1) Read ISO27001 and ISO27002 and write all Annex A controls on a single page this will help you to remember controls. (Try to create your own mind map) as given on page 2 of this document. (Exercise – A)

Organizational controls

5.1 Policies for information security
5.2 Information security roles and responsibilities
5.3 Segregation of duties
5.4 Management responsibilities
5.5 Contact with authorities
5.6 Contact with special interest groups
5.7 Threat intelligence
5.8 Information security in project management
5.9 Inventory of information and other associated assets
5.10 Acceptable use of information and other associated assets
5.11 Return of assets
5.12 Classification of information
5.13 Labelling of information
5.14 Information transfer
5.15 Access control
5.16 Identity management
5.17 Authentication information
5.18 Access rights
5.19 Information security in supplier relationships
5.20 Addressing information security within supplier agreements
5.21 Managing information security in the information and communication technology (ICT) supply chain
5.22 Monitoring, review and change management of supplier services
5.23 Information security for use of cloud services
5.24 Information security incident management planning and preparation
5.25 Assessment and decision on information security events
5.26 Response to information security incidents
5.27 Learning from information security incidents
5.28 Collection of evidence
5.29 Information security during disruption
5.30 ICT readiness for business continuity
5.31 Legal, statutory, regulatory and contractual requirements
5.32 Intellectual property rights Control
5.33 Protection of records
5.34 Privacy and protection of personal identifiable information (PII)
5.35 Independent review of information security
5.36 Compliance with policies, rules and standards for information security
5.37 Documented operating procedures

People controls

6.1 Screening
6.2 Terms and conditions of employment
6.3 Information security awareness, education and training
6.4 Disciplinary process
6.5 Responsibilities after termination or change of employment

6.6 Confidentiality or non-disclosure agreements
6.7 Remote working
6.8 Information security event reporting

Physical controls

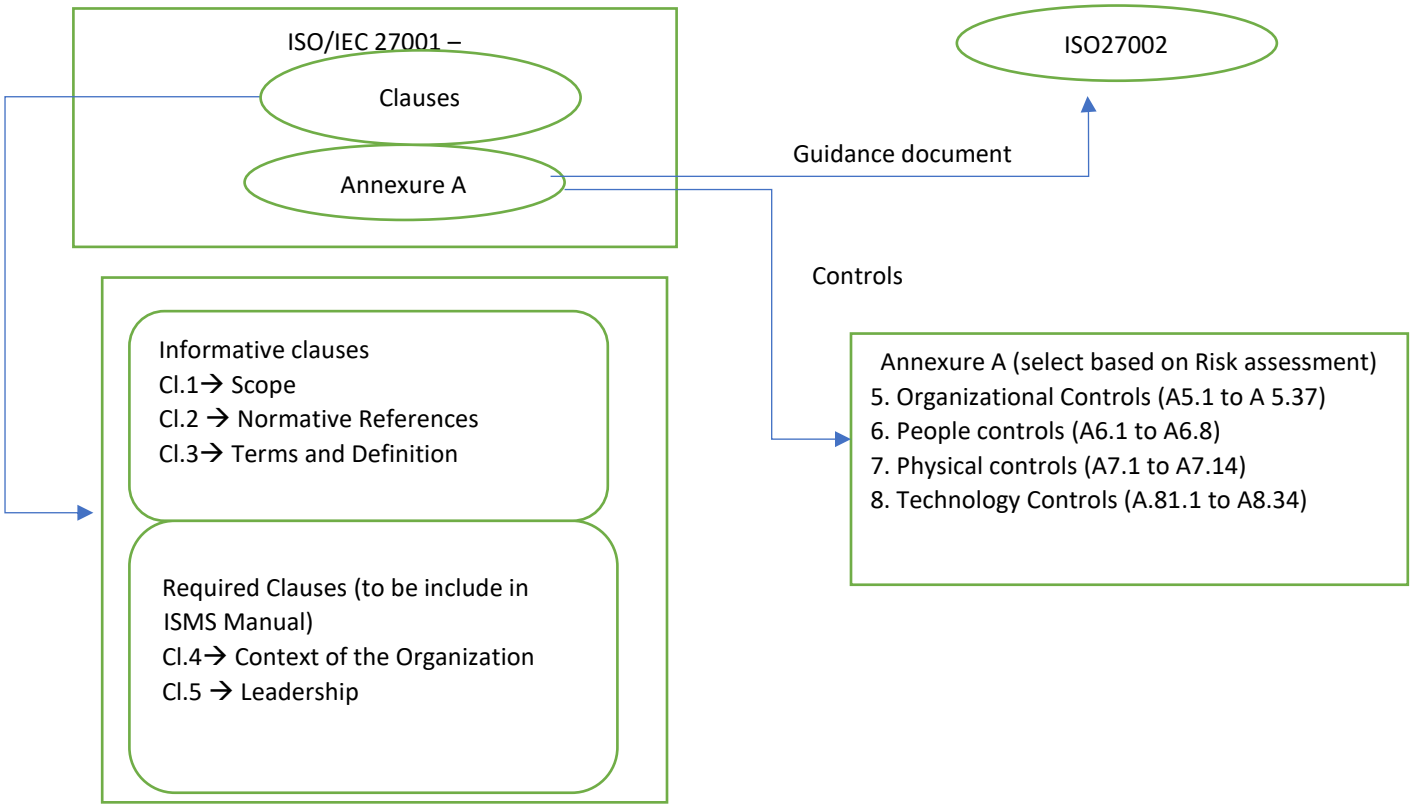
7.1 Physical security perimeters
7.2 Physical entry
7.3 Securing offices, rooms and facilities
7.4 Physical security monitoring
7.5 Protecting against physical and environmental threats
7.6 Working in secure areas
7.7 Clear desk and clear screen
7.8 Equipment siting and protection
7.9 Security of assets off-premises
7.10 Storage media
7.11 Supporting utilities
7.13 Equipment maintenance
7.14 Secure disposal or re-use of equipment

Technological controls

8.1 User end point devices
8.2 Privileged access rights
8.3 Information access restriction
8.4 Access to source code
8.5 Secure authentication
8.6 Capacity management
8.7 Protection against malware
8.8 Management of technical vulnerabilities
8.9 Configuration management
8.10 Information deletion
8.11 Data masking
8.12 Data leakage prevention
8.13 Information backup
8.14 Redundancy of information processing facilities
8.15 Logging
8.16 Monitoring activities
8.17 Clock synchronization
8.18 Use of privileged utility programs
8.19 Installation of software on operational systems
8.20 Networks security
8.21 Security of network services
8.22 Segregation of networks
8.23 Web filtering
8.24 Use of cryptography
8.25 Secure development life cycle
8.26 Application security requirements
8.27 Secure system architecture and engineering principles

8.28 Secure coding
8.29 Security testing in development and acceptance
8.30 Outsourced development
8.31 Separation of development, test and production environments
8.32 Change management
8.33 Test information
8.34 Protection of information systems during audit testing

Submitted on 15th November 2022



Case (Imaginary): Axis Bank
Submitted on 15th November 2022

Exercise -1 **Terms & Definitions pertaining to** Information **Security**

Term	Definition / Standard Terms

1. Base measure	I		~~A~~	Person or body that is recognized as being independent of the parties involved, as concerns the issue in question.
2. Audit scope	W		~~B~~	Effect of uncertainty on objectives.
3. Conformity	G		~~C~~	Continual and iterative processes that an organization conducts to provide, share or obtain information, and to engage in dialogue with stakeholders regarding the management risk.
4. Confidentiality	P		~~D~~	Occurrence or change of particular set of circumstances.
5. Derived measure	MK		~~F~~	Property being accessible and usable by an authorized entity.
6. Decision criteria	Z		~~P~~	Property that information is not made available or disclosed to unauthorized individuals, entitles or processes.
7. Event	D		~~G~~	Fulfillment of requirement.
8. Record	N		K	Measure that is defined as a function of two or more values of base measures.
9. Risk	B		~~W~~	Extent and boundaries of an audit.
10. Availability	F		~~J~~	Potential cause of an unwanted incident, which may result in harm to a system or organization
11. Risk communication and consultation	C		~~M~~	Measure that is defined as a function of two more values of base measures.
12. Vulnerability	O		~~I~~	Means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of administrative, technical, management, or legal nature.
13. Third party	A		~~Z~~	Measure defined in terms of an attribute and the method for quantifying it.
14. Threat	J		~~N~~	Document stating result achieved or providing evidence of activities performed.
15. Derived measure	MK		~~O~~	Weakness of an asset or control that can be exploited by one or more threats.

Exercise-2 **Auditing Information Security Principles**

#	Management Principle	#	Management Principle	#	Management Principle

1	**Awareness of the need for information security**	**2**	**Assignment of responsibility for information security**	**3**	**Incorporating management commitment and the interests of stakeholders**
4	**Enhancing societal values**	**5**	**Risk assessments determining appropriate controls to reach acceptable levels of risk**	**6**	**Security incorporated as an essential element of information networks and systems**
7	**Active prevention and detection of information security incidents;**	**8**	**Ensuring a comprehensive approach to information security management;**	**9**	**Continual reassessment of information security and making of modifications as appropriate**

Submitted on 16th November 2022

#	Scenario – Note > **Some scenarios may demonstrate correct implementation of one or more principle(s) OR may be violating one or more principle(s).**	**Principle (Syl. #)**
1	The Data Privacy policy of the organization focusses on giving respect to privacy of all the Interested Parties and mitigation of all risks for the same	8
2	The process owners of the organization review their residual risks (as a disciplined activity) every six months and updates the approved residual risks	5
3	Five delivery executives of the online shopping portal company, do not collect the identity of the person to whom delivery made, as per delivery policy & process	3
4	The Housing Society declares a special Information Security awareness training to enhance the knowledge of the residents on the subject and give an idea of prioritization of risks – for the benefit of the residential colony member's benefit	1
5	The school principal investigated the incident of the Artificial Intelligence examination paper of final year vanishing from his locker	7
6	The Car rental company collects the identity of the person hiring car without driver and in one case of Ms Jene, did not collect the driving license	9
7	The General Manager who also happens to be in Governance Board of the automotive company, wanted the R&D manager to give presentation on the new steering technology used for which the R&D Manager in the upcoming Tech. conference – the R&D manager refused to do so as per organization's risk assessment control of R&D department	3
8	The Passenger lost his boarding pass after security clearance – wanted to go back to check-in counter to get the duplicate boarding pass – security personnel escorted to check-in counter to verify and ensure that this person is the same and boarding pass belongs to the same person	7
9	Incident records in the DR server got corrupted… and the main server also went down. at the same time this was already identified an approved residual risk (low probability) that both might go down at the same time	9
10	The incident details (including causes) were envisaged as new ones – updated into ISMS KEDB and Risk Assessments	6
11	The traditional way of risk assessments in Excel is replaced by locally developed tool with Risk Assessments for C, I & A done separately, as part of Board decision taken	9
12	The College has introduced an online training module for giving training on Information Security Management Systems (ISO 27001:2022) for benefit of college staff and students	1
13	The Zonal Sales Manager recommended termination of the Salesman as he stole the mobile of the Board Member visiting office for a meeting (left mobile on table before going to washroom) – entire incident was captured in CCTV	7
14	The Business Continuity Plan includes testing of Encrypted Data Retrieval to ensure the Data Integrity reliability – risk assessment shows the approved residual risk of the failure of the De-encryption (low possibility)	5
15	The organization does Gap Analysis towards GDPR compliance (as per Board Instructions) for the purpose complying to GDPR, if applicable to business	4

Exercise -3

Read the Iso27001:2022 standard and try to write down

Introduction

This document outlines the standards for information security which have been derived for the controls introduced in Annex A of ISO27001:2022 standard.

Scope
The scope of this document is as per Axis Bank's Information Security Management System (ISMS) framework detailed in the ISMS Manual.

Information Security in Project Management

Information Security in Project Management

Information security should be addressed in project management, regardless of the type of the project and integrated into Axis Bank's project management process. Information security should be managed throughout the project management phases:

- Initiation
- Planning
- Execution
- Controlling
- Closing

Initiation

Information security objectives associated with project should be clearly identified & documented in project initiation documents.

Planning

Information security risks, associated with project and its information security objectives should be clearly identified & documented.

External and Internal Issues – list down the external and internal issues consider you company as case study for ISO27001 implementation.

Submitted on 16th November 2022

Issues	Type (External / Internal)
1. Information Security Incident	Internal
2. Application Outage	Internal
3. Network Outage/ Issues / General Communication	Internal
4. Information Security Event/ Cyber Attack	External
5. Fraud / Regulation Violation	External
6. Requirement/ Changes in Supplier Services	External

Exercise -4

List down interested parties

Submitted on 16th November 2022

Interest parties	Expectation
Board of directors	Provide secure, safe Banking services while maintaining good financial Support of the hospital
CISO	IT services and medical equipment are available as need to provide Banking Services to its customer
staff (Mangers, RM, CSR …)	Training on the effective usage IT and banking equipment.
Support staff (Office boys, Technicians, front desk, Telephone operators …)	Safe working environment, training on the IT systems, clarity on role and responsibilities.
Suppliers and Vendors	Accurate projection of the requirement and delivery timelines, correct and timely payment of invoices

Exercise -5

Write Scope statement

Submitted on 16th November 2022

The ISMS of 'Axis Bank' applies to Information Security Department at Worli, Mumbai; Infrastructure Services Group – Operating Systems, Infrastructure Services Group – Databases, Infrastructure Services Group – Application Support, Infrastructure Services Group – Middleware, Infrastructure Services Group – Networks, IS – Security Admins, IT Ops (Operations) at Airoli – Navi Mumbai

Exercise -6

Write your Information security policy

Submitted on 16th November 2022

Introduction

This document outlines the standards for information security which have been derived for the controls introduced in Annex A of ISO27001:2013 standard.

Scope

The scope of this document is as per Axis Bank's Information Security Management System (ISMS) framework detailed in the ISMS Manual.

Information Security in Project Management

Information Security in Project Management

Information security should be addressed in project management, regardless of the type of the project and integrated into Axis Bank's project management process. Information security should be managed throughout the project management phases:

- Initiation
- Planning
- Execution
- Controlling
- Closing

Initiation

Information security objectives associated with project should be clearly identified & documented in project initiation documents.

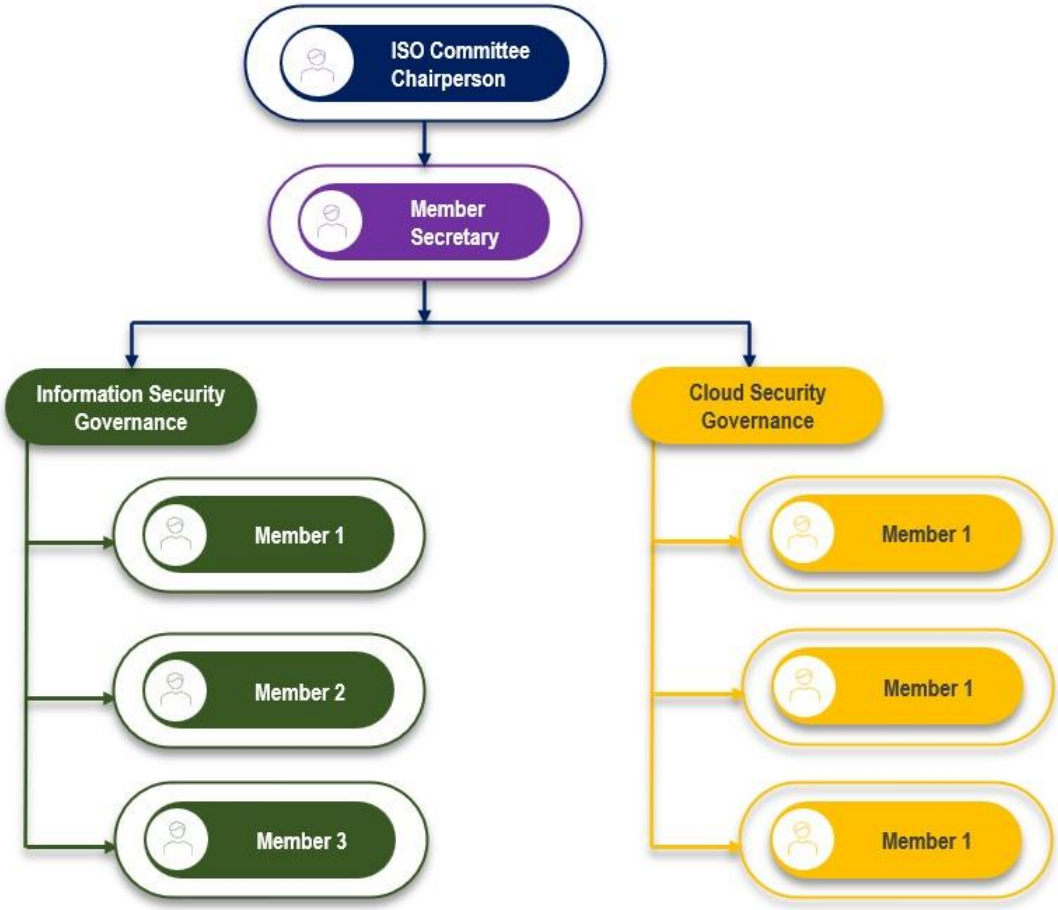
Planning

Information security risks, associated with project and its information security objectives should be clearly identified & documented.

Exercise -7

Draw Organization chart as per your company structure (only to cover information security team & concerned team)

Submitted on 16th November 2022


ISO Committee Chairperson
Member Secretary
Information Security Governance
Member 1
Member 2
Member 3
Cloud Security Governance
Member 1
Member 1
Member 1