ISO/IEC 27001 Internal Audit Checklist

Auditees:		**Audit Scope:**	
Auditor(s):		**Date(s) of Audit:**	

Recommended Questions	Outcome (C, NC, OFI)	Audit Findings	Evidence Reviewed
4. Context of the Organisation			
4.1 Understanding the organization and its context			
1. What are the internal and external issues that are relevant to the Information Security Management System (ISMS)?			
4.2 Understanding the needs and expectations of interested parties			
1. Who are the interested parties? 2. What are their requirements? 3. Which of these requirements will be addressed through the ISMS?			
4.3 Determining the scope of the ISMS			
1. What is the scope of the ISMS? Is it documented? 2. Does it consider external and internal issues, requirements of interested parties and interfaces and dependencies between activities performed by the organisation, and those performed by other organisations?			
4.4 ISMS			
1. How established is the ISMS? 2. How long has it been running for? 3. How much evidence has been collected so far e.g., records?			
5. Leadership			

Recommended Questions	Outcome (C, NC, OFI)	Audit Findings	Evidence Reviewed
5.1 Leadership and Commitment			
1. Who is defined as top management within the scope of the ISMS? 2. How does top management demonstrate leadership and commitment? 3. Are information security policy and objectives established? 4. Are enough resources allocated to the ISMS? 5. How does top management communicate to everyone involved in the ISMS?			
5.2 Policy			
1. Does the policy appropriate and cover the required areas? 2. Does it include the required commitments? 3. How has it been communicated and distributed and to whom?			
5.3 Organizational roles, responsibilities and authorities			
1. What are the roles within the ISMS? 2. Does everyone understand what their responsibilities and authorities are? 3. Who has the responsibility and authority for conformance and reporting?			
6. Planning			
6.1 Actions to address risks and opportunities			
1. Is there a documented risk assessment process? 2. Does it address risk acceptance criteria and when assessments should be done? 3. Does it identify a reasonable set of risks and specify owners?			

Recommended Questions	Outcome (C, NC, OFI)	Audit Findings	Evidence Reviewed
4. Are the likelihood and impact of risks assessed appropriately and risk levels determined? 5. How are the risks then evaluated and prioritized? 6. Is there a documented risk treatment process? 7. Are reasonable risk treatment options selected? 8. Are the controls chosen to treat the risks stated clearly? 9. Has a Statement of Applicability been produced and are inclusions and exclusions reasonable? 10. Has the risk treatment plan been signed off by the risk owners?			
6.2 Information security objectives and planning to achieve them			
1. Are there documented information security objectives? 2. Is there a plan to achieve the objectives?			
6.3 Planning of changes			
1. Are changes to the ISMS carried out in a planned manner?			
7. Support			
7.1 Resources			
1. How are the resources needed for the ISMS determined? 2. Are the required resources provided?			
7.2 Competence			
1. Have the necessary competences of the people involved in the ISMS been determined? 2. What actions have been identified to acquire the necessary competence?			

Recommended Questions	Outcome (C, NC, OFI)	Audit Findings	Evidence Reviewed
3. Have they been completed and is there evidence of this?			
7.3 Awareness			
1. What approach has been taken to providing awareness of the information security policy, contribution to the ISMS and implications of not conforming? 2. Has everyone been covered?			
7.4 Communication			
1. How has the need for communication been established? 2. Is the approach to communication documented?			
7.5 Documented information			
1. Is all of the documented information required by the standard in place? 2. Are appropriate documentation standards in place e.g., identification, format? 3. Are retention and disposition of documented information defined? 4. Are appropriate controls in place to control versions and manage changes? 5. How are documents of external origin handled?			
8. Operation			
8.1 Operational planning and control			
1. Are criteria for processes established and control of the processes implemented in accordance with the criteria?			

Recommended Questions	Outcome (C, NC, OFI)	Audit Findings	Evidence Reviewed
2. Are documented information available to have confidence that the processes have been carried out as planned? 3. What planned changes have taken place recently and how were they controlled? 4. How are externally provided processes, products or services that are relevant to the ISMS controlled?			
8.2 Information security risk assessment			
1. What are the planned intervals for risk assessments? 2. What significant changes have happened that have prompted a risk assessment to be carried out?			
8.3 Information security risk treatment			
1. What is the status of the risk treatment plan(s)? 2. How is it updated?			
9. Performance Evaluation			
9.1 Monitoring, measurement, analysis and evaluation			
1. How is it determined what should be monitored and measured? 2. What procedures are in place to cover monitoring and measurement in different areas? 3. How are results reported?			
9.2 Internal audit			
1. How often are internal audits carried out? 2. Who carries them out? 3. Are the auditors objective and impartial?			

Recommended Questions	Outcome (C, NC, OFI)	Audit Findings	Evidence Reviewed
4. Have any nonconformities resulting from previous audits been addressed? 5. Does the audit programme cover the complete scope of the ISMS?			
9.3 Management review			
1. How often are management reviews carried out? 2. Who attends them? 3. Are they minuted? 4. Does the management review represent a reasonable assessment of the health of the ISMS?			
10. Improvement			
10.1 Continual improvement			
1. How are improvements identified? 2. What evidence of continual improvement can be demonstrated?			
10.2 Nonconformity and corrective action			
1. How are nonconformities identified? 2. How are they recorded? 3. Was appropriate action taken to correct it and address the underlying causes? 4. Was the effectiveness of the corrective action reviewed?			
ISO/IEC 27001 Annex A Reference Controls / PIMS-specific Guidance Related to ISO/IEC 27002 – Note that not all may be applicable.			
A5. Organisational Controls			
5.1 Policies for information security 1. Are information security policy and topic-specific policies defined, approved by management, published, communicated to and			

Recommended Questions	Outcome (C, NC, OFI)	Audit Findings	Evidence Reviewed
acknowledged by relevant personnel and relevant interested parties? 2. Are the policies reviewed at planned intervals and if significant changes occur?			
5.2 Information security roles and responsibilities 1. Are information security roles and responsibilities defined and allocated according to the organization needs?			
5.3 Segregation of duties 1. Are conflicting duties and conflicting areas of responsibility segregated?			
5.4 Management responsibilities 1. Does management require all personnel to apply information security in accordance with the established policy, topic-specific policies and procedures of the organization?			
5.5 Contact with authorities 1. Does the organization establish and maintain contact with relevant authorities?			
5.6 Contact with special interest groups 1. Does the organization establish and maintain contact with special interest groups or other specialist security forums and professional associations?			
5.7 Threat intelligence 1. Is information relating to information security threats collected? 2. Are they analysed to produce threat intelligence?			
5.8 Information security in project management 1. Is information security integrated into project management?			

Recommended Questions	Outcome (C, NC, OFI)	Audit Findings	Evidence Reviewed
5.9 Inventory of information and other associated assets 1. Is inventory of information and other associated assets developed and maintained? 2. Are information / asset owners assigned in the inventory?			
5.10 Acceptable use of information and other associated assets 1. Are rules for the acceptable use and procedures for handling information and other associated assets identified, documented and implemented?			
5.11 Return of assets 1. Do personnel and other interested parties as appropriate return all the organization's assets in their possession upon change or termination of their employment, contract or agreement?			
5.12 Classification of information 1. Is information classified according to the information security needs of the organization based on confidentiality, integrity, availability, and relevant interested party requirements? 2. Is personal data categorized either sensitive or not and the categorization is evident in the information classification scheme?			
5.13 Labelling of information 1. Is an appropriate set of procedures for information labelling developed and implemented in accordance with the information classification scheme adopted by the organization?			
5.14 Information transfer			

Recommended Questions	Outcome (C, NC, OFI)	Audit Findings	Evidence Reviewed
1. Are there information transfer rules, procedures, or agreements in place for all types of transfer facilities within the organization and between the organization and other parties?			
5.15 Access control 1. Are rules to control physical and logical access to information and other associated assets established and implemented based on business and information security requirements? 2. Are there secured use of every admin account in respect of operating system, database application or network device?			
5.16 Identity management 1. Is the full life cycle of identities managed?			
5.17 Authentication information 1. Are the allocation and management of authentication information controlled by a management process? 2. Does it include advising personnel on appropriate handling of authentication information?			
5.18 Access rights 1. Are the access rights to information and other associated assets provisioned, reviewed, modified and removed in accordance with the organization's topic-specific policy on and rules for access control?			
5.19 Information security in supplier relationships 1. Are processes and procedures defined and implemented to manage the information			

Recommended Questions	Outcome (C, NC, OFI)	Audit Findings	Evidence Reviewed
security risks associated with the use of supplier's products or services?			
5.20 Addressing information security within supplier agreements 1. Are the relevant information security requirements established and agreed with each supplier based on the type of supplier relationship?			
5.21 Managing information security in the information and communication technology (ICT) supply chain 1. Are processes and procedures shall be defined and implemented to manage the information security risks associated with the ICT products and services supply chain?			
5.22 Monitoring, review and change management of supplier services 1. Does the organization regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery?			
5.23 Information security for use of cloud services 1. Are processes for acquisition, use, management and exit from cloud services established in accordance with the organization's information security requirements?			
5.24 Information security incident management planning and preparation 1. Does the organization plan and prepare for managing information security incidents by defining, establishing and communicating incident management processes, roles and responsibilities?			

Recommended Questions	Outcome (C, NC, OFI)	Audit Findings	Evidence Reviewed
5.25 Assessment and decision on information security events 1. Does the organization assess information security events and decide if they are to be categorized as incidents?			
5.26 Response to information security incidents 1. Are information security incidents responded to in accordance with the documented procedures?			
5.27 Learning from information security incidents 1. Are knowledge gained from information security incidents used to strengthen and improve the information security controls?			
5.28 Collection of evidence 1. Does the organization establish and implement procedures for the identification, collection, acquisition and preservation of evidence related to information security events?			
5.29 Information security during disruption 1. Does the organization plan how to maintain information security at an appropriate level during disruption?			
5.30 ICT readiness for business continuity 1. Is ICT readiness planned, implemented and maintained based on business continuity objectives and ICT continuity requirements? 2. Is it tested?			
5.31 Legal, statutory, regulatory and contractual requirements 1. Are legal, statutory, regulatory and contractual requirements relevant to information security and the organization's approach to meet these			

Recommended Questions	Outcome (C, NC, OFI)	Audit Findings	Evidence Reviewed
requirements identified, documented and kept up to date?			
5.32 Intellectual property rights 1. Does the organization implement appropriate procedures to protect intellectual property rights?			
5.33 Protection of records 1. Are records protected from loss, destruction, falsification, unauthorized access and unauthorized release?			
5.34 Privacy and protection of personal identifiable information (PII) 1. Does the organization identify and meet the requirements regarding the preservation of privacy and protection of personal data according to applicable laws and regulations and contractual requirements?			
5.35 Independent review of information security 1. Does the organization's approach to managing information security and its implementation including people, processes and technologies reviewed independently at planned intervals, or when significant changes occur?			
5.36 Compliance with policies, rules and standards for information security security 1. Is compliance with the organization's information security policy, topic-specific policies, rules and standards regularly reviewed?			
5.37 Documented operating procedures 1. Are operating procedures for information processing facilities documented?			

Recommended Questions	Outcome (C, NC, OFI)	Audit Findings	Evidence Reviewed
2. Are these made available to personnel who need them?			
A6. People Controls			
6.1 Screening 1. Are background verification checks on all candidates to become personnel carried out prior to joining the organization and on an ongoing basis? 2. Does it take into consideration applicable laws, regulations and ethics and be proportional to the business requirements, the classification of the information to be accessed and the perceived risks?			
6.2 Terms and conditions of employment 1. Do employment contractual agreements state the personnel's and the organization's responsibilities for information security?			
6.3 Information security awareness, education and training 1. Do personnel of the organization and relevant interested parties receive appropriate information security awareness, education and training and regular updates of the organization's information security policy, topic-specific policies and procedures, as relevant for their job function?			
6.4 Disciplinary process 1. Is a disciplinary process formalized and communicated to take actions against personnel and other relevant interested parties who have committed an information security policy violation?			

Recommended Questions	Outcome (C, NC, OFI)	Audit Findings	Evidence Reviewed
6.5 Responsibilities after termination or change of employment 1. Are information security responsibilities and duties that remain valid after termination or change of employment defined, enforced and communicated to relevant personnel and other interested parties?			
6.6 Confidentiality or non-disclosure agreements 1. Are confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information identified, documented, regularly reviewed and signed by personnel and other relevant interested parties?			
6.7 Remote working 1. Are information security measures implemented when personnel are working remotely to protect information accessed, processed or stored outside the organization's premises?			
6.8 Information security event reporting 1. Does the organization provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner?			
A7. Physical Controls			
7.1 Physical security perimeters 1. Are security perimeters defined and used to protect areas that contain information and other associated assets?			
7.2 Physical entry 1. Are secure areas protected by appropriate entry controls and access points?			

Recommended Questions	Outcome (C, NC, OFI)	Audit Findings	Evidence Reviewed
7.3 Securing offices, rooms and facilities 1. Is physical security for offices, rooms and facilities designed and implemented?			
7.4 Physical security monitoring 1. Are premises continuously monitored for unauthorized physical access?			
7.5 Protecting against physical and environmental threats 1. Is protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure designed and implemented?			
7.6 Working in secure areas 1. Are security measures for working in secure areas designed and implemented?			
7.7 Clear desk and clear screen 1. Are clear desk rules for papers and removable storage media and clear screen rules for information processing facilities defined? 2. Are these appropriately enforced?			
7.8 Equipment siting and protection 1. Are equipment sited securely and protected?			
7.9 Security of assets off-premises 1. Are off-site assets protected?			
7.10 Storage media 1. Are storage media managed through their life cycle of acquisition, use, transportation and disposal in accordance with the organization's classification scheme and handling requirements?			
7.11 Supporting utilities			

Recommended Questions	Outcome (C, NC, OFI)	Audit Findings	Evidence Reviewed
1. Are information processing facilities protected from power failures and other disruptions caused by failures in supporting utilities?			
7.12 Cabling security 1. Are cables carrying power, data or supporting information services protected from interception, interference or damage?			
7.13 Equipment maintenance 1. Are equipment maintained correctly to ensure availability, integrity and confidentiality of information?			
7.14 Secure disposal or re-use of equipment 1. Are items of equipment containing storage media verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use?			
A8. Technological Controls			
8.1 User end point devices 1. How are information stored on, processed by or accessible via user end point devices protected?			
8.2 Privileged access rights 1. How is the allocation and use of privileged access rights restricted and managed?			
8.3 Information access restriction 1. Is access to information and other associated assets restricted in accordance with the established topic-specific policy on access control?			
8.4 Access to source code			

Recommended Questions	Outcome (C, NC, OFI)	Audit Findings	Evidence Reviewed
1. Is read and write access to source code, development tools and software libraries appropriately managed?			
8.5 Secure authentication 1. Are secure authentication technologies and procedures implemented based on information access restrictions and the topic-specific policy on access control?			
8.6 Capacity management 1. Is the use of resources monitored and adjusted in line with current and expected capacity requirements?			
8.7 Protection against malware 1. Is protection against malware implemented and supported by appropriate user awareness?			
8.8 Management of technical vulnerabilities 1. Is information about technical vulnerabilities of information systems in use obtained? 2. Is the organization's exposure to such vulnerabilities evaluated and appropriate measures taken? 3. Are vulnerabilities address in a timely manner (e.g., by applying security patches, etc)?			
8.9 Configuration management 1. Are configurations, including security configurations, of hardware, software, services and networks established, documented, and implemented? 2. Are they monitored and reviewed?			
8.10 Information deletion 1. Is information stored in information systems, devices or in any other storage media deleted when no longer required?			

Recommended Questions	Outcome (C, NC, OFI)	Audit Findings	Evidence Reviewed
8.11 Data masking 1. Is data masking used in accordance with the organization's topic-specific policy on access control and other related topic-specific policies, and business requirements, taking applicable legislation into consideration?			
8.12 Data leakage prevention 1. Are data leakage prevention measures applied to systems, networks and any other devices that process, store or transmit sensitive information?			
8.13 Information backup 1. Are backup copies of information, software and systems maintained? 2. Are these regularly tested in accordance with the agreed topic-specific policy on backup?			
8.14 Redundancy of information processing facilities 1. Are information processing facilities implemented with redundancy sufficient to meet availability requirements?			
8.15 Logging 1. Are logs that record activities, exceptions, faults and other relevant events produced, stored and protected? 2. Are these analysed?			
8.16 Monitoring activities 1. Are networks, systems and applications monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents?			
8.17 Clock synchronization			

Recommended Questions	Outcome (C, NC, OFI)	Audit Findings	Evidence Reviewed
1. Are the clocks of information processing systems used by the organization synchronized to approved time sources?			
8.18 Use of privileged utility programs 1. Is the use of utility programs that can be capable of overriding system and application controls restricted and tightly controlled?			
8.19 Installation of software on operational systems 1. Are there procedures and measures implemented to securely manage software installation on operational systems?			
8.20 Networks security 1. Are networks and network devices secured, managed and controlled to protect information in systems and applications?			
8.21 Security of network services 1. Are security mechanisms, service levels and service requirements of network services identified, implemented and monitored?			
8.22 Segregation of networks 1. Are groups of information services, users and information systems segregated in the organization's networks?			
8.23 Web filtering 1. Is access to external websites managed to reduce exposure to malicious content?			
8.24 Use of cryptography 1. Are rules for the effective use of cryptography, including cryptographic key management, defined and implemented?			
8.25 Secure development life cycle 1. Are rules for the secure development of software and systems established and applied?			

Recommended Questions	Outcome (C, NC, OFI)	Audit Findings	Evidence Reviewed
8.26 Application security requirements 1. Are information security requirements identified, specified and approved when developing or acquiring applications?			
8.27 Secure system architecture and engineering principles 1. Are principles for engineering secure systems established, documented, maintained and applied to any information system development activities?			
8.28 Secure coding 1. Are secure coding principles applied to software development?			
8.29 Security testing in development and acceptance 1. Are security testing processes defined and implemented in the development life cycle?			
8.30 Outsourced development 1. Does the organization direct, monitor and review the activities related to outsourced system development?			
8.31 Separation of development, test and production environments 1. Are development, testing and production environments separated and secured?			
8.32 Change management 1. Are changes to information processing facilities and information systems subject to change management procedures?			
8.33 Test information 1. Is test information appropriately selected, protected and managed?			
8.34 Protection of information systems during audit testing			

Recommended Questions	Outcome (C, NC, OFI)	Audit Findings	Evidence Reviewed
1. Are audit tests and other assurance activities involving assessment of operational systems planned and agreed between the tester and appropriate management?			