**Comparison between ISO 27001: 2013 Version and ISO 27001: 2022 Version**

When we speak of security we must also keep in mind the corrective and reformative measure it carries along with it. Security without a specific standard and procedure of following is of no reliability.

A standard follows specific requirements such as:

* Establishing
* Implementing
* Maintaining
* Continuous Improvement

An important point to note is that these requirements are generic and are **applicable to all** organisations irrespective of size, nature, business operations.

All standards and procedures reduce down to the organisation. If we understand the organisation, we understand their security umbrella.

Understanding the organisations’ :

* Context
* Expectations of interested entities
* Scope of ISMS
* ISMS

--------------------------------------------------------------------------------------------------------------------------------------

|  |  |
| --- | --- |
| **2013 Version** | **2022 Version** |
| Number of controls in Annexure A was 114 | Number of Controls in Annexure A was reduced to 93 |
| There were 14 Domains | The theme revolved around 4 components: Organisation, People, Physical, Technological |
| A bit more complex structure due to large number of controls | Comparatively less complex as number of controls reduced |
| Formed the basis | Utilised the 2013 version as the basis |

The potential reasons for why the version was revised be:

* An increase in the type, structure, amount and theme of cyber attacks
* To update the version the same way we software update our devices
* To reduce the complex nature of the old version
* Creating a compact structure by dividing the 93 controls of the new version into 4 themes/ components
* All changes made and decisions taken were done keeping in mind the perspective of the ever changing industry

--------------------------------------------------------------------------------------------------------------------------------------

The important points serialised from 4-10 with their sub divisions namely as given below are nearly the same with just a few subpoints added in the new version to offer more clarity and transparency to the entire process.

*The subpoints highlighted in yellow are the newly added subpoints in the 2022 version:*

**4. Context of the organization**

**4.1 Understanding the organization and its context**

Internal external issues

**4.2 Understanding the needs and expectations of interested parties**

Relevant parties, requirements, method of addressing

**4.3 Determining the scope of the information security management system**

Issues, requirements, interfaces and dependencies

**4.4 Information security management system**

Establish, implement, maintain, improve

**5. Leadership**

**5.1 Leadership and commitment**

Objectives, requirements, resources, importance of ISMS, improvement

**5.2 Policy**

Purpose, objectives, requirements, improvements

**5.3 Organizational roles, responsibilities and authorities**

Communicated within the organisation

**6. Planning**

**6.1 Actions to address risks and opportunities**

**6.1.1 General**

Outcomes, reduce undesired effect, improvement

**6.1.2 Information security risk assessment**

Risk acceptance criteria, criteria for performing the assessment

**6.1.3 Information security risk treatment**

Apply appropriate controls, produce SOA, formulate a plan, obtain approval

**6.2 Information security objectives and planning to achieve them**

Consistency, measureable, requirements, monitoring, communication, updating

**6.3 Planning of changes**

Changes carried out in a planned manner

**7. Support**

**7.1 Resources**

Needed for the establishment, implementation, maintenance and continual improvement

**7.2 Competence**

Determine the individuals, ensure on basis of education, experience

**7.3 Awareness**

Infosec policy, effectiveness of ISMS, non conformity

**7.4 Communication**

On what to, when to, with whom to, how to communicate

**7.5 Documented information**

**7.5.1 General**

Size, type, processes, complexity of organisations

**7.5.2 Creating and updating**

Identification and description, format, review

**7.5.3 Control of documented information**

Available, protected, distributed, storage, retention

**8. Operation**

**8.1 Operational planning and control**

Establish criteria, implement control, availability of resources, changes

**8.2 Information security risk assessment**

When changes occur

**8.3 Information security risk treatment**

Plan and retain the information at end

**9. Performance Evaluation**

**9.1 Monitoring, measurement, analysis and evaluation**

What needs to be monitored, methods used, when it will be conducted, who shall conduct

**9.2 Internal Audit**

**9.2.1 General**

To provide information on the ISMS, conforms to organisations’ and the standard’s requirements

**9.2.2 Internal audit programme**

Shall plan, establish, implement and maintain an audit programme

**9.3 Management review**

**9.3.1 General**

To ensure its continuing suitability, adequacy and effectiveness

**9.3.2 Management review inputs**

Status from previous results, changes in issues, needs, feedback, non conformities, audit results

**9.3.3 Management review results**

Decisions related to continuous improvements

**10. Improvement**

**10.1 Continual Improvement**

Suitability, adequacy and effectiveness of the ISMS

**10.2 Nonconformity and corrective action**

React, evaluate need to eliminate, implement action, review effectiveness, make necessary changes, nature of NM, result of corrective action

--------------------------------------------------------------------------------------------------------------------------------------

**Difference between *Annexure A – Reference control objectives and controls* of 2013 version and 2022 version**

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| A.5 Information Security Policy | A.5 Organisation Controls |
| A.5.1 Management Direction for information security | A.5.1 Policies for Information Security |
| A.5.11 Policies for Information Security |  |
| A.5.1.2 Review of policies for information security |  |

* Policies control definition remains the same for both the versions where policies must be defined, approved by management
* There is an additional subdivision seen in the 2013 version: A.5.1.2 Review of policies for information security. It specifies that the policies must be reviewed at regular intervals
* This subdomain has been merged into the A.5.1 classification in the 2022 version

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| A.6 Organisation of information security | A. 5.2 Information security roles and responsibilities |
| A.6.1 Internal Organisation |  |
| A.6.1.1 Information Security roles and responsibilities |  |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| A.6 Organisation of information security | A. 5.3 Segregation of duties |
| A.6.1 Internal Organisation |  |
| A.6.1.2 Segregation of duties |  |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| - | A. 5.4 Management responsibilities |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| A.6 Organisation of information security | A. 5.5 Contact with authorities |
| A.6.1 Internal Organisation |  |
| A.6.1.3 Contact with authorities |  |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| A.6 Organisation of information security | A. 5.6 Contact with special interest groups |
| A.6.1 Internal Organisation |  |
| A.6.1.4 Contact with special interest groups |  |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| - | A. 5.7 Threat Intelligence |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| A.6 Organisation of information security | A. 5.8 Information security in project management |
| A.6.1 Internal Organisation |  |
| A.6.1.5 Information security in project management |  |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| A.8. Asset Management | A. 5.9 Inventory of information and other associated assets. |
| A.8.1 Responsibility for assets |  |
| A.8.1.1 Inventory of assets |  |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| A.8. Asset Management | - |
| A.8.1 Responsibility for assets |  |
| A.8.1.2 Ownership of Assets |  |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| A.8. Asset Management | A. 5.10 Acceptable use of information and other associated assets. |
| A.8.1 Responsibility for assets |  |
| A.8.1.3 Acceptable use of assets |  |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| A.8. Asset Management | A. 5.11. Return of assets |
| A.8.1 Responsibility for assets |  |
| A.8.1.4 Return of assets |  |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| A.8. Asset Management | A. 5.12 Classification of information |
| A.8.2 Information Classification |  |
| A.8.2.1 Classification of information |  |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| A.8. Asset Management | A. 5.13 Labelling of information |
| A.8.2 Information Classification |  |
| A.8.2.1 Labelling of information |  |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| A.8. Asset Management | A. 5.14 Information Transfer |
| A.8.2 Information Classification |  |
| A.8.2.3 Handling of assets |  |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| A.9. Access Control | A. 5.15 Access Control |
| A.9.1 Business requirements of access control |  |
| A.9.1.1 Access Control Policy |  |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| A.9. Access Control | A. 5.16 Identity Management |
| A.9.2 User Access Management |  |
| A.9.2.1 User registration and de- registration |  |
| A.9.2.2 User access provisioning |  |
| **ISO 27001 2013** | **ISO 27001 2022** |
| A.9. Access Control | A. 5.17 Authentication information |
| A.9.2 User Access Management |  |
| A.9.2.3 Management of privileged access right |  |
| A.9.2.4 Management of secret authentication information of users |  |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| A.9. Access Control | A. 5.18 Access rights |
| A.9.2 User Access Management |  |
| A.9.2.5 Review of user access rights |  |
| A.9.2.6 Removal or adjustment of access rights |  |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| A.15 Supplier relationships | A. 5.19 Information security in supplier relationships |
| A.15.1 Information security in supplier relationships |  |
| A.15.1.1 Information security policy for supplier relationships |  |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| A.15 Supplier relationships | A. 5.20 Addressing information security within supplier agreements |
| A.15.1 Information security in supplier relationships |  |
| A.15.1.2 Addressing security within supplier agreements |  |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| A.15 Supplier relationships | A. 5.21 Managing information security in the information and communication technology (ICT) supply chain |
| A.15.1 Information security in supplier relationships |  |
| A.15.1.3 Information and communication technology supply chain |  |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| A.15 Supplier relationships | A.5.22 Monitoring, review and change management of supplier services |
| A.15.2 Supplier service delivery management |  |
| A.15.2.1 Monitoring and review of supplier services |  |
| A.15.2.2 Managing changes to supplier services |  |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| - | A.5.23 Information security for use of cloud services |

* Acquisition, use, management and exit from cloud services

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| A.16 Information security incident management | A.5.24 Information security incident management planning and preparation |
| A.16.1 Management of information security incidents and improvements |  |
| A.16.1.1 Responsibilities and procedures |  |
| A.16.1.2 Reporting information security events |  |
| A.16.1.3 Reporting information security weakness |  |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| A.16 Information security incident management | A.5.25 Assessment and decision on information security events |
| A.16.1 Management of information security incidents and improvements |  |
| A.16.1.4 Assessment of and decision on information security events |  |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| A.16 Information security incident management | A.5.26 Response to information security incidents |
| A.16.1 Management of information security incidents and improvements |  |
| A.16.1.5 Response to information security incidents |  |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| A.16 Information security incident management | A.5.27 Learning from information security incidents |
| A.16.1 Management of information security incidents and improvements |  |
| A.16.1.6 Learning from information security incidents |  |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| A.16 Information security incident management | A.5.28 Collection of evidence |
| A.16.1 Management of information security incidents and improvements |  |
| A.16.1.7 Collection of evidence |  |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| A.17 Information security aspects of business continuity | A.5.29 Information security during disruption. |
| A.17.1 Information security continuity |  |
| A.17.1.1 Planning information security continuity |  |
| A.17.1.2 Implementing Information security continuity |  |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| A.17 Information security aspects of business continuity | A.5.30 ICT readiness for business continuity |
| A.17.1 Information security continuity |  |
| A.17.1.3 Verify, review and evaluate information security continuity |  |
| A.17.2 Redundancies |  |
| A.17.2.1 Availability of information processing facilities |  |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| A.17 Information security aspects of business continuity | A.5.30 ICT readiness for business continuity |
| A.17.1 Information security continuity |  |
| A.17.1.3 Verify, review and evaluate information security continuity |  |
| A.17.2 Redundancies |  |
| A.17.2.1 Availability of information processing facilities |  |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| A.18 Compliance | A.5.31 Legal, Statutory, regulatory and contractual requirements |
| A.18.1 Compliance with legal and contractual requirements |  |
| A. 18.1.1 Identification of applicable legislation and contractual requirements |  |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| A.18 Compliance | A.5.32 Intellectual property rights |
| A.18.1 Compliance with legal and contractual requirements |  |
| A. 18.1.2 Intellectual property rights |  |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| A.18 Compliance | A.5.33 Protection of records |
| A.18.1 Compliance with legal and contractual requirements |  |
| A. 18.1.3 Protection of records |  |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| A.18 Compliance | A.5.34 Privacy and protection of personal identifiable information (PII) |
| A.18.1 Compliance with legal and contractual requirements |  |
| A. 18.1.4 Privacy and protection of personal identifiable information |  |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| A.18.1.5 Regulation of cryptographic controls | - |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| A.18 Compliance | A.5.35 Independent review of information security |
| A.18.2 Information security reviews |  |
| A. 18.2.1 Independent review of information security |  |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| A.18 Compliance | A.5.36 Compliance with policies, rules and standards for information security |
| A.18.2 Information security reviews | A.5.37. Documented operation procedures |
| A. 18.2.2 Compliance with security policies and standards |  |
| A.18.2.3 Technical compliance review |  |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
|  | A.6. People Controls |
| A.7 Human resource security | 6.1 Screening |
| A.7.1 Prior to employment |  |
| A.7.1.1 Screening |  |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
|  | 6.2 Terms and conditions of employment |
| A.7 Human resource security |  |
| A.7.1 Prior to employment |  |
| A.7.1.2 Terms and conditions of employment |  |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| A.7 Human resource security | 6.3 Information security awareness, education and training |
| A.7.2 During employment |  |
| A.7.2.1 Management responsibilities |  |
| A.7.2.2 Information security awareness, education and training |  |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| A.7 Human resource security | 6.4 Disciplinary process |
| A.7.2 During employment |  |
| A.7.2.3 Disciplinary process |  |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| A.7 Human resource security | 6.5 Responsibilities after termination or change of employment |
| A.7.3 Termination and change of employment |  |
| A.7.3.1 Termination or change of employment responsibilities |  |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| A.13 Communication security | 6.6 Confidentiality or non-disclosure agreements |
| A.13.2 Information transfer |  |
| A.13.2.4 Confidentiality or non- disclosure agreements |  |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| - | 6.7 Remote working |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| A.16 Information security incident management | 6.8 Information security event reporting |
| A.16.1 Management of information security incidents and improvements |  |
| A.16.1.2 Reporting information security events |  |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| A.11 Physical and environmental security | A.7 Physical Controls |
| A.11.1 Secure areas | 7.1 Physical security perimeters |
| A.11.1.1 Physical security perimeter |  |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| A.11 Physical and environmental security | 7.2 Physical entry |
| A.11.1 Secure areas |  |
| A.11.1.2 Physical entry |  |
| **ISO 27001 2013** | **ISO 27001 2022** |
| A.11 Physical and environmental security | 7.3 Securing offices, rooms and facilities |
| A.11.1 Secure areas |  |
| A.11.1.3 Securing offices, rooms and facilities |  |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| A.11 Physical and environmental security | 7.4 Physical security monitoring |
| A.11.1 Secure areas | 7.5 Protecting against physical and environmental threats |
| A.11.1.4 Protecting against external and environmental threats |  |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| A.11 Physical and environmental security | 7.6 Working in secure areas |
| A.11.1 Secure areas |  |
| A.11.1.5 Working in secure areas |  |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| A.11.1.6 Delivery and loading areas | - |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| A.11.2 Equipment | 7.7 Clear desk and clear screen |
| A.11.2.9 Clear desk and clear screen policy |  |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| A.11.2 Equipment | 7.8 Equipment siting and protection |
| A.11.2.1 Equipment siting and protection |  |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| A.11.2 Equipment | 7.9 Security of assets off-premises |
| A.11.2.6 Security of equipment and assets off-premises |  |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| A.13 Communication security | 7.10 Storage media |
| A.13.2 Information transfer |  |
| A.13.2.1 Information transfer policies and procedures |  |
| A.13.2.2 Agreements on information transfer |  |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| A.11.2 Equipment | 7.11 Supporting utilities |
| A.11.2.2 Supporting utilities |  |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| A.11.2 Equipment | 7.12 Cabling security |
| A.11.2.3 Cabling security |  |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| A.11.2 Equipment | 7.13 Equipment maintenance |
| A.11.2.4 Equipment maintenance |  |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| A.11.2 Equipment | 7.14 Secure disposal or re-use of equipment |
| A.11.2.7 Secure disposal or re-use of equipment |  |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| A.6 Organisation and information security | A.8 Technological controls |
| A.6.2 Mobile devices and teleworking | 8.1 User end point devices |
| A.6.2.1 Mobile device policy |  |
| A.6.2.2 Teleworking |  |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| A.9.2 User Access Management | 8.2 Privileged access rights |
| A.9.2.3 Management of privileged access rights |  |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| A.9.4 System and application access control | 8.3 Information access restriction |
| A.9.4.1 Information access restriction |  |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| A.9.4 System and application access control | 8.4 Access to source code |
| A.9.4.5 Access control to program source code |  |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| A.9.3 User responsibilities | 8.5 Secure Authentication |
| A.9.3.1 Use of secret authentication information |  |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| A.12 Operations security | 8.6 Capacity management |
| A.12.1 Operational procedures and responsibilities |  |
| A.12.1.3 Capacity Management |  |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| A.12 Operations security | 8.7 Protection against malware |
| A.12.2 Protection from malware |  |
| A.12.2.1 Controls against malware |  |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| A.12 Operations security | 8.8 Management of technical vulnerabilities |
| A.12.6 Technical vulnerability management |  |
| A.12.6.1 Management of technical vulnerabilities |  |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| A.12 Operations security | 8.9 Configuration Management |
| A.12.1 Operational procedures and responsibilities |  |
| A.12.1.4 Separation of development, testing and operational environment |  |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| A.8 Asset Management | 8.10 Information deletion |
| A.8.3 Media Handling |  |
| A.8.3.2 Disposal of media |  |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| A.8 Asset Management | 8.11 Data Masking |
| A.8.2 Information Classification |  |
| A.8.2.1 Classification of information |  |
| A.8.2.2 Labelling of information |  |
| A.8.2.3 Handling of assets |  |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| - | 8.12 Data leakage prevention |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| A.12 Operations Security | 8.13 Information backup |
| A.12.3 Backup |  |
| A.12.3.1 Information Backup |  |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| A.17 Information security aspects of business continuity management | 8.14 Redundancy of information processing facilities |
| A.17.2 Redundancies |  |
| A.17.2.1 Availability of information processing facilities |  |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| A.12 Operations Security | 8.15 Logging |
| A.12.4 Logging and Monitoring |  |
| A.12.4.1 Event Logging |  |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| A.12 Operations Security | 8.16 Monitoring activities |
| A.12.4 Logging and Monitoring |  |
| A.12.4.2 Protection of log information |  |
| A.12.4.3 Administrator and operator logs |  |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| A.12 Operations Security | 8.17 Clock synchronisation |
| A.12.4 Logging and Monitoring |  |
| A.12.4.4 Clock synchronisation |  |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| A.9 Access control | 8.18 Use of privileged utility program |
| A.9.2 User access management |  |
| A.9.2.3 Management of privileged access rights |  |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| A.12 Operations Security | 8.19 Installation of software on operational systems |
| A.12.5 Control of operational software |  |
| A.12.5.1 Installation of software on operational systems |  |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| A.13 Communications security | 8.20 Network Security |
| A.13.1 Network Security Management |  |
| A.13.1.1 Network Controls |  |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| A.13 Communications security | 8.21 Security of network services |
| A.13.1 Network Security Management |  |
| A.13.1.2 Security of network services |  |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| A.13 Communications security | 8.22 Segregation of networks |
| A.13.1 Network Security Management |  |
| A.13.1.3 Segregation in networks |  |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| - | 8.23 Web Filtering |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| A.10 Cryptography | 8.24 Use of cryptography |
| A.10.1 Cryptographic controls |  |
| A.10.1.1 Policy on the use of cryptographic controls |  |
| A.10.1.2 Key Management |  |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| - | 8.25 Secure development life cycle |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| A.14 System acquisition, development and maintenance | 8.26 Application security requirements |
| A.14.1 Security requirements of information systems |  |
| A.14.1.1 Information security requirements analysis and specifications |  |
| A.14.1.2 Securing application services on public networks |  |
| A.14.1.3 Protecting application services transactions |  |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| A.14 System acquisition, development and maintenance | 8.27 Secure system architecture and engineering principles |
| A.14.2 Security in development and support processes |  |
| A.14.2.5 Secure system engineering principles |  |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| A.14 System acquisition, development and maintenance | 8.28 Secure coding |
| A.14.2 Security in development and support processes |  |
| A.14.2.6 Secure development environment |  |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| A.14 System acquisition, development and maintenance | 8.29 Security testing in development and acceptance |
| A.14.2 Security in development and support processes |  |
| A.14.2.8 System security testing |  |
| A.14.2.9 System acceptance testing |  |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| A.14 System acquisition, development and maintenance | 8.30 Outsource development |
| A.14.2 Security in development and support processes |  |
| A.14.2.7 Outsourced development |  |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| A.12 Operations security | 8.31 Separation of development, test and production environments |
| A.12.1 Operational procedures and responsibilities |  |
| A.12.1.4 Separation of development, testing and operational environment |  |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| A.12 Operations security | 8.32 Change management |
| A.12.1 Operational procedures and responsibilities |  |
| A.12.1.2 Change Management |  |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| A.14 System acquisition, development and maintenance | 8.33 Test information |
| A.14.3 Test data |  |
| A.14.3.1 Protection of test data |  |

|  |  |
| --- | --- |
| **ISO 27001 2013** | **ISO 27001 2022** |
| A.12 Operations security | 8.34 Protection of information systems during audit testing |
| A.12.7 Information systems audit considerations |  |
| A.12.7.1 Information systems audit controls |  |