Understanding ISO 27001:2022

The Information Security Management Standard, Simplified

About Me

JAGBIR SINGH

JAGBIR@INFOCUS-IT.COM
M-91-8178210903

Paralegal Cyber Security Consultant, Risk Advisor, Penetration Tester & Trainer

Experience : 15+ years

Areas of Expertise

- ISMS
- ITSM
- BCMS
- VA & PT
- Enterprise Risk Management
- Third Party Risk Management
- Internal Audits
- Audit Planning & Execution
- PIMS
- Disaster Recovery Management .
- IT Governance Risk & Compliance

Industry Sectors

- Contact Center
- Insurance
- IT/ ITES
- Automobile Industry
- Software development
- Consulting
- Law Firms
- Banks
- NBFC

Education / Certifications

- CISA
- CEH
- CHFI
- Diploma into Cyber Law
- ISO 27701:2019
- ISO 27001:2013 LA
- ISO 22301:2012 LI
- ISO 20000:2012 LA
- ISO 9001:2008 LA
- GNIIT
- M.Tech(CS)
- “O” Level DOEACC

Action Agenda

- **ISMS/ISO27001: 2022 – Simplified**
- **What is ISO27001 and ISO27002**
- **What's New In the new Version of ISO27001**
- **Prerequisite to Learn and Implement ISO27001**

Course Schedule

ISO27001:2022 LEAD IMPLEMENTOR COURSE		
Date	Time	Topic covered
12th Nov. 2022	11-1.30 Pm IST	ISMS Intro and Changes into New Vesion . Practical worksheet Clause 4: Context of the organization - Scope statement Clause 5: Leadership - Policy Docs
13th Nov. 2022	11-1.30 Pm IST	ISMS Clause 6: Planning - How to perform Risk Assessment , Type of Risk assement and workbook Clause 7: Support - Policy Documents
19th Nov. 2022	11-1.30 Pm IST	ISMS clause 8 ,9 , 10
20th Nov. 2022	11-1.30 Pm IST	Annex A Controls and Policy docs

Activities Home – Task

Exercise-0	Your Objective from this course & Exercise
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 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-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

Exercise A – Start here

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	**7. Physical controls**	8.9. Configuration management
5.10. Acceptable use of information and other associated assets	7.1. Physical security perimeter	8.10. Information deletion
5.11. Return of assets	7.2. Physical entry	8.11. Data masking
5.12. Classification of information	7.3. Securing offices, rooms and facilities	8.12. Data leakage prevention
5.13. Labelling of information	7.4. Physical security monitoring	8.13. Information backup
5.14. Information transfer	7.5. Protecting against physical and environmental threats	8.14. Redundancy of information processing facilities
5.15. Access control	7.6. Working in secure areas	8.15. Logging
5.16. Identity management	7.7. Clear desk and clear screen	8.16. Monitoring activities
5.17. Authentication information	7.8. Equipment siting and protection	8.17. Clock synchronization
5.18. Access rights	7.9. Security of assets off-premises	8.18. Use of privileged utility programs
5.19. Information security in supplier relationships	7.10. Storage media	8.19. Installation of software on operational systems
5.20. Addressing information security within supplier agreements	7.11. Supporting utilities	8.20. Network security
5.21. Managing information security in the ICT supply chain	7.12. Cabling security	8.21. Security of network services
5.22. Monitoring, review and change management of supplier services	7.13. Equipment maintenance	8.22. Segregation of networks
5.23. Information security for use of cloud services	7.14. Secure disposal or re-use of equipment	8.23. Web filtering
5.24. Information security incident management planning and preparation		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