CPE EVENT ON:

ISO 27002:2022 new revision overview with ISO 27002:2013 comparison and certification process

Host for the Webinar : Saurabh Singh

ISACA
New Delhi Chapter

Rules of the Session:

1. 1 CPE will be credited to participants who have logged in for more than 50 minutes.
2. Questions can be asked through typing in the chat box.
3. Presentation deck will be posted on ISACA New Delhi Chapter portal.
4. Recorded video will be published on ISACA New Delhi YouTube channel (https://bit.ly/3yBaqhl)
5. Feedback form will be shared at the end of the session for your valuable input.

For any additional support with Certification or chapter queries : Connect with ISACA New Delhi chapter representatives or email us @ info@isacanewdelhi.org WhatsApp @ +91-9818422212

ISACA New Delhi Chapter

Harisaiprasad K

CISA, APP, ISO 27001 LA, ISO 22301 LI, ISO 9001 LA, Six Sigma Green Belt

Consultant in a private sector company. He has 14+ years of experience in the industry, works in the area of SOX audits and controls review. He has also conducted ISO 27001 audits, regulatory audits, third-party audits, internal audits, IT audits, BCP reviews, user awareness training, internal auditor training, risk assessments and implemented ISO 27001, among other tasks. He is currently ISACA New Delhi (India) Chapter leader and social media chair. He is also a topic leader for the ISACA Certified Information Systems Auditor (CISA) online forum and GLS task force member. He has spoken in international conferences, published articles related to the information security domain in the ISACA Now blog, COBIT Focus, and in the ISACA Journal

ISACA
New Delhi Chapter

Contents

- Learning Objectives
- Introduction of ISO 27002:2022 standard
- Clauses & Controls
- Elements of Controls
- Comparison between ISO 27002:2013 and ISO 27002:2022
- Process of ISO 27001 certification
- Implementation of ISO 27001

Learning Objectives

- Understand ISO 27002:2022 Standard
- Know the differences between the current version and previous version
- Have knowledge of implementing new controls, updating documentation based on merged controls
- Help their organization process getting certified for ISO 27001

Introduction to ISO 27002:2022

- ISO is specialized system for worldwide standardization. Standard provides guidelines for Information security, cybersecurity and privacy protection of Information security controls
- Provides a generic mixture of organizational, people, physical and technological information security controls derived from internationally recognized best practices
- Guidance document for an organisation for determining and implementing commonly accepted information security controls
- Developing industry and organisation specific information security management guidelines
- Helps in developing controls necessary to ensure that the residual risk to the organization meets its risk acceptance criteria

Main changes to ISO 27002:2022

- Modified title “Information security, cybersecurity and privacy protection - Information security controls”
- Changed structure with controls having simplified taxonomy, and associated attributes
- Some controls are merged, deleted, and new controls are introduced in Annex B

Clauses and Controls

Clause Number	Clause Name	Number of controls	Remarks
5	Organisational	37	34 existing, 3 new
6	People	8	All existing
7	Physical controls	14	13 existing, 1 new
8	Technological controls	34	27 existing, 7 new

New Controls

Type of Control	Control	
Organisational Control	5.7	Threat intelligence
Organisational Control	5.23	Information security for use of cloud services
Organisational Control	5.30	ICT readiness for business continuity
Physical Control	7.4	Physical Security Monitoring
Technological Control	8.9	Configuration management
Technological Control	8.10	Information Deletion
Technological Control	8.11	Data masking
Technological Control	8.12	Data leakage prevention
Technological Control	8.16	Monitoring activities
Technological Control	8.23	Web filtering
Technological Control	8.28	Secure coding

Renamed Controls

ISO/IEC 27002:2013 control		ISO/IEC 27002:2022 control	
6.2.2	Teleworking	6.7	Remote working
9.2.1	User registration and de-registration	5.16	Identity management
9.2.3	Management of privileged access rights	8.2	Privileged access rights
9.4.2	Secure log-on procedures	8.5	Secure authentication
9.4.5	Access control to program source code	8.4	Access to source code
7.3.1	Termination or change of employment responsibilities	6.5	Responsibilities after termination or change of employment
11.1.1	Physical security perimeter	7.1	Physical security perimeters
11.2.6	Security of equipment and assets off-premises	7.9	Security of assets off-premises
11.2.9	Clear desk and clear screen policy	7.7	Clear desk and clear screen
12.2.1	Controls against malware	8.7	Protection against malware

Renamed Controls

ISO/IEC 27002:2013 control		ISO/IEC 27002:2022 control	
12.7.1	Information systems audit controls	8.34	Protection of information systems during audit testing
13.1.1	Network controls	8.20	Networks security
13.1.3	Segregation in networks	8.22	Segregation of networks
14.2.1	Secure development policy	8.25	Secure development life cycle
14.2.5	Secure system engineering principles	8.27	Secure system architecture and engineering principles
14.3.1	Protection of test data	8.33	Test information
15.1.1	Information security policy for supplier relationships	5.19	Information security in supplier relationships
15.1.2	Addressing security within supplier agreements	5.20	Addressing information security within supplier agreements

Renamed Controls

ISO/IEC 27002:2013 control		ISO/IEC 27002:2022 control	
15.1.3	Information and communication technology supply chain	5.21	Managing information security in the ICT supply chain
16.1.1	Responsibilities and procedures	5.24	Information security incident management planning and preparation
16.1.4	Assessment of and decision on information security events	5.25	Assessment and decision on information security events
18.1.4	Privacy and protection of personally identifiable information	5.34	Privacy and protection of PII

Merged Controls

ISO/IEC 27002:2013 control		ISO/IEC 27002:2022 control	
5.1.1 5.1.2	Policies for information security Review of the policies for information security	5.1	Policies for information security
6.1.5 14.1.1	Info. Sec. in project management Information security requirements analysis and specification	5.8	Information security in project management
6.2.1 11.2.8	Mobile device policy Unattended user equipment	8.1	User end point devices
8.1.1 8.1.2	Inventory of assets Ownership of assets	5.9	Inventory of information and other associated assets
8.1.3 8.2.3	Acceptable use of assets Handling of assets	5.10	Acceptable use of information and other associated assets

Merged Controls

ISO/IEC 27002:2013 control		ISO/IEC 27002:2022 control	
8.3.1 8.3.2 8.3.3 11.2.5	Management of removable media Disposal of media Physical media transfer Removal of assets	7.10	Storage media
9.1.1 9.1.2	Access control policy Access to networks and network services	5.15	Access control
9.2.2 9.2.5 9.2.6	User access provisioning Review of user access rights Removal or adjustment of access rights	5.18	Access rights

Merged Controls

ISO/IEC 27002:2013 control		ISO/IEC 27002:2022 control
9.2.4 9.3.1 9.4.3	Management of secret authentication information of users Use of secret authentication information Password management system	5.17 Authentication information
10.1.1 10.1.2	Policy on the use of cryptographic controls Key management	8.24 Use of cryptography
11.1.2 11.1.6	Physical entry controls Delivery and loading areas	7.2 Physical entry

Merged Controls

ISO/IEC 27002:2013 control		ISO/IEC 27002:2022 control
12.1.2 14.2.2 14.2.3 14.2.4	Change management System change control procedures Technical review of applications after operating platform changes Restrictions on changes to software packages	8.32 Change management
12.1.4 14.2.6	Separation of development, testing and operational environments Secure development environment	8.31 Separation of development, test and production environments
12.4.1 12.4.2 12.4.3	Event logging Protection of log information Administrator and operator logs	8.15 Logging

Merged Controls

ISO/IEC 27002:2013 control		ISO/IEC 27002:2022 control
12.5.1 12.6.2	Installation of software on operational systems Restrictions on software installation	8.19 Installation of software on operational systems
12.6.1 18.2.3	Management of technical vulnerabilities Technical compliance review	8.8 Management of technical vulnerabilities
13.2.1 13.2.2 13.2.3	Information transfer policies and procedures Agreements on information transfer Electronic messaging	5.14 Information transfer

Merged Controls

ISO/IEC 27002:2013 control		ISO/IEC 27002:2022 control	
14.1.2 14.1.3	Securing application services on public networks Protecting application services transactions	8.26	Application security requirements
14.2.8 14.2.9	System security testing System acceptance testing	8.29	Security testing in development and acceptance
15.2.1 15.2.2	Monitoring and review of supplier services Managing changes to supplier services	5.22	Monitoring, review and change management of supplier services
16.1.2 16.1.3	Reporting information security events Reporting information security weaknesses	6.8	Information security event reporting

Merged Controls

ISO/IEC 27002:2013 control		ISO/IEC 27002:2022 control
17.1.1 17.1.2 17.1.3	Planning information security continuity Implementing information security continuity Verify, review and evaluate information security continuity	5.29 Information security during disruption
18.1.1 18.1.5	Identification of applicable legislation and contractual requirements Regulation of cryptographic controls	5.31 Legal, statutory, regulatory and contractual requirements
18.2.2 18.2.3	Compliance with security policies and standards Technical compliance review	5.36 Conformance with policies, rules and standards for information security

Split Controls

There is only one control that was split: 18.2.3 Technical compliance review was split into 5.36 Conformance with policies, rules and standards for information security and 8.8 Management of technical vulnerabilities.

Elements of each control

New Elements – Attribute Table

S.No	Attributes	Control
1	Control types	Preventive, Detective, and Corrective
2	Info. Sec. properties	Confidentiality, Integrity, and Availability
3	Cybersecurity concepts	Identify, Protect, Detect, Respond, and Recover
4	Operational Capabilities	Governance, Asset mgmt., Info. protection, HR sec., Physical sec., S/m & network sec., Application sec., Sec. configuration, IAM, Threat and vulnerability management, Continuity, Supplier relationships sec., Legal and compliance, Info. Sec. event management, and Info. Sec. assurance
5	Security domains	Governance and ecosystem, Protection, Defense, and Resilience

Status of already existing elements in ISO 27002:2013

The elements that already existed in the ISO 27002:2013 & remain in this new revision are:

- ***Control title: T***he name of the control.
- ***Control:*** A description of what needs to be accomplished to be compliant with the control.
- ***Guidance:*** Tips on how the control should be implemented.
- ***Other information:*** Complementary information to understand the control and references to other documents for consultation.

Control Layout

- Control title
- Attribute table
- Control
- Purpose
- Guidance
- other information

ISO 27002 Control Identifier	Control Name	Control Type	Info. Sec. Properties	Cybersec. Concepts	Opertnal. Capabilities	Security Domains
5.30	ICT readiness for BC	Corrective	Availability	Respond	Continuity	Resilience

Sample – Control 5.5 Contact with Authorities

Control Type	Info. Sec. Properties	Cybersecurity concepts	Operational Capabilities	Security Domains
Preventive Corrective	Confidentiality Integrity Availability	Identify & Protect Respond & Recover	Governance	Defence Resilience

Control: The organisation should establish and maintain contact with relevant authorities

Purpose: To ensure appropriate flow of information takes place with respect to information security between the organisation and relevant legal, regulatory and supervisory authorities

Sample – Control 5.5 Contact with Authorities

Guidance: The organisation should specify when and by whom authorities (eg., law enforcement, regulatory bodies, supervisory authorities) should be contacted and how identified information security incidents should be reported in a timely manner.
Contact with authorities should also be used to facilitate the understanding about the current and upcoming expectations of these authorities (eg., application information security regulations)
Other information Organisations under attack can request authorities to take action against the attack source.

Maintaining such contacts can be requirement to support information security incident management (see 5.24 to 5.28) or the contingency planning and business continuity process (see 5.29 and 5.30). Contacts with regulatory bodies are also useful to anticipate and prepare for upcoming changes in relevant laws or regulations that affect the organisations. Contacts with other authorities include utilities, emergency services, electricity suppliers and health and safety (eg., fire departments (in connection with business continuity), telecommunication providers (in connection with line routing and availability) and water suppliers (in connection wit cooling facilities for equipment)

Using Attributes – Annex A

- Select what an organisation wants to view
- Add/delete attributes as suitable
- Approach that is useful for navigating the controls relation to events risk scenarios, risk treatment plan, compliance requirements, etc.,
- Useful in tools (GRC, spreadsheets, reports)

ISO 27002:2013 and ISO 27002:2022 Comparison

S.No	ISO 27002:2013	ISO 27002:2022
1	Information technology - Security techniques - Code of practice for information security controls	Information security, cybersecurity and privacy protection - Information security controls
2	Assets associated with information and information processing facilities Organisation assets Assets	Information and other assets ***Primary assets*** Information business processes and activities ***Supporting assets (on which primary assets rely)*** • Hardware, software, Network, Personnel, Site, organisations structure

ISO 27002:2013 and ISO 27002:2022 Comparison

S.No	ISO 27002:2013	ISO 27002:2022
3	Through a risk assessment, threats to assets are identified	Information security specific risk assessment
4	14 Control clauses, 114 controls	4 Clauses, 93 controls

ISO 27002:2013 and ISO 27002:2022 Comparison

ISO 27002:2013

5 Information security policies
5.1 Management direction for information security

Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

5.1.1 Policies for information security

Control

A set of policies for information security should be defined, approved by management, published and communicated to employees and relevant external parties.

Implementation guidance

At the highest level, organizations should define an "information security policy" which is approved by management and which sets out the organization's approach to managing its information security objectives.

Information security policies should address requirements created by:

... ...

Other information

Some organizations use other terms for these policy documents, such as "Standards", "Directives" or "Rules".

ISO 27002:2022

5 Organizational controls

5.1 Policies for information security

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Governance	#Governance_and_Ecosystem #Resilience

Control

Information security policy and topic-specific policies should be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.

Purpose

To ensure continuing suitability, adequacy, effectiveness of management direction and support for information security in accordance with business requirements, legal, statutory, regulatory and contractual requirements.

Guidance

At the highest level, organizations should define an "information security policy" which is approved by top management and which sets out the organization's approach to managing its information security.

The information security policy should take into consideration requirements derived from:

... ...

Other information

Topic-specific policies can vary across organizations.

Process of ISO 27001 certification

- Gap Analysis
- Documentation
- Implementation
- Awareness training
- Selecting Certification body
- Operation
- Records and metrics
- Pre-assessment
- Internal Audit
- Corrective action plan
- Management review
- Stage 1 & Stage 2 Audit
- Certification
- Surveillance audits (annual)

Implementation of ISO 27001

- Risk assessment along with justification of exclusion of controls
- Requirements
- Agility
- Roles and responsibilities defined
- Metrics
- Continual improvements
- Reporting

Road Ahead

- Gap assessment with the control of ISO 27002:2022 with that of your organisation
- Audit you processes based on the new controls, document their status and determine requirements of implementation
- Update and get approval of Statement of Applicability, risk assessment, process procedures and metrics
- Get certified with revised standard within the grace period

References

- ISO 27001:2013 - Information technology — Security techniques — Information security management systems — Requirements
- ISO 27002:2013 - Information technology — Security techniques — Code of practice for information security controls
- ISO 27002:2022 - Information security, cybersecurity and privacy protection — Information security controls

Questions ?

Contact: harisaiprasad@gmail.com

https://www.linkedin.com/in/harisaiprasad-k-cisa-app-b4225015/

Thank You !