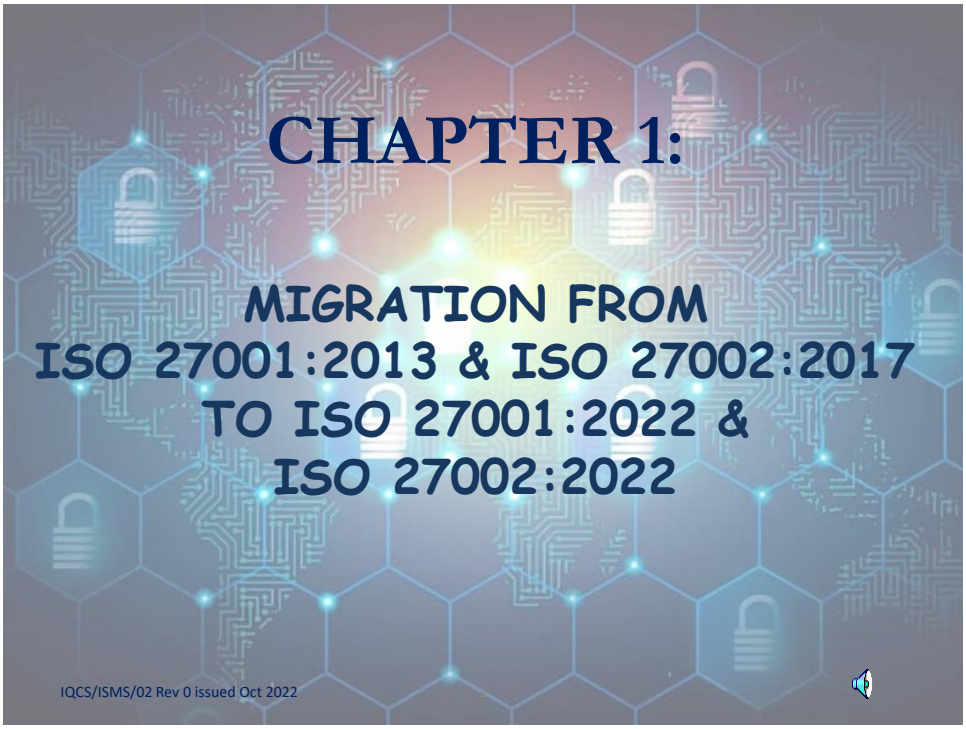
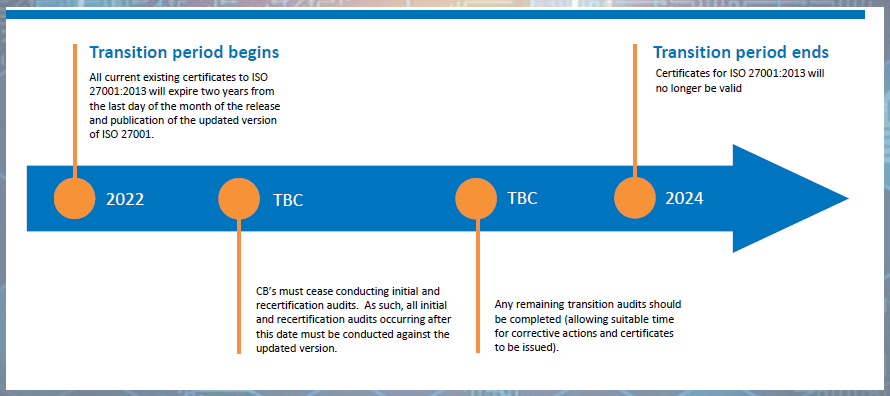

IQCS
CQI
IRCA
APPROVED TRAINING PARTNER
ISMS FDIS ISO 27001:2022
LATEST CHANGES
(pre-course reading purpose)
IQCS/ISMS/02 Rev 0 issued Oct 2022
1


CHAPTER 1:
MIGRATION FROM
ISO 27001:2013 & ISO 27002:2017
TO ISO 27001:2022 &
ISO 27002:2022
IQCS/ISMS/02 Rev 0 issued Oct 2022

Transition period



Changes ISO 27001:2022

- Refinement of 4.2 Interested parties
- Refinement of 4.3 Scope
- Refinement of 6.1.3 Risk treatment
- Addition of 6.3 Change management
- Splitting 9.2 into 9.2.1 General / 9.2.2 Audit program
- Splitting 9.3 into 9.3.1 General / 9.3.2 Input / 9.3.3 Output

Changes ISO 27001:2022

Clause 8.2
The organisation shall perform information security risk assessments at planned intervals **or when significant changes are proposed or occur.**
Clause 6.1.3
b) Determine all controls that are necessary to implement the information security risk treatment options c) **Compare the controls determined in 6.1.3 b) with those in Annex A and verify that no necessary controls have been omitted** d) Produce a statement of applicability e) Formulate an information security risk treatment plan

Changes ISO 27002:2022

2017	Information technology – Security techniques – Code of practise for information security controls (ISO/IEC 27002:2013)
2022	Information security, cybersecurity and privacy protection – Information security controls

Changes ISO 27002:2022

2017 14 Control Groups

Control Groups	
5. Policies	12. Operations
6. Organisation	13. Communications
7. Human resources	14. Dev and maintenance
8. Asset management	15. Suppliers
9. Access Control	16. Incidents
10. Cryptography	17. Business Continuity
11. Physical	18. Compliance

2022 4 Themes

Theme clauses	
5. Organisational	7. Physical
6. People	8. Technology

Changes ISO 27002:2022

2017

6 Organization of information security

6.1 Internal organization

~~Objective: To establish a management framework to initiate and control the implementation and operation of information security within the organization.~~

6.1.1 Information security roles and responsibilities

Control

All information security responsibilities should be defined and allocated.

Changes ISO 27002:2022

2017 114 controls

19 controls consolidated
11 new controls
n deleted controls?

2022 93 controls

Changes ISO 27002:2022

Attributes are used to create different views of the controls

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive #Detective #Corrective	#Confidentiality #Integrity #Availability	#Identity #Protect #Detect #Respond #Recover	#Governance #Asset_management #Information_protection #Human_resource_security #Physical_security #System_and_network_security #Application_security #Secure_configuration #Identity_and_access_management #Threat_and_vulnerability #Continuity #Supplier_relationships_security #Legal_and_compliance #Information_security_event_management #Information_security_assurance	#Governance_and_Ecosystem #Protection #Defence #Resilience

Changes ISO 27002:2022

Attributes are used to create different views of the controls

8.6 Capacity management

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive #Detective	#Integrity #Availability	#Identify #Protect #Detect	#Continuity	#Governance_and_Ecosystem #Protection

Control

The use of resources should be monitored and adjusted in line with current and expected capacity requirements.

Changes ISO 27002:2022

You can create your own attributes
You can ignore those in the standard

For example:

1. Assign risk references to the controls treating specific risks
2. Maturity implementation level
3. Implementation state
4. Responsible department

Control	Treating risk	Implementation maturity	Implementation state	Responsible department	Information security properties	Operational capabilities
5.7 Threat intelligence	#6 #15	#Level_2	#Partially_implemented	#CISO	#Confidentiality #Integrity #Availability	#Threat_and_vulnerability_management
5.8 Information security in project management	#2	#Level_3	#Fully_implemented	#CISO #CSO	#Confidentiality #Integrity #Availability	#Governance

Changes ISO 27002:2022

You can create your own attributes
You can ignore those in the standard

For example:

1. Assign risk references to the controls treating specific risks
2. Maturity implementation level
3. Implementation state
4. Responsible department

Control	Treating risk	Implementation maturity	Implementation state	Responsible department	Information security properties	Operational capabilities
5.7 Threat intelligence	#6 #15	#Level_2	#Partially_implemented	#CISO	#Confidentiality #Integrity #Availability	#Threat_and_vulnerability_management
5.8 Information security in project management	#2	#Level_3	#Fully_implemented	#CISO #CSO	#Confidentiality #Integrity #Availability	#Governance

Changes ISO 27002:2022

ISO/IEC 27002:2022 New Controls

A.5.7 Threat Intelligence
A.7.4 Physical security monitoring
A.8.9 Configuration management
A.8.10 Information deletion
A.8.11 Data masking
A.8.12 Data leakage prevention

Changes ISO 27002:2022

ISO/IEC 27002:2022 New Controls

A.8.23 Web filtering
A.8.28 Secure coding
A.8.16 Monitoring activities
A.5.23 Information security for use of cloud services
A.5.30 ICT readiness for business continuity

Merged controls

57 controls from the 2013 version, have been merged into 24 new controls:

ISO/IEC 27002:2013 Control	**ISO/IEC 27002:2022** Control
5.1.1 Policies for information security 5.1.2 Review of the policies for information security	5.1 Policies for information security
6.1.5 Information security in project management 14.1.1 Information security requirements analysis and specification	5.8 Information security in project management
8.1.1 Inventory of assets 8.1.2 Ownership of assets	5.9 Inventory of information and other associated assets
8.1.3 Acceptable use of assets 8.2.3 Handling of assets	5.10 Acceptable use of information and other associated assets

13.2.1 Information transfer policies and procedures 13.2.2 Agreements on information transfer 13.2.3 Electronic messaging	5.14 Information transfer
9.1.1 Access control policy 9.1.2 Access to networks and network services	5.15 Access control
9.2.4 Management of secret authentication information of users 9.3.1 Use of secret authentication information 9.4.3 Password management system	5.17 Authentication information
9.2.2 User access provisioning 9.2.5 Review of user access rights 9.2.6 Removal or adjustment of access rights	5.18 Access rights
15.2.1 Monitoring and review of supplier services 15.2.2 Managing changes to supplier services	5.22 Monitoring, review and change management of supplier services

17.1.1 Planning information security continuity 17.1.2 Implementing information security continuity 17.1.3 Verify, review and evaluate information security continuity	5.29 Information security during disruption
18.1.1 Identification of applicable legislation and contractual requirements 18.1.5 Regulation of cryptographic controls	5.31 Legal, statutory, regulatory and contractual requirements
18.2.2 Compliance with security policies and standards 18.2.3 Technical compliance review	5.36 Compliance with policies, rules and standards for information security
16.1.2 Reporting information security events 16.1.3 Reporting information security weaknesses	6.8 Information security event reporting
11.1.2 Physical entry controls 11.1.6 Delivery and loading areas	7.2 Physical entry
8.3.1 Management of removable media 8.3.2 Disposal of media 8.3.3 Physical media transfer 11.2.5 Removal of assets	7.10 Storage media

6.2.1 Mobile device policy 11.2.8 Unattended user equipment	8.1 User endpoint devices
12.6.1 Management of technical vulnerabilities 18.2.3 Technical compliance review	8.8 Management of technical vulnerabilities
12.4.1 Event logging 12.4.2 Protection of log information 12.4.3 Administrator and operator logs	8.15 Logging
12.5.1 Installation of software on operational systems 12.6.2 Restrictions on software installation	8.19 Installation of software on operational systems
10.1.1 Policy on the use of cryptographic controls 10.1.2 Key management	8.24 Use of cryptography
14.1.2 Securing application services on public networks 14.1.3 Protecting application services transactions	8.26 Application security requirements

ISO/IEC 27002:2013 Control	**ISO/IEC 27002:2022** Control
14.2.8 System security testing 14.2.9 System acceptance testing	8.29 Security testing in development and acceptance
12.1.4 Separation of development, testing and operational environments 14.2.6 Secure development environment	8.31 Separation of development, test and production environments
12.1.2 Change management 14.2.2 System change control procedures 14.2.3 Technical review of applications after operating platform changes 14.2.4 Restrictions on changes to software packages	8.32 Change management

Renamed controls

23 controls have changed their names. However, their purpose is the same as in the previous 2013 version.

ISO/IEC 27002:2013 Control	**ISO/IEC 27002:2022** Control
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
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
7.3.1 Termination or change of employment responsibilities	6.5 Responsibilities after termination or change of employment
6.2.2 Teleworking	6.7 Remote working

ISO/IEC 27002:2013 Control	ISO/IEC 27002:2022 Control
9.4.2 Secure log-on procedures	8.5 Secure authentication
12.2.1 Controls against malware	8.7 Protection against malware
17.2.1 Availability of information processing facilities	8.14 Availability of information processing facilities
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

12.7.1 Information systems audit controls	8.34 Protection of information systems during audit testing
11.1.1 Physical security perimeter	7.1 Physical security perimeters
11.2.9 Clear desk and clear screen policy	7.7 Clear desk and clear screen
11.2.6 Security of equipment and assets off-premises	7.9 Security of assets off-premises
9.2.3 Management of privileged access rights	8.2 Privileged access rights
9.4.5 Access control to program source code	8.4 Access to source code

Same name, different control number

These 35 controls remained the same, only changing their control number:

ISO/IEC 27002:2013 Control	**ISO/IEC 27002:2022** Control
6.1.1 Information security roles and responsibilities	5.2 Information security roles and responsibilities
6.1.2 Segregation of duties	5.3 Segregation of duties
7.2.1 Management responsibilities	5.4 Management responsibilities
6.1.3 Contact with authorities	5.5 Contact with authorities

6.1.4 Contact with special interest groups	5.6 Contact with special interest groups
8.1.4 Return of assets	5.11 Return of assets
8.2.1 Classification of information	5.12 Classification of information
8.2.2 Labelling of information	5.13 Labelling of information
16.1.5 Response to information security incidents	5.26 Response to information security incidents
16.1.6 Learning from information security incidents	5.27 Learning from information security incidents
16.1.7 Collection of evidence	5.28 Collection of evidence
18.1.2 Intellectual property rights	5.32 Intellectual property rights
18.1.3 Protection of records	5.33 Protection of records

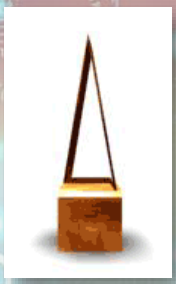
18.2.1 Independent review of information security	5.35 Independent review of information security
12.1.1 Documented operating procedures	5.37 Documented operating procedures
7.1.1 Screening	6.1 Screening
7.1.2 Terms and conditions of employment	6.2 Terms and conditions of employment
7.2.2 Information security awareness, education and training	6.3 Information security awareness, education and training
7.2.3 Disciplinary process	6.4 Disciplinary process
13.2.4 Confidentiality or non-disclosure agreements	6.6 Confidentiality or non-disclosure agreements

13.2.4 Confidentiality or non-disclosure agreements	6.6 Confidentiality or non-disclosure agreements
11.1.3 Securing offices, rooms and facilities	7.3 Securing offices, rooms and facilities
11.1.4 Protecting against external and environmental threats	7.5 Protecting against external and environmental threats
11.1.5 Working in secure areas	7.6 Working in secure areas
11.2.1 Equipment siting and protection	7.8 Equipment siting and protection
11.2.2 Supporting utilities	7.11 Supporting utilities
11.2.3 Cabling security	7.12 Cabling security
11.2.4 Equipment maintenance	7.13 Equipment maintenance

11.2.7 Secure disposal or re-use of equipment	7.14 Secure disposal or re-use of equipment
9.4.1 Information access restriction	8.3 Information access restriction
12.1.3 Capacity management	8.6 Capacity management

ISO/IEC 27002:2013 Control	**ISO/IEC 27002:2022** Control
12.3.1 Information backup	8.13 Information backup
12.4.4 Clock synchronization	8.17 Clock synchronization
9.4.4 Use of privileged utility programs	8.18 Use of privileged utility programs
13.1.2 Security of network services	8.21 Security of network services
14.2.7 Outsourced development	8.30 Outsourced development

CHAPTER 2:



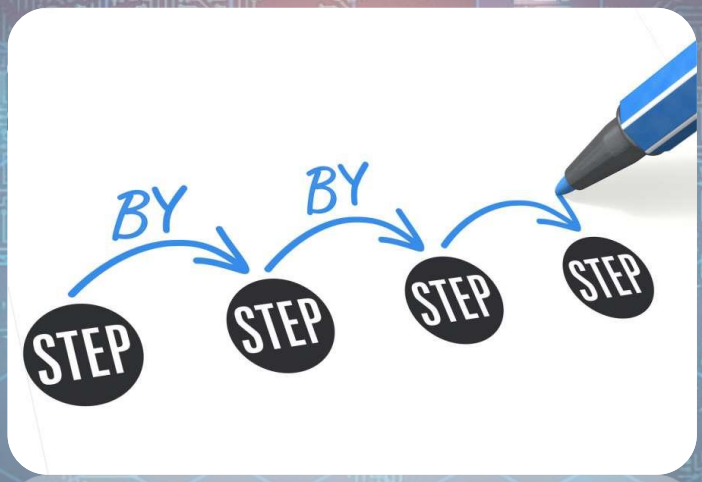
AUDITING THE ISO FDIS 27001 2022 REQUIREMENTS

IQCS/ISMS/02 Rev 0 issued Oct 2022

The fundamental elements for ISMS are based on

- *4 Context of the organization*
- *5 Leadership*
- *6 Planning*
- *7 Support*
- *8 Operation*
- *9 Performance evaluation*
- *10 Improvement*

IQCS/ISMS/02 Rev 0 issued Oct 2022



4.1 Understanding the organization and its context

Example Internal issues

ORGANIZATIONAL MATTERS (EMPLOYEES)	I
RESPONSIBILITIES (EMPLOYEES)	I
INTER DEPARTMENTARY RELATIONS (MANAGEMENT- HOLDERS)	I
INFORMATION SYSTEMS	I
STATEGY, POLICY OF COMPANY	I

Example external issues

LEGISLATION (STATE/ AUTHORITIES)	E
COMPETITIVE ENVIRONMENT (BUSINESS)	E
SUPPLIES/ SERVICES	E
Software	E

Example of legislation involved in ISO 27001

- intellectual property;
- content, protection and retention of organizational records;
- data protection and privacy;
- regulation of cryptographic controls;
  anti-terrorism;
- electronic commerce;
- electronic and digital signatures;
- workplace surveillance;
- Workplace ergonomics;
- telecommunications interception and monitoring of data (e.g. e-mail),
- computer abuse,
  electronic evidence collection,
- penetration testing,
- etc.;

What to understand - Clarification

Examples:

a) External issues:

1) the cultural, social, political, legal, financial, technological, economic and natural surroundings and market competition

2) introduction of new competitors, contractors, subcontractors, suppliers, partners and providers, new technologies, new laws and the emergence of new occupations;

3) new knowledge on products

4) key drivers and trends relevant to the industry

What to understand – Clarification

5) relationships with external interested parties;
6) changes in relation to any of the above;

b) Internal issues:
governance, organizational structure, roles and accountabilities, policies, objectives, information systems, introduction of new products, materials, services, tools, software, premises and equipment, perceptions and values, standards, guidelines, outsourced activities, working time arrangements, working conditions

4.2

Understanding the needs and expectations of interested parties

INTEREST PARTIES (example: Bank)

1. Stakeholders
2. Customers
3. National Bank of state
4. European Central Bank (ECB)
5. Markets (national and all over the world)
6. Stock exchange
7. Corporations and trade
8. Ministries and state
9. Authorities
10. Cybersecurity authorities

etc…. etc….

Under 4.2 : Why? - Clarification

It's necessary because your ISMS system will need to be able to manage all of these influences.

- **You influence, you are being influenced as well!!**
- These needs and expectations

➡

become **compliance obligation**

Under 4.2 : Why? - Clarification

Examples

1. legal and regulatory authorities
2. Other organizations;
3. suppliers, contractors and subcontractors;
4. owners, shareholders, clients, visitors
5. customers, media, business associations
6. ISMS and governaal organizations,

Some needs and expectations are mandatory have been incorporated into laws and regulations

4.3 Determining the scope of the information security management system

This is common in all Management systems

4.4 Information security management system

The organization shall establish, implement, maintain and continually improve an information security management system, including the processes needed and their interactions, in accordance with the requirements of ISO 27001

5. Leadership

5.1 Leadership and commitment

EXAMPLE

Leadership is **a skill which involves motivating a group of individuals to work towards a common goal**. In a business setting, this involves leading and guiding staff and colleagues with a strategy or a plan to meet the business needs of the company.

EXAMPLE

How can top management demonstrate leadership and commitment to the information security management system?

Top Management must direct and support persons to contribute to the effectiveness of the information security management system. They must also support other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility. They must promote continual improvement

5.2

Policy

Example An ISMS policy suggestion

- The policy should state that the workplace has clear rules for ISMS work behavior.
- The policy should state what type of education or training program will be provided by the company to ensure that employees can meet their responsibilities..

Example An ISMS policy suggestion

https://www.yokogawa.com/solutions/products-and-services/lifecycle-services/safety-and-security/cybersecurity-lifecycle-management/policies-procedures/

5.3 Organizational roles, responsibilities and authorities

Examples on Roles, responsibilities and authorities

Members of the Board	1. Members of the Board shall ensure that the necessary information security controls are implemented and complied with as per this policy.
Information Security Manager	1. Establish and revise the information security strategy, policy and standards for change management and control with input from interest groups and subsidiaries; 2. Facilitate and co-ordinate the necessary counter measures to change management and control initiatives and evaluate such policies and standards; 3. Establish the security requirements for change management and control directives and approval of the change management and control standards and change control/ version control products; 4. Co-ordinate the overall communication and awareness strategy for change management; 5. Acts as the management champion for change management and control; 6. Provide technical input to the service requirements and co-ordinate affected changes to SLA's where applicable. 7. Establish and co-ordinate appropriate interest group forums to represent, feedback, implement and monitor change management and control initiatives; and 8. Co-ordinate the implementation of new or additional security controls for change management.

Examples on Roles, responsibilities and authorities

Operations Manager	• Implement, maintain and update the change management and control strategy, baselines, standards, policies and procedures with input from all stakeholders; • Approve and authorise change management and control measures • Ensure that all application owners are aware of the applicable policies, standards, procedures and guidelines for change management and control; • Ensure that policy, standards and procedural changes are communicated to applicable owners and management forums; • Appoint the necessary representation to the interest groups and other forums created by each company for Information Security Management relating to change management and control; • Establish and revise the information security strategy, policy and standards for change management and control; • Facilitate and co-ordinate the necessary change management and control initiatives within each company;

Examples on Roles, responsibilities and authorities

Operations Manager	• Report and evaluate changes to change management and control policies and standards; • Co-ordinate the overall communication and awareness strategy for change management and control; • Co-ordinate the implementation of new or additional security controls for change management and control • Review the effectiveness of change management and control strategy and implement remedial controls where deficits are identified; • Provide regular updates on change management and control initiatives and the suitable application; • Evaluate and recommend changes to change management/ version control solutions; and • Co-ordinate awareness strategies and rollouts to effectively communicate change management and control mitigation solutions in each company.

Examples on Roles, responsibilities and authorities

Operations Manager	• Establish and implement the necessary standards and procedures that conform to the Information Security policy; • Responsible for approving, authorising, monitoring and enforcing change management initiatives and related security controls within all <ORGANISATION> companies and divisions; • Ensure that all solution owners are aware of policies, standards, procedures and guidelines for change management and control. • Ensure the compliance of this policy and report deviations to the Information Manager.

Examples on Roles, responsibilities and authorities

IT Service Provider	• Shall comply with all change management and control statements of this policy.
Information Owners eg employess	• Shall comply with all information security policies, standards and procedures for change management and control; and • Report all deviations.

6 Planning

6.1 Actions to address risks and opportunities

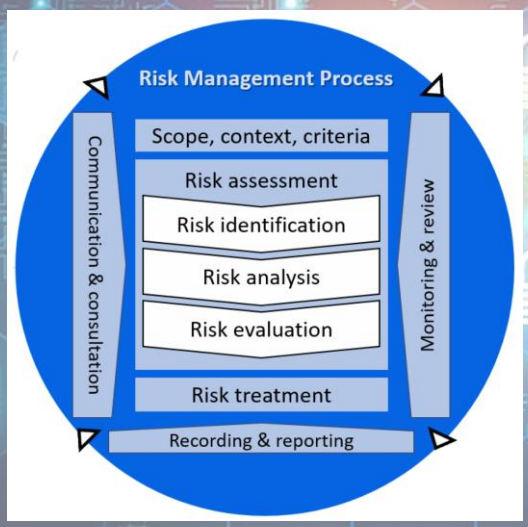
6.1.1 General

When planning for the information security management system, the organization shall consider the issues referred to in 4.1 and the requirements referred to in 4.2 and determine the risks and opportunities that need to be addressed

6.1.2 Information security risk assessment

6.1.3 Information security risk treatment

security risk assessment-security risk treatment



https://www.mdpi.com/2071-1050/12/14/5770/htm

example Within 6.1.3 Information security risk treatment the organization must produce a **Statement of Applicability (SoA)** that contains:

- **the necessary controls**
- **justification for their inclusion;**
- **whether the necessary controls are implemented or not; and**
- **the justification for excluding any of the Annex A controls.**

Example SoA in standard requiremets

Statement of Applicability ISOFDIS 27001 2022

Section	ISO/IEC 27001 requirement	Status	Notes
4,2	**Interested parties**		
4.2 (a)	Identify **interested parties** including applicable laws, regulations, contracts *etc.*	Limited	
4.2 (b)	Determine their information security-relevant **requirements** and obligations	Initial	
4,3	**ISMS scope**		
4,3	Determine and document the **ISMS scope**	Limited	
4,4	**ISMS**		
4,4	Establish, implement, maintain and continually improve an **ISMS** according to the standard!	Nonexistent	
5	**Leadership**		
5,1	**Leadership & commitment**		
5,1	Top management must demonstrate **leadership & commitment** to the ISMS	Defined	
5,2	**Policy**		
5,2	Document the **information security policy**	Nonexistent	
5,3	**Organizational roles, responsibilities & authorities**		
5,3	Assign and communicate information security **rôles & responsibilities**	Not applicable	
6	**Planning**		
6,1	**Actions to address risks & opportunities**		
6.1.1	Design/plan the ISMS to satisfy the requirements, addressing risks & opportunities	Limited	
6.1.2	Define and apply an **information security risk assessment process**	Optimized	
6.1.3	Document and apply an **information security risk treatment process**	? Unknown	

Intro & copyright | **Mandatory ISMS requirements** | Annex A controls | Metrics | Φύλλο1

Example SoA in CONTROLS requirements

Statement of Applicability and status of information security controls

Section	Information security control	Status	Notes
A5	**Information security policies**		
A.5.1	Policies for information secu-rity	Managed	
A.5.2	Information security roles and responsilibities	Limited	
A.5.3	Segregation of duties	Defined	
A.5.4	Management responsibilities	Managed	
A.5.5	Contact with authorities	Managed	
A.5.6	Cont ac t w it h special interest groups	Not applicable	
A.5.7	Threat intelligence	Limited	
A.5.8	Information security in project management	Optimized	
A.5.9	Inventory of information andother associated assets	Managed	
A.5.10	Acceptable use of information and other associated assets	Managed	
A.5.11	Return of assets	Managed	
A.5.12	Classification of information	Managed	
A.5.13	Labelling of information	Managed	
A.5.14	Information transfer	Managed	

Intro & copyright | Mandatory ISMS requirements | **Annex A controls** | Metrics | Φύλλο1

IQCS/ISMS/02 Rev 0 issued Oct 2022

Example SoA in CONTROLS requirements

Statement of Applicability and status of information security controls

Section	Information security control	Status	Notes
A.5.15	Access control	Managed	
A.5.16	Identity management	Managed	
A.5.17	Authentication information	Managed	
A.5.18	Access rights	Managed	
A.5.19	Information security in supplier relationships	Managed	
A.5.20	Addressing information security within supplier agreements	Managed	
A.5.21	Managing information security in the information and communication technology (ICT) supply chain	Managed	
A.5.22	Monitoring, review and change management of supplier services	Managed	
A.5.23	Information security for use of cloud services	Managed	
A.5.24	Information securit y incident management planning and prepa- ration	Managed	
A.5.25	Assessment and decision on in-formation security events	Managed	
A.5.26	Response to information security incidents	Managed	
A.5.27	Learning from information se-curity incidents	Managed	
A.5.28	Collection of evidence	Managed	
A.5.29	Information security during disruption	Managed	

Intro & copyright | Mandatory ISMS requirements | **Annex A controls** | Metrics | Φύλλο1

IQCS/ISMS/02 Rev 0 issued Oct 2022

Example SoA in CONTROLS requirements

Statement of Applicability and status of information security controls

Section	Information security control	Status	Notes
A.5.30	ICT readiness for business con-tinuity	Managed	
A.5.31	Legal, statutory, regulatory and contractual requirements	Managed	
A.5.32	Intellectual property rights	Managed	
A.5.33	Protection of records	Managed	
A.5.34	Privacy and protection of person-al identifiable information (PII)	Managed	
A.5.35	Independent review of informa-tion securitu	Managed	
A.5.36	Compliance with policies, rules and standards for information security	Managed	
A.5.37	Documented operating proce-dures	Managed	
A.6.1	Screening	Managed	
A.6.2	Terms and conditions of employment	Managed	
A.6.3	Information security awareness,education and training	Managed	
A.6.4	Disciplinary process	Managed	
A.6.5	Responsibilities after termination or change of employment	Managed	
A.6.6	Confidentiality or non-disclosure agreements	Managed	
A.6.7	Remote working	Managed	

Intro & copyright | Mandatory ISMS requirements | Annex A controls | Metrics | Φύλλο1

Example SoA in CONTROLS requirements

Statement of Applicability and status of information security controls

Section	Information security control	Status	Notes
A.6.8	Information security event reporting	Managed	
A.7.1	Physical security perimeters	Managed	
A.7.2	Physical entry	Managed	
A.7.3	Securing offices, rooms and faacilities	Managed	
A.7.4	Physical security monitoring	Managed	
A.7.5	Protecting against physical and environmental threats	Managed	
A.7.6	Working in secure areas	Managed	
A.7.7	Clear desk and clear screen	Managed	
A.7.8	Equipment siting and protection	Managed	
A.7.9	Security of assets off-premises	Managed	
A.7.10	Storage media	Managed	
A.7.11	Supporting utilities	Managed	
A.7.12	Cabling security	Managed	
A.7.13	Equipment maintenance	Managed	
A.8.1	User end point devices	Managed	

Intro & copyright | Mandatory ISMS requirements | Annex A controls | Metrics | Φύλλο1

Example SoA in CONTROLS requirements

Statement of Applicability and status of information security controls

Section	Information security control	Status	Notes
A.8.2	Privileged access rights	Managed	
A.8.3	Information access restriction	Managed	
A.8.4	Access to source code	Managed	
A.8.5	Secure authentication	Managed	
A.8.6	Capacity management	Managed	
A.8.7	Protection against malware	Managed	
A.8.8	Management of technical vulnerabilities-	Managed	
A.8.9	Configuration management	Managed	
A.8.10	Information deletion	Managed	
A.8.11	Data masking	Managed	
A.8.12	Data leakage prevention	Managed	
A.8.13	Information backup	Managed	
A.8.14	Redundancy of information processing facilities	Managed	
A.8.15	Logging	Managed	
A.8.16	Monitoring activities	Managed	
A.8.17	Clock synchronization	Managed	

Intro & copyright | Mandatory ISMS requirements | Annex A controls | Metrics | Φύλλο1

IQCS/ISMS/02 Rev 0 issued Oct 2022

Example SoA in CONTROLS requirements

Statement of Applicability and status of information security controls

Section	Information security control	Status	Notes
A.8.17	Clock synchronization	Managed	
A.8.18	Use of privileged utility programs	Managed	
A.8.19	Installation of software on operational systems	Managed	
A.8.20	Networks security	Managed	
A.8.21	Security of network services	Managed	
A.8.22	Segregation of networks	Managed	
A.8.23	Web filtering	Managed	
A.8.24	Use of cryptography	Managed	
A.8.25	Secure development life cycle	Managed	
A.8.26	Application security requiments	Managed	
A.8.27	Secure system architecture and engineering principles	Managed	
A.8.28	Secure coding	Managed	
A.8.29	Security testing in development and acceptance	Managed	
A.8.30	Outsourced development	Managed	
A.8.31	Separation of development, test and production environments	Managed	
A.8.32	Change management	Managed	
A.8.33	Test information	Managed	
A.8.34	Protection of information systems during audit testing	Managed	

Intro & copyright | Mandatory ISMS requirements | Annex A controls | Metrics | Φύλλο1

IQCS/ISMS/02 Rev 0 issued Oct 2022

Risk based thinking or Risk management addresses

Auditors don't forget or neglect

- System risk
- Project risk
- Business risk
- Safety and risks to the public

RISK ANALYSIS, example

									Current Controls			Recommended Controls			Action Results				
															Implemented Controls				
Business / Service	Asset Name	Function	Potential Failure Mode(s)	Potential Technical Effect(s) of Failure	Potential Business Consequence(s) of Failure	S e v e r	Potential Cause(s)/ Mechanism(s) of Failure	P r o b	Preventive Controls	Detective Controls	R P N	Preventive Controls	Detective Controls	Responsibility & Target Completion Date	Preventive Controls	Detective Controls	Rev Sev	Rev Prob	Rev RPN
Protecting IT Assets	Firewall	To block unauthorized requests	Rules not appropriately configured	IP Spoofing	Diversion of sensitive data traffic, fraud	8	Procedures not followed	2	Procedures available		16		Increase audit frequency	MANAGER by end Jan 2025		Increase audit frequency	5	3	15
Protecting IT Assets	Firewall	To block unauthorized requests	Rules not appropriately configured	Entry for External Hackers	Disclosure or modification of business records; prosecution; bad PR; customer defection	7	Procedures not followed	2		Log Monitoring	14		Increase audit frequency	MANAGER by end Jan 2025		Increase audit frequency	5	3	15
Protecting IT Assets	Firewall	To identify trusted zones by encryption	Authentication mechanism using legacy systems having improper configuration	User may not have access to the requested service	Staff unable to work; backlogs; bad PR	6	Policies not fully implemented	1	Policies Defined		6	User Awareness		MANAGER by end Jan 2025	User Awareness		1	5	5
Protecting IT Assets	Firewall	To block unauthorized requests	Rules not appropriately configured	Entry for External Hackers	Disclosure or modification of business records; prosecution; bad PR; customer defection	7	Procedures not followed	2	Procedures available		14		Increase audit frequency	MANAGER by end Jan 2025		Increase audit frequency	1	4	4
Protecting IT Assets	Firewall	To identify trusted zones by encryption	Encryption level (56 bit or 128 bit) mismatch	Data will be exposed as plain text	Disclosure of customer database; commercial and privacy issues	7	Policies not fully implemented	2	Policies Defined		14	User Awareness		MANAGER by end Jan 2025	User Awareness		2	2	4
Protecting IT Assets	Firewall	To block unauthorized requests	Rules not appropriately configured	Data Theft	Commercial and privacy consequences	7	Procedures not available	2	Nil		14	User Awareness		MANAGER by end Jan 2025	User Awareness		2	2	4
PC SECURITY	PC password	To block unauthorized requests	Rules not appropriately configured	Data Theft	Commercial and privacy consequences	7	Policies not fully implemented	3	Nil	Log Monitoring	21	User Awareness	training	MANAGER by end Jan 2025	User Awareness	Increase audit frequency	2	2	4

6.2 Information security objectives and planning to achieve them

Examples of security objectives

- Maintain a Safe Network. ...
- Maintain Vulnerability Management. ...
- Prevent Unauthorized Access. ...
- Ensure Security Flaws are Immediately Reported. ...
- Maintain Integrity of Data Assets.

6.3
Planning of changes

These are no difference

as in ISO 9001 or 14001

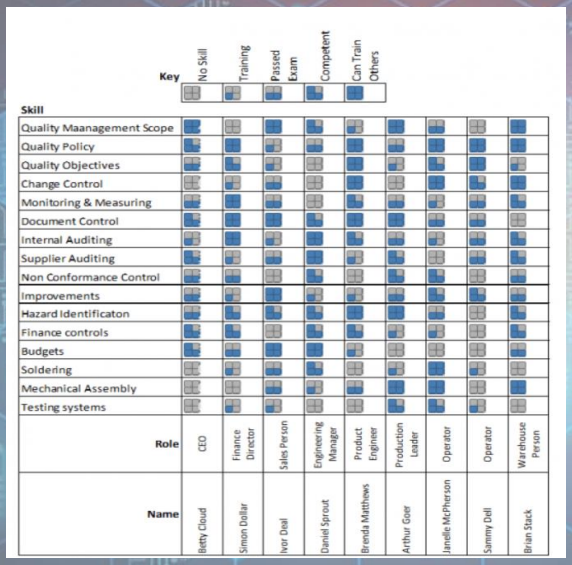
7. Support

7.1 Resources

7.2 Competence

7.3 Awareness

7.4 Communication



Competence

example of skill matrix

https://www.manycaps.com/blog/iso27001-resources-and-competence-requirements.html

IQCS/ISMS/02 Rev 0 issued Oct 2022

75

Is Communication important????

How to Prepare a Cybersecurity Communications Strategy

https://iq360inc.com/blog/c-suite/cybersecurity-communications-prep/

"…when a company is compromised from a cybersecurity standpoint, the communications team will likely need to engage with an entirely different universe of players and may need to trigger additional protocols."

IQCS/ISMS/02 Rev 0 issued Oct 2022

76

Is Communication important????

How to Prepare a Cybersecurity Communications Strategy

•https://iq360inc.com/blog/c-suite/cybersecurity-communications-prep/

Think through your cybersecurity communications strategy in advance. Keep the following in mind when tackling your cybersecurity communications preparedness plan:

POTENTIAL SCENARIOS

Sit down with your CISO (chief information security officer) or CSO (chief security officer) and discuss the possible scenarios that pose a threat to your company. Think through each possible threat and identify the internal and external audiences who will be impacted.

Is Communication important????

How to Prepare a Cybersecurity Communications Strategy

•https://iq360inc.com/blog/c-suite/cybersecurity-communications-prep/

LEGAL OBLIGATIONS

A cybersecurity attack could trigger a host of disclosure protocols that the communications department will not fully understand without talking to the legal department. Does law enforcement need to be notified? What are the guidelines in terms of public disclosures? What is the timeframe for notifying customers during an investigation? Think through these questions now because when the breach is upon you, some actions will have to occur immediately

Is Communication important????

How to Prepare a Cybersecurity Communications Strategy

•https://iq360inc.com/blog/c-suite/cybersecurity-communications-prep/

CHOOSING SPOKESPEOPLE

Cybersecurity attacks could merit positioning spokespeople who are not typically the face of the company in a crisis. Prepare spokespeople in advance who can address the technical security questions. This means formal media training, and also engaging in low-stakes practice interviews as often and as early as possible. You don't want the spokesperson's first interview to be the one where everything is on the line.

Is Communication important????

How to Prepare a Cybersecurity Communications Strategy

•https://iq360inc.com/blog/c-suite/cybersecurity-communications-prep/

VENDORS

It is likely that your company's threat management, detection, and response initiatives are bolstered by a team of vendors behind the scenes. Be aware of these entities and how they work with the technology experts at your company..

7.5

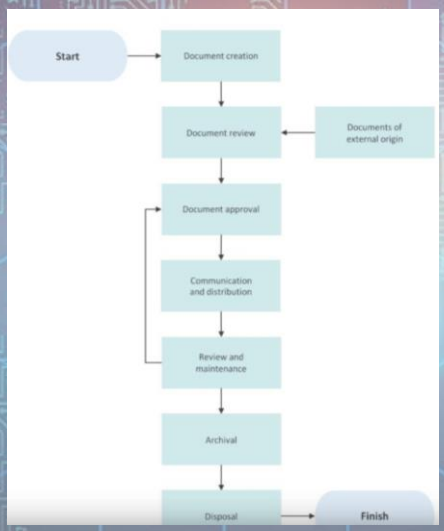
Documented information

The organization's information security management system shall include:

a) documented information required by this document; and

b) documented information determined by the organization as being necessary for the effectiveness of the information security management system.

Flowchart Documented information



Examples Procedures- Instructions- Documents

(P-I-D)

- SoA- Statement of Applicability (I-D)
- Information Inventory (I-D)
- Information Management (I-D)
- Information Classification (I-D)
- Information Security Manual (P)
- ISMS Policy (D)
- ISMS Operation procedures (P)

Examples Procedures- Instructions- Documents

(P-I-D)

- Impact Analysis (I-D)
- Internal audit (D)
- Non conformities (P)
- NCR- Non conformity Request (D)
- Data Restoration form (I-D)
- BCP- Business Continuity Plan (P)
- Job description (I)
- Roles (I-D)
- Risk analysis (I-D)
- Information assets (I-D)

DOCUMENTS TO MAITAIN AND RETAIN

SN	Documented Information	Maintained	Retained
1	Scope of the ISMS	✓	
2	Information security policy and objectives	✓	
3	Risk assessment and risk treatment methodology	✓	
4	Statement of Applicability	✓	
5	Risk treatment plan	✓	
6	Risk assessment report	✓	
7	Definition of security roles and responsibilities	✓	
8	Inventory of assets	✓	
9	Records of training, skills, experience and qualifications		✓
10	Monitoring and measurement results		✓
11	Internal audit program		✓
12	Results of internal audits		✓
13	Results of the management review		✓
14	Results of corrective actions		✓
15	Logs of user activities, exceptions, and security events		✓

8.

Operation

8.1 Operational planning and control

8.2 Information security risk assessment

8.3 Information security risk treatment

How to carry out the Risk Assessment (RA) using Failure Mode and Effect Analysis

1	Identify the businesses or the services rendered by the department under the scope of 27001
2	Compute the assets that deliver or support the business or service identified
3	Write down the asset number (to avoid duplication)
4	Write down the function of the asset in delivering or maintain the identified business or service
5	Now identify the **failure modes** for the identified function. Please note that there could be more than one failure mode for each function
6	Now identify the **effect, if the identified failure mode happens**. That if the identified failure mode happens what will be the effect on the business or service.
7	Now refer the **severity chart** and choose the number relevant to the effect of the failure mode
8	Now identify the **cause for the failure mode**. Please note that each failure mode can have more than one cause.
9	Now refer to the **probability chart** and choose the number that is more relevant to the frequency of the cause happening.

How to carry out the Risk Assessment (RA) using Failure Mode and Effect Analysis

10	Now list down the **current controls**. Categorize the controls as preventive and detective controls. Write each control in separate rows.
11	Now refer to the **detectability chart** and choose a number relevant to the effectiveness of the controls.
12	You can now see the **Risk Priority Number** calculated for a failure mode of the respective asset function.
14	Now identify who will implement the recommended control and by what target date the recommended control would be implemented.
15	Now if the RPN is under the acceptable value then the risk status shows "LOW RISK". Else it displays as HIGH RISK. If it is HIGH RISK then the process has to be repeated from step 1.
16	Refer the Probability Chart
17	Refer the Detectability Chart
18	New RPN is calculated. Compare it with the acceptable norms and if not satisfying then redo the same process.

Effect	SEVERITY of Effect	Ranking
Catastrophic	Resource not available / Problem unknown	10
Extreme	Resource not available / Problem known and cannot be controlled	9
Very High	Resource not available / Problem known and can be controlled	8
High	Resource Available / Major violation of policies	7
Moderate	Resource Available / Major violations of process	6
Low	Resource Available / Major violations of procedures	5
Very Low	Resource Available / Minor violations of policies	4
Minor	Resource Available / Minor violations of process	3
Very Minor	Resource Available / Minor violations of procedures	2
None	No effect	1

PROBABILITY of Failure	Failure Prob	Ranking
Very High: Failure is almost inevitable	>1 in 2	10
	1 in 3	9
High: Repeated failures	1 in 8	8
	1 in 20	7
Moderate: Occasional failures	1 in 80	6
	1 in 400	5
	1 in 2,000	4
Low: Relatively few failures	1 in 15,000	3
	1 in 150,000	2
Remote: Failure is unlikely	<1 in 1,500,000	1

Detection	Likelihood of DETECTION	Ranking
Absolute Uncertainty	Control cannot prevent / detect potential cause/mechanism and subsequent failure mode	10
Very Remote	Very remote chance the control will prevent / detect potential cause/mechanism and subsequent failure mode	9
Remote	Remote chance the control will prevent / detect potential cause/mechanism and subsequent failure mode	8
Very Low	Very low chance the control will prevent / detect potential cause/mechanism and subsequent failure mode	7
Low	Low chance the control will prevent / detect potential cause/mechanism and subsequent failure mode	6
Moderate	Moderate chance the control will prevent / detect potential cause/mechanism and subsequent failure mode	5
Moderately High	Moderately High chance the control will prevent / detect potential cause/mechanism and subsequent failure mode	4
High	High chance the control will prevent / detect potential cause/mechanism and subsequent failure mode	3
Very High	Very high chance the control will prevent / detect potential cause/mechanism and subsequent failure mode	2
Almost Certain	Control will prevent / detect potential cause/mechanism and subsequent failure mode	1

security risk assessment, example

Sl.No.	Business / Service	Asset Name	Asset Number	Function	Potential Failure Mode(s)	Potential Technical Effect(s) of Failure	Potential Business Consequence(s) of Failure	Sev	Potential Cause(s)/ Mechanism(s) of Failure	Occ	Current Controls		Det	RPN	Recommended Controls		Responsibility & Target Completion Date	Action Results				
											Preventive Controls	Detective Controls			Preventive Controls	Detective Controls		Implemented Controls		New Sev	New Occ	New DET	New RPN
																		Preventive Controls	Detective Controls				
8	Protecting IT Assets	Firewall	5000	To block unauthorized requests	Rules not appropriately configured	IP Spoofing	Diversion of sensitive data traffic, fraud	8	Procedures not followed	2	Procedures available		4	64		Increase audit frequency	XYZ by end Jan 2006		Increase audit frequency	5	3	2	30
4	Protecting IT Assets	Firewall	5000	To block unauthorized requests	Rules not appropriately configured	Entry for External Hackers	Disclosure or modification of business records; prosecution; bad PR; customer defection	7	Procedures not followed	2		Log Monitoring	4	56		Increase audit frequency	XYZ by end Jan 2006		Increase audit frequency	5	3	2	30
9	Protecting IT Assets	Firewall	5000	To block unauthorized requests	Rules not appropriately configured	DDOS Attack	Inability to process electronic transactions; bad PR; customer defection	10	Procedures not followed	2	Procedures available		2	40		Increase audit frequency	XYZ by end Jan 2006		Increase audit frequency	2	5	2	20
7	Protecting IT Assets	Firewall	5000	To identify trusted zones by encryption	User awareness	CIA Compromised	Disclosure of customer database; commercial and privacy issues	5	Procedures not followed	6	Policies Defined		1	30	Not Required	Not Required	Business owner to formally accept risk			5	2	2	20
5	Protecting IT Assets	Firewall	5000	To identify trusted zones by encryption	Authentication mechanism using legacy systems having improper configuration	User may not have access to the requested service	Staff unable to work; backlogs; bad PR	6	Policies not fully implemented	1	Policies Defined		5	30	User Awareness		XYZ by end March 2006	User Awareness		1	5	3	15
3	Protecting IT Assets	Firewall	5000	To block unauthorized requests	Rules not appropriately configured	Entry for External Hackers	Disclosure or modification of business records; prosecution; bad PR; customer defection	7	Procedures not followed	2	Procedures available		2	28		Increase audit frequency	XYZ by end Jan 2006		Increase audit frequency	1	4	2	8
6	Protecting IT Assets	Firewall	5000	To block unauthorized requests	Rules not appropriately configured	DDOS Attack	Inability to process electronic transactions; bad PR; customer defection	10	Procedures not followed	2		Log Monitoring	1	20		Increase audit frequency	XYZ by end Jan 2006		Increase audit frequency	1	4	2	8
2	Protecting IT Assets	Firewall	5000	To identify trusted zones by encryption	Encryption level (56 bit or 128 bit) mismatch	Data will be exposed as plain text	Disclosure of customer database; commercial and privacy issues	7	Policies not fully implemented	2	Policies Defined		1	14	User Awareness		XYZ by end March 2006	User Awareness		2	2	2	8
1	Protecting IT Assets	Firewall	5000	To block unauthorized requests	Rules not appropriately configured	Data Theft	Commercial and privacy consequences	7	Procedures not available	2	Nil		1	14	User Awareness		XYZ by end March 2006	User Awareness		2	2	1	4

security risk assessment, focus on one aspect

No.	Business / Service	Asset Name	Asset Number	Function	Potential Failure Mode(s)	Potential Technical Effect(s) of Failure	Potential Consequence of Failure
8	Protecting IT Assets	Firewall	5000	To block unauthorized requests	Rules not appropriately configured	IP Spoofing	Diversion of sensitive data traffic, fraud

Sev	Potential Cause(s)/ Mechanism(s) of Failure	Prob	Current Controls		Det	RPN
			Preventive Controls	Detective Controls		
8	Procedures not followed	2	Procedures available		4	64 = 8 X 2 X 4

Recommended Controls		Responsibility & Target Completion Date	Action Results		New Sev	New Occ	New Det	New RPN
			Implemented Controls					
Preventive Controls	Detective Controls		Preventive Controls	Detective Controls				
	Increase audit frequency	XYZ by end Jan 2024		Increase audit frequency	5	3	2	30= 5 X 3 X 2

9

Performance evaluation

9.1 Monitoring, measurement, analysis and evaluation

FOR MEASUREMENTS SEE ISO 27002: 2022- CONTROLS

9.2

Internal audit

•The organization shall conduct internal audits at planned intervals to provide information on whether the information security management system

•The organization shall plan, establish, implement and maintain an audit programme(s)

9.3 Management review

Top management shall review the organization's information security management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness.

10

Improvement

10.1 Continual improvement

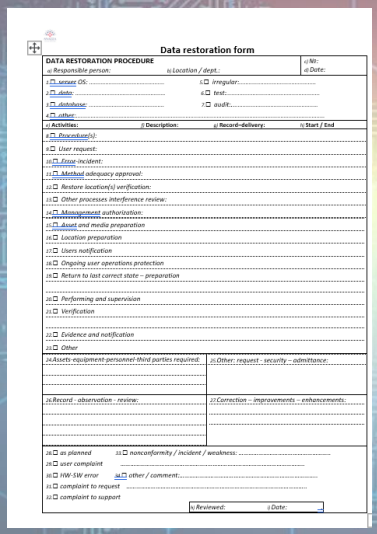
The organization shall continually improve the suitability, adequacy and effectiveness of the information security management system.

10.2 Nonconformity and corrective action

When a nonconformity occurs, the organization shall:

a)react to the nonconformity

b)evaluate the need for action to eliminate the causes of nonconformity



Data restoration form

DATA RESTORATION PROCEDURE		a) Nr:
a) Responsible person:	b) Location / dept.:	d) Date:
c ☐ server OS:	e ☐ irregular:.....	
f ☐ data:	g ☐ test:.....	
h ☐ database:	i ☐ audit:.....	
j ☐ other:		

k) Activities:	l) Description:	m) Record-delivery:	n) Start / End
o ☐ Procedure(s):			
p ☐ User request:			
q ☐ Close incident:			
r) ☐ Method adequacy approval:			
s) ☐ Restore location(s) verification:			
t) ☐ Other processes interference review:			
u) ☐ Management authorization:			
v) ☐ Asset and media preparation			
w) ☐ Location preparation			
x) ☐ Users notification			
y) ☐ Ongoing user operations protection			
z) ☐ Return to last correct state – preparation			
aa) ☐ Performing and supervision			
ab) ☐ Verification			
ac) ☐ Evidence and notification			
ad) ☐ Other			

ae) Assets-equipment-personnel-third parties required:	af) Other: request - security – admittance:
ag) Record - observation - review:	ah) Correction – improvements – enhancements:

ai) ☐ as planned	aj) ☐ nonconformity / incident / weakness: .....
ak) ☐ user complaint	.....
al) ☐ HW-SW error	am) ☐ other / comment:.....
an) ☐ complaint to request	.....
ao) ☐ complaint to support	

ap) Reviewed:	aq) Date:

EXAMPLE OF NCR, Data restoration form

A.5	Organizational controls	
A.5.1	Policies for information security	Control Information security policy and topic-specific policies shall be de fined, 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.
A.5.2	Information security roles and responsibilities	Control Information securit y roles and responsibilities shall be defined and allocated according to the organization needs.
A.5.3	Segregation of duties	Control Conf licting duties and conf licting areas of responsibility shall be seg regated.
A.5.4	Management responsibilities	Control Management shall require all personnel to apply information security in accordance with the established information security policy, top ic-specific policies and procedures of the organization.
A.5.5	Contact with authorities	Control The organization shall establish and maintain contact with relevant authorities.
A.5.6	Cont ac t w it h special interest groups	Control The organization shall establish and maintain contact with special interest groups or other specialist security forums and professional associations.

A.5.7	Threat intelligence	Control Information relating to information security threats shall be collected and analysed to produce threat intelligence.
A.5.8	Information security in project management	Control Information security shall be integrated into project management.
A.5.9	Inventor y of information and other associated assets	Control An inventory of information and other associated assets, including owners, shall be developed and maintained.
A.5.10	Acceptable use of information and other associated assets	Control Rules for the acceptable use and procedures for handling information and other associated assets shall be identified, documented and implemented.
A.5.11	Return of assets	Control Personnel and other interested parties as appropriate shall return all the organization's assets in their possession upon change or termination of their employment, contract or agreement.

A.5.12	Classification of information	Control Information shall be classified according to the information security needs of the organization based on confidentiality, integrity, availability and relevant interested party requirements.
A.5.13	Labelling of information	Control An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information clas sification scheme adopted by the organization.
A.5.14	Information transfer	Control Information transfer rules, procedures, or agreements shall be in place for all types of transfer facilities within the organization and between the organization and other parties.
A.5.15	Access control	Control Rules to control physical and logical access to information and other associated assets shall be established and implemented based on busi ness and information security requirements.
A.5.16	Identity management	Control The full life cycle of identities shall be managed.
A.5.17	Authentication information	Control Allocation and management of authentication information shall be controlled by a management process, including advising personnel on appropriate handling of authentication information.

A.5.18	Access rights	Control Access right s to information and other associated asset s shall be provisioned, reviewed, modified and removed in accordance with the organization's topic-specific policy on and rules for access control.
A.5.19	Information security in supplier relationships	Control Processes and procedures shall be defined and implemented to manage the information securit y risks associated with the use of supplier's products or services.
A.5.20	Addressing information security within supplier agreements	Control Relevant information security requirements shall be established and agreed with each supplier based on the type of supplier relationship.
A.5.21	Managing information security in the information and commu nication technology (ICT) supply chain	Control Processes and procedures shall be defined and implemented to manage the information security risks associated with the ICT products and services supply chain.
A.5.22	Monitoring, review and change management of supplier services	Control The organization shall regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery.
A.5.23	Information security for use of cloud services	Control Processes for acquisition, use, management and exit from cloud services shall be established in accordance with the organization's information security requirements.

A.5.24	Information securit y incident management planning and prepa ration	Control The organization shall plan and prepare for managing information secu rity incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities.
A.5.25	Assessment and decision on in formation security events	Control The organization shall assess information security events and decide if they are to be categorized as information security incidents.
A.5.26	Response to information security incidents	Control Information security incidents shall be responded to in accordance with the documented procedures.
A.5.27	Learning from information se curity incidents	Control Knowledge gained from information security incidents shall be used to strengthen and improve the information security controls.
A.5.28	Collection of evidence	Control The organization shall establish and implement procedures for the iden tification, collection, acquisition and preservation of evidence related to information security events.

A.5.29	Infor mat ion sec ur it y dur ing disruption	Control The organization shall plan how to maintain information security at an appropriate level during disruption.
A.5.30	ICT readiness for business con tinuity	Control ICT readiness shall be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements.
A.5.31	Legal, statutory, regulatory and contractual requirements	Control Legal, statutory, regulatory and contractual requirements relevant to information securit y and the organization's approach to meet these requirements shall be identified, documented and kept up to date.
A.5.32	Intellectual property rights	Control The organization shall implement appropriate procedures to protect intellectual property rights.
A.5.33	Protection of records	Control Records shall be protected from loss, destruction, falsification, unau thorized access and unauthorized release.
A.5.34	Privacy and protection of person al identifiable information (PII)	Control The organization shall identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements.

A.5.35	Independent review of informa tion security	Control The organization's approach to managing information securit y and its implementation including people, processes and technologies shall be reviewed independently at planned intervals, or when significant changes occur.
A.5.36	Compliance with policies, rules and standards for information security	Control Compliance with the organization's information security policy, top ic-specific policies, rules and standards shall be regularly reviewed.
A.5.37	Documented operating proce dures	Control Operating procedures for information processing facilities shall be documented and made available to personnel who need them.

A.6.1	Screening	Control Background verification checks on all candidates to become personnel shall be carried out prior to joining the organization and on an ongoing basis taking into consideration applicable laws, regulations and ethics and be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.
A.6.2	Ter ms and condit ions of em ployment	Control The employment contractual agreements shall state the personnel's and the organization's responsibilities for information security.
A.6.3	Information security awareness, education and training	Control Personnel of the organization and relevant interested parties shall receive appropriate information security awareness, education and training and regular updates of the organization's information security policy, topic-specific policies and procedures, as relevant for their job function.
A.6.4	Disciplinary process	Control A disciplinary process shall be formalized and communicated to take actions against personnel and other relevant interested parties who have committed an information security policy violation.
A.6.5	Responsibilities after termination or change of employment	Control Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, enforced and communicated to relevant personnel and other interested parties.
A.6.6	Confidentiality or non-disclosure agreements	Control Confidentialit y or non-disclosure agreements ref lecting the organ ization's needs for the protection of information shall be identified, documented, regularly reviewed and signed by personnel and other relevant interested parties.

A.6.7	Remote working	Control Security measures shall be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organization's premises.
A.6.8	Information security event re porting	Control The organization shall provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner.
7	Physical controls	
A.7.1	Physical security perimeters	Control Securit y perimeters shall be defined and used to protect areas that contain information and other associated assets.
A.7.2	Physical entry	Control Secure areas shall be protected by appropriate entr y controls and access points.
A.7.3	Securing offices, rooms and fa cilities	Control Physical security for offices, rooms and facilities shall be designed and implemented.
A.7.4	Physical security monitoring	Control Premises shall be continuously monitored for unauthorized physical access.

A.7.5	Protecting against physical and environmental threats	Control Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure shall be designed and implemented.
A.7.6	Working in secure areas	Control Security measures for working in secure areas shall be designed and implemented.
A.7.7	Clear desk and clear screen	Control Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities shall be defined and appropriately enforced.
A.7.8	Equipment siting and protection	Control Equipment shall be sited securely and protected.
A.7.9	Security of assets off-premises	Control Offsite assets shall be protected.
A.7.10	Storage media	Control Storage media shall be managed through their life cycle of acquisition, use, transportation and disposal in accordance with the organization's classification scheme and handling requirements.
A.7.11	Supporting utilities	Control Information processing facilities shall be protected from power failures and other disruptions caused by failures in supporting utilities.

A.7.12	Cabling security	Control Cables carrying power, data or supporting information services shall be protected from interception, interference or damage.
A.7.13	Equipment maintenance	Control Equipment shall be maintained correctly to ensure availability, integrity and confidentiality of information.
A.7.14	Sec ure disposa l or reuse of equipment	Control Items of equipment containing storage media shall be verified to en sure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.
8	Technological controls	
A.8.1	User end point devices	Control Information stored on, processed by or accessible via user end point devices shall be protected.
A.8.2	Privileged access rights	Control The allocation and use of privileged access rights shall be restricted and managed.
A.8.3	Information access restriction	Control Access to information and other associated assets shall be restricted in accordance with the established topic-specific policy on access control.
A.8.4	Access to source code	Control Read and write access to source code, development tools and software libraries shall be appropriately managed.

A.8.5	Secure authentication	Control Secure authentication technologies and procedures shall be implemented based on information access restrictions and the topic-specific policy on access control.
A.8.6	Capacity management	Control The use of resources shall be monitored and adjusted in line with current and expected capacity requirements.
A.8.7	Protection against malware	Control Protection against malware shall be implemented and supported by appropriate user awareness.
A.8.8	Management of technical vul nerabilities	Control Information about technical vulnerabilities of information systems in use shall be obtained, the organization's exposure to such vulnerabilities shall be evaluated and appropriate measures shall be taken.
A.8.9	Configuration management	Control Configurations, including security configurations, of hardware, software, services and networks shall be established, documented, implemented, monitored and reviewed.
A.8.10	Information deletion	Control Information stored in information systems, devices or in any other storage media shall be deleted when no longer required.

A.8.11	Data masking	Control Dat a masking shall be used in accordance with the organization's topic-specific policy on access control and other related topic-specific policies, and business requirements, taking applicable legislation into consideration.
A.8.12	Data leakage prevention	Control Data leakage prevention measures shall be applied to systems, net works and any other devices that process, store or transmit sensitive information.
A.8.13	Information backup	Control Backup copies of information, software and systems shall be maintained and regularly tested in accordance with the agreed topic-specific policy on backup.
A.8.14	Redundancy of information pro cessing facilities	Control Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.
A.8.15	Logging	Control Logs that record activities, exceptions, faults and other relevant events shall be produced, stored, protected and analysed.
A.8.16	Monitoring activities	Control Networks, systems and applications shall be monitored for anomalous behaviour and appropriate actions taken to evaluate potential infor mation security incidents.
A.8.17	Clock synchronization	Control The clocks of information processing systems used by the organization shall be synchronized to approved time sources.

A.8.18	Use of privileged utility programs	Control The use of utility programs that can be capable of overriding system and application controls shall be restricted and tightly controlled.
A.8.19	Installation of software on op erational systems	Control Procedures and measures shall be implemented to securely manage software installation on operational systems.
A.8.20	Networks security	Control Networks and network devices shall be secured, managed and controlled to protect information in systems and applications.
A.8.21	Security of network services	Control Security mechanisms, service levels and service requirements of network services shall be identified, implemented and monitored.
A.8.22	Segregation of networks	Control Groups of information services, users and information systems shall be segregated in the organization's networks.
A.8.23	Web filtering	Control Access to external websites shall be managed to reduce exposure to malicious content.
A.8.24	Use of cryptography	Control Rules for the effective use of cryptography, including cryptographic key management, shall be defined and implemented.

A.8.25	Secure development life cycle	Control Rules for the secure development of soft ware and systems shall be established and applied.
A.8.26	Application securit y require ments	Control Information security requirements shall be identified, specified and approved when developing or acquiring applications.
A.8.27	Secure system architecture and engineering principles	Control Principles for engineering secure systems shall be established, docu mented, maintained and applied to any information system development activities.
A.8.28	Secure coding	Control Secure coding principles shall be applied to software development.
A.8.29	Security testing in development and acceptance	Control Securit y testing processes shall be defined and implemented in the development life cycle.
A.8.30	Outsourced development	Control The organization shall direct, monitor and review the activities related to outsourced system development.
A.8.31	Separation of development, test and production environments	Control Development, testing and production environments shall be separated and secured.
A.8.32	Change management	Control Changes to information processing facilities and information systems shall be subject to change management procedures.

A.8.33	Test information	Control Test information shall be appropriately selected, protected and managed.
A.8.34	Protection of information sys tems during audit testing	Control Audit tests and other assurance activities involving assessment of op erational systems shall be planned and agreed between the tester and appropriate management.

LET US SEE SOME EXAMPLES

A6. EXAMPLE: What we can possible audit under people control

Prior to employment. Determine whether information security roles and responsibilities are defined in job descriptions, terms and conditions of employment etc. for specific IT security staff, system/network managers, managers and end users in general. Are there suitable confidentiality and similar clauses? Are staff and contractors recruited into sensitive positions pre screened (including taking out of references and security clearance where appropriate)? Are there enhanced screening processes for staff/managers in particularly sensitive roles (e.g. those with ROOT-equivalent access to sensitive systems) or sites? Are there appropriate HR policies and procedures e.g. disciplinary actions for staff and contractors that transgress IT security rules?

A6. EXAMPLE: What we can possible audit under people control

During employment. Review information security awareness, training and educational arrangements. Do end users and their managers routinely receive appropriate training on information security including roles and responsibilities, login procedures etc., within the context of general IT systems training? Review disciplinary procedures, ideally using one or more recent cases involving information security to assess the process as followed.

Termination or change of employment. Review policies, standards, procedures and guidelines relating to information security elements of the termination process e.g. retrieving information assets (papers, data, systems), keys, removal of access rights etc.

A5.9. EXAMPLE: What we can possible audit under Inventory of information and other associated assets

ISMS Review the information asset inventory and information security risks identified by the organization. Are all relevant in-scope information assets included? Are accountable owners identified for all the assets? Review the analysis/evaluation of threats, vulnerabilities and impacts, the documentation of risk scenarios plus the prioritization or ranking of risks. Look for risks that are materially mis-stated or under-played, for example those where the corresponding controls are expensive or difficult to implement, perhaps where the risks have been misunderstood

Review the organization's Statement of Applicability documenting and justifying the control objectives and controls, both those that are applicable and any that have been excluded/deselected. Confirm that suitable entries exist for all control objectives and controls listed in Annex A of ISO/IEC 27001. Has the Statement of Applicability been reviewed and endorsed/authorized by an appropriate level of management?

Review the ISMS as implemented and operated against the documented ISMS requirements by sampling. Look for evidence supporting or refuting the correlation between documented risks and controls and those actually in operation.

List of Business Database and Valuation of Business Databases

Business Database Title	Business Database Details		Value
NO USE OF BUSINESS DATABASE	Asset ID	N/A	
	Owner	N/A	
	Users	N/A	
	Location	N/A	
	Sys Admin	N/A	
	Life Cycle	N/A	
	Application / Business Specific requirements	N/A	
	Technical Contact	N/A	
	Vendor	N/A	
	Expected Life	N/A	
	Expired Life	N/A	
	Maintenance Status	N/A	
	Purpose / Service / Role	N/A	
	Dependency	N/A	
	Backup Schedule	N/A	
	Backup Location	N/A	
	Confidentiality Requirements		H
	Integrity Requirements		H
	Availability Requirements		H

Databases | Software | Network Devices | Desktops

Inventory of all assets, ex:

Databases

Software

Network devices

Desktops

Laptops

Media (cameras etc)

11 new controls introduced in the ISO 27001 2022 :

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

Let us see examples, comments and audit hints on each one of the 11 new controls introduced in the ISO 27001:2022

•

EXAMPLE: What we can possible audit under Technological control A 5.7 Threat intelligence

This control requires you to gather information about threats and analyze them, in order to take appropriate mitigation actions. This information could be about particular attacks, about methods and technologies the attackers are using, and/or about attack trends. You should gather this information internally, as well as from external sources like vendor reports, government agency announcements, etc.
Smaller companies probably do not need any new technology related to this control; rather, they will have to figure out how to extract the threat information from their existing systems. If they do not have one already, larger companies will need to acquire a system that will alert them to new threats (as well as to vulnerabilities and incidents).
Companies of any size will have to use threat information to harden their systems.
You should set the processes for how to gather and use the threat information to introduce preventive controls in your IT systems, to improve your risk assessment, and to introduce new methods for security testing.
Make employees aware of the importance of sending threat notifications, and train them on how and to whom these threats are to be communicated.
Documentation. No documentation is required by ISO 27001; however, you might include rules about threat intelligence in the following documents:
•Supplier Security Policy –
•Incident Management Procedure –
•Security Operating Procedures –

EXAMPLE: What we can possible audit under Technological control A 5.23 Information security for use of cloud services

This control requires you to set security requirements for cloud services in order to have better protection of your information in the cloud. This includes purchasing, using, managing, and terminating the use of cloud services.
In most cases, new technology will not be needed, because the majority of cloud services already have security features. In some cases, you might need to upgrade your service to a more secure one, while in some rare cases you will need to change the cloud provider if it does not have security features. For the most part, the only change required will be using existing cloud security features in a more thorough way.
You should set up a process to determine security requirements for cloud services and for determining the criteria for selecting a cloud provider; further, you should define a process for determining acceptable use of the cloud, and also the security requirements when cancelling the use of a cloud service.
Make employees aware of the security risks of using cloud services, and train them on how to use the security features of cloud services.
No documentation is required by ISO 27001; however, if you are a smaller company, you might include rules about cloud services in the Supplier Security Policy. Larger companies might develop a separate policy that would focus specifically on security for cloud services.

EXAMPLE: What we can possible audit under Technological control A 5.30 ICT readiness for business continuity

This control requires your information and communication technology to be ready for potential disruptions so that required information and assets are available when needed. This includes readiness planning, implementation, maintenance, and testing.
If you did not invest in solutions that enable resilience and redundancy of your systems, you might need to introduce such technology – this might range from data backup to redundant communication links. These solutions need to be planned based on your risk assessment and how quickly you need your data and your systems to be recovered.
Besides the planning process, which needs to take into account the risks and business needs for recovery, you should also set up the maintenance process for your technology, and the testing process for your disaster recovery and/or business continuity plans.
Make employees aware of potential disruptions that could happen, and train them on how to maintain IT and communication technology so that it is ready for a disruption.
Documentation. No documentation is required by ISO 27001; however, if you are a smaller company, you might include the ICT readiness in the following documents:
•Disaster Recovery Plan – readiness planning, implementation, and maintenance
•Internal Audit Report – readiness testing
see ISO 22301

EXAMPLE: What we can possible audit under Technological control A 7.4 Physical security monitoring

This control requires you to monitor sensitive areas in order to enable only authorized people to access them. This might include your offices, production facilities, warehouses, and other premises.
Depending on your risks, you might need to implement alarm systems or video monitoring; you might also decide to implement a non-tech solution like a person observing the area (e.g., a guard).
You should define who is in charge of the monitoring of sensitive areas, and what communication channels to use to report an incident.
People. Make employees aware of the risks of unauthorized physical entry into sensitive areas, and train them how to use the monitoring technology.
No documentation is required by ISO 27001; however, you might include physical security monitoring in the following documents:
•Procedures that Regulate Physical Security – what is monitored, and who is in charge of monitoring
•Incident Management Procedure – how to report and handle a physical security incident

EXAMPLE: What we can possible audit under Technological control A 8.9 Configuration management

This control requires you to manage the whole cycle of security configuration for your technology to ensure a proper level of security and to avoid any unauthorized changes. This includes configuration definition, implementation, monitoring, and review.
The technology whose configuration needs to be managed could include software, hardware, services, or networks. Smaller companies will probably be able to handle configuration management without any additional tools, whereas larger companies probably need some software that enforces defined configurations.
You should set up a process for proposing, reviewing, and approving security configurations, as well as the processes for managing and monitoring the configurations.
Make employees aware of why strict control of security configuration is needed, and train them on how to define and implement security configurations.
Documentation. ISO 27001 requires this control to be documented. If you are a small company, you can document the configuration rules in your Security Operating Procedures. Larger companies will typically have a separate procedure that defines the configuration process.
You will usually have separate specifications that define security configurations for each of your systems, in order to avoid frequent updates of the documents mentioned in the previous paragraph. Further, all changes to configurations need to be logged to enable an audit trail.

EXAMPLE: What we can possible audit under Technological control A 8.10 Information deletion

This control requires you to delete data when no longer required, in order to avoid leakage of sensitive information and to enable compliance with privacy and other requirements. This could include deletion in your IT systems, removable media, or cloud services.
You should be using tools for secure deletion, according to regulatory or contractual requirements, or in line with your risk assessment.
Organization/processes. You should set up a process that will define which data need to be deleted and when, and define responsibilities and methods for deletion.
People. Make employees aware of why deleting sensitive information is important, and train them on how to do this properly.
Documentation. No documentation is required by ISO 27001; however, you might include rules about information deletion in the following documents:
•Disposal and Destruction Policy – how the information on removable media is deleted
•Acceptable Use Policy – how regular users need to delete the sensitive information on their computers and mobile devices
•Security Operating Procedures – how system administrators need to delete the sensitive information on servers and networks

EXAMPLE: What we can possible audit under Technological control A 8.11 Data masking

This control requires you to use data masking together with access control in order to limit the exposure of sensitive information. This primarily means personal data, because they are heavily regulated through privacy regulations, but it could also include other categories of sensitive data.
Companies can use tools for pseudonymization or anonymization in order to mask data if this is required by privacy or other regulations. Other methods like encryption or obfuscation can also be used.
You should set up processes that will determine which data need to be masked, who can access which type of data, and which methods will be used to mask the data.
Make employees aware of why masking data is important, and train them
Documentation. No documentation is required by ISO 27001; however, you might include rules on data masking in the following documents:
•Information Classification Policy – determine which data are sensitive and what categories of data need to be masked
•Access Control Policy – defines who can access what type of masked or unmasked data
•Secure Development Policy – defines the technology of masking the data
•Privacy Policy / Personal Data Protection Policy –responsibilities for data masking
•Anonymization and Pseudonymization Policy – details on how data masking is implemented in the context of a privacy regulation

EXAMPLE: What we can possible audit under Technological control A 8.12 Data leakage prevention

A.8.12 Data leakage prevention
Description. This control requires you to apply various data leakage measures in order to avoid unauthorized disclosure of sensitive information, and if such incidents happen, to detect them in a timely manner. This includes information in IT systems, networks, or any devices.
Technology. For this purpose, you could use systems to monitor potential leakage channels, including emails, removable storage devices, mobile devices, etc., and systems that prevent information from leaking – e.g., disabling download to removable storage, email quarantine, restricting copy and paste of data, restricting upload of data to external systems, encryption, etc.
Organization/processes. You should set up processes that determine the sensitivity of data, assess the risks of various technologies (e.g., risks of taking photos of sensitive information with a smartphone), monitor channels with the potential of data leakage, and define which technology to use to block the exposure of sensitive data.
People. Make employees aware of what kind of sensitive data is handled in the company and why it is important to prevent leakages, and train them on what is and what isn't allowed when handling sensitive data.
Documentation. No documentation is required by ISO 27001; however, you might include rules on data leakage prevention in the following documents:

- Information Classification Policy – the more sensitive the data are, the more prevention needs to be applied
- Security Operating Procedures – which systems for monitoring and prevention should be used by administrators
- Policy on Acceptable Use – what is and what isn't allowed for regular users

EXAMPLE: What we can possible audit under Technological control A 8.16 Monitoring activities

This control requires you to monitor your systems in order to recognize unusual activities and, if needed, to activate the appropriate incident response. This includes monitoring of your IT systems, networks, and applications.
For your networks, systems, and applications, you could monitor the following: security tool logs, event logs, who is accessing what, activities of your main administrators, inbound and outbound traffic, proper execution of the code, and how the system resources are performing.
You should set up a process that defines which systems will be monitored; how the responsibilities for monitoring are determined; and the methods of monitoring, establishing a baseline for unusual activities, and reporting events and incidents.
Make employees aware that their activities will be monitored, and explain what is and what is not considered normal behavior. Train IT administrators to use monitoring tools.
Documentation. No documentation is required by ISO 27001; however, if you are a smaller company, you might include rules about monitoring in the Security Operating Procedures. Larger companies might develop a separate procedure that would describe how to monitor their systems.
On top of this, it would be useful to keep records of monitoring activities.

EXAMPLE: What we can possible audit under Technological control A 8.23 Web filtering

This control requires you to manage which websites your users are accessing, in order to protect your IT systems. This way, you can prevent your systems from being compromised by malicious code, and also prevent users from using illegal materials from the Internet.

You could use tools that block access to particular IP addresses, which could include the usage of anti-malware software. You could also use non-tech methods like developing a list of forbidden websites and asking users not to visit them.

You should set up processes that determine which types of websites are not allowed, and how the web filtering tools are maintained.

Make employees aware of the dangers of using the Internet and where to find guidelines for safe use, and train your system administrators on how to perform web filtering.

Documentation. No documentation is required by ISO 27001; however if you are a smaller company, you might include rules about web filtering in the following documents:

•Security Operating Procedures – Define rules for system administrators on how to implement web filtering.

•Acceptable Use Policy – Define rules for all users on what is acceptable usage of Internet.

EXAMPLE: What we can possible audit under Technological control A 8.28 Secure coding

This control requires you to establish secure coding principles and apply them to your software development in order to reduce security vulnerabilities in the software. This could include activities before, during, and after the coding.

You might be using tools for maintaining an inventory of libraries, for protecting the source code from tampering, for logging errors and attacks, and for testing; you could also use security components like authentication, encryption, etc.

You should set up a process for defining the minimum baseline of secure coding – both for internal software development and for software components from third parties, a process for monitoring emerging threats and advice on secure coding, a process for deciding which external tools and libraries can be used, and a process that defines activities done before the coding, during the coding, after the coding (review and maintenance), and for software modification.

Make your software developers aware of the importance of using secure coding principles, and train them on methods and tools for secure coding.

Documentation. No documentation is required by ISO 27001; however if you are a smaller company, you might include rules about secure coding in the Secure Development Policy. Larger companies might develop separate procedures for secure coding for each of their software development projects


Effective ISMS is a
STRATEGIC
decision
for an organisation
Thank You!
IQCS/ISMS/02 Rev 0 issued Oct 2022