Domain & Job Task Analysis

PEEB 27001 Lead Auditor

M19 2RE Stockport Road
Manchester United Kingdom,
Tel: +441614251310
Email: info@peebonline.com

Sr. No.	Domain Category	Percentage
Domain 1	Fundamentals/ Concepts of Information Security Management System (ISMS) 27001 Audit	10%
Domain 2	Requirements for Information Security Management System (ISMS)	12%
Domain 3	Fundamental Audit Concepts and Principles	11%
Domain 4	Managing /Organising an ISO 27001 Audit Programme	20%
Domain 5	Conducting an Audit (Stages/Process)	20%
Domain 6	Conducting the Closing of ISO 27001 Audit	15%
Domain 7	Assessment/Managing an ISO 27001 Lead Auditor Programme	12%

1 Domain 1. Fundamentals/Concepts of Information Security Management System (ISMS) 27001 Audit – 10%

Knowledge of:

1. Information security laws, regulations, international and industry standards, contracts, market practices, internal policies, etc., an organization must comply with
2. Main standards related to information security
3. Main concepts and terminology of ISO 27001
4. Concept of risk and its application in information security
5. Relationship between information security aspects
6. Difference and characteristics of security objectives and controls
7. Difference between preventive, detective, and corrective controls
8. Main characteristics of big data, artificial intelligence, machine learning, cloud computing, and outsourcing operations

Skills:

1. Ability to understand and explain the main concepts of the information security management system
2. Explain the organization's operations and the development of information security standards
3. Identify, analyse, and evaluate the information security compliance requirements for an organization
4. Ability to explain and illustrate the main concepts in information security and information security risk management
5. Distinguish and explain the difference between information asset, data, and record
6. Understand, interpret, and illustrate the relationship between information security aspects such as controls, vulnerabilities, threats, risks, and assets
7. Ability to identify and illustrate big data, artificial intelligence, machine learning, cloud computing, and outsourcing operations

2 Domain 2. Requirements for Information Security Management System (ISMS) – 12%

Knowledge of:

1. Supporting standards of ISO 27001
2. Concepts, principles, and terminology related to management systems
3. Principal characteristics of an integrated management system
4. ISO 27001 requirements presented in the clauses 4 to 10
5. Main steps to establish the ISMS and security policies, security objectives, processes, and procedures relevant to managing risks, and improving information security to deliver results in accordance with an organization's overall policies and objectives
6. Risk assessment approach and methodology
7. Concept of continual improvement and its application to an ISMS
8. Security objectives and controls
9. Statement of Applicability document

Skills:

1. Understand the ISO 27001 requirements and the structure of the standard
2. Understand the components of an information security management system based on ISO 27001 and its principal processes
3. Interpret, and analyse the requirements of ISO 27001
4. Understand whether the organization has satisfied the needs of the interested parties
5. Explain, and illustrate the main steps to establish, implement, operate, monitor, review, maintain, and improve an organization's ISMS
6. Ability to understand the risk assessment approach and methodology
7. Ability to understand the selection of appropriate controls based upon Annex A of ISO 27001

3 Domain 3. Fundamental Audit Concepts and Principles – 11%

Knowledge for:

1. Main audit concepts and principles as described in ISO 19011
2. Differences between first, second, and third-party audits
3. Principles of auditing: integrity, fair presentation, due professional care, confidentiality, independence, evidence-based approach, and risk-based approach
4. Auditor's professional responsibility and the PEEB Code of Ethics
5. Evidence-based approach in an audit
6. Different types of audit evidence: physical, mathematical, confirmative, technical, analytical, documentary, and verbal
7. Laws and regulations applicable to the auditee and the country it operates in, etc.
8. Use of big data in audits
9. Knowledge of the auditing of outsourced operations

Skills:

1. Evaluate the audit management and auditing Performance of audit team.
2. Understand, explain, and illustrate the application of the audit principles in an ISMS audit
3. Differentiate first, second, and third-party audits
4. Identify and judge situations that would discredit the professionalism of the auditor and violate the PEEB Code of Ethics
5. Identify and judge ethical issues considering the obligations related to the audit client, auditee, law enforcement, and regulatory authorities
6. Understand the legal implications related to any irregularities committed by the auditee
7. Ability to understand the impact of trends and technology in auditing
8. Illustrate, and apply the audit evidence approach in the context of an ISMS audit
9. Explain and compare evidence types and their characteristics
10. Determine and justify the type and amount of evidence required in an ISMS audit

4 Domain 4. Managing /Organizing an ISO 27001 Audit Programme – 20%

Knowledge of:

1. Risk-based approach to an audit and the different types of risks related to audit activities such as inherent risk, control risk, and detection risk
2. Concept of materiality and its application to an audit
3. Concept of reasonable assurance and its application to an audit
4. Main responsibilities of the audit team leader and audit team members
5. Roles and responsibilities of technical experts
6. Audit objectives, audit scope, and audit criteria
7. Difference between an ISMS scope and the audit scope
8. Factors to consider during the audit feasibility
9. Cultural aspects to consider in an audit
10. Characteristics of terms of the audit engagement and the best practices to establish the initial contact with an auditee

Skills:

1. Ability to conduct desk review
2. Audit to the ISO 27001/19011 system theories/ of reasonable assurance and its application.
3. Determine and evaluate the level of materiality and apply the risk-based approach during the different stages of an ISMS audit
4. Judge the appropriate level of reasonable assurance needed for an ISMS audit
5. Ability to understand and illustrate the steps and activities to prepare an ISMS audit considering the specific context of the audit
6. Ability to understand and explain the roles and responsibilities of the audit team leader, audit team members, and technical experts
7. Determine and evaluate the level of materiality during the different stages of an ISMS audit
8. Determine the audit feasibility
9. Evaluate, and confirm the audit objectives, the audit criteria, and the audit scope for an ISMS audit
10. Explain, illustrate, and define the characteristics of the terms of the audit engagement and apply the best practices to establish the initial contact with an auditee

5 Domain 5. Conducting an Audit (Stages/Process) – 20%

Knowledge of:

1. Objectives and the content of the opening meeting in an audit
2. Difference between stage 1 audit and stage 2 audit
3. Stage 1 audit requirements, steps, and activities
4. Documented information evaluation criteria and ISO 27001 requirements
5. Stage 2 audit requirements, steps, and activities
6. Best communication practices during an audit
7. Roles and responsibilities of guides and observers during an audit
8. Different conflict resolution techniques
9. Evidence collection procedures and tools such as interview, documented information review, observation, analysis, sampling, and technical verification
10. Evidence analysis techniques: corroboration and evaluation
11. Main concepts, principles, and evidence collection procedures used in an audit
12. Advantages and disadvantages of using audit checklists

13. Main audit sampling methods and their characteristics
14. Audit plan preparation procedure
15. Preparation and development of audit working papers
16. Best practices for the creation of audit test plans
17. Evidence evaluation process: to draft audit findings

Skills:

1. Conduct the stage 1 audit, considering the documented information evaluation criteria
2. Organize and conduct an opening meeting
3. Conduct the stage 2 audit by appropriately following the procedures that this stage entails
4. Best practices of communication to collect the appropriate audit evidence
5. Consider the roles and responsibilities of all the interested parties involved
6. Explain, illustrate, and apply evidence collection procedures and tools
7. Explain, illustrate, and apply the main audit sampling methods
8. Gather appropriate evidence from the available information during an audit and evaluate it objectively
9. Explain, illustrate, and apply the audit evidence approach in an ISMS audit
10. Develop audit working papers and elaborate appropriate audit test plans in an ISMS audit
11. Explain and apply the evidence evaluation process: drafting audit findings
12. Understand, explain, and illustrate the concept of the benefit of the doubt
13. Report appropriate audit observations in accordance with audit rules and principles
14. Conduct quality reviews to audit documentation
15. Complete audit working documents

6 Domain 6. Conducting the Closing of ISO 27001 Audit – 15%

Knowledge of:

1. Evidence evaluation process: to prepare audit conclusions
2. Guidelines and best practices to present audit conclusions to the management of an audited organization
3. Possible recommendations that an auditor can issue during the certification audit
4. Closing meeting agenda
5. Guidelines and best practices to evaluate action plans

Skills:

1. Explain and apply the evidence evaluation process: preparing audit conclusions
2. Justify the recommendation for certification
3. Draft and present audit conclusions
4. Organize and conduct a closing meeting
5. Write and distribute an ISO 27001 audit report
6. Evaluate action plans

7 Domain 7. Assessment/Managing an ISO 27001 Lead Auditor Programme – 12%

Knowledge for:

1. Audit follow-ups, surveillance audits, and recertification audit requirements, steps, and activities
2. Conditions for the modification, extension, suspension, or withdrawal of an organization's certification
3. Application of the PDCA cycle in the management of an audit program
4. Requirements, guidelines, and best practices regarding audit resources, procedures, and policies
5. Types of tools used by professional auditors
6. Requirements, guidelines, and best practices regarding the management of audit records
7. Application of the continual improvement concept to the management of an audit program
8. Particularities to implement and manage a first, second, or third-party audit program
9. Competency concept and its application to auditors
10. Management of combined audits
11. Personal attributes and behaviors of a professional auditor

Skills:

1. Conduct the activities following an initial audit, including audit follow-ups and surveillance activities
2. Understand and explain the establishment of an audit program and the application of the PDCA cycle into an audit program
3. Understand and explain the importance of protecting the integrity, availability, and confidentiality of audit records and the auditors' responsibilities in this regard
4. Understand and explain the responsibilities to protect the integrity, availability, and confidentiality of audit records
5. Understand the requirements related to the components of the management system of an audit program as quality management, record management, complaint management
6. Understand and explain the way that the combined audits are handled in an audit program
7. Understand the documented information management process
8. Understand the process of evaluating the efficiency of the audit program by monitoring the performance of each auditor and audit team member
9. Demonstrate the application of the personal attributes and behaviors associated with professional auditors