Information Security Management Systems Lead Implementor Training Course based on ISO 27001:2022

INSTRUCTIONS FOR PARTICIPANTS:

1) This workbook dully filled ones shall, be used for participants continuous assessment on every day. Please ensure that you submit this workbook to the tutor(s), for daily continuous assessment at the end of each day.
2) On the last day, please send your workbook for review to your tutor or mail at support@infocus-it.com

3) Tips for **SUCCESSFUL COMPLETION OF THE COURSE**:
   - Be attentive and be present on all days, all modules have to be attended;
   - Please clarify all doubts from the tutors during breaks as well;
   - Your active participation is desired – throughout the course;
4) 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)

Exercise - A

5. Organizational controls	6. People controls	8. Technological controls
5.1. Policies for information security	6.1. Screening	8.1. User endpoint devices
5.2. Information security roles and responsibilities	6.2. Terms and conditions of employment	8.2. Privileged access rights
5.3. Segregation of duties	6.3. Information security awareness, education and training	8.3. Information access restriction
5.4. Management responsibilities	6.4. Disciplinary process	8.4. Access to source code
5.5. Contact with authorities	6.5. Responsibilities after termination or change of employment	8.5. Secure authentication
5.6. Contact with special interest groups	6.6. Confidentiality or non-disclosure agreements	8.6. Capacity management
5.7. Threat intelligence	6.7. Remote working	8.7. Protection against malware
5.8. Information security in project management	6.8. Information security event reporting	8.8. Management of technical vulnerabilities
5.9. Inventory of information and other associated assets		8.9. Configuration management
5.10. Acceptable use of information and other associated assets	**7. Physical controls**	8.10. Information deletion
5.11. Return of assets	7.1. Physical security perimeter	8.11. Data masking
5.12. Classification of information	7.2. Physical entry	8.12. Data leakage prevention
5.13. Labelling of information	7.3. Securing offices, rooms and facilities	8.13. Information backup
5.14. Information transfer	7.4. Physical security monitoring	8.14. Redundancy of information processing facilities
5.15. Access control	7.5. Protecting against physical and environmental threats	8.15. Logging
5.16. Identity management	7.6. Working in secure areas	8.16. Monitoring activities
5.17. Authentication information	7.7. Clear desk and clear screen	8.17. Clock synchronization
5.18. Access rights	7.8. Equipment siting and protection	8.18. Use of privileged utility programs
5.19. Information security in supplier relationships	7.9. Security of assets off-premises	8.19. Installation of software on operational systems
5.20. Addressing information security within supplier agreements	7.10. Storage media	8.20. Network security
5.21. Managing information security in the ICT supply chain	7.11. Supporting utilities	8.21. Security of network services
5.22. Monitoring, review and change management of supplier services	7.12. Cabling security	8.22. Segregation of networks
5.23. Information security for use of cloud services	7.13. Equipment maintenance	8.23. Web filtering
5.24. Information security incident management planning and preparation	7.14. Secure disposal or re-use of equipment	8.24. Use of cryptography
5.25. Assessment and decision on information security events		8.25. Secure development life cycle
5.26. Response to information security incidents		8.26. Application security requirements
5.27. Learning from information security incidents		8.27. Secure system architecture and engineering principles
5.28. Collection of evidence		8.28. Secure coding
5.29. Information security during disruption		8.29. Security testing in development and acceptance
5.30. ICT readiness for business continuity		8.30. Outsourced development
5.31. Legal, statutory, regulatory and contractual requirements		8.31. Separation of development, test and production environments
5.32. Intellectual property rights		8.32. Change management
5.33. Protection of records		8.33. Test information
5.34. Privacy and protection of PII		8.34. Protection of information systems during audit testing
5.35. Independent review of information security		
5.36. Compliance with policies, rules and standards for information security		
5.37. Documented operating procedures		

*New control, 2022

Exercise -1

Terms & Definitions pertaining to Information Security

Term			Definition / Standard Terms	
1. Base measure			A	Person or body that is recognized as being independent of the parties involved, as concerns the issue in question.
2. Audit scope			B	Effect of uncertainty on objectives.
3. Conformity			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			D	Occurrence or change of particular set of circumstances.
5. Derived measure			F	Property being accessible and usable by an authorized entity.
6. Decision criteria			P	Property that information is not made available or disclosed to unauthorized individuals, entitles or processes.
7. Event			G	Fulfillment of requirement.
8. Record			K	Measure that is defined as a function of two or more values of base measures.
9. Risk			W	Extent and boundaries of an audit.
10. Availability			J	Potential cause of an unwanted incident, which may result in harm to a system or organization
11. Risk communication and consultation			M	Measure that is defined as a function of two more values of base measures.
12. Vulnerability			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			Z	Measure defined in terms of an attribute and the method for quantifying it.
14. Threat			N	Document stating result achieved or providing evidence of activities performed.
15. Derived measure			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**

#	Scenario – Note > **Some scenarios may demonstrate correct implementation of one or more principle(s) OR may be violating one or more principle(s).**	**Principle (Srl. #)**
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	
2	The process owners of the organization review their residual risks (as a disciplined activity) every six months and updates the approved residual risks	
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	
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	
5	The school principal investigated the incident of the Artificial Intelligence examination paper of final year vanishing from his locker	
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	
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	
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	
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	
10	The incident details (including causes) were envisaged as new ones – updated into ISMS KEDB and Risk Assessments	
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	
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	
13	The Zonal Sales Manager recommended termination of the Sales Man 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	
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)	
15	The organization does Gap Analysis towards GDPR compliance (as per Board Instructions) for the purpose complying to GDPR, if applicable to business	

Exercise -3

Read the Iso27001:2022 standard and try to write down

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

Exercise -4
List down interested parties

Exercise -5
Write Scope statement

Exercise -6

Write your Information security policy

Exercise -7

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

Exercise -8

Define Roles and responsibilities as per the organization chart in exercise -7

Exercise -9

Risk Assessment and Risk Assessment methodology.
Asset base V/s Issue base Risk assessment

Exercise -9A

Make a list of information asset (Inventory)
Exercise -9B
Make a list of Risk / Issues as per your organization

Exercise -9C

List down information security objectives of your organization

Exercise-10

Resource and Competence matrix

Exercise-11
Resource and Competence matrix
Policy / process doc for Document control

Exercise-12

Define communication Plan /policy

Exercise-12

Risk treatment plan

Exercise-13

Define Internal Audit Schedule
Internal Audit training

Exercise-14

Internal Audit Process

Exercise-15
Management Review Process

Exercise-16
Corrective action process Management Review Process

CHECKLIST FOR COMPLETE IMPLEMENTATION – ISO27001:2022

ASSESSMENT CRITERIA	OBJECTIVE EVIDENCE
4 CONTEXT OF THE ORGANIZATION **4.1 Understanding of the organization and its context** **4.2 Understanding the needs and expectations of interested parties** 4.2.1 General 4.2.2 Legal and regulatory requirements **4.3 Determining the scope of the Information Security management system** 4.3.1 General 4.3.2 Scope of the ISMS **4.4 Information Security management system**	
5 LEADERSHIP 5.1 Leadership and commitment 5.2 Policy 5.3 Organizational roles, responsibilities and authorities	
6 PLANNING 6.1 Actions to address risks and opportunities 6.2 Information Security objectives and plans to achieve them	
7 SUPPORT **7.2 Competence** **7.4 Communication** **7.5 Documented information** 7.2.1 General 7.2.2 Creating and updating 7.2.3 Control of documented information	
OPERATION **8.1 Operational planning and control** **8.2 Information security risk assessment** **8.3 Information security risk treatment**	
9 PERFORMANCE EVALUATION **9.1 Monitoring, measurement, analysis and evaluation** 9.1.1 General 9.1.2 Evaluation of Information Security procedures **9.2 Internal audit** **9.3 Management review**	
10 IMPROVEMENT 10.1 Continual improvement 10.2 Nonconformity and corrective action	

INTERNAL AUDIT

Assessment Plan		**Date: DD/MM/YYYY (Atleast 7 days prior)**			
Organization:					
Scope:					
Objective of Assessment:					
Criteria		System Documentation:			
Team Leader:		Audit Start Date:		Opening Meeting:	
Team Member:		Audit End Date:		Closing Meeting:	
Audit Schedule					

Date	**Client Function**	**Auditor**	**Time (hrs)**

Clause#	CHECK POINT (For Verification)	Conclusion (Compliance/ NC)	Evidences for NC
4 Context of the Organization			
5 Leadership			

6 Planning			
7 Support			
8 Operation			

9 Performance Evaluation			
10 Improvement			

Exercise – Non Conformity (NC)

Incident 1

A Bank's back has outsourced the Archiving of its Paper Documents (Daily vouchers, etc.) to a company called "Document Bank" [DB] . The process involves (as per contract) 1. DC shall collect the documents from the Bank (every three months) and put them in Boxes having BAR Code takes the same for stage in their warehouse 2.In warehouse for each BOX - they scan every document in Software, which after scanning the system puts a separate watermark of document unique Bar Code. 3. Keeps the BOX in the located, allocate by system. 4. The scanned documents are converted to CD's and hand delivered to the BANK, in next cycle, when they go to pick up the same (for access soft copy of the docs., when needed – if need be the Bank might ask for original and the Warehouse delivery vehicle delivers the BOX – all movements tracked. This service has been going on for 10 years. In half yearly reconciliation, it was found that the for last two visits, the CD's were not delivered, and the Bank also have not escalated this matter. The DB did not log this as an Incident, saying that the Delivery process is outsourced and now they have made a change in the software for online daily reconciliation and escalating the reconciliation exceptional report to Supervisor and Operations head on daily basis. There is no risk of such kind in the Risk Assessment identified.

NON-CONFORMITY NOTE: 01

ISO 27001:2022 CLAUSE No: _____		
Company Documents	Area unit involve	MAJOR / MINOR [Strike out as required]
Requirement:		

Failure (Nonconformity): NC Impact(s):		
Confidentiality	**Integrity**	**Availability**
□ YES / □ NO	□ YES / □ NO	□ YES / □ NO
Evidence (reference of Process/Personnel/Documents):		
Auditor	Auditee	Date

Incident 2

The commercial DATA Centre (TIER 3) operations applied for ISMS Certification. During Stage 1 review of ISMS documentation review, you observed that there exists a list of IT Assets SPOF (Single point of failures – without redundancies) which includes Routers which are very important for continuity of Networks. Further analysis shows, the Asset list of SPOF comprises of 30% of total IT Network assets and also includes 2 of total 10 Firewalls. On enquiry, the IT Manager says, now a days business is down and require lot of budgets….once business grows due to certification, all the redundancies would be procured and used. The list of Single point of failures have been approved by Management in Risk Assessment.

NON CONFORMITY NOTE: 02

ISO 27001:2022 CLAUSE No: _____		
Company Documents	Area unit involved	MAJOR / MINOR [Strike out as required]
Requirement:		

Failure (Nonconformity):		
NC Impact(s):		
Confidentiality	**Integrity**	**Availability**
□ YES / □ NO	□ YES / □ NO	□ YES / □ NO
Evidence (reference of Process/Personnel/Documents):		
Auditor	Auditee	Date

Incident 3

A Pen drive containing formula of a medicine (for enhance the eye site) with Quality Testing Software was given to the Quality Head (QH) given by Managing Director (who has gone to USA for research in University), with encryption and opens with VPN connectivity & operates with special password only. This is used during every batch of product testing by QH ONLY. One evening, the QH when entered the laboratory for performing that day's last batch testing, was surprised to see the Pen Drive was missing from the Lap Top (which was in the USP port, used in previous testing). An incident report was made and started to search for the same… never to be found again. The MD informed from US "Stop production, I am coming back and sorry – I do not have backup and very disappointed by this negligence of QH & Laboratory functioning".

NON-CONFORMITY NOTE: 03

ISO 27001:2022 CLAUSE No: _____		
Company Documents	Area unit involved	MAJOR / MINOR [Strike out as required]

Requirement:
Failure (Nonconformity): NC Impact(s):

Confidentiality	Integrity	Availability
□ YES / □ NO	□ YES / □ NO	□ YES / □ NO

Evidence (reference of Process/Personnel/Documents):		
Auditor	Auditee	Date

Incident 4

An employee was to attend a conference abroad and forgot her Pouch (containing Passport, Ticket, $ & local currency, Debit & Credit Cards) in the taxi, after reaching the airport and paying off the fare (distracted due to a call on mobile) and at the check-in counter realizes that she does not have the Pouch – all she has is her luggage, ladies purse and boarding pass. She tries call the cab (multiple times) but no response. She comes out of Airport, call her BOSS, who directs her to come to office. She leaves for office in another cab, but blocks her cards by calling bank (to prevent further losses) and also uses her mobile for recording FIR with local police. In the evening, she goes home but surprised to see Police in the house. The police shows her Passport and informs that this passport was found near a dead body of a person. On observing her Passport, she points out that this was her Passport but the Photograph in the Passport is not hers and Police was also surprised. Further she shows all evidences to Policy (FIR, all cab payment receipts, calls she made to Bank to block her cards etc. The police leaves the premises saying "They would be investigating and she might be required for clarifications, if need be.

NON CONFORMITY NOTE: 04

ISO 27001:2022 CLAUSE No: _____		
Company Documents	Area unit involved	**MAJOR** / MINOR [Strike out as required]
Requirement:		

Failure (Nonconformity): NC Impact(s):		
Confidentiality	**Integrity**	**Availability**
□ YES / □ NO	□ YES / □ NO	□ YES / □ NO
Evidence (reference of Process/Personnel/Documents):		
Auditor	Auditee	*Date*

Incident 5

In an Audit of a Public Sector Bank, you observed in Incident # 202 that in activity EOD (End of Day) as on 4th April, in daily P & L Statement, the reminder value of the balance is credited into an account of a person every day, who happens to ex-employee in IT department, who developed the software (grandson of Ex-Board of Director, on whose recommendation he was employed). Further observing revealed that, there were no debit entry to this credit entry, as per Accounting Principle# 1 of Bank's operating manual Ver.2.0 Dt. 5th March 2017, which says there has to be corresponding debit entry for each credit entry. All stake holders involved in doing EOD, have declared that they don't have this manual & were not aware of this thing has been happening since last 10 years. No other action taken rather than releasing a new version of the software with this flaw removed – no incident was recorded, subsequently.

NON-CONFORMITY NOTE: 05

ISO 27001:2022 CLAUSE No: _____		
Company Documents	Area unit involved	MAJOR / MINOR [Strike out as required]
Requirement:		

Failure (Nonconformity):

NC Impact(s):

Confidentiality	Integrity	Availability
□ YES / □ NO	□ YES / □ NO	□ YES / □ NO

Evidence (reference of Process/Personnel/Documents):

Auditor	Auditee	Date

Excercise -26 – NC Template

NON CONFORMITY NOTE : 01

ISO 27001:2022 CLAUSE No: _____		
Company documents	Area unit involved	**MAJOR** / MINOR [Strike out as required]
Requirement:		

Failure (Nonconformity):

NC Impact(s):

Confidentiality	Integrity	Availability
☐ YES / ☐ NO	☐ YES / ☐ NO	☐ YES / ☐ NO

Impacts witnessed in Risk Assessment of the organization

Confidentiality	Integrity	Availability
☐ YES / ☐ NO	☐ YES / ☐ NO	☐ YES / ☐ NO

Evidence (reference of Process/Personnel/Documents):

Exercise – 27

AUDIT REPORT- ASSESSMENT AS PER ISO27001:2022 - MOCK ASSESSMENT

Name of Company (Organization):	
Address:	
Contact Person:	Position:
Alternate Contact Person:	Position:
Registration Scope:	
No. of Employees:	No. of Shifts:
Company's Key Documented Information Reference (if any):	
Management Standard:	
Assessment Type:	
Assessment Commencement Date: Assessment Completion Date:	
Assessment Team: Name Mandays :	
Nonconformities raised during Assessment	

NCR Ref. No.	NC 01	NC 02		
Minor/Major	**Minor**	**Minor**		

Nonconformities raised during last visit

NCR Ref. No.	NA			
Closed/Open				

Areas Assessed:

Audit Conclusion & Appropriateness of the Certification Scope

Disclaimer - Auditing & its conclusion is based on a sampling process of the available information

Non-applicability of requirements (with suitable justification)

ISMS ASSESSMENT COMMENTARY

Context of the Organization

Leadership

Planning

Support

Operation

Performance Evaluation

Improvement

ASSESSMENT COMMENTARY

Positive Issues:

Observations:

(Write NA if this sheet if not applicable)

NONCONFORMITY REPORT

NCR Reference	Details of nonconformity	Management Standard Reference

Exercise-0	Your Objective from this course & Exercise -A
Exercise-1	**Terms & Definitions pertaining to ISO27001**
Exercise-2	**Auditing Information Security Principles**
Exercise-3	**External and Internal Issues – list down the external and internal issues consider you company as**
Exercise-4	**List down interested parties**
Exercise-5	**Write Scope statement**
Exercise-6	**Write your Information security policy**
Exercise-7	**Draw Organization chart as per your company structure (only to cover information security tean**
Exercise-8	**Define Roles and responsibilities as per the organization chart in exercise -7**
Exercise-9	**Risk Assessment and Risk Ass Asset base V/s Issue base Risk assessment**
Exercise-10	**Make a list of information asset (Inventory)**
Exercise-11	**Make a list of Risk / Issues as per your organization**
Exercise-12	**List down information security objectives of your organization**
Exercise-13	**Resource and Competence matrix**
Exercise-14	**Resource and Competence matrix**
Exercise-15	**Policy / process doc for Document control**
Exercise-16	**Define communication Plan /policy**

Exercise-17	Risk treatment plan
Exercise-18	Define Internal Audit Schedule
Exercise-19	Internal Audit training
Exercise-20	Internal Audit Process
Exercise-21	Management Review Process
Exercise-22	Corrective action process Management Review Process
Exercise-23	Prepare Your own checklist - for Implemention & Audit
Exercise-24	Internal Audit template
Exercise-25	Non Confirmity Exercise
Exercise-26	NC - Template
Exercise-27	Final Audit Report - Template