

ISO 27001:2022 AUDIT CHECKLIST

PART 1: CLAUSES

qmsdp

مشاوره و آموزش سیستم های مدیریتی

www.qmsdp.com

@Nasiri.qmsdp

@qmsdp

ISO 27001:2022 Clauses	Sub Clauses	Gap Assessment Questionnaire	Response
4 Context of the organization	4.1 - Understanding organization and its context	Have the internal and external issues that are relevant to the organization's ISMS determined	
		Have impact and the risk associated to the issues determined	
		Have the remediation plan for issues documented	
	4.2 - Understanding the needs and expectations of interested parties	Has the organization determined the interested parties that are relevant to the ISMS	
		Has the organization determined the needs and expectations of these interested parties	
		Have the requirements of these interested parties been determined, including legal, regulatory and contractual requirements?	
	4.3 - Determining the scope of the information security management system	Have the boundaries and applicability of the ISMS been determined to establish its scope, taking into consideration the external and internal issues, the requirements of interested parties and the interfaces and dependencies with other organizations?	
		Has the organization defined the scope of ISMS including the in scope departments, interfaces, dependences and the locations	
		Is ISMS scope been documented	
5 Leadership	5.1 - Leadership and commitment	Is the organization's leadership commitment to the ISMS demonstrated by establishing the information security policy and objectives, compatible with the strategic direction of the organization, and in promotion of continual improvement?	
		Has the leadership ensured the integration of the ISMS requirements into its business processes?	
		Has the leadership ensured resources are available for the ISMS, and directing and supporting individuals, including management, who contribute to its effectiveness?	
		Has the leadership communicated the importance of effective information security and conformance to ISMS requirements?	
		Has the leadership directing and supporting relevant roles to contribute to the effectiveness of ISMS	
	5.2 - Policy	Is there an established information security policy that is appropriate to ISMS	
		Does the information security policy gives a framework for setting objectives, and demonstrates commitment for continual improvement of ISMS	
		Is the policy documented and communicated to employees and relevant interested parties?	
	5.3 - Organizational roles,	Are the roles, responsibilities & authorities relevant to ISMS scope clearly defined and communicated?	
		Is the Org Chart defined and inline with the defined roles and responsibilities	

qmsdp

مشاوره و آموزش سیستم های مدیریتی

www.qmsdp.com


@Nasiri.qmsdp

@qmsdp

	responsibilities and authorities	Are the responsibilities and authorities for conformance and reporting on ISMS performance assigned?	
Clause 6	6.1 - Actions to address risks and opportunities	Have the internal and external issues, and the requirements of interested parties been considered to determine the risks and opportunities that need to be addressed to ensure that the ISMS achieves its outcome	
		Have actions to address risks and opportunities been planned, and integrated into the ISMS processes, and are they evaluated for effectiveness?	
		Has an information security risk assessment process that establishes the criteria for performing information security risk assessments, including risk acceptance criteria been defined?	
		Is the information security risk assessment process repeatable and does it produce consistent, valid and comparable results?	
	6.1.2 - Information security risk assessment	Does the information security risk assessment process identify risks associated with loss of confidentiality, integrity and availability for information within the scope of the ISMS, and are risk owners identified?	
		Are information security risks analysed to assess the realistic likelihood and potential consequences that would result, if they were to occur, and have the levels of risk been determined?	
		Are information security risks compared to the established risk criteria and prioritised?	
		Is documented information about the information security risk assessment process available?	
	6.1.3 - Information security risk treatment	Is there an information security risk treatment process to select appropriate risk treatment options for the results of the information security risk assessment, and are controls determined to implement the risk treatment option chosen?	
		Have the controls determined, been compared with ISO/IEC 27001:2022 Annex A to verify that no necessary controls have been missed?	
		Has a Statement of Applicability been produced to justify Annex A exclusions, and inclusions together with the control implementation status?	
		Has the organization formulated an information security risk treatment plan and obtained the risk owners approval for residual risk acceptance	
	6.2 - Information security objectives and planning to achieve them	Have measurable ISMS objectives and targets been established, documented and communicated throughout the organization?	
		In setting its objectives, has the organization determined what needs to be done, when and by whom?	
		Is everyone within the organization's control aware of the importance of the information security policy, their contribution to the effectiveness of the ISMS and the implications of not conforming?	
		Has the organization determined the need for internal and external communications relevant to the ISMS, including	

		what to communicate, when, with whom, and who by, and the processes by which this is achieved?	
7 Support	7.1 - Resources	Has the organization determined the resources needed for ISMS	
	7.2 - Competence	Has the organization determined the competency of the persons relevant to ISMS	
		Has the organization taken corrective measures to acquire the necessary competency of the persons relevant to ISMS	
		Has the organization retained information as evidence for showcasing that the persons relevant to ISMS have necessary competency	
	7.3 - Awareness	Has the organization defined and documented Information Security Awareness Plan	
		Does the employees undergo security awareness sessions upon hire and on periodic basis	
		Does the organization have a method to evaluate the effectiveness of the awareness training	
		How does the organization ensures that the employees are aware about the information security policy	
		Are the employees aware of the implications of not confirming to information security requirements	
	7.4 - Communication	Has the organization developed internal and external communication plan	
		Does the communication plan include the details of what to share, when to share, whom to share, how to share and with whom to share	
	7.5.1 - General 7.5.2 - Creating and updating 7.5.3 - Control of documented information	Has the organization determined the documented information necessary for the effectiveness of the ISMS?	
		Is the documented information in the appropriate format, and has it been identified, reviewed and approved for suitability?	
		Has the organization defined naming conventions including (document title, date, author & approval)	
		While creating and updating the documents does the organization ensure the integrity of the documents by capturing version numbers and appropriate approvals	
		Does the organization have a process to control the distribution of its documented information to ensure it is only available for intended persons	
		Does the organization protects the documented information from loss of confidentiality, integrity and availability	
		Is the documented information properly stored and adequately preserved for its legibility	
		Has the organization identified and documentation of external origin	
8 Operation	8.1 - Operational planning and control	Does the organization has a programme to ensure that the ISMS achieves its outcomes, requirements and objectives been developed and implemented?	
		Is documented evidence retained to demonstrate that processes have been carried out as planned?	
		Are changes planned and controlled, and unintended changes reviewed to mitigate any adverse results?	

<p>qmsdp مشاوره و آموزش سیستم های مدیریتی www.qmsdp.com @Nasiri.qmsdp @qmsdp</p> <p>9 Performance evaluation</p>		How does the organization control outsourced processes/services relevant to ISMS	
		Does the organization have documented information as an evidence to ensure that the processes are carried out and implemented as planned.	
	8.2 - Information security risk assessment	Are information security risk assessments performed at planned intervals or when significant changes occur, and is documented information retained?	
		Does the organization retain relevant documented information of the results of the information security risk assessments	
	8.3 - Information security risk treatment	Has the information security risk treatment plan been implemented as per the information risk treatment plan	
		Does the organization retain relevant documented information of the results of the information security risk treatment	
	9.1 - Monitoring, measurement, analysis and evaluation	Is the information security performance and effectiveness of the ISMS evaluated?	
		How does the organization determine the processes and controls that needs to be monitored and controlled	
		How does the organization determine the methods for monitoring, measurement, analysis and evaluation of security processes and controls	
		How does the organization ensure that the selected methods produce comparable, repeatable and reproducible results	
		Has the organization determined the frequency for monitoring, measurement, analysis and evaluation of security processes and controls	
		Has the organization determined when to analyze the results of monitoring, measurement, analysis and evaluation of security processes and controls	
		Has the organization determined what needs to be monitored and measured, when, and by whom	
		Is documented information retained as evidence of the results of monitoring and measurement?	
	9.2 - Internal audit	Does the organization plan, establish, implement and maintain an internal audit program	
		Has the organization defined the frequency of internal audits	
		Has the organization defined the objective and criteria for the internal audit	
		Has the organization defined the frequency, methods, responsibilities and requirements for the audit program	
		Are internal audits conducted periodically to check that the ISMS is effective and conforms to both ISO/IEC 27001:2022 and the organization's requirements?	
		Does the audit program take into consideration of importance of the process during the audit	
		Are the audits performed by competent personnel	
		How does the organization ensure objectivity and impartiality of the audit	

 <p>مشاوره و آموزش سیستم های مدیریتی www.qmsdp.com @Nasiri.qmsdp @qmsdp</p>		Are the results of the internal audit reported to relevant management personnel	
		Are results of audits reported to management, and is documented information about the audit programme and audit results retained?	
	9.3 - Management review	Does the review consider results from previous management reviews	
		Does the Top Management review the effectiveness of ISMS at planned intervals	
		Does the review consider changes to the internal and external issues	
		Does the review consider changes to the needs and expectations of interested parties	
		Does the review consider the non conformities and corrective actions	
		Does the review consider monitoring and measurement results	
		Does the review consider audit results	
		Does the review consider feedback from interested parties	
		Does the review consider results of risk assessment and risk treatment	
		Does the review consider opportunities for continual improvement	
		Does the outputs of the review include decisions related to continual improvement and any needs for changes to ISMS	
		Has the organization retained documented information as evidence for the results of management reviews	
		Are the results of the management review documented, acted upon and communicated to interested parties as appropriate?	
	10.1 - Continual improvement	Does the organization continually improve the suitability, adequacy and effectiveness of the ISMS	
	10.2 - Nonconformity and corrective action	What are the steps taken by the organization on the non conformities identified	
		Does the organization takes actions to control and correct the non conformities	
		Does the organization identifies the root cause for the non conformity	
		Does the organization take steps to eliminate the root cause	
		Does the organization take steps to identify similar non conformities within the organization.	
		Does the Organization take steps to review the effectiveness of corrective actions taken'	
		Is documented information retained as evidence of the nature of non-conformities, actions taken and the results?	

PART 2: CONTROLS – CONTINUED



**FOLLOW US ON
LINKEDIN FOR MORE
FREE CHECKLISTS**

**PLAYBOOK
MADE WITH
qmsdp**



**MINISTRY
OF
SECURITY**

مشاوره و آموزش سیستم های مدیریتی

www.qmsdp.com

 @Nasiri.qmsdp

 @qmsdp

ISO 27001:2022

AUDIT CHECKLIST

PART 2 A.5 ORGANISATION CONTROLS

Type text here

**MINISTRY
OF
SECURITY**

qmsdp

مشاوره و آموزش سیستم های مدیریتی

www.qmsdp.com

@Nasiri.qmsdp

@qmsdp

A.5 Operational Controls

Control No.	Control	Control Description	Gap Assessment Questions	Response
5.1	Policies for information security	Information security policy and topic-specific policies shall be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.	<ol style="list-style-type: none"> 1. Do Security policies exist. 2. Are all policies approved by management. 3. Are policies properly communicated to employees. 4. Are security policies subject to review. 5. Are the reviews conducted at regular intervals. 6. Are reviews conducted when circumstances change. 	
5.2	Information security roles and responsibilities	Information security roles and responsibilities shall be defined and allocated according to the organization needs.	<ol style="list-style-type: none"> 1. Are the employees properly briefed on their information security roles and responsibilities prior to being granted access to the organization's information and other associated assets. 2. Are responsibilities for the protection of individual assets and Responsibilities for information security risk management activities and in particular for acceptance of residual risks should be defined. 	
5.3	Segregation of duties	Conflicting duties and conflicting areas of responsibility shall be segregated.	<ol style="list-style-type: none"> 1. Are duties and areas of responsibility separated, in order to reduce opportunities for unauthorized modification or misuse of information, or services. 	
5.4	Management responsibilities	Management shall require all personnel to apply information security in accordance with the established information security policy, topic-specific policies and procedures of the organization.	<ol style="list-style-type: none"> 1. Does the management demonstrate support of the information security policy, topic-specific policies, procedures and information security controls. 2. Does the management ensures that personnel achieve a level of awareness of information security relevant to their roles and responsibilities within the organization. 3. Does the management ensures that personnel are provided with adequate resources and project planning time for implementing the organization's security-related processes and controls. 	
5.5	Contact with authorities	The organization shall establish and maintain contact with relevant authorities.	<ol style="list-style-type: none"> 1. Is there a procedure documenting when, and by whom, contact with relevant authorities (law enforcement etc.) will be made. 2. Is there a process, which details how and when contact, is required? 3. Is there a process for routine contact and intelligence sharing. 	
5.6	Contact with special interest groups	The organization shall establish and maintain contact with special interest groups or other specialist security forums and professional associations.	<ol style="list-style-type: none"> 1. Do relevant individuals within the organisation maintain active membership in relevant special interest groups. 2. Does relevant individuals within the organization gain knowledge about best practices and stay up to date with relevant security information. 3. Does relevant individuals within the organization share and exchange information about new technologies, products, services, threats or vulnerabilities. 	

5.7	Threat intelligence	Information relating to information security threats shall be collected and analyzed to produce threat intelligence.	<ol style="list-style-type: none"> 1. Is there a documented policy/procedure describing process for collecting, analyzing and evaluating information related to information security threats. 2. Does the threat intelligence program ensure that the information collected related to information security threats are relevant, insightful, contextual and actionable. 3. Does the threat intelligence program has a formal process for identifying, vetting and selecting internal and external information security threat sources and analyzing information to understand the impact to the organization. 	
5.8	Information security in project management	Information security shall be integrated into project management.	<ol style="list-style-type: none"> 1. Is there a documented policy/procedure describing process to ensure information security risks related to projects and deliverables are effectively addressed in project management throughout the project life cycle. 2. Are the information security risks assessed and treated at an early stage and periodically as part of project risks throughout the project life cycle. 3. Are the requirements regards to compliance with the legal, statutory, regulatory and contractual requirements considered throughout the project management life cycle? 	
5.9	Inventory of information and other associated assets	An inventory of information and other associated assets, including owners, shall be developed and maintained.	<ol style="list-style-type: none"> 1. Is there an inventory of all assets associated with information and information processing facilities. 2. Is the inventory accurate and kept up to date. 3. Are the asset owners identified and tagged to all assets. 4. Is the asset inventory updated when assets are procured, decommissioned or disposed. 	
5.10	Acceptable use of information and other associated assets	Rules for the acceptable use and procedures for handling information and other associated assets shall be identified, documented and implemented.	<ol style="list-style-type: none"> 1. Is there a documented policy/procedure describing process to ensure information and other associated assets are appropriately protected, used and handled. 2. Is the policy approved by the management. 3. Is the policy communicated to all individuals of the organization. 4. Does the policy at minimum covers expected and unacceptable behaviors of employees from an information security perspective. 	
5.11	Return of assets	Personnel and other interested parties as appropriate shall return all the organization's assets in their possession upon change or termination of their employment, contract or agreement.	<ol style="list-style-type: none"> 1. Is there a process in place to ensure all employees and external users return the organisation's assets on termination of their employment, contract or agreement. 2. Is the organization following the defined process for collecting all physical and electronic assets provided to the employee. 	

5.12	Classification of information	Information shall be classified according to the information security needs of the organization based on confidentiality, integrity, availability and relevant interested party requirements.	<ol style="list-style-type: none"> 1. Is there a documented policy/procedure describing process to classify information and assets based on the criticality and sensitivity of the information. 2. Are the requirements for confidentiality, integrity and availability considered for the classification. 3. Is the classification scheme defined and followed for information classification. 4. Are the information owners involved in classifying the information under their control. 5. Is there a defined process for declassifying or to change the classification of the information. 6. Is the information classification reviewed on periodic basis. 	
5.13	Labelling of information	An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.	<ol style="list-style-type: none"> 1. Is there a documented policy/procedure describing process to label the information within the organization. 2. Does the labelling process defined the contents to be included in the label. 	
5.14	Information transfer	Information transfer rules, procedures, or agreements shall be in place for all types of transfer facilities within the organization and between the organization and other parties.	<ol style="list-style-type: none"> 1. Is there a documented policy/procedure describing process to maintain the security of information transferred within an organization and with any external interested parties. 2. Are procedures for how data should be transferred made available to all employees. 3. Are relevant technical controls in place to prevent non-authorised forms of data transfer 4. Is there a documented policy and process detailing how physical media should be transported. 5. Is media in transport protected against unauthorised access, misuse or corruption. 	
5.15	Access control	Rules to control physical and logical access to information and other associated assets shall be established and implemented based on business and information security requirements.	<ol style="list-style-type: none"> 1. Is there a documented policy/procedure describing process to manage logical and physical access to information, assets and information processing assets. 2. Is the policy based on business requirements. 3. Is the policy communicated appropriately. 4. Does the access management include the principles of "need-to-know" and "need-to-use" for managing logical and physical access to information, assets and information processing facilities. 	
5.16	Identity management	The full life cycle of identities shall be managed.	<ol style="list-style-type: none"> 1. Are the employees provided with unique IDs for accessing information, assets and information processing facilities. 2. Shared user IDs/Accounts are only authorized when necessary for business purposes and after approvals 3. Are the Identities removed/disabled when no longer needed. 	

5.17	Authentication information	Allocation and management of authentication information shall be controlled by a management process, including advising personnel on appropriate handling of authentication information.	<ol style="list-style-type: none"> 1. Is there a documented policy/procedure describing process to distribute or assign authentication credentials for employees. 2. Is there a documented policy/procedure describing the baseline requirements of authentication credentials (passwords/passphrases/PINs) used for accessing organization information, assets and information processing facilities. 2. Are the passwords/authentication credentials communicated to employees via a secured channel. 3. Are the employees prompted to change the credentials upon first login. 4. Is there a formal process for resetting authentication credentials. 	
5.18	Access rights	Access rights to information and other associated assets shall be provisioned, reviewed, modified and removed in accordance with the organization's topic-specific policy on and rules for access control.	<ol style="list-style-type: none"> 1. Are the access rights assigned considering the business requirements and individual's roles and responsibilities. 2. Is the principle of segregation of duties considered while provisioning access rights. 3. Are appropriate approvals taken from asset/information owners for provisioning or revoking access rights. 4. Is there a predefined frequency for reviewing the access rights. 5. Are the access rights modified upon change of job role or termination. 	
5.19	Information security in supplier relationships	Processes and procedures shall be defined and implemented to manage the information security risks associated with the use of supplier's products or services.	<ol style="list-style-type: none"> 1. Is there a documented policy/procedure describing process to manage information security risks associated with the use of supplier's products or services. 2. Are the vendors/suppliers evaluated with the organization's requirements for information security. 3. Are the process defined for handling incidents and contingencies associated with supplier products and services. 4. Are suppliers/vendors provided with documented security requirements? 5. Is supplier/vendor's access to information assets & infrastructure controlled and monitored? 	
5.20	Addressing information security within supplier agreements	Relevant information security requirements shall be established and agreed with each supplier based on the type of supplier relationship.	<ol style="list-style-type: none"> 1. Are the information security requirements included in contracts established with suppliers and service providers? 2. Does the contracts established with supplier and service providers include legal, statutory, regulatory, data protection, handling of personally identifiable information (PII), intellectual property rights and copyright requirements. 3. Does the contracts established with supplier and service providers include rules of acceptable use of organization's information and information assets. 	
5.21	Managing information security in the information and communication technology (ICT) supply chain	Processes and procedures shall be defined and implemented to manage the information security risks associated with the ICT products and services supply chain.	<ol style="list-style-type: none"> 1. Do supplier agreements include requirements to address information security within the service & product supply chain. 	

5.22	Monitoring, review and change management of supplier services	The organization shall regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery.	<ol style="list-style-type: none"> 1. Is there a documented policy/procedure describing process to maintain an agreed level of information security and service delivery in line with supplier agreements. 2. Are the SLA's (Service Level Agreements) defined for all service providers . 3. Are there any periodic checks done to ensure the supplier is delivering the agreed level of services to the organization. 	
5.23	Information security for use of cloud services	Processes for acquisition, use, management and exit from cloud services shall be established in accordance with the organization's information security requirements.	<ol style="list-style-type: none"> 1. Is there a documented policy/procedure describing process to manage information security for the use of cloud services within the organization. 2. Are the roles and responsibilities related to the use and management of cloud services defined. 3. Is there a process defined to obtain assurance on information security controls implemented by cloud service providers. 4. Is there a process defined for handling information security incidents that occur in relation to the use of cloud services. 	
5.24	Information security incident management planning and preparation	The organization shall plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities.	<ol style="list-style-type: none"> 1. Is there a documented policy/procedure describing process for quick, effective, consistent and orderly response to information security incidents. 2. Is there a process for reporting of identified information security weaknesses. 3. Is this process communicated to all employees and interested parties as applicable 4. Are the members of incident management team provided with appropriate training for managing incidents. 5. Is the incident response plan tested on periodic basis. 	
5.25	Assessment and decision on information security events	The organization shall assess information security events and decide if they are to be categorized as information security incidents.	<ol style="list-style-type: none"> 1. Is there a process to ensure information security events are properly assessed and classified. 2. Is there a process to categorize and prioritise incidents based on the impact. 	
5.26	Response to information security incidents	Information security incidents shall be responded to in accordance with the documented procedures.	<ol style="list-style-type: none"> 1. Is there a process defined for responding to information security incidents. 2. Is there documented response timelines for all categories of incidents. 3. Is there a process to understand and analyse the root cause for the incidents. 4. Are the actions taken to mitigate the incident effective . 	
5.27	Learning from information security incidents	Knowledge gained from information security incidents shall be used to strengthen and improve the information security controls.	<ol style="list-style-type: none"> 1. Is there a process or framework which allows the organisation to learn from information security incidents and reduce the impact / probability of future events. 2. Is there a process to enhance the incident management plan including incident scenarios and procedures from the learnings. 	

5.28	Collection of evidence	The organization shall establish and implement procedures for the identification, collection, acquisition and preservation of evidence related to information security events.	<ol style="list-style-type: none"> 1. Is there a process in place to ensure a consistent and effective management of evidence related to information security incidents. 2. In the event of an information security incident is relevant data collected in a manner which allows it to be used as evidence. 	
5.29	Information security during disruption	The organization shall plan how to maintain information security at an appropriate level during disruption.	<ol style="list-style-type: none"> 1. Is there a documented policy/procedure describing process to protect information and other associated assets during disruption. 2. Is there a process to maintain existing information security controls during disruption. 	
5.30	ICT readiness for business continuity	ICT readiness shall be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements.	<ol style="list-style-type: none"> 1. Is there a documented policy/procedure to ensure the availability of the organization's information and other associated assets during disruption. 2. Is information security included in the organisation's continuity plans. 3. Do information processing facilities have sufficient redundancy to meet the organisations availability requirements. 4. Does the organization test its continuity plan on a periodic basis. 	
5.31	Legal, statutory, regulatory and contractual requirements	Legal, statutory, regulatory and contractual requirements relevant to information security and the organization's approach to meet these requirements shall be identified, documented and kept up to date.	<ol style="list-style-type: none"> 1. Is there a process in place to ensure compliance with legal, statutory, regulatory and contractual requirements related to information security. 2. Are the responsibilities assigned to individuals for managing legal, statutory, regulatory and contractual requirements related to information security. 3. Are the actions taken to meet legal, statutory, regulatory and contractual requirements related to information security reviewed to check their effectiveness. 	
5.32	Intellectual property rights	The organization shall implement appropriate procedures to protect intellectual property rights.	<ol style="list-style-type: none"> 1. Does the organisation keep a record of all intellectual property rights and use of proprietary software products. 2. Does the organisation monitor for the use of unlicensed software. 3. Are processes in place for acquiring software only through known and reputable sources, to ensure that copyright is not violated. 4. Are processes in place to ensure that any maximum number of users permitted within the license is not exceeded. 	
5.33	Protection of records	Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release.	<ol style="list-style-type: none"> 1. Are records protected from loss, destruction, falsification and unauthorized access or release in accordance with legislative, regulatory, contractual and business requirements. 2. Are controls on place for storage, handling chain of custody and disposal of records. 	
5.34	Privacy and protection of personal identifiable information (PII)	The organization shall identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements.	<ol style="list-style-type: none"> 1. Is there a process in place to ensure compliance with legal, statutory, regulatory and contractual requirements related to the information security aspects of the protection of PII. 2. Is the process communicated to all relevant interested parties involved in the processing of personally identifiable information. 	

5.35	Independent review of information security	The organization's approach to managing information security and its implementation including people, processes and technologies shall be reviewed independently at planned intervals, or when significant changes occur.	<ol style="list-style-type: none"> 1. Is there a process in place to ensure the continuing suitability, adequacy and effectiveness of the organization's approach to managing information security. 2. Is the organisations approach to managing information security subject to regular independent review? 3. Is the implementation of security controls subject to regular independent review. 	
5.36	Compliance with policies, rules and standards for information security	Compliance with the organization's information security policy, topic-specific policies, rules and standards shall be regularly reviewed.	<ol style="list-style-type: none"> 1. Is there a process in place to ensure that information security is implemented and operated in accordance with the organization's information security policy, topic-specific policies, rules and standards. 2. If a non compliance is identified is there a process to identify the causes of the non-compliance, implementing corrective actions and reviewing the actions taken to evaluate the effectiveness. 	
5.37	Documented operating procedures	Operating procedures for information processing facilities shall be documented and made available to personnel who need them.	<ol style="list-style-type: none"> 1. Are operating procedures well documented. 2. Are the procedures made available to all users who need them. 3. Does the operating procedures specify responsibilities of individuals. 	

FOLLOWED BY PART 3: A.6 - PEOPLE CONTROLS & A.7 - PHYSICAL CONTROLS

qmsdp

مشاوره و آموزش سیستم های مدیریتی

www.qmsdp.com

 @Nasiri.qmsdp

 @qmsdp

www.qmsdp.com



**FOLLOW US ON
LINKEDIN FOR MORE
FREE CHECKLISTS**

**PLAYBOOK
MADE WITH**



**MINISTRY
OF
SECURITY**

ISO 27001:2022

AUDIT CHECKLIST

PART 3

A.6 PEOPLE CONTROLS

&

A.7 PHYSICAL CONTROLS

qmsdp

مشاوره و آموزش سیستم های مدیریتی

www.qmsdp.com

@Nasiri.qmsdp

@qmsdp

MINISTRY
OF
SECURITY

A.6 People Controls

Control No.	Control	Control Description	Assessment Questions	Response
6.1	Screening	Background verification checks on all candidates to become personnel shall be carried out prior to joining the organization and on an ongoing basis taking 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.	1. Is there a screening process for onboarding full-time, part-time and temporary staff. 2. Are background verification checks carried out on all new candidates for employment? 3. Does the background verification process consider checking professional experience, academic qualifications, independent identity verification, criminal records verification and credit review. 4. Are the checks compliant with relevant laws, regulations and ethics?	
6.2	Terms and conditions of employment	The employment contractual agreements shall state the personnel's and the organization's responsibilities for information security.	1. Is there a formal terms and conditions of employment documented and communicated to all full-time, part-time and temporary staff before onboarding. 2. Does the terms and conditions of employment include organization's information security policy and relevant topic-specific policies. 3. Does the terms and conditions of employment include legal responsibilities and rights like copyright laws or data protection legislations. 4. Does the terms and conditions of employment include responsibilities for the handling of information received from interested parties. 5. Does the terms and conditions of employment include actions to be taken if personnel disregard the organization's security requirements.	
6.3	Information security awareness, education and training	Personnel of the organization and relevant interested parties shall 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.	1. Do all employees, contractors and 3rd party users undergo regular security awareness training appropriate to their role and function within the organisation. 2. Does the Information security awareness program cover information security policy and topic-specific policies, standards, laws, statutes, regulations, contracts and agreements. 3. Does the Information security awareness program cover personal accountability for one's own actions and inactions, and general responsibilities towards securing or protecting information belonging to the organization and interested parties. 4. Does the organization have a formal process to access the effectiveness of the information security awareness program by ensuring that all employees take up quiz.	

qmsdp

مشاوره و آموزش سیستم‌های مدیریتی

www.qmsdp.com

6.4	Disciplinary process	A disciplinary process shall be formalized and communicated to take actions against personnel and other relevant interested parties who have committed an information security policy violation.	<p>1. Is there a formal disciplinary process which allows the organisation to take action against employees who have committed an information security breach.</p> <p>2. Is the formal disciplinary process approved by the top management.</p> <p>3. Is the formal disciplinary process communicated to all employees.</p> <p>4. Does the formal disciplinary process take into consideration factors such as:</p> <ul style="list-style-type: none"> • The nature (who, what, when, how) and gravity of the breach and its consequences • Whether the offence was intentional (malicious) or unintentional (accidental) • whether or not this is a first or repeated offence • whether or not the violator was properly trained 	
6.5	Responsibilities after termination or change of employment	Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, enforced and communicated to relevant personnel and other interested parties.	<p>1. Does the employee termination process define the information security responsibilities and duties that shall remain valid after termination or change of job roles for all full-time, part-time, and temporary staff.</p> <p>2. Are the responsibilities and duties that remain valid after termination of employment or contract included in the individual's terms and conditions of employment, contract or agreement.</p>	
6.6	Confidentiality or non-disclosure agreements	Confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information should be identified, documented, regularly reviewed and signed by personnel and other relevant interested parties.	<p>1. Are the full-time, part-time and temporary staff required to sign confidentiality or non-disclosure agreements prior to being given access to organization's confidential information and other associated assets.</p> <p>2. Does the confidentiality or non-disclosure agreements include:</p> <ul style="list-style-type: none"> • The definition of the information to be protected. • Validity of the agreement. • The ownership of information, trade secrets and intellectual property. • The terms for information to be returned or destroyed at agreement termination. 	

6.7	Remote working	Security measures shall be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organization's premises.	<p>1. Is there a formal policy covering the information security requirements for allowing personnel to work and access organization's information remotely.</p> <p>2. Is the remote working policy approved by the top management.</p> <p>3. Is the remote working policy communicated to all full-time, part-time and temporary staff who work remotely.</p> <p>4. Does the remote working policy consider physical security requirements.</p> <p>5. Does the remote working policy consider of the remote working site such as lockable filing cabinets, secure transportation between locations and rules for remote access, clear desk, printing and disposal of information.</p> <p>6. Does the remote working policy consider the communications security requirements.</p> <p>7. Does the remote working policy consider the threat of unauthorized access to information or resources from other persons in public places.</p> <p>8. Does the remote working policy consider use of security measures, such as firewalls and protection against malware.</p>	
6.8	Information security event reporting	The organization shall provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner.	<p>1. Are all full-time, part-time, and temporary staff made aware of their responsibility to report information security events.</p> <p>2. Are all full-time, part-time, and temporary staff made aware of the procedure for reporting information security.</p> <p>3. Are all full-time, part-time and temporary staff made aware of the communication contact details and communication medium for reporting information security events.</p>	

A.8 Physical Controls

Control No.	Control	Control Description	Assessment Questions	Response
7.1	Physical security perimeters	Security perimeters shall be defined and used to protect areas that contain information and other associated assets.	1. Is there a designated security perimeter. 2. Are sensitive or critical information areas segregated and appropriately controlled. 3. Has the organization implemented physically sound perimeters for a building or site containing information processing facilities.	
7.2	Physical entry	Secure areas should be protected by appropriate entry controls and access points.	1. Has the organization established a formal process for the management of access rights to physical areas. 2. Does the process include the provisioning, periodical review, update and revocation of authorizations for physical access. 3. Is there a process for maintaining and monitoring a physical logbook or electronic audit trail of all physical access. 4. Are adequate authentication mechanisms like access cards, biometrics or two-factor authentication such as an access card and secret PIN implemented for physical access to information processing facilities. 5. Is there a formal process for managing access to visitors. 6. Are the visitors given a Visitor Badge which distinguishes them from the employees. 7. Are the visitor logs maintained including the date, time in, time out, purpose of visit and personnel authorising the visitor's entry. 8. Are the visitors verified for their identity by checking the National ID or their company ID. 9. Are the visitors accompanied by organization's personnel and escorted to all places within the organization. 10. Are the internal and external doors of delivery and loading adequately secured. 11. Are the incoming deliveries inspected and examined for explosives, chemicals or other hazardous materials before they are moved from delivery and loading areas. 12. Are the incoming deliveries registered in accordance with asset management procedures. 13. Are the incoming deliveries inspected for tampering or meddling.	

7.3	Securing offices, rooms and facilities	Physical security for offices, rooms and facilities shall be designed and implemented.	1. Are the offices, rooms and critical information processing facilities sited to prevent unauthorised access. 2. Are controls implemented for critical process facilities to prevent confidential information or activities from being visible and audible from the outside.	
7.4	Physical security monitoring	Premises should be continuously monitored for unauthorized physical access.	1. Are the organization's physical premises monitored by surveillance systems, security guards, or intruder alarms. 2. Are the entry and exit points of critical information processing facilities equipped with video monitoring systems. 3. Is the access to video monitoring/CCTV systems restricted to authorized personnel. 4. Is the video monitoring/CCTV footage retained as per organizations and legal requirements.	
7.5	Protecting against physical and environmental threats	Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure should be designed and implemented.	1. Are the critical information processing facilities protected against physical and environmental threats. 2. Are adequate controls implemented to protect personnel and assets against fire, flooding, electrical surging, lightning, explosives etc.	
7.6	Working in secure areas	To protect information and other associated assets in secure areas from damage and unauthorized interference by personnel working in these areas.	1. Are the personnel aware of the existence of the secure areas. 2. Activities within secure areas communicated only to authorised personnel on need-to-know basis. 3. Are the secure areas periodically inspected to identify any vacant areas. 4. Are controls in place to restrict photographic, video, audio or other recording equipment, such as cameras in user endpoint devices, unless authorized within secure areas.	
7.7	Clear desk and clear screen	Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities shall be defined and appropriately enforced.	1. has the organization defined a formal clear desk and clear screen policy. 2. Is the clear desk and clear screen policy approved by the top management. 3. Is the clear desk and clear screen policy communicated to all full-time, part-time and temporary staff. 4. Does the clear desk and clear screen policy include the requirements for protecting user endpoint devices by key locks or other security means when not in use or unattended. 5. Does the clear desk and clear screen policy include the requirements for configuring user endpoint devices with a secure screen saver after certain period of inactivity. 6. Does the clear desk and clear screen	

qmsdp

مشاوره و آموزش سیستم های مدیریتی

www.qmsdp.com

@Nasiri.qmsdp

@qmsdp

			<p>policy include the requirements for the use of printers with an authentication function.</p> <p>7. Does the clear desk and clear screen policy include the requirements for securely storing documents and removable storage media containing sensitive information.</p> <p>8. Does the clear desk and clear screen policy include the requirements for clearing sensitive or critical information on whiteboards and other types of display when no longer required.</p>	
7.8	Equipment siting and protection	Equipment shall be sited securely and protected.	<p>1. Are the equipments handling sensitive data situated adequately to reduce the risk of information being viewed by unauthorized persons during their use.</p> <p>2. Are the equipments situated adequately to protect against physical and environmental threats.</p> <p>3. Has the organization established guidelines for eating, drinking, and smoking in proximity to information processing facilities.</p> <p>4. Are controls in place for monitoring environmental conditions, such as temperature and humidity of the surroundings.</p>	
7.9	Security of assets off-premises	Off-site assets shall be protected.	<p>1. Has the organization defined a formal process for the protection of devices which store or process information outside the organization's premises.</p> <p>2. Are the personnel made aware of guidelines for handling organization's assets off-premises.</p> <p>3. Are logs maintained for tracking equipments taken outside the organization.</p> <p>4. Are controls implemented to track location of the assets and remote wiping of devices.</p>	

7.10	Storage media	Storage media shall be managed through their life cycle of acquisition, use, transportation and disposal in accordance with the organization's classification scheme and handling requirements.	<ol style="list-style-type: none"> 1. Has the organization defined a formal process for managing removable storage media. 2. Is the removable media policy approved by the top management. 3. Is the removable media policy communicated to all full-time, part-time and temporary staff. 4. Does the removable storage media policy consider requirements for restricting the use of removable storage media only to authorised personnel on need to have basis. 5. Does the removable storage media policy consider requirements for managing an inventory of removable storage media. 6. Does the removable storage media policy consider requirements for maintaining audit logs for taking removable storage media outside the organization. 7. Does the removable storage media policy consider requirements for storing the removable storage media with adequate protection. 8. Does the removable storage media policy consider requirements for using cryptographic techniques for securing/protecting data within removable storage media. 9. Does the removable storage media policy consider requirements for enabling USB or SD card slots only on system with need to have basis. 	
 <p>مشاوره و آموزش سیستم های مدیریتی</p> <p>www.qmsdp.com</p> <p>@Nasiri.qmsdp @qmsdp</p>				
7.11	Supporting utilities	Information processing facilities should be protected from power failures and other disruptions caused by failures in supporting utilities.	<ol style="list-style-type: none"> 1. Are the equipments supporting the utilities is configured, operated and maintained in accordance with the relevant manufacturer's specifications. 2. Is there a process to manage the capacity requirements of supporting utilities. 3. Are the equipments supporting the utilities is inspected and tested regularly to ensure their proper functioning. 4. Are the emergency switches and valves to cut off power, water, gas or other utilities implemented. 5. Does the organization have adequate emergency lighting and communications. 	
7.12	Cabling security	Cables carrying power, data or supporting information services should be protected from interception, interference, or damage.	<ol style="list-style-type: none"> 1. Are the power and telecommunications lines into information processing facilities fed underground wherever possible or equipped with adequate protection like floor cable protector or utility poles. 2. Are the power and telecommunication cables separated to prevent interference. 3. Are the cables labelled at each end 	

			with sufficient source and destination details to enable the physical identification and inspection of the cable.	
7.13	Equipment maintenance	Equipment should be maintained correctly to ensure availability, integrity and confidentiality of information.	<ol style="list-style-type: none"> 1. Are the equipments maintained in accordance with the supplier's recommended service frequency and specifications. 2. Does the organization ensure only authorized maintenance personnel carrying out repairs and maintenance on equipment. 3. Is there a process to supervise maintenance personnel when carrying out maintenance on site. 4. Is there a process for authorizing and controlling access for remote maintenance. 5. Is there a process for inspecting the equipments before putting the back into operation after maintenance, to ensure that the equipment has not been tampered with and is functioning properly. 	
7.14	Secure disposal or re-use of equipment	Items of equipment containing storage media should be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.	<ol style="list-style-type: none"> 1. Has the organization defined a formal process for secure disposal and reuse of equipments/assets. 2. Does the organization ensure to physically destroy or erase the data in storage devices before disposal. 3. Does the organization ensure to remove labels and markings identifying the organization or indicating the classification, owner, system or network before disposal. 	



**FOLLOW US ON
LINKEDIN FOR MORE
FREE CHECKLISTS**

**PLAYBOOK
MADE WITH**



**MINISTRY
OF
SECURITY**



www.qmsdp.com

ISO 27001:2022

**AUDIT
CHECKLIST**

**PART 4
A.8 TECHNOLOGICAL
CONTROLS**

**MINISTRY
OF
SECURITY**

A.8 Technological Controls				
Control No.	Control	Control Description	Assessment Questions	Response
8.1	User end point devices	Information stored on, processed by or accessible via user end point devices shall be protected	1. Whether a mobile device policy exists and is approved? 2. Inventory details of the mobile devices registered 3. Whether policy document address additional risk of using mobile devices (eg. Theft of devices, use of open Wi-Fi hotspots? 4. Whether organisation have access control and malware protection in place for mobile devices? 5. Does organisation take regular backup of mobile devices? 6. Is there a process for registration of user endpoint devices? 7. Is there any restriction of software installation on user endpoint devices? 8. Is there any remote disabling, deletion or lockout controls implemented on user endpoint devices? 9. Are the USB ports disabled on user endpoint devices?	
8.2	Privileged access rights	The allocation and use of privileged access rights shall be restricted and managed	1. What are the criteria that your organisation has planned for a user to be assigned access privileges? 2. How your authorise and record access privileges and maintain them? 3. Whether there is an access control policy? 4. How organisation notify their employees about their assigned privileged access? 5. Procedure in place for preventing unauthorised use of generic ID 6. Whether organisation defined the conditions of expiry for privilege access? 7. Is there a process to review the privilege access rights assigned to users? 8. How often are the access review performed?	
8.3	Information access restriction	Access to information and other associated assets shall be restricted in accordance with the established topic-specific policy on access control.	1. Do you ensure that sensitive information is kept confidential, and no unauthorised identities have access to that information? 2. Whether organisation has a defined, maintained and controlled what data can be accessed by whom? 3. Does the organisation control which identified will have which access (Read, write, delete, execute) 4. Whether the organisation provide physical/logical access control for isolating sensitive systems, application and data?	

qmsdp

مشاوره و آموزش سیستم های مدیریتی

www.qmsdp.com

@Nasiri.qmsdp

@qmsdp

MINISTRY
OF
SECURITY

8.4	Access to source code	Read and write access to source code, development tools and software libraries shall be appropriately managed	<p>1. Whether the organisation manages the access to program source code and its libraries according to established procedures.</p> <p>2. Whether granting and revoking of read/ write access is on need basis?</p> <p>3. Does your organisation assure that the developers have source code access only through developer tools which has proper authorisation?</p> <p>4. Does your organisation maintain the audit log of all accesses and all changes done to source code?</p>	
8.5	Secure authentication	Secure authentication technologies and procedures shall be implemented based on information access restrictions and the topic-specific policy on access control	<p>1. Does your organisation test that no confidential information is displayed before log on process has successfully completed?</p> <p>2. Whether your organisation displays generic notices /warnings that systems should be accessed by authorised users only?</p> <p>3. Whether there is a defined limit on unsuccessful login attempts?</p> <p>4. Whether a procedure is defined for raising a security issue?</p> <p>5. Whether passwords are masked?</p> <p>6. Whether the passwords are encrypted before transmission?</p> <p>7. Whether a session time out is in place to logout the inactive sessions?</p> <p>8. Are the users mandated to change passwords upon first login?</p> <p>9. Are the default vendor accounts and passwords changed?</p>	
8.6	Capacity management	The use of resources shall be monitored and adjusted in line with current and expected capacity requirement	<p>1. Is there a process to manage capacity requirements of all systems based on the business process and criticality of the process.</p> <p>2. Is there a process to identify expected capacity requirements for the future.</p> <p>3. Are there any detective controls implemented to indicate problems and notify administrators.</p> <p>4. Whether the organisation follows the retention practices and removes absolute data?</p>	
8.7	Protection against malware	Protection against malware shall be implemented and supported by appropriate user awareness.	<p>1. Whether your organisation created a formal policy for managing Malware?</p> <p>2. Is the Antimalware solution implemented on all systems?</p> <p>3. Is the antimalware solution configured to perform periodic scans?</p> <p>4. Is the antimalware solution configured to get signature updates on a regular basis?</p> <p>5. Is the antimalware solution configured to send alerts to system administrators upon identifying malware?</p> <p>6. Is there a process in place for detecting malicious websites?</p>	

8.8	Management of technical vulnerabilities	Information about technical vulnerabilities of information systems in use shall be obtained, the organization's exposure to such vulnerabilities shall be evaluated and appropriate measures shall be take	<ol style="list-style-type: none"> 1. Are the Roles and responsibilities pertaining to vulnerability monitoring, vulnerability risk assessment, patching defined? 2. Is the scope and frequency of technical vulnerability assessments defined? 3. Is there a process to rate the vulnerabilities as Critical, High, Medium and Low? 4. Are the remediation timelines defined as per the vulnerability ratings? 5. Is there a formal process to install patches for remediating vulnerabilities? 6. Are we testing and evaluating the patches before they are installed? 	
8.9	Configuration management	Configurations, including security configurations, of hardware, software, services and networks shall be established, documented, implemented, monitored and reviewed.	<ol style="list-style-type: none"> 1. Whether your organisation has a policy and procedure in place for documenting the configurations of hardware, software and network devices? 2. Is there a proper role and ownership assigned to individuals for managing configuration on device? 3. Whether organisation follows a standardised template for hardening hardware's and softwares? 4. Does organisation have appropriate mechanism in place to review system, hardware updates at regular intervals and any current security threats to ensure optimal performance? 	
8.1	Information deletion	Information stored in information systems, devices or in any other storage media shall be deleted when no longer required.	<ol style="list-style-type: none"> 1. Does your organisation have policy that covers maintenance activities related to deletion and destruction of data and or IT assets including the utilisation of specialised software and liaison with vendors specialising in data and device deletion? 2. Whether organisation regularly identifies data which is no longer in use and needs to be removed to prevent from unauthorised access or misuse? 3. When employing specialised deletion vendor, whether sufficient evidence is obtained (via documentation) that the deletion has been performed? 	
8.11	Data masking	Data masking shall be 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	<ol style="list-style-type: none"> 1. Whether the organisation has a policy and procedure in place to ensure anonymization or pseudonymization of data for protection of data as per legal and regulatory requirements? 2. Process in place to discover how masked data is accessed? 3. Whether data masking policy and procedure includes following requirements? <ul style="list-style-type: none"> -Implement masking techniques to expose only the lowest possible amount of data those who use it -At the request of the subject, certain data may be hidden and staff access to relevant sections is restricted to only certain members. -Constructing their data masking procedure in accordance with legal and regulatory requirements. 	

			-Pseudonymization requires use of an algorithm to unmask data and this must be kept secure	
8.12	Data leakage prevention	Data leakage prevention measures shall be applied to systems, networks and any other devices that process, store or transmit sensitive information	<ol style="list-style-type: none"> 1. Has the organisation defined a procedure in place to reduce the risks of data leakage from emails, inward outward file transfer and USB devices? 2. Has the organisation established proper measures to ensure data is organised according to industry standards to assign different levels of risk? 3. Has organisation setup proper authorisation methods? 4. Whether the data in back up and all sensitive data is encrypted? 5. Whether organisation has implemented gateway security and leakage retention measures to protect against external influences? 6. Has the organization identified monitoring channels for identifying data leakage? 	
8.13	Information backup	Backup copies of information, software and systems shall be maintained and regularly tested in accordance with the agreed topic-specific policy on backup.	<ol style="list-style-type: none"> 1. Has organisation got approved policy and procedure for managing backup of data on devices, storage media, cloud, DB and servers? 2. How often the servers and configuration data are getting backed up ? 3. Whether the backed up data are restored and checked at regular intervals. 4. Whether the results of restorations are recorded? 5. Whether backup plan is updated on regular basis? 6. Has the organization defined the backup restoration testing frequency? 	
8.14	Redundancy of information processing facilities	Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements	<ol style="list-style-type: none"> 1. Has the organisation have a policy and procedure in place to ensure data processed through any ICT technology, physical facility, software is duplicated to ensure availability in event of disruption? 2. Has organisation considered geographically disparate locations when outsourcing data services (file storage/data centre amenities) 3. Whether redundancy is in place for all systems to ensure availability of information processing facility 	

8.15	Logging	Logs that record activities, exceptions, faults and other relevant events shall be produced, stored, protected and analysed	<p>1. Do you have a process to review security audit logs in timely and act upon threats ?</p> <p>2.Are appropriate event logs maintained and regularly reviewed?</p> <p>3.Whether logging facilities protected against tampering and unauthorised access?</p> <p>4.Whether system admin /operator activities logged and reviewed regularly?</p> <p>5.Whether NTP services are deployed and systems are synced with the NTP services</p> <p>6.Whether log archives are maintained ?</p> <p>7.How log collection and aggregating from different network ,security , servers , DB, Identity systems and applications is managed?</p>	
8.16	Monitoring activities	Networks, systems and applications shall be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.	<p>1. Whether company has a policy and procedure in place to suspect events which should be reported to relevant personnel in order to maintain the network integrity and improve business continuity</p> <p>2. Has the organization established a baseline for normal working conditions to identify anomalies in the network?</p>	
8.17	Clock synchronization	The clocks of information processing systems used by the organization shall be synchronized to approved time sources	<p>1. Has the organization identified reputed time source?</p> <p>2. Whether all devices are in sync with this NTP server hosted in organisation</p> <p>3. Is there a process to restrict access to time data in the organization?</p> <p>4. Is there a process to identify and monitor all changes to NTP systems?</p>	
8.18	Use of privileged utility programs	The use of utility programs that can be capable of overriding see	<p>1.Whether organisation has defined list of utility programs?</p> <p>2. Does organisation has procedure in place to identify, authorise and authenticate using utility programs?</p> <p>3.Whether ad hoc utility programs ae used? If yes, the approval process for the same.</p> <p>4. Details of logging for utility program</p>	
8.19	Installation of software on operational systems	Procedures and measures shall be implemented to securely manage software installation on operational systems	<p>1.Policy and procedure in place for software installation and to upgrade existing software's</p> <p>2.List of whitelisted software approved by management to be used in organisation</p> <p>3.Audit logs maintained for changes carried out?</p> <p>4. Change management procedure, policy for installing/upgrading new software's</p> <p>5.Sample change management tickets raised for such installation and upgradation of software's</p>	

8.20	Networks security	Networks and network devices shall be secured, managed and controlled to protect information in systems and applications	<p>1.Does the organisation have a approved copy of the network diagram?</p> <p>2.Network asset inventory for the organisation?</p> <p>3.Whether logging and monitoring of network equipment's in place?</p> <p>4.Details of network configuration files storage and their backup?</p> <p>5. What is the encryption controls deployed for data in transit?</p> <p>6.Is there a Procedure in place for authenticating network devices?</p>	
8.21	Security of network services	Security mechanisms, service levels and service requirements of network services shall be identified, implemented and monitored	<p>1. Policy and procedure in place for network security management?</p> <p>2.Procdeure for updating the OS patches, NW OS?</p> <p>3.Details of approved individuals who can make changes to network ?</p> <p>4. Details of SIEM,DLP.SOAR,IDS,IPS implemented?</p> <p>5. Is there a procedure in place to access network devices?</p>	
8.22	Segregation of networks	Groups of information services, users and information systems shall be segregated in the organization's networks.	<p>1. What security controls are implemented to ensure Segregation of access for production, testing and development environment?</p> <p>2. How is the network segmented and how is the access monitored to different segments of network?</p>	
8.23	Web filtering	Access to external websites shall be managed to reduce exposure to malicious content.	<p>1. Are the Web filtering rules implemented to permit access to specific websites only?</p> <p>2.Whether there is an approved list of high risk website/content category</p> <p>3. are the controls implemented to block malicious content from being downloaded(Eg.Web proxy, email gateway, ant phishing module, EDR ?</p>	
8.24	Use of cryptography	Rules for the effective use of cryptography, including cryptographic key management, shall be defined and implemented	<p>1. Has organisation got an cryptography policy in place?</p> <p>2. How are the cryptographic keys accessed, stored and safeguarded?</p> <p>3. Is the Inventory of cryptography keys and certificates used maintained?</p> <p>4. Is there a process defined to decide the encryption key strength and encryption algorithm?</p> <p>5. Is the crypto period defined for all encryption keys?</p>	
8.25	Secure development life cycle	Rules for the secure development of software and systems shall be established and applied	<p>1. Does the organization have a Secure application development policy?</p> <p>2. Are security requirements considered in all phases of development?</p> <p>3. Is there any secure coding guidelines used for development?</p> <p>4. Does the organization have secure source code repositories?</p>	

			5. Does the organization maintain version controlling on source code?	
8.26	Application security requirements	Information security requirements shall be identified, specified and approved when developing or acquiring applications	<p>1. Is there a process to ensure identify all information security requirements when developing or acquiring applications?</p> <p>2. Are the legal, statutory and regulatory requirements considered during application development</p> <p>3. Are the privacy requirements considered during application development?</p>	
8.27	Secure system architecture and engineering principles	Principles for engineering secure systems shall be established, documented, maintained and applied to any information system development activities	<p>1.Documented standards, evidence for engineering secure system and system architecture</p> <p>2. Whether Secure Engineering guidelines include the following</p> <ul style="list-style-type: none"> -Methods of user authentication -Secure session control guidance -Procedure for sanitising and validating data -Security measures for protecting information assets and systems against known threats -Security measures analysed for their ability to identify, eliminate and respond to security threats -How and where the security measures will be implemented <p>3. Procedure in place for validating the practises, standards of service provider/third parties so they are in line with secure engineering protocols</p>	
8.28	Secure coding	Secure coding principles shall be applied to software development	<p>1. Details of Secure Development policy and procedures</p> <p>2. Threat and vulnerability process</p> <p>3.Tools for secure code development if any</p> <p>4.Reports on Secure code review, SAST,DAST</p> <p>5.Whether development team is regularly trained on real world threats</p> <p>6.Whether secure coding takes into account following points</p> <ul style="list-style-type: none"> -Details on attack surface - OWASP Top 10 Vulnerabilities 	
8.29	Security testing in development and acceptance	Security testing processes shall be defined and implemented in the development life cycle.	<p>1.Whether user authentication, access restrictions and use of cryptographic techniques tested?</p> <p>2.Whether organisation tests the secure configs of OS , firewalls and other components</p> <p>3.Whether the organisation has a test plan defined, documented and implemented?</p> <p>4. Whether organization carries out VA , if yes the frequency and reports of the same</p> <p>5. Whether organisation conducts PT, if yes the frequency and the reports of the same</p> <p>6.Whether organisation tests their DB for their security</p>	

8.3	Outsourced development	The organization shall direct, monitor and review the activities related to outsourced system development.	1. Whether licensing, code ownership and IPR related to outsourced development in place? 2. Does organisation have contractual requirements for secure design, coding and testing practises 3. Whether provision for threat modelling considered by external developers? 4. Whether UAT is done and approved 5. Details of software ESCROW in place 6. Details of organisation conducting an audit on third party in place?	
8.31	Separation of development, test and production environments	Development, testing and production environments shall be separated and secured	1. Whether organisation has segregated environment for application (Development, test and production) 2. Access control list for each environment and review of the same. 3. Privilege user access management process in place 4. Patch, Backup management process in place 5. VAPT detailed reports 6. Details of web application security	
8.32	Change management	Changes to information processing facilities and information systems shall be subject to change management procedures.	1. Whether organisation has a change management policy and procedure? 2. Is there a formal change request process? 3. Are the change Impact assessment, testing and roll back plan defined for all changes? 4. Are the changes approved before implementation? 5. Is there a process to manage emergency changes?	
8.33	Test information	Test information shall be appropriately selected, protected and managed	1. Whether organisation applies same access control procedures to test and production environments? 2. Details of approval if prod data is copied to testing environment? 3. Sample of data used in testing, development and production environment? 4. Does organisation have defined the data management process and guidelines in place	
8.34	Protection of information systems during audit testing	Audit tests and other assurance activities involving assessment of operational systems shall be planned and agreed between the tester and appropriate management	1. Whether organisation has a system audit and assurance plan? 2. List of all privacy laws and regulations 3. Details of the audit calendar and recent audit reports 4. Procedure in place for protecting the PII data 5. User awareness records of personal involving system operations	



**FOLLOW US ON
LINKEDIN FOR MORE
FREE CHECKLISTS**

**PLAYBOOK
MADE WITH**



qmsdp

مشاوره و آموزش سیستم های مدیریتی

www.qmsdp.com

 @Nasiri.qmsdp

 @qmsdp

**MINISTRY
OF
SECURITY**