Comparison of Controls between ISO/IEC 27001:2013 & ISO/IEC 27001:2005

Introduction

The new standard ISO/IEC 27001:2013 has been released officially on 1st October 2013.

Since we understand that information security management system is an integral part of the organization's processes and overall management structure, we have put together this particular document for the better overview of the controls on the new standard ISO/IEC 27001:2013 released.

This document gives you an overview of the controls mentioned in ISO/IEC 27001:2013. The comparison section between the new standard controls with the old standard will give a better understanding on the transition to the new standard. The document can be used and serves as a basic guideline for the transition from the older standard ISO/IEC 27001:2005 to the newer standard ISO/IEC 27001:2013.

Comparison of controls (Annexure A) between ISO/IEC 27001:2005 & ISO/IEC 27001:2013

The old standard (ISO/IEC 27001:2005) had 133 controls mentioned in the standard, while the new standard (ISO/IEC 27001:2013) has 114 controls mentioned in the standard of which 11 new controls have been included. Also the organizations have the liberty of implementing controls from other sources and use this annexure as a reference for the controls implemented. Below comparison would give you a better understanding on how the controls have been arranged and on how the controls can be implemented.

ISO/IEC 27001:2013	ISO/IEC 27001:2005
A.5 Information Security Policy	
A.5.1 Management Directions for Information Security	
Objective: *To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.*	
A.5.1.1 Policies for information security	A.5.1.1 Information security policy document
A.5.1.2 Review of the policies for information security	A.5.1.2 Review of the information security policy
A.6 Organisation of Information Security	
A.6.1 Internal Organisation	
Objective: *To establish a management framework to initiate and control the implementation of information security within the organization.*	
A.6.1.1 Information security roles and responsibilities	A.6.1.3 Allocation of information security responsibilities
	A.8.1.1 Roles and responsibilities
A.6.1.2 Contact with authorities	A.6.1.6 Contact with authorities
A.6.1.3 Contact with special interest groups	A.6.1.7 Contact with special interest groups
A.6.1.4 Information security in project management	
A.6.1.5 Segregation of duties	A.10.1.3 Segregation of duties
A.6.2 Mobile devices and teleworking	
Objective: *To ensure the security of teleworking and use of mobile devices.*	
A.6.2.1 Mobile device policy	A.11.7.1 Mobile computing and

	communications
A.6.2.2 Teleworking	A.11.7.2 Teleworking

A.7 Human Resource Security	
A.7.1 Prior to employment	
Objective: *To ensure that employees, contractors and external party users understand their responsibilities and are suitable for the roles they are considered for.*	
A.7.1.1 Screening	A.8.1.2 Screening
A.7.1.2 Terms and conditions of employment	A.8.1.3 Terms and conditions of employment
A.7.2 During Employment	
Objective: *To ensure that employees and external party users are aware of, and fulfill, their information security responsibilities.*	
A.7.2.1 Management responsibilities	A.8.2.1 Management responsibilities
A.7.2.2 Information security awareness, education and training	A.8.2.2 Information security awareness, education and training
A.7.2.3 Disciplinary process	A.8.2.3 Disciplinary process
A.7.3 Termination and change of employment	
Objective: *To protect the organization's interests as part of the process of changing or terminating employment.*	
A.7.3.1 Termination or change of employment responsibilities	A.8.3.1 Termination responsibilities

A.8 Asset Management	
A.8.1 Responsibility for Assets	
Objective: *To achieve and maintain appropriate protection of organizational assets.*	
A.8.1.1 Inventory of assets	A.7.1.1 Inventory of assets
A.8.1.2 Ownership of assets	A.7.1.2 Ownership of assets
A.8.1.3 Acceptable use of assets	A.7.1.3 Acceptable use of assets
A.8.2 Information classification	
Objective: *To ensure that information receives an appropriate level of protection in accordance with its importance to the organization.*	
A.8.2.1 Classification of information	A.7.2.1 Classification guidelines
A.8.2.2 Labeling of information	A.7.2.2 Information labeling and handling
A.8.2.3 Handling of assets	A.10.7.3 Information Handling procedures
A.8.2.4 Return of assets	A.8.3.2 Return of assets

A.8.3 Media Handling	
Objective: *To prevent unauthorized disclosure, modification, removal or destruction of information stored on media.*	
A.8.3.1 Management of removable media	A.10.7.1 Management of removable media
A.8.3.2 Disposal of media	A.10.7.2 Disposal of Media
A.8.3.3 Physical media transfer	A.10.8.3 Physical media in transit

A.9 Logical Security / Access Control	
A.9.1 Business requirements of access control	
Objective: *To restrict access to information and information processing facilities.*	
A.9.1.1 Access control policy	A.11.1.1 Access control policy
A.9.1.2 Policy on the use of network services	A.11.4.1 Policy on use of network services
A.9.2 User access management	
Objective: *To ensure authorized user access and to prevent unauthorized access to systems and services.*	
A.9.2.1 User registration and de-registration	A.11.2.1 User registration
	A.11.5.2 User identification and authentication
A.9.2.2 Privilege management	A.11.2.2 Privilege management
A.9.2.3 Management of secret authentication information of users	A.11.2.3 User password management
A.9.2.4 Review of user access rights	A.11.2.4 Review of user access rights
A.9.2.5 Removal or adjustment of access rights	A.8.3.3 Removal of access rights
A.9.3 User responsibilities	
Objective: *To make users accountable for safeguarding their authentication information.*	
A.9.3.1 Use of secret authentication information	A.11.3.1 Password use
A.9.4 System and application access control	
Objective: To prevent unauthorized access to systems and applications.	
A.9.4.1 Information access restriction	A.11.6.1 Information access restriction
A.9.4.2 Secure log-on procedures	A.11.5.1 Secure log-on procedures
	A.11.5.5 Session time-out
	A.11.5.6 Limitation of connection time
A.9.4.3 Password management system	A.11.5.3 Password management system
A.9.4.4 Use of privileged utility programs	A.11.5.4 Use of system utilities
A.9.4.5 Access control to program source code	A.12.4.3 Access control to program source code

A.10 Cryptography	
A.10.1 Cryptographic controls	
Objective: *To ensure proper and effective use of cryptography to protect the confidentiality, authenticity or integrity of information.*	
A.10.1.1 Policy on the use of cryptographic controls	A.12.3.1 Policy on the use of cryptographic controls
A.10.1.2 Key management	A.12.3.2 Key management

A.11 Physical and environmental Security	
A.11.1 Secure areas	
Objective: *To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities.*	
A.11.1.1 Physical security perimeter	A.9.1.1 Physical security perimeter
A.11.1.2 Physical entry controls	A.9.1.2 Physical entry controls
A.11.1.3 Securing office, room and facilities	A.9.1.3 Securing offices, rooms and facilities
A.11.1.4 Protecting against external end environmental threats	A.9.1.4 Protecting against external and environmental threats
A.11.1.5 Working in secure areas	A.9.1.5 Working in secure areas
A.11.1.6 Delivery and loading areas	A.9.1.6 Public access, delivery and loading areas
A.11.2 Equipment	
Objective: *To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.*	
A.11.2.1 Equipment siting and protection	A.9.2.1 Equipment sitting and protection
A.11.2.2 Supporting utilities	A.9.2.2 Supporting utilities
A.11.2.3 Cabling security	A.9.2.3 Cabling security
A.11.2.4 Equipment maintenance	A.9.2.4 Equipment maintenance
A.11.2.5 Removal of assets	A.9.2.7 Removal of property
A.11.2.6 Security of equipment and assets off-premises	A.9.2.5 Security of equipment off-premises
A.11.2.7 Security disposal or re-use of equipment	A.9.2.6 Secure disposal or re-use of equipment
A.11.2.8 Unattended user equipment	A.11.3.2 Unattended user equipment
A.11.2.9 Clear desk and clear screen policy	A.11.3.3 Clear desk and clear screen policy

A.12 Operations Security	
A.12.1 Operational Procedures and Responsibilities	
Objective: *To ensure the correct and secure operation of information processing facilities.*	
A.12.1.1 Documented operating procedures	A.10.1.1 Documented operating procedures
A.12.1.2 Change management	A.10.1.2 Change management
A.12.1.3 Capacity management	A.10.3.1 Capacity management
A.12.1.4 Separation of development, test and operational environments	A.10.1.4 Separation of development, test and operational facilities
A.12.2 Protection from Malware	
Objective: *To ensure that information and information processing facilities are protected against malware.*	
A.12.2.1 Controls against malware	A.10.4.1 Controls against malicious code
A.12.3 Back-Up	
Objective: *To protect against loss of data.*	
A.12.3.1 Information backup	A.10.5.1 Information back-up
A.12.4 Logging and Monitoring To record events and generate evidence.	
Objective: *To record events and generate evidence*	
A.12.4.1 Event logging	A.10.10.1 Audit logging
A.12.4.2 Protection of log information	A.10.10.3 Protection of log information
A.12.4.3 Administrator and operator logs	A.10.10.3 Protection of log information
	A.10.10.4 Administrator and operator logs
A.12.4.4 Clock Synchronization	A.10.10.6 Clock synchronization
A.12.5 Control of operational software	
Objective: *To ensure the integrity of operational systems.*	
A.12.5.1 Installation of software on operational systems	A.12.4.1 Control of operational software
A.12.6 Technical Vulnerability Management	
Objective: *To prevent exploitation of technical vulnerabilities.*	
A.12.6.1 Management of technical vulnerabilities	A.12.6.1 Control of technical vulnerabilities
A.12.6.2 Restrictions on software installation	
A.12.7 Information Systems Audit Considerations	
Objective: *To minimize the impact of audit activities on operational systems.*	
A.12.7.1 Information systems audit controls	A.15.3.1 Information system audit controls

A.13 Communications Security	
A.13.1 Network Security Management	
Objective: *To ensure the protection of information in networks and its supporting information processing facilities.*	
A.13.1.1 Network controls	A.10.6.1 Network controls
A.13.1.2 Security of network services	A.10.6.2 Security of network services
A.13.1.3 Segregation in networks	A.11.4.5 Segregation in Networks
A.13.2 Information transfer	
Objective: *To maintain the security of information transferred within an organization and with any external entity.*	
A.13.2.1 Information transfer policies and procedures	A.10.8.1 Information exchange policies and procedures
A.13.2.2 Agreements on information transfer	A.10.8.2 Exchange agreements
A.13.2.3 Electronic messaging	A.10.8.4 Electronic messaging
A.13.2.4 Confidentiality or non-disclosure agreements	A.6.1.5 Confidentiality agreements

A.14 System acquisition, development and maintenance	
A.14.1 Security requirements of information systems	
Objective: *To ensure that security is an integral part of information systems across the entire lifecycle. This includes in particular specific security requirement for information systems which provide services over public networks.*	
A.14.1.1 Security requirements analysis and specification	A.12.1.1 Security requirements analysis and specification
A.14.1.2 Securing applications services on public networks	A.10.9.1 Electronic commerce
	A.10.9.3 Publicly available information
A.14.1.3 Protecting application services transactions	A.10.9.2 Online-transactions
A.14.2 Security in development and support processes	
Objective: *To ensure that information security is designed and implemented within the development lifecycle of information systems.*	
A.14.2.1 Secure development policy	
A.14.2.2 Change control procedures	A.12.5.1 Change control procedures
A.14.2.3 Technical review of applications after operating platform changes	A.12.5.2 Technical review of applications after operating system changes
A.14.2.4 Restrictions on changes to software	A.12.5.3 Restrictions on changes to software

packages	packages
A.14.2.5 System development procedures	
A.14.2.6 Secure development environment	
A.14.2.7 Outsourced development	A.12.5.5 Outsourced software development
A.14.2.8 System security testing	
A.14.2.9 System acceptance testing	A.10.3.2 System Acceptance
A.14.3 Test data	
Objective: *To ensure the protection of data used for testing.*	
A.14.3.1 Protection of test data	A.12.4.2 Protection of system test data

A.15 Supplier relationships	
A.15.1 Security in supplier relationship	
Objective: *To ensure protection of the organization's information that is accessible by suppliers.*	
A.15.1.1 Information security policy for supplier relationships	A.6.2.3 Addressing security in third party agreements
A.15.1.2 Addressing security within supplier agreements	A.6.2.3 Addressing security in third party agreements
A.15.1.3 ICT Supply chain	
A.15.2 Supplier service delivery management	
Objective: *To maintain an agreed level of information security and service delivery in line with supplier agreements.*	
A.15.2.1 Monitoring and review of supplier services	A.10.2.2 Monitoring and review of third party services
A.15.2.2 Managing changes to supplier services	A.10.2.3 Managing changes to third party services

A.16 Information Security Incident Management	
A.16.1 Management of information security incidents and improvements	
Objective: *To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.*	
A.16.1.1 Responsibilities and procedures	A.13.2.1 Responsibilities and Procedures
A.16.1.2 Reporting information security events	A.13.1.1 Reporting information security events
A.16.1.3 Reporting information security weaknesses	A.13.1.2 Reporting security weakness
A.16.1.4 Assessment and decision of information security events	

A.16.1.5 Response to information security incidents	
A.16.1.6 Learning from information security incidents	A.13.2.2 Learning from information security incidents
A.16.1.7 Collection of evidence	A.13.2.3 Collection of evidence

A.17 Business Continuity	
A.17.1 Information security aspects of business continuity management	
Objective: *Information security continuity should be embedded in organization's business continuity management (BCM) to ensure protection of information at any time and to anticipate adverse occurrences.*	
A.17.1.1 Planning information security continuity	A.14.1.2 Business continuity and risk assessment
A.17.1.2 Implementing information security continuity	
A.17.1.3 Verify, review and evaluate information security continuity	A.14.1.5 Testing, maintaining and re-assessing business continuity plans
A.17.2 Redundancies	
Objective: *To ensure availability of information processing facilities.*	
A.17.2.1 Availability of information processing facilities	

A.18 Compliance	
A.18.1 Compliance with legal and contractual requirements	
Objective: *To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements*	
A.18.1.1 Identification of applicable legislation and contractual requirements	A.15.1.1 Identification of applicable legislation
A.18.1.2 Intellectual property rights	A.15.1.2 Intellectual property rights (IPR)
A.18.1.3 Protection of records	A.15.1.3 Protection of organisational records
A.18.1.4 Privacy and protection of personally identifiable information	A.15.1.4 Data protection and privacy of personal information
A.18.1.5 Regulation of cryptographic controls	A.15.1.6 Regulation of cryptographic controls
A.18.2 Information security reviews	

Objective: *To ensure that information security is implemented and operated in accordance with the organizational policies and procedures*	
A.18.2.1 Independent review of information security	A.6.1.8 Independent review of information security
A.18.2.2 Compliance with security policies and standards	A.15.2.1 Compliance with security policies and standards
A.18.2.3 Technical compliance review	A.15.2.2 Technical compliance checking

Controls not considered in ISO/IEC 27001:2013

Below mentioned are the controls which have not been considered in the new standard.

27001:2005 controls omitted
A.6.1.1 Management commitment to information security
A.6.1.2 Information security coordination
A.6.1.4 Authorization process for information processing facilities
A.6.2.1 Identification of risks related to external parties
A.6.2.2 Addressing security when dealing with customers
A.10.2.1 Service delivery
A.10.7.4 Security of system documentation
A.10.8.5 Business Information Systems
A.10.10.2 Monitoring system use
A.10.10.5 Fault logging
A.11.4.2 User authentication for external connections
A.11.4.3 Equipment identification in networks
A.11.4.4 Remote Diagnostic and configuration port protection
A.11.4.6 Network Connection control
A.11.4.7 Network routing control
A.11.6.2 Sensitive system isolation
A.12.2.1 Input data validation
A.12.2.2 Control of internal processing
A.12.2.3 Message integrity
A.12.2.4 Output data validation
A.12.5.4 Information leakage
A.14.1.1 Including information security in the business continuity management process
A.14.1.3 Developing and implementing continuity plans including formation security.
A.14.1.4 Business continuity planning framework
A.15.1.5 Prevention of misuse of information processing facilities
A.15.3.2 Protection of information systems audit tools


Wings2i
Enabling Ideas and Innovations
Wings2i IT Solutions Pvt Ltd.
3rd Floor, BOSS SQUARE,
No:80, 1st Cross, 2nd Main,
BTM Layout 2nd Stage,
Bangalore - 560 076
info@wings2i.com
+91-80-65371700/1