feel the change.

Will have an additional impact when they enlarge to related standards and various national standards that have adopted the guidance

**Good Practice guidelines for ISO 27002:**

**Physical and Environmental:** Proper controls and procedures will ensure physical safety against unauthorised access as well as protecting them against physical/ environmental disasters such as flood etc.

*Security Techniques:*

* Monitor and restrict physical access to the premises
* Support Infrastructures for eg. Air conditioning, power
* Partial / restricted access to sensitive areas. List containing number of authorised individuals periodically reviewed and approved
* Digital recording must be forbidden in restricted areas except for when explicitly granted permission of a relevant authority. Such an example can be when images required for internal audit
* Surveillance must be set around places such as entry, exit, restricted areas. The footage must be carefully monitored by the surveillance personnel and the retention period must be in accordance with the company policy but in regular cases it must be stored for atleast a month
* Restricted access can be granted in the form of access cards, one time passwords or surveillance warrants
* Visitors must be accompanied by employees at all times

**Human Resources:** Measures to ensure the information is safe in perspective of the employees

*HR Security Standards:*

* Employee screening before employment process. Must make sure all the information provided is accurate and credible
* Employees must agree to sign NDAs. It will guide them on the level of discretion
* Employee status updation must be done to all departments
* Employee status must be followed by an updation the relevant physical and logical access rights
* Managers must follow up to assure proper keys, access cards collection and returning all company assets before termination

**Access Control:**

Involves keys, passwords, access cards etc. designed to limit the accessibility of the assets and infrastructure

* Role based and rule based access control. These are specified by the asset owners or procedures
* Appropriate alerts must be set to lock out users after number of failed attempts. These must be followed up by elimination
* All in-house workstations must be password protected and a timeout must be set of less than 10 minutes
* Privileged access rights must be periodically reviewed
* Passwords kept must be complex, lengthy, completely un-guessable. Must be a combination of numbers, special characters
* Must be stored in unreadable formats
* All write access to removable media must be disabled unless specifically authorised