STANDARD BASED SECURITY AUDIT AND ASSESSMENT

001 Report – Assignment Submission Point

EMMANUEL ATEJI
33043543

Table of Contents

Executive Summary

This report outlines the key deliverables for developing an Information Security Management System (ISMS) based on the provided case study to prevent current or future information security breaches at the organization.

The first section provides a set of 15 carefully crafted audit interview questions designed to thoroughly examine the organization's incident management process. The questions target audiences at the strategic, tactical, and operational levels, and are mapped to the relevant clauses and controls of the ISO/IEC 27001:2022 & ISO/IEC 27002:2022 standard.

Next, the report identifies three major areas of concern from the case study materials. For each finding, a detailed non-conformity report or observation is provided, with clear references to the specific ISO 27001 clauses or Annex A controls that are not being met. Relevant excerpts and document references from the case study are cited as evidence for each finding.

The centrepiece of the report is a comprehensive guidebook written for a junior auditor who is new to conducting ISO 27001 audits. The guidebook clearly explains the purpose and stages of an ISO 27001 audit. It describes in detail the stage 1 and stage 2 audits, their goals, key activities, and outputs. The mandatory documents from ISO 27001 are listed and their importance explained. A sample stage 2 audit plan specific to the case study organization is provided. The crucial concepts of objective evidence and auditor competencies are covered, along with audit checklists and tips for conducting opening and closing meetings. Throughout the guidebook, relevant clauses from the ISO 27001, ISO 19011 and ISO 17021 standards are referenced to reinforce the best practices being taught.

By carefully following the recommendations in this report, the organization can establish an effective ISMS to better protect its sensitive information assets and prevent future security incidents. The audit questions, non-conformity reports, and junior auditor guidebook provide a solid foundation to identify current gaps and implement stronger controls in alignment with the globally recognized ISO/IEC 27001 standard.

Introduction

This report provides recommendations for Lake Dale Contact Centre (LDCC) to establish an Information Security Management System (ISMS) based on the ISO/IEC 27001:2022 and other relevant and applicable ISO standards. The case study reveals areas of concern that could compromise the confidentiality, integrity, and availability of sensitive data, contrary to LDCC's strategic mission.

The report includes targeted audit interview questions for incident management, non-conformity reports highlighting key issues, and a comprehensive ISO 27001 audit guidebook for junior auditors. By implementing these recommendations and aligning with ISO 27001, LDCC can effectively manage information security risks, safeguard customer information, ensure compliance, and boost stakeholder confidence.

Audit Interview Questions

The following set of 15 audit interview questions is designed to thoroughly assess Lake Dale Contact Centre's (LDCC) incident management process in alignment with the ISO/IEC 27001:2022 standard and ISO/IEC 27002:2022 controls. The questions are tailored for audiences at the strategic, tactical, and operational levels to gain a comprehensive understanding of how incidents are identified, reported, evaluated, and responded to within the organization. By mapping each question to the relevant ISO clauses and controls, this question set aims to uncover potential gaps and areas for improvement in LDCC's incident management practice.

Strategic Level

1. **Open-ended Question:**
   How does the overall incident management process align with LDCC's strategic mission? [ISO/IEC 27001:2022 Clause 5.2, ISO/IEC 27002:2022 Annex A 5.24].
2. **Hypothetical Question:**
   What would be the impact on LDCC if major incidents were not properly managed? [ISO/IEC 27001:2022 Clause 6.1.2, ISO/IEC 27002:2022 Annex A 5.24].
3. **Specific Question:**
   Who is responsible for ensuring the incident management process achieves its intended outcomes at LDCC? [ISO/IEC 27001:2022 Clause 5.3, ISO/IEC 27002:2022 Annex A 5.24]
4. **Rhetorical Question:**
   Regularly reviewing incidents is critical to improving LDCC's process, isn't it? [ISO/IEC 27001:2022 Clause 10.1, ISO/IEC 27002:2022 Annex A 5.27].
5. **Closed-ended Question:**
   Does LDCC's incident management policy align with the overall information security policy? [ISO/IEC 27001:2022 Clause 5.2, ISO/IEC 27002:2022 Annex A 5.24].

Tactical Level

6. **Open-ended Question:**
   Walk me through how incidents are categorized and prioritized once detected at LDCC. [ISO/IEC 27002:2022 Annex A 5.25].
7. **Probing Question:**
   You mentioned LDCC's incident response plans. How often are these tested and updated? [ISO/IEC 27002:2022 Annex A 5.24].
8. **Leading Question:**
   I assume the criteria for what constitutes an information security incident are clearly defined in LDCC's process? [ISO/IEC 27002:2022 Annex A 5.24].
9. **Hypothetical Question:**
   What would happen if LDCC's incident response team did not have the necessary competencies? [ISO/IEC 27001:2022 Clause 7.2, ISO/IEC 27002:2022 Annex A 5.24].
10. **Closed-ended Question:**
    Are LDCC's incident management responsibilities and procedures documented? [ISO/IEC 27002:2022 Annex A 5.24].

Operational Level

11. **Open-ended Question:**
    Describe how information security events get reported by LDCC personnel. [ISO/IEC 27002:2022 Annex A 6.8].
12. **Specific Question:**
    Who at LDCC conducts the initial assessment to determine if a security event should be classified as an incident? [ISO/IEC 27002:2022 Annex A 5.25].

13. **Reflective Question:**
    So detailed records are kept of all incident response activities at LDCC, is that right? [ISO/IEC 27002:2022 Annex A 5.26].
14. **Rhetorical Question:**
    LDCC personnel must be made aware of their responsibility to report suspected incidents promptly, mustn't they? [ISO/IEC 27002:2022 Annex A 6.8]
15. **Closed-ended Question:**
    Does LDCC have a defined point of contact to which information security events should be reported? [ISO/IEC 27002:2022 Annex A 6.8].

By conducting interviews with key stakeholders across various levels of the organization, the auditor can assess the effectiveness and maturity of LDCC's incident management policy, procedures, roles and responsibilities, reporting mechanisms, and continual improvement efforts. Analysing the responses and identifying deviations from the standards will help provide meaningful recommendations to strengthen LDCC's incident management capabilities and overall information security posture, which is crucial for the audit process.

Non-Conformity Reports

This section presents three non-conformity reports based on the review of LDCC's case study. The identified areas of concern are assessed against the requirements of ISO/IEC 27001:2022 and the controls specified in ISO/IEC 27002:2022. Each finding is documented using the R.E.D. (Requirement, Evidence, Deficiency) guide from the handbook, ensuring that the non-conformities are clearly stated, supported by objective evidence, and linked to the relevant ISO clauses and controls. By thoroughly examining the case study and applying the ISO 27001 and 27002 standards, these reports aim to highlight significant gaps in the organization's Information Security Management System (ISMS) and provide a basis for corrective actions and improvements.

1. **Non-Conformity Report for the "Performance Analysis and Evaluation (Extract) - D38 - Issue 2" Document – Page 151**

NON-CONFORMITY REPORT
Company: LDCC (Lake Dale Contact Centre)
Report Number: NCR-LDCC-001
Name of Auditor: Emmanuel Ateji
ISO 27001:2022 Clause Number: Clause 9.1, 10.1 **ISO 27002:2022 Annex Control:** A.5.36
Date of Audit: 08/05/2024
Category: Major non-conformity
Non-Conformity Description: LDCC's Performance Analysis and Evaluation (Extract) - D38 - Issue 2 document demonstrates a lack of proper analysis and evaluation of monitored ISMS performance data. Several items are marked as "?" for their most recent status, and key controls lack depth of analysis, with "No comment" listed under Conclusion.
Requirement: • ISO 27001:2022 Clause 9.1 requires the organization to evaluate the information security performance and effectiveness of the ISMS. • ISO 27001:2022 Clause 10.1 requires the organization to continually improve the suitability, adequacy, and effectiveness of the ISMS. • ISO 27002:2022 Annex Control A.5.36 requires compliance with the organization's information security policy, topic-specific policies, rules and standards to be regularly reviewed.
Evidence: Performance Analysis and Evaluation (Extract) - D38 - Issue 2 document, showing: • Several performance monitoring items marked as "?" for their most recent status. • Items related to key controls like Legal, Resources, Physical Protection, Passwords, and Media Protection have "No comment" listed under Conclusion.

Deficiency of the system:

The lack of proper analysis and evaluation of ISMS performance data indicates that LDCC is not effectively assessing the suitability, adequacy, and effectiveness of their ISMS as required by ISO 27001. Without thorough reviews, LDCC may miss opportunities for improvement and fail to identify and address potential weaknesses in their ISMS.

Recommendation:

LDCC (Lake Dale Contact Centre) should take the following steps:

1. Ensure all monitored performance data is properly collected and updated in a timely manner. [ISO 27001:2022 Clause 9.1, ISO 27002:2022 Annex Control A.5.36].
2. Conduct thorough analysis of the performance data, particularly for key controls, and document meaningful conclusions and recommendations. [ISO 27001:2022 Clause 9.1, 10.1, ISO 27002:2022 Annex Control A.5.36].
3. Use the analysis results to drive continual improvement of the ISMS, addressing any identified weaknesses or areas for enhancement. [ISO 27001:2022 Clause 10.1].
4. Regularly review and update the Performance Analysis and Evaluation process to ensure it remains suitable and effective for assessing ISMS performance. [ISO 27001:2022 Clause 9.1, 10.1, ISO 27002:2022 Annex Control A.5.36].

2. **Non-Conformity Report for the "Internal Audit Programme (201x) [Extract] - D39 - Issue 1" Document – Page 161**

NON-CONFORMITY REPORT

Company: LDCC (Lake Dale Contact Centre)

Report Number: NCR-LDCC-002

Name of Auditor: Emmanuel Ateji

ISO 27001:2022 Clause Number: Clause 9.2

ISO 27002:2022 Annex Control: A.5.35

Date of Audit: 10/05/2024

Category: Major non-conformity

Non-Conformity Description:

LDCC's Internal Audit Programme (201x) [Extract] - D39 - Issue 1 document reveals gaps in the organization's internal audit schedule. Critical areas such as risk assessment, incident management, and business continuity are not covered, and the frequency of audits for access control and asset management appears insufficient.

Requirement:

- ISO 27001:2022 Clause 9.2 requires the organization to conduct internal audits at planned intervals to provide information on whether the ISMS conforms to the organization's own

requirements and the requirements of the ISO 27001 standard and is effectively implemented and maintained.
- ISO 27002:2022 Annex Control A.5.35 requires the organization's approach to managing information security and its implementation to be independently reviewed at planned intervals or when significant changes occur.

Evidence:

Internal Audit Programme (201x) [Extract] - D39 - Issue 1 document, showing:
- Critical areas like risk assessment, incident management, and business continuity are missing from the audit schedule.
- Access control and asset management are only audited once a year.

Deficiency of the system:

The gaps in LDCC's internal audit program indicate that the organization is not adequately assessing the conformity and effectiveness of its ISMS as required by ISO 27001. The absence of audits for critical areas and the insufficient frequency of audits for key controls may result in unidentified nonconformities, weaknesses, or opportunities for improvement in the ISMS.

Recommendation:

LDCC (Lake Dale Contact Centre) should take the following steps:

1. Review and update the internal audit program to ensure it covers all critical areas of the ISMS, including risk assessment, incident management, and business continuity. [ISO 27001:2022 Clause 9.2].
2. Increase the frequency of audits for key controls such as access control and asset management to provide adequate assurance of their effectiveness. [ISO 27001:2022 Clause 9.2].
3. Ensure the updated internal audit program is implemented, and audits are conducted as planned. [ISO 27001:2022 Clause 9.2].
4. Regularly review and adjust the internal audit program based on the results of previous audits, changes in the organization's ISMS, and any relevant external factors. [ISO 27001:2022 Clause 9.2, ISO 27002:2022 Annex Control A.5.35].

3. Non-Conformity Report for the "Visitor Book (extract) - D28 - Issue 1" Document– Page 104

NON-CONFORMITY REPORT
Company: LDCC (Lake Dale Contact Centre)
Report Number: NCR-LDCC-003
Name of Auditor: Emmanuel Ateji
ISO 27001:2022 Clause Number: Clause 7.5.3, 8.1 **ISO 27002:2022 Annex Control:** A.7.2
Date of Audit: 12/05/2024

Category: Minor Conformity

Non-Conformity Description:

LDCC's Visitor Book (extract) - D28 - Issue 1 document reveals inconsistencies and weaknesses in the organization's visitor management process. The document shows Rasheeda Guerro, a visitor from a government office, visited the MD's office without a recorded time out, while other visitors, including Renata Mcgrane and Angelo Lamarche, were granted access outside normal business hours.

Requirement:

- ISO 27001:2022 Clause 7.5.3 requires the organization to control documented information determined by the organization as being necessary for the effectiveness of the information security management system.
- ISO 27001:2022 Clause 8.1 requires the organization to plan, implement and control the processes needed to meet information security requirements.
- ISO 27002:2022 Annex Control A.7.2 requires secure areas to be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.

Evidence:

Visitor Book (extract) - D28 - Issue 1 document, showing:

- Incomplete visitor information (missing car registration numbers for some visitors).
- A government official visiting the MD without a recorded time out.
- A visitor not being accompanied by an LDCC staff member.
- A police officer with a warrant granted access to the MD's office outside of normal hours without a recorded time out.

Deficiency of the system:

The issues identified in the Visitor Book extract demonstrate that LDCC's visitor management process is not effectively controlled or implemented, as required by ISO 27001 and ISO 27002. These deficiencies may lead to unauthorized access to sensitive information, facilities, and personnel, potentially compromising the confidentiality, integrity, and availability of information assets.

Recommendation:

LDCC (Lake Dale Contact Centre) should take the following steps:

1. Ensure all visitor information, including car registration numbers and time out, is consistently recorded in the Visitor Book. [ISO 27001:2022 Clause 7.5.3, 8.1]
2. Investigate the instances of visitors not being accompanied by LDCC staff and accessing sensitive areas outside of normal business hours and take appropriate corrective action. [ISO 27001:2022 Clause 8.1, ISO 27002:2022 Annex Control A.7.2]
3. Review and update the visitor management process to address the identified weaknesses and ensure compliance with ISO 27001 and ISO 27002 requirements. [ISO 27001:2022 Clause 7.5.3, 8.1, ISO 27002:2022 Annex Control A.7.2]
4. Provide training to reception and security staff on the updated visitor management process and their responsibilities in maintaining accurate visitor records and enforcing access controls. [ISO 27001:2022 Clause 7.5.3, 8.1]

Junior Auditor Guidebook

Junior Auditor Guidebooks aims to help understand the key concepts, stages, and requirements of an ISO 27001 audit, and develop the necessary competencies to conduct an effective audit. The guidebook references relevant clauses and annexes from ISO/IEC 27001:2022, ISO 19011:2018, and ISO/IEC 17021-1:2015 to ensure consistent, reliable, and valuable audits. By following the steps and guidance provided, junior auditors will be well-prepared to contribute to the audit process and support their team in assessing an organization's Information Security Management System (ISMS).

Purpose of an ISO 27001 Audit

The purpose of an ISO 27001 audit is to systematically and independently assess an organization's Information Security Management System (ISMS) to determine the extent to which it:

1. Conforms to the requirements of the ISO/IEC 27001 standard (ISO/IEC 27001:2022, Clause 1 and Clause 9.2.1)
2. Aligns with the organization's own information security policies and objectives (ISO/IEC 17021-1:2015, Clause 9.2.1.2)
3. Complies with applicable legal, statutory, and regulatory requirements (ISO/IEC 17021-1:2015, Clause 9.2.1.2)
4. Is effectively implemented and maintained (ISO/IEC 27001:2022, Clause 9.2.1)
5. Achieves the organization's information security objectives (ISO/IEC 27001:2022, Clause 9.2.1)

The audit provides an independent evaluation of the ISMS, helping the organization identify areas for improvement and ensuring that its information security practices are robust, consistent, and aligned with internationally recognized standards.

Stages of an ISO 27001 Audit

The stages of an ISO 27001 audit, as defined by ISO/IEC 17021-1:2015 and ISO/IEC 27001:2022, consist of two main phases: Stage 1 and Stage 2 audits. These audits are conducted for the initial certification of an organization's Information Security Management System (ISMS) (Berry, 2022).

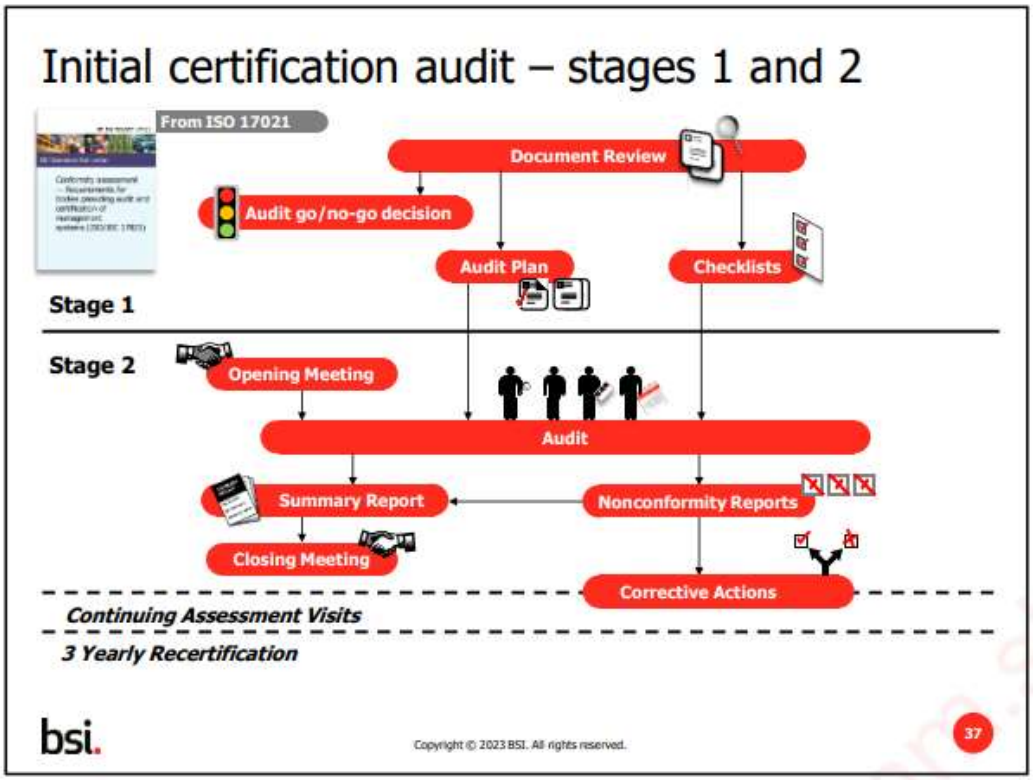

Figure 1: Stages of audit; Retrieved from 02 slides (mimeo) page 37.

Stage 1 Audit (ISO/IEC 17021-1:2015, Clause 9.3.1.2):

- Review the organization's ISMS documentation (Clause 9.3.1.2.2.a).
- Evaluate the client's on-site specific conditions and understanding of ISO 27001 requirements (Clause 9.3.1.2.2.b, c).
- Gather necessary information regarding the scope of the ISMS (Clause 9.3.1.2.2.d).
- Evaluate the allocation of resources for Stage 2 (Clause 9.3.1.2.2.e).
- Provide a focus for planning the Stage 2 audit (Clause 9.3.1.2.2.f).
- Evaluate if internal audits and management reviews are being planned and performed (Clause 9.3.1.2.2.g; ISO/IEC 27001:2022, Clauses 9.2, 9.3)
- Determine the preparedness of the organization for the Stage 2 audit (Clause 9.3.1.2.2.b)

Stage 2 Audit (ISO/IEC 17021-1:2015, Clause 9.3.1.3; ISO/IEC 27001:2022, Clause 9.2):

- Evaluate the implementation and effectiveness of the organization's ISMS.
- Assess conformity to all ISO 27001 requirements through on-site auditing activities, including interviews, observations, and document review (ISO/IEC 17021-1:2015, Clause 9.4.4.2)
- Verify that the ISMS can achieve the organization's policy objectives (ISO/IEC 27001:2022, Clause 6.2)
- Identify areas of potential improvement (ISO/IEC 17021-1:2015, Clause 9.4.5.2)
- The Stage 2 audit may be conducted in multiple visits, depending on the size and complexity of the organization.

After the initial certification, the organization undergoes post-certification audits (ISO/IEC 17021-1:2015, Clause 9.6) to maintain its certification status (ISOQAR, 2024):

Surveillance Audits (ISO/IEC 17021-1:2015, Clause 9.6.2):

- Conducted to maintain confidence that the certified ISMS continues to fulfil requirements between recertification audits (RiskOptics, 2023).
- Less comprehensive than recertification audits.
- Focus on the critical aspects of the ISMS, such as internal audits, management review, and corrective actions from previous audits.

Recertification Audits (ISO/IEC 17021-1:2015, Clause 9.6.3):

- Planned and conducted to evaluate the continued fulfilment of all the requirements of the relevant management system standard or other normative documents.
- Consider the performance of the ISMS over the period of certification.
- Include a review of previous surveillance audit reports.

Audit Competence

Auditor competence is the demonstrated ability to apply knowledge and skills to achieve intended results (ISO 19011:2018, Clause 3.22; ISO/IEC 17021-1:2015, Clause 3.7). It is composed of personal behaviour, knowledge, and skills (ISO 19011:2018, Clause 7.1). Auditor competence is essential for ensuring the effectiveness, reliability, and credibility of the audit process (ISO 19011:2018, Clause 7.1; ISO/IEC 17021-1:2015, Clause 7.1.1).

Importance of audit competence for LDCC

Lake Dale Contact Centre (LDCC), auditor competence plays a crucial role in assessing the conformity and effectiveness of the Information Security Management System (ISMS). LDCC must ensure that auditors possess the necessary knowledge, skills, and personal attributes to evaluate the organization's ISMS against the requirements of ISO/IEC 27001 (ISO/IEC 17021-1:2015, Clause 7.1.2).

For example, Gordon Black, the ISMS auditor, should have in-depth knowledge of ISO/IEC 27001, auditing techniques, and LDCC's ISMS. Additionally, he should possess strong analytical and observational skills to effectively identify nonconformities and areas for improvement (ISO 19011:2018, Clause 7.2.3.2; ISO/IEC 17021-1:2015, Clause 7.1.2). Competent auditors like Gordon can identify areas of strength, nonconformities, and opportunities for improvement, thereby helping LDCC maintain and enhance its ISMS performance.

Table representing Auditor Competencies:

Name	Role	Responsibility	Competence (Knowledge, Skills, Personal Attributes)	Applicable ISO 27001	Applicable ISO 17021
Clive Prichard	IS Manager/Management representative	Ensuring the ISMS conforms to ISO 27001 requirements	- Knowledge of ISMS, ISO 27001, and LDCC's processes. - Leadership and communication skills - Objective and impartial.	Clause 5.3	Clause 5.2, 7.1.2, 7.2.8
Gordon Black	Controls Manager/ISMS Auditor	Planning and conducting ISMS audits, reporting to the ISF	- Knowledge of ISO 27001, auditing techniques, and LDCC's ISMS. - Analytical and observational skills. - Ethical and detail-oriented.	Clause 9.2	Clause 7.1.2, 7.2.2, 7.2.3, 7.2.4, 7.2.5, Annex A
Fay Woodward	Team Leader/ISMS Auditor	Assisting in ISMS audits, reporting to the Controls Manager	- Knowledge of ISO 27001, LDCC's ISMS, and auditing methods. Communication and interpersonal skills. - Professional and adaptable	Clause 9.2	Clause 7.1.2, 7.2.2, 7.2.3, 7.2.4, 7.2.5, Annex A
John Bishop	IT Team Leader/IT Manager	Ensuring the implementation of controls related to IT systems.	- Knowledge of IT systems, security controls, and ISO 27001. - Problem-solving and decision-making skills. - Responsible and reliable.	Clauses 6.1.3, 8.1, 8.2, 8.3	Clause 7.1.4
Raj Patel	HR Director	Overseeing human resource security and competence management.	- Knowledge of HR processes, competence management, and ISO 27001. - Strategic thinking and people management skills. - Trustworthy.	Clauses 7.2, 7.3	Clause 7.1.2, 7.2.3, 7.2.7

Stage 1 Audit

Description and Evaluation of a Stage 1 Audit:

A Stage 1 audit is the first phase of the initial certification audit process (ISO/IEC 17021-1:2015, Clause 9.3.1.1). It is carried out to assess the organization's readiness for the Stage 2 audit by evaluating the implementation of the ISMS (ISO/IEC 17021-1:2015, Clause 9.3.1.2).

The Stage 1 audit is crucial for understanding the organization's context, identifying potential gaps or non-conformities, and planning for the Stage 2 audit. It helps ensure that the certification body and the auditee are well-prepared for the more comprehensive Stage 2 audit, which assesses the effectiveness of the ISMS.

Purpose of a Stage 1 Audit (ISO/IEC 17021-1:2015, Clause 9.3.1.2.2):

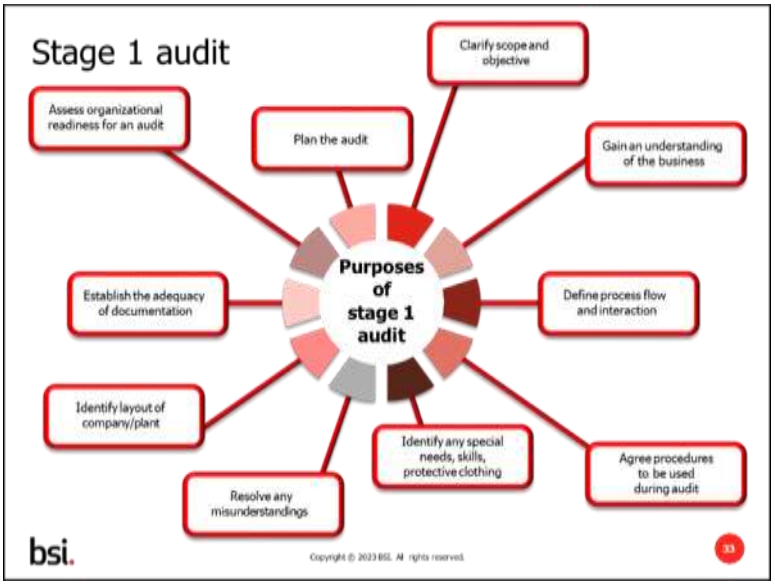

Figure 2: Retrieved from 02 slides (mimeo) page 33.

1. Clarifying the scope and objective of an audit (ISO/IEC 17021-1:2015, Clause 9.3.1.2.2.d)
2. Gain an understanding of the business (ISO/IEC 17021-1:2015, Clause 9.3.1.2.2.f)
3. Define process flow and interaction (ISO/IEC 17021-1:2015, Clause 9.3.1.2.2.d)
4. Agree procedures to be used during audit (ISO/IEC 17021-1:2015, Clause 9.3.1.2.2.e)
5. Resolve any misunderstandings (Not explicitly mentioned in ISO/IEC 17021-1:2015)
6. Identify any special needs, skills, protective clothing (ISO/IEC 17021-1:2015, Clause 9.3.1.2.2.e)
7. Identify layout of company/plant (ISO/IEC 17021-1:2015, Clause 9.3.1.2.2.d)
8. Establish the adequacy of documentation (ISO/IEC 17021-1:2015, Clause 9.3.1.2.2.a)
9. Assess the organizations readiness for the next stage (ISO/IEC 17021-1:2015, Clause 9.3.1.2.2.b, 9.3.1.2.2.g)
10. Plan the next stage of the audit (ISO/IEC 17021-1:2015, Clause 9.3.1.2.2.f)

The Stage 1 audit, as per ISO/IEC 17021-1:2015, lays the groundwork for the Stage 2 audit by clarifying objectives, assessing readiness, identifying issues, and planning the audit process, ensuring an efficient and effective Stage 2 audit.

Relevant Areas, Activities, and Outputs:

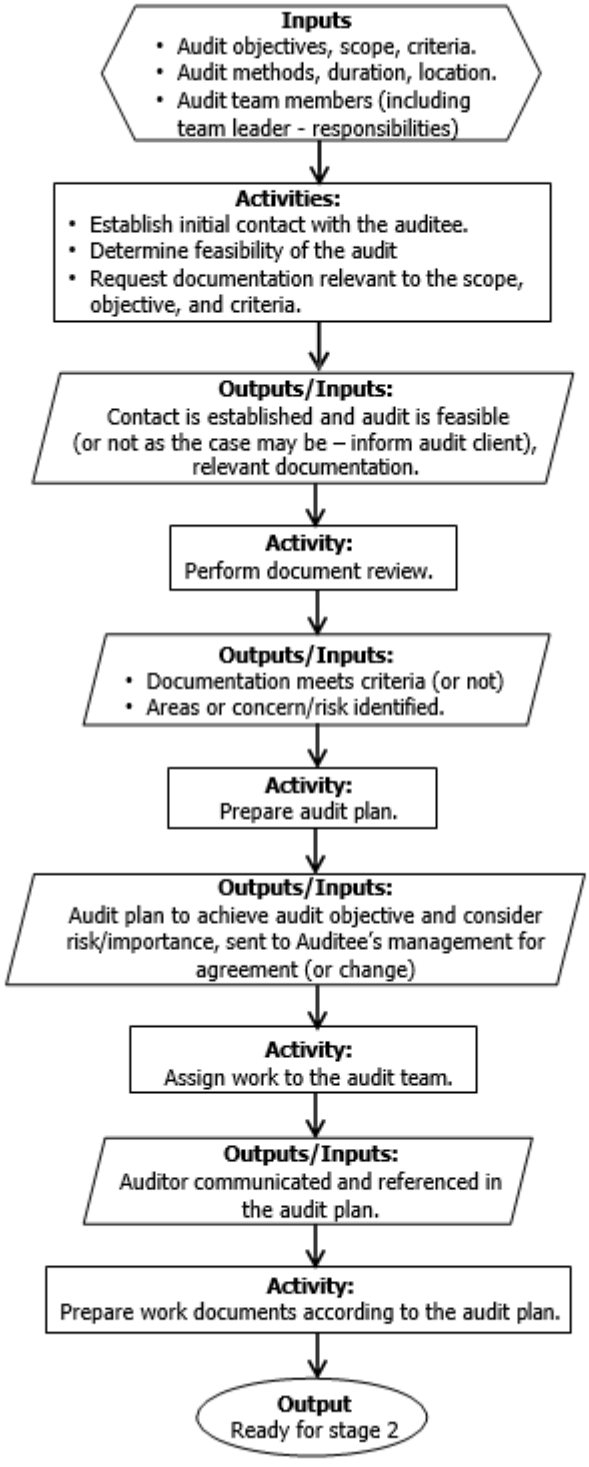

Figure 3: Retrieved from 02 slides (mimeo) page 35.

Inputs: **(ISO/IEC 17021-1:2015, Clause 9.3.1.2)**	• Audit objectives, scope, criteria (ISO/IEC 17021-1:2015, Clause 9.2.1; ISO 19011:2018, Clause 6.3.1). • Audit methods, duration, locations (ISO/IEC 17021-1:2015, Clause 9.2.3.2; ISO 19011:2018, Clause 6.3.2). • Audit team members (roles and responsibilities) (ISO/IEC 17021-1:2015, Clause 9.2.2; ISO 19011:2018, Clause 5.5.4). • Client's ISMS documentation (ISO/IEC 27001:2022, Clause 7.5; ISO/IEC 17021-1:2015, Clause 9.3.1.2.2.a).
Activities	1. Establish initial contact with the auditee (ISO/IEC 17021-1:2015, Clause 9.3.1.2.1) 2. Determine feasibility of the audit (ISO/IEC 17021-1:2015, Clause 9.3.1.2.2) 3. Request documentation relevant to the scope, objectives, and criteria (ISO/IEC 17021-1:2015, Clause 9.3.1.2.2.a)
Outputs/Inputs	Contact is established, and audit is feasible (or not as the case may be), necessary documentation received for relevant documentation (ISO/IEC 17021-1:2015, Clause 9.3.1.2.3).
Activity	• Perform document review (ISO/IEC 17021-1:2015, Clause 9.3.1.2.2.a). • Review the organization's ISMS documentation to identify potential non-conformities or areas of concern (ISO/IEC 17021-1:2015, Clause 9.3.1.2.2.a; ISO 19011:2018, Clause 6.4.6). • Assess the adequacy and completeness of the documentation against ISO/IEC 27001 requirements (ISO/IEC 27001:2022, Clause 7.5; ISO/IEC 17021-1:2015, Clause 9.3.1.2.2.a). • Determine if the documented ISMS appears to meet the audit criteria and objectives (ISO/IEC 17021-1:2015, Clause 9.3.1.2.2.f; ISO 19011:2018, Clause 6.4.1).
Outputs/Inputs	1. Documentation review completed (or not) (ISO/IEC 17021-1:2015, Clause 9.3.1.2.3). 2. Potential non-conformities or areas of concern identified (ISO/IEC 17021-1:2015, Clause 9.3.1.2.3; ISO 19011:2018, Clause 6.4.5). 3. Adequacy and completeness of documentation assessed (ISO/IEC 27001:2022, Clause 7.5; ISO/IEC 17021-1:2015, Clause 9.3.1.2.2.a).
Activity	Evaluation of on-site conditions (ISO/IEC 17021-1:2015, Clause 9.3.1.2.2.b, c).
Outputs/Inputs	The auditor will assess the company's site-specific conditions, including resource utilization, employee count, equipment, and number of sites.
Activity	Prepare audit plan (ISO/IEC 17021-1:2015, Clause 9.2.3).
Outputs/Inputs	Audit plan is produced based on document review outcomes and considering factors such as travel, accommodation, logistics, etc., to Auditee's site (ISO/IEC 17021-1:2015, Clause 9.2.3.2).
Activity	Assign work to the audit team (ISO/IEC 17021-1:2015, Clause 9.2.2.1.5)
Outputs/Inputs	Auditor competence is considered, and work assigned in line with the audit plan (ISO/IEC 17021-1:2015, Clause 9.2.2.1.5).
Activity	Prepare work documents according to the audit plan (ISO/IEC 17021-1:2015, Clause 9.2.3.4).

Output	Ready for stage 2

Audit Checklists

An audit checklist is a tool used by auditors to ensure that all relevant aspects of the ISMS are covered during the audit (ISO 19011:2018, Clause A.5). The purpose of an audit checklist is to:

- Serve as a guide for conducting the audit.
- Ensure consistency in the audit approach.
- Provide a means for recording audit findings and evidence.

To create an effective audit checklist (ISO 19011:2018, Clause 6.3.4):

1. Identify the audit objectives, scope, and criteria.
2. Break down the requirements of the standard into smaller, auditable elements.
3. Organize the checklist in a logical sequence.
4. Include space for recording observations, findings, and evidence.

Sample Checklist (based on ISO/IEC 27001:2022 and LDCC Case Study):

Clause	Requirement	Source	Evidence	Observations/Findings
4.1	Understanding the organization and its context.	- Strategic Mission Statement (D1). - Security Context (D6).	- Does the Strategic Mission Statement (D1) outline LDCC's objectives and mission? - Does the Security Context document (D6) provide a comprehensive analysis of LDCC's external and internal issues?	- The Strategic Mission Statement (D1) outlines LDCC's objectives and mission. - The Security Context document (D6) provides a comprehensive analysis of LDCC's external and internal issues.
4.2	Understanding the needs and expectations of interested parties.	Interested Parties (D7)	- Does the Interested Parties document (D7) identify key stakeholders and their information security requirements?	- The Interested Parties document (D7) identifies key stakeholders and their information security requirements
5.1	Leadership and commitment.	- Information Security Policy (D2). - Management Review Minutes (D5).	- Does the Information Security Policy (D2) demonstrate top management's commitment to ISMS? - Do the Management Review Meeting Minutes (D5) show leadership involvement in ISMS review?	- Inconsistent attendance and participation of top management in Management Review Meetings (D5). - The policy does not clearly communicate top management's commitment to ensure the integration of the

				ISMS requirements into the organization's processes.
6.1.2	Information security risk assessment.	- Information Security Risk Assessment Procedure (D11). - Risk Assessment Template (D13)	- Does the Information Security Risk Assessment Procedure (D11) define the risk assessment methodology? - Does the Risk Assessment Template (D13) show risks are identified, analysed, and evaluated?	The Risk Assessment Template (D13) demonstrates a structured approach to risk identification, analysis, and evaluation.
7.2	Competence	- Training Records (Extract) (D19). - Individual Training Records (D20).	- Do the Training Records (Extract) (D19) show the necessary competencies for ISMS roles? - Do the Individual Training Records (D20) demonstrate that training is provided, and competence is evaluated?	- There are some inconsistencies in the Individual Training Records (D20). - The Training Records (Extract) (D19) provides an overview of the competencies required for key ISMS roles.
8.1	Operational planning and control.	- Backup Procedure (D23). - Backup Log (D24).	- Does the Backup Procedure (D23) define the processes for backing up and recovering information? - Does the Backup Log (D24) show that backups are performed and tested regularly?	- Gaps in the Backup Log (D24) indicate that backups are not always performed consistently. - The Backup Procedure (D23) is well-documented and includes provisions for testing backups.
9.1	Monitoring, measurement, analysis, and evaluation.	- Performance Monitoring and Measurement (Extract) (D37). - Performance Analysis and Evaluation (Extract) (D38).	- Does the Performance Monitoring and Measurement (Extract) (D37) define key performance indicators for ISMS? - Does the Performance Analysis and Evaluation (Extract) (D38) demonstrate that ISMS performance is regularly monitored, analysed, and evaluated?	- Some inconsistencies and gaps in the Performance Analysis and Evaluation (Extract) (D38). - The Performance Monitoring and Measurement (Extract) (D37) identifies relevant KPIs for monitoring ISMS performance.

Application of Auditor Competencies in Stage 1 Audit

Auditors conducting a Stage 1 audit should possess the following competencies (ISO/IEC 17021-1:2015, Clause 7.1.2; ISO 19011:2018, Clause 7.2.3):

1. Knowledge of ISMS, ISO 27001 requirements, and the client's processes (ISO/IEC 17021-1:2015, Clause 7.1.2; ISO 19011:2018, Clause 7.2.3.2; ISO/IEC 27001:2022, Clause 7.2): Auditors apply this knowledge to understand the organization's context, ISMS scope, and documentation, and to identify potential non-conformities or areas of concern during the document review.
2. Ability to review and assess documentation (ISO/IEC 17021-1:2015, Clause 7.1.2; ISO 19011:2018, Clause 7.2.3.1): Auditors demonstrate this ability by effectively reviewing the organization's ISMS documentation, assessing its adequacy and completeness against ISO/IEC 27001 requirements, and determining if the documented ISMS appears to meet the audit criteria and objectives.
3. Analytical and observational skills to identify areas of concern (ISO/IEC 17021-1:2015, Clause 7.1.2; ISO 19011:2018, Clause 7.2.3.2): Auditors use these skills to analyse the documentation and identify potential non-conformities, gaps, or areas requiring further investigation during the Stage 2 audit.
4. Communication and interpersonal skills to establish effective contact with the auditee (ISO/IEC 17021-1:2015, Clause 7.1.2; ISO 19011:2018, Clause 7.2.2): Auditors apply these skills to communicate the Stage 1 audit objectives, scope, and requirements to the auditee, and to establish a positive and professional relationship that facilitates the audit process.
5. Planning and organizational skills to develop an appropriate audit plan (ISO/IEC 17021-1:2015, Clause 7.1.2; ISO 19011:2018, Clause 7.2.3.4): Auditors demonstrate these skills by creating a comprehensive and tailored audit plan based on the document review outcomes, considering factors such as the organization's size, complexity, and specific needs.

Mandatory documents from ISO/IEC 27001 and its importance.

S/N	ISO 27001 Clause	Mandatory Documents	Importance
1	4.3	Scope.	Defines the boundaries and applicability of the ISMS, considering the organization's context, interested parties, and interfaces with other systems.
2	5.2	Policy.	Provides top management's direction and support for information security in alignment with business objectives and relevant laws and regulations.
3	6.1.2	Information security risk assessment process.	Ensures that information security risks are consistently assessed, considering the organization's context, assets, threats, and vulnerabilities.
4	6.1.3	Statement of Applicability	Documents the organization's decisions regarding risk treatment, the selected

		Information security risk treatment plan. Information security risk treatment process.	controls, and the justification for inclusions and exclusions, forming the basis for implementation and continuous improvement.
5	6.2	Information security objectives.	Establishes clear, measurable goals for information security, aligned with the policy and risk assessment results, to drive the ISMS implementation and improvement.
6	6.3	Planning of changes.	Ensures that changes to the ISMS are carried out in a planned and controlled manner, minimizing potential disruptions and maintaining the integrity of the system.
7	7.2	Evidence of competence.	Demonstrates that personnel involved in the ISMS have the necessary skills, training, and experience to perform their roles effectively.
8	7.5.1	Documented information required by the standard and determined by the organization for ISMS effectiveness.	Ensures that the organization maintains a comprehensive and up-to-date set of documents and records necessary for the effective operation and continuous improvement of the ISMS.
9	7.5.3	Documented information of external origin determined by the organization to be necessary.	Ensures that relevant external documents, such as laws, regulations, and contracts, are identified, managed, and controlled within the ISMS.
10	8.1	Information to the extent necessary to have confidence that the processes have been carried out as planned.	Provides evidence that the ISMS processes are being executed as designed and that the system is operating effectively.
11	8.2	Results of information security risk assessments.	Documents the outcomes of risk assessments, enabling the organization to make informed decisions about risk treatment and control implementation.
12	8.3	Results of information security risk treatment.	Records the outcomes of risk treatment activities, demonstrating that the organization is effectively managing its information security risks.

13	9.1	Evidence of monitoring and measurement results.	Provides data and insights into the performance and effectiveness of the ISMS, enabling the organization to identify areas for improvement and demonstrate compliance.
14	9.2	Audit programme(s) Evidence of the implementation of the audit programme(s) and the audit results.	Documents the planned internal audit activities and their outcomes, providing assurance that the ISMS conforms to the organization's requirements and the ISO 27001 standard.
15	9.3	Information as evidence of the results of the management reviews.	Records the outcomes of management reviews, demonstrating top management's ongoing commitment, oversight, and decision-making related to the ISMS.
16	10.1	Information of the nature of the nonconformities and any subsequent actions taken, and the results of any corrective action.	Documents identified nonconformities, the organization's response, and the effectiveness of corrective actions, supporting continuous improvement of the ISMS.

Stage 2 Audit Plan

A Stage 2 audit plan is essential for the initial certification process (ISO/IEC 17021-1:2015, Clause 9.3.1.3) as it provides the basis for agreement regarding the conduct and scheduling of audit activities (ISO/IEC 17021-1:2015, Clause 9.2.3.1). The plan outlines the audit objectives, scope, and criteria (ISO 19011:2018, Clause 6.3.2.2), ensures agreement between the audit team and the audited organization on the audit activities and schedule (ISO 19011:2018, Clause 6.3.2.4), and helps the audit team focus on key areas of the ISMS and allocate resources effectively (ISO 19011:2018, Clause 5.5.2). The Stage 2 audit plan also facilitates communication of the audit activities to the audited organization (ISO 19011:2018, Clause 6.3.2.4) and should be tailored to the specific context of the organization, considering factors such as its size, ISMS complexity, and Stage 1 audit results (ISO/IEC 17021-1:2015, Clause 9.3.1.2).

General Information

Audit Objective	To determine the conformity of Lake Dale Contact Centre's (LDCC) ISMS with the requirements of ISO/IEC 27001:2022 and its own policies and objectives (ISO/IEC 17021-1:2015, Clause 9.2.1.2; ISO 19011:2018, Clause 6.3.2.1).
Audit Scope	- The ISMS scope covers the provision of telephony services, the management of information, and business support services at

	LDCC's Mumbai site, in accordance with the Statement of Applicability revision 03, dated 21/Sept/20xx (Case Study, ISMS Scope; ISO/IEC 17021-1:2015, Clause 9.2.1.3; ISO 19011:2018, Clause 6.3.2.1). - The audit will cover LDCC's functions, including HR, Operations, Facilities, Finance, Sales and Marketing, and IT, as well as the processes within the ISMS scope.
Audit Criteria	- ISO/IEC 27001:2022 requirements (ISO/IEC 17021-1:2015, Clause 9.2.1.4; ISO 19011:2018, Clause 6.3.2.1). - LDCC's ISMS policies, procedures, and controls as defined in its documentation (ISO/IEC 17021-1:2015, Clause 9.2.1.4; ISO 19011:2018, Clause 6.3.2.1).
Auditing Company	Clearview Audit group
Audit Team	Lead Auditor: Emmanuel Ateji Auditor 1: Sarah Johnson Auditor 2: Michael Brown Technical Expert: Jennifer Davis Observer: Mark Wilson
Type of Audit	Stage 2 audit (ISO/IEC 17021-1:2015, Clause 9.3.1.3).
Language	English (assumed based on the case study documentation)
Auditee	Lake Dale Contact Centre (LDCC) [Case Study, Strategic Mission Statement]
Date & Time	Date: Monday, 20 May 2024 Time: 9:00-17:45
Location	Mumbai, India

Roles and Responsibility

S/N	Role	Responsibility
1	Lead Auditor: Emmanuel Ateji	- Conduct opening meeting (ISO 19011:2018, Clause 6.4.3). - Lead the audit team and manage the audit process (ISO 19011:2018, Clause 5.5.5).

		- Communicate with the auditee's management (ISO 19011:2018, Clause 6.4.2). - Prepare and present the audit report (ISO/IEC 17021-1:2015, Clause 9.4.8; ISO 19011:2018, Clause 6.5.1)
2	Auditor 1: Sarah Johnson	- Interview HR Director Raj Patel and HR Manager Sarah Pippins (Case Study, Staff List). - Review HR policies, procedures, and records related to information security (ISO/IEC 27001:2022, Clause 7.2; ISO 19011:2018, Clause 6.4.7)
3	Auditor 2: Micheal Brown	- Interview Operations Manager Amanda French and Tele Manager Lucy Carr (Case Study, Staff List). - Review operations policies, procedures, and records related to information security (ISO/IEC 27001:2022, Clause 8; ISO 19011:2018, Clause 6.4.7)
4	Technical Expert: Jennifer Davis	- Provide expertise in the organization's specific technology and systems (ISO 19011:2018, Clause 3.16). - Assist the audit team in understanding the technical aspects of the ISMS (ISO 19011:2018, Clause 5.4.1)
5	Guides and Observers: Mark Wilson (Clearview Audit group Representative).	- Observe the audit process and provide feedback to Clearview Audit group (ISO/IEC 17021-1:2015, Clause 9.4.2). - Ensure the audit is conducted in accordance with Clearview Audit group's procedures (ISO/IEC 17021-1:2015, Clause 5.1.3)

The lead auditor's responsibilities are mapped to ISO 19011:2018 and ISO/IEC 17021-1:2015 clauses. The auditors' responsibilities are mapped to the relevant ISO/IEC 27001:2022 clauses and ISO 19011:2018. The technical expert's role is defined in ISO 19011:2018, Clause 3.16, and their responsibilities are mapped to ISO 19011:2018, Clause 5.4.1. The observer's role and responsibilities are mapped to ISO/IEC 17021-1:2015 clauses.

Stage 2 Audit Plan and Activities

Time	Audit Activities	Auditors- in-Charge	Applicable ISO Clause 19011	Applicable to ISO 27001	Relevant Documents
DAY 1					
09:00 -09:30	Opening meeting.	Emmanuel Ateji (Lead Auditor)	6.4.3	N/A	Audit plan
09:30 -10:30	ISMS Documentation Review.	Sarah Johnson (Auditor 1)	6.4.6	7.5	ISMS Manual (D2), Policies (D2, D3, D6), Procedures (D21, D23, D25).
10:30 -11:00	Review of Corrective Actions from Previous Audits.	Emmanuel Ateji (Lead Auditor)	6.4.5	10.1	Previous Audit Reports (D40), Corrective Action Plans (D41).
11:00 -12:00	Interview with HR Director Raj Patel.	Sarah Johnson (Auditor 1)	6.4.7	7.1, 7.2, 7.3	HR Policies (D33, D34), Training Records (D19, D20).
13:00 -14:00	Interview with IT Manager John Bishop.	Michael Brown (Auditor 2)	6.4.7	8.1, 8.2, 8.3, 8.4	IT Policies, Access Control Records
14:00 -15:00	Observation of IT Operations.	Michael Brown (Auditor 2)	6.4.7	8.1, 8.2, 8.3, 8.4	IT Procedures (D23), System Logs
15:00 -16:00	Interview with Operations Manager Amanda French	Sarah Johnson (Auditor 1)	6.4.7	8.1, 8.2, 8.3, 8.4	Operations Policies, Incident Reports
16:00-17:00	Audit Team Meeting	Emmanuel Ateji (Lead Auditor)	6.4.3	N/A	Audit Notes, Findings
DAY 2					
09:00-10:00	Preparation of Audit Conclusions	Emmanuel Ateji (Lead Auditor)	6.4.9	N/A	Audit Evidence, Findings
10:00 -11:00	Interview with Tele Manager Lucy Carr	Michael Brown (Auditor 2)	6.4.7	8.1, 8.2, 8.3, 8.4	Tele Policies, Call Records.
11:00 -12:00	Observation of HR Processes	Sarah Johnson (Auditor 1)	6.4.7	7.1, 7.2, 7.3	HR Procedures, Personnel Files

13:00 -14:00	Evaluation of ISMS Effectiveness	Emmanuel Ateji (Lead Auditor)	N/A	9.3	ISMS Performance Reports, KPIs
14:00 -15:00	Review of Continual Improvement	Emmanuel Ateji (Lead Auditor)	N/A	10.2	Improvement Plans, Management Review Minutes
15:00 -16:00	Preparation of Audit Report	Emmanuel Ateji (Lead Auditor)	6.5.1	N/A	Audit Evidence, Findings
DAY 3					
09:00 -10:00	Interview with Finance Manager Philip Hernshaw Smyth	Sarah Johnson (Auditor 1)	6.4.7	8.1, 8.2, 8.3, 8.4	Finance Policies, Financial Records
10:00 -11:00	Observation of Finance Processes	Sarah Johnson (Auditor 1)	6.4.7	8.1, 8.2, 8.3, 8.4	Finance Procedures, Invoices, Contracts
11:00 -12:00	Interview with Facilities Manager Simon Lock.	Michael Brown (Auditor 2)	6.4.7	11.1, 11.2	Physical Security Policies, Access Control Records
13:00 -14:00	Observation of Physical Security Controls.	Michael Brown (Auditor 2)	6.4.7	11.1, 11.2	CCTV Footage, Visitor Logs
14:00 -15:00	Review of Business Continuity and Incident Management	Emmanuel Ateji (Lead Auditor)	6.4.6	16.1, 17.1	Business Continuity Plans, Incident Reports.
15:00-16:00	Audit Team Meeting	Emmanuel Ateji (Lead Auditor)	6.4.3	N/A	Audit Notes, Findings
DAY 4					
09:00 -10:00	Interview with Sales Manager Clive Page.	Sarah Johnson (Auditor 1)	6.4.7	8.1, 8.2, 8.3, 8.4	Sales Policies, Customer Contracts
10:00 -11:00	Observation of Sales Processes	Sarah Johnson (Auditor 1)	6.4.7	| 8.1, 8.2, 8.3, 8.4	Sales Procedures, CRM System
11:00 -12:00	Review of Supplier Management.	Michael Brown (Auditor 2)	6.4.6	15.1, 15.2	Supplier Agreements, Risk Assessments
13:00 -14:00	Interview with IS Manager Clive Prichard.	Emmanuel Ateji (Lead Auditor)	6.4.7	5.1, 6.1, 9.1, 9.2, 9.3	ISMS Policies, Risk Assessment Reports
14:00 -15:00	Review of Risk Assessment and Treatment	Emmanuel Ateji (Lead Auditor)	6.4.6	6.1, 6.2	Risk Assessment Methodology, Risk Treatment Plans
15:00 -16:00	Audit Team Meeting	Emmanuel Ateji (Lead Auditor)	6.4.3	N/A	Audit Notes, Findings

DAY 5					
09:00 -10:00	Preparation of Audit Report	Emmanuel Ateji (Lead Auditor)	6.5.1	N/A	Audit Evidence, Findings.
10:00 -11:00	Closing Meeting	Emmanuel Ateji (Lead Auditor)	6.4.10	N/A	Audit Report, Nonconformities
11:00 -12:00	Distribution of Audit Report	Emmanuel Ateji (Lead Auditor)	6.5.2, ISO/IEC 17021-1 Clause 9.4.8	N/A	Audit Report

Stage 2 Audit

Description and Evaluation of a Stage 2 Audit (ISO/IEC 17021-1:2015, Clause 9.3.1.3)

A Stage 2 audit is the second and most comprehensive phase of the initial certification audit process for an organization seeking certification of its Information Security Management System (ISMS) as per ISO/IEC 27001.

Purpose of a stage 2 Audit (ISO/IEC 17021-1:2015, Clause 9.3.1.3):

The purpose of the Stage 2 audit is to evaluate the implementation, including the effectiveness, of the organization's ISMS. Specifically, the Stage 2 audit aims to:

- Verify the organization's conformity to all requirements of ISO/IEC 27001 and the applicable information security controls (Reporting and writing non-conformity reports if found).
- Evaluate the performance monitoring, measurement, reporting, and review against the ISMS objectives and targets.
- Assess the ISMS's ability to meet applicable statutory, regulatory, and contractual requirements.
- Evaluate the operational control of processes and the implementation of information security controls.
- Review the internal audit and management review processes.
- Assess top management's commitment and involvement in the ISMS.

Relevant Areas, Activities, and Outputs:

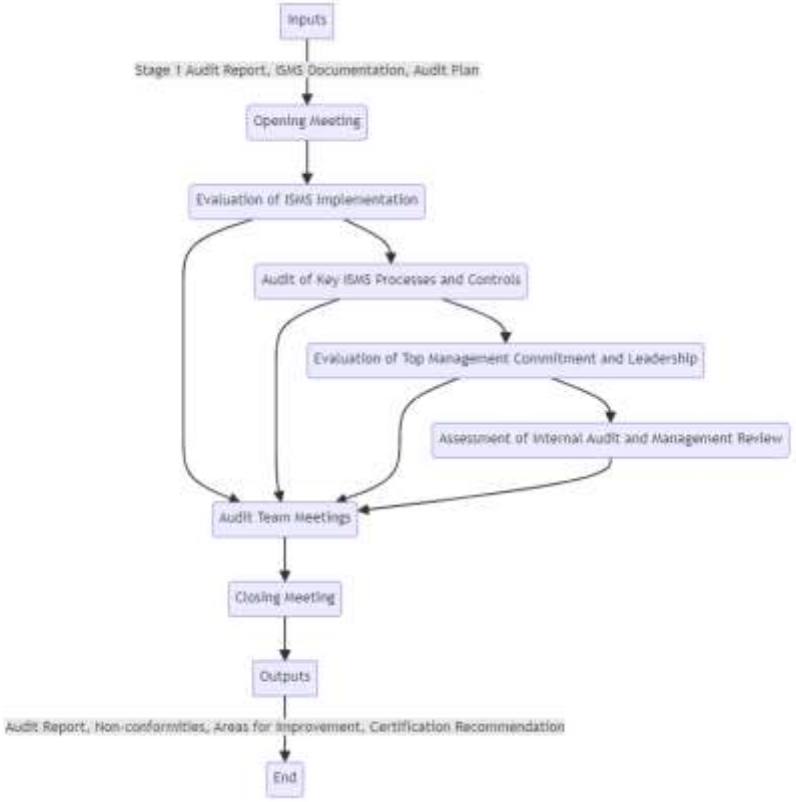

Figure 4: Flow diagram for stage 2 Audit

Inputs (ISO/IEC 27001:2022, Clause 9.3.1.2.3; ISO/IEC 17021-1:2015, Clauses 9.3.1.3 and 9.3.1.4):

- Stage 1 audit report and conclusions.
- Identified areas of concern or potential non-conformities from Stage 1.
- Documented information of the ISMS (policies, procedures, records, etc.).
- Audit plan and objectives.

Activities:

1. Opening Meeting (ISO/IEC 17021-1:2015, Clause 9.4.2; ISO 19011:2018, Clause 6.4.3)
    - Introduction of the audit team and participants.
    - Confirmation of the audit scope, objectives, and criteria.
    - Overview of the audit plan and schedule.
    - Explanation of the audit methodology and reporting process.

2. Evaluation of ISMS Implementation (ISO/IEC 27001:2022, Clause 9.3.1.3; ISO 19011:2018, Clauses 6.4.4, 6.4.6, and 6.4.7)
    - Review of documented information (policies, procedures, records, etc.)
    - Interviews with personnel from various functions and levels
    - Observation of operational activities and practices
    - Verification of the implementation and effectiveness of controls
    - Assessment of performance monitoring, measurement, and reporting
3. Audit of Key ISMS Processes and Controls (ISO/IEC 27001:2022, Annex A)

- Information security risk assessment and treatment (ISO/IEC 27001:2022, Clauses 6.1.2 and 6.1.3)
- Management of information assets and classification (ISO/IEC 27001:2022, Clause 8.1)
- Human resources security (ISO/IEC 27001:2022, Clause 7.2)
- Physical and environmental security (ISO/IEC 27001:2022, Clause 11)
- Operations security (ISO/IEC 27001:2022, Clause 12)
- Communications security (ISO/IEC 27001:2022, Clause 13)
- System acquisition, development, and maintenance (ISO/IEC 27001:2022, Clause 14)
- Supplier relationships and outsourcing (ISO/IEC 27001:2022, Clause 15)
- Information security incident management (ISO/IEC 27001:2022, Clause 16)
- Business continuity management (ISO/IEC 27001:2022, Clause 17)
- Compliance with policies, standards, and legal/regulatory requirements (ISO/IEC 27001:2022, Clause 18)

4. Evaluation of Top Management Commitment and Leadership (ISO/IEC 27001:2022, Clause 5.1)
    - Interviews with top management
    - Review of management's involvement in the ISMS
5. Assessment of Internal Audit and Management Review (ISO/IEC 27001:2022, Clauses 9.2 and 9.3)
    - Verification of the effectiveness of internal audits
    - Review of management review inputs, outputs, and actions taken
6. Audit Team Meetings (ISO 19011:2018, Clause 6.4.3)
    - Coordination among the audit team
    - Discussion of findings and progress
    - Preparation of audit conclusions
7. Closing Meeting (ISO/IEC 17021-1:2015, Clause 9.4.7; ISO 19011:2018, Clause 6.4.10)
    - Presentation of audit findings and conclusions
    - Discussion of non-conformities and areas for improvement
    - Explanation of the next steps in the certification process

Outputs (ISO/IEC 17021-1:2015, Clause 9.4.8):

- Audit report detailing the audit findings, conclusions, and recommendations.
- List of identified non-conformities and areas for improvement.
- Determination of the ISMS's effectiveness and conformity to ISO/IEC 27001
- Recommendation on certification decision (grant, deny, or additional actions required).

Application of Auditor Competencies in Stage 2 Audit (ISO/IEC 17021-1:2015, Clause 7.1.2; ISO 19011:2018, Clause 7.2.3).

Auditors conducting a Stage 2 audit should possess the following competencies:

1. In-depth knowledge of ISO/IEC 27001 requirements and information security controls (ISO/IEC 17021-1:2015, Clause 7.1.2; ISO 19011:2018, Clause 7.2.3.2)
2. Understanding of the organization's context, processes, and operations (ISO/IEC 17021-1:2015, Clause 7.1.2; ISO 19011:2018, Clause 7.2.3.2)

3. Interviewing and communication skills (ISO/IEC 17021-1:2015, Clause 7.1.2; ISO 19011:2018, Clauses 7.2.2 and 7.2.3.1).
4. Observation and assessment skills (ISO/IEC 17021-1:2015, Clause 7.1.2; ISO 19011:2018, Clause 7.2.3.1).
5. Analytical and critical thinking skills (ISO/IEC 17021-1:2015, Clause 7.1.2; ISO 19011:2018, Clause 7.2.3.1).
6. Audit management and team leadership skills (for the lead auditor) (ISO/IEC 17021-1:2015, Clause 7.2.3.4; ISO 19011:2018, Clause 7.2.3.4).

Auditors apply these competencies throughout the Stage 2 audit to effectively evaluate the organization's ISMS implementation and provide a well-informed recommendation on certification.

Stage 2 Sample Audit Opening Meeting (ISO 19011:2018, Clause 6.4.3; ISO/IEC 17021-1:2015, Clause 9.4.2).

Date: 20/05/2024
Time: 09:00 - 09:00
Location: Mumbai, India

Attendees:

- Audit Team: Emmanuel Ateji (Lead Auditor), Sarah Johnson (Auditor), Michael Brown (Auditor).
- LDCC Representatives: Alan Swan (MD/CEO), Clive Prichard (IS Manager/Management.
- Representative for ISMS), Amanda French (Operations Manager), Raj Patel (HR Director), John Bishop (IT Manager).

Agenda:

1. Welcome and Introductions (ISO 19011:2018, Clause 6.4.3)
    - Lead Auditor Emmanuel Ateji welcomes the participants and introduces the audit team members.
    - LDCC representatives introduce themselves and their roles within the organization.

2. Confirmation of Audit Objectives, Scope, and Criteria (ISO/IEC 17021-1:2015, Clause 9.2.1; ISO 19011:2018, Clause 6.3.2.1).
    - Lead Auditor Emmanuel Ateji confirms the audit objectives, which are to evaluate the implementation and effectiveness of LDCC's ISMS and determine its conformity to ISO/IEC 27001:2022 requirements.
    - The audit scope is confirmed as the ISMS covering the provision of telephony services, management of information, and business support services at LDCC's Mumbai site, as defined in the Statement of Applicability Rev. 03 dated 21/Sept/20XX (Case Study, ISMS Scope).
    - The audit criteria are identified as the requirements of ISO/IEC 27001:2022 and LDCC's ISMS policies and procedures (ISO/IEC 17021-1:2015, Clause 9.2.1.4).

3. Confirmation of Audit Plan and Schedule (ISO 19011:2018, Clause 6.3.2).

- Lead Auditor Emmanuel Ateji presents the audit plan and schedule, highlighting the key activities, areas to be audited, and allocated time for each activity.
- The audit team and LDCC representatives confirm their availability and commitment to the plan.

4. Explanation of Audit Methods and Procedures (ISO 19011:2018, Clause 6.4).
    - Lead Auditor Emmanuel Ateji explains the audit methods, which include interviews, observation of processes, and review of documentation and records (ISO 19011:2018, Clause 6.4.7).
    - The lead auditor also outlines the procedure for identifying and reporting non-conformities and observations (ISO/IEC 17021-1:2015, Clause 9.4.5).

5. Confirmation of Communication Channels and Confidentiality (ISO/IEC 17021-1:2015, Clause 8.4).
    - Lead Auditor Emmanuel Ateji confirms the communication channels between the audit team and LDCC representatives during the audit.
    - The lead auditor emphasizes the confidentiality of audit findings and information gained during the audit process (ISO/IEC 17021-1:2015, Clause 8.4).

6. Clarification of Any Questions or Concerns
    - Lead Auditor Emmanuel Ateji invites LDCC representatives to raise any questions or concerns regarding the audit process.
    - The audit team addresses the questions and concerns to ensure clarity and understanding.
7. Closing
    - Lead Auditor Emmanuel Ateji thanks the participants for their attendance and reiterates the importance of their cooperation and support during the audit process.
    - The meeting is closed, and the audit team proceeds with the Stage 2 audit activities as per the agreed plan.

Stage 2 Sample Audit Closing Meeting (ISO 19011:2018, Clause 6.4.10; ISO/IEC 17021-1:2015, Clause 9.4.7).

Date: 21/05/2024
Time: 10:00 – 11:00
Location: Mumbai, India

Attendees:

- Audit Team: Emmanuel Ateji (Lead Auditor), Sarah Johnson (Auditor 1), Michael Brown (Auditor 2).
- LDCC Representatives: Alan Swan (MD/CEO), Clive Prichard (IS Manager/Management Representative for ISMS), Amanda French (Operations Manager), Raj Patel (HR Director), John Bishop (IT Manager).

Agenda:

1. Welcome and Appreciation (ISO 19011:2018, Clause 6.4.10)

- Lead Auditor Emmanuel Ateji welcomes the participants and expresses appreciation for their cooperation and support throughout the audit process.

2. Presentation of Audit Findings and Conclusions (ISO/IEC 17021-1:2015, Clause 9.4.8)
   - Lead Auditor Emmanuel Ateji presents the audit findings and conclusions, which include:
   - Strengths and positive observations of LDCC's ISMS implementation
   - Non-conformities identified during the audit, with reference to specific ISO/IEC 27001:2022 clauses and LDCC's ISMS policies and procedures.
   - Opportunities for improvement and areas of concern.

3. Discussion of Non-Conformities and Their Severity (ISO/IEC 17021-1:2015, Clause 9.4.5.3).
   - Lead Auditor Emmanuel Ateji explains the severity of the identified non-conformities (major or minor) and their potential impact on the effectiveness of LDCC's ISMS.
   - LDCC representatives are given the opportunity to discuss and clarify the non-conformities and provide any additional information or evidence.

4. Agreement on Corrective Action Timeframes (ISO/IEC 17021-1:2015, Clause 9.4.10).
   - Lead Auditor Emmanuel Ateji and LDCC representatives agree on the timeframes for submitting corrective action plans and implementing corrective actions for the identified non-conformities.
   - The lead auditor emphasizes the importance of addressing the non-conformities within the agreed timeframes to maintain the effectiveness of the ISMS and ensure continued conformity to ISO/IEC 27001:2022.

5. Explanation of the Next Steps in the Certification Process (ISO/IEC 17021-1:2015, Clause 9.5). Lead Auditor Emmanuel Ateji outlines the next steps in the certification process, which include:
   - Submission of the audit report to the certification body for review (ISO/IEC 17021-1:2015, Clause 9.4.8)
   - Review of the corrective action plans submitted by LDCC (ISO/IEC 17021-1:2015, Clause 9.4.10).
   - Verification of the effectiveness of the implemented corrective actions (ISO/IEC 17021-1:2015, Clause 9.4.10)
   - Certification decision by the certification body (ISO/IEC 17021-1:2015, Clause 9.5).

6. Opportunity for Questions and Feedback from the Auditee.
   - Lead Auditor Emmanuel Ateji invites LDCC representatives to ask any questions or provide feedback regarding the audit process and findings.
   - The audit team addresses the questions and feedback, providing clarifications and ensuring a clear understanding of the audit outcomes.

7. Closing Remarks and Appreciation for Cooperation.
   - Lead Auditor Emmanuel Ateji concludes the meeting by thanking LDCC representatives for their active participation and cooperation throughout the audit process.
   - The lead auditor reiterates the importance of maintaining and continually improving the ISMS to ensure its ongoing effectiveness and conformity to ISO/IEC 27001:2022.

Objective Evidence

Objective evidence is verifiable information, records, or statements of fact that can be proven true, based on observation, measurement, test, or other means (ISO 19011:2018, Clause 3.8). It is data supporting the existence or verity of something and can be obtained through observation, measurement, test, or other means (ISO/IEC 17021-1:2015, Clause 9.4.4.1).

Importance of objective evidence

Objective evidence plays a crucial role in the audit process by providing a factual and unbiased foundation for determining conformity to audit criteria (ISO/IEC 17021-1:2015, Clause 9.4.4.1) and reaching reliable and reproducible audit conclusions (ISO 19011:2018, Clause 4f). It enables auditors to verify that the organization's Information Security Management System (ISMS) conforms to the requirements of ISO/IEC 27001 (ISO/IEC 17021-1:2015, Clause 9.2.1.2) and its own policies, objectives, and targets (ISO/IEC 17021-1:2015, Clause 9.2.1.2).

By relying on objective evidence, auditors ensure that their findings and conclusions are based on facts rather than subjective opinions or assumptions. This approach enhances the credibility and reliability of the audit process and its outcomes (ISO 19011:2018, Clause 6.4.7). Furthermore, objective evidence facilitates understanding and acceptance of audit findings and conclusions by the auditee and other interested parties (ISO/IEC 17021-1:2015, Clause 9.4.8.2).

Examples of objective evidence from LDCC’s case study

1. **Asset Register (Case Study Document D12):**
   The asset register in the case study aims to identify and document the organization's assets and their owners, as required by ISO/IEC 27001:2022, Clause 8.1, and ISO/IEC 27002:2022, Control 5.9. While it provides a comprehensive list of assets for risk assessment and management, there are instances of incomplete information, such as missing risk owners for certain assets. For example, the asset "LDCC-S-11 (a network switch)" lacks a documented owner, indicating non-compliance with the ISO standards. To ensure full compliance, the organization should address these gaps in the asset register.

2. **Information Security Policy (Case Study Document D2):**
   The information security policy in the case study demonstrates top management's commitment and provides high-level direction, aligning with ISO/IEC 27001:2022, Clause 5.2. It is a documented policy that covers essential elements and aligns with the organization's strategic objectives and legal/regulatory requirements. However, the policy lacks evidence of regular reviews and updates to ensure ongoing relevance and effectiveness, as required by the standard. For example, while the policy states, "This policy will be implemented through a recognised Information Security Management System that has been self-declared by the ISF," there is no proof of periodic reviews and updates.

3. **Risk Assessment Template (Case Study Document D13):**
   The risk assessment template in the case study documents the organization's process for assessing information security risks, aligning with ISO/IEC 27001:2022, Clause 6.1.2. It provides a structured approach to identifying, analysing, and evaluating risks, forming the basis for risk treatment decisions. However, the case study reveals inconsistencies in the risk assessment results, such as misaligned risk treatment options. For example, the risk "A7 LDCC IT Systems" has the highest risk level of 81 but is assigned a "Reduce Likelihood" treatment, while the lower-risk "A10 Phones - Desk" is assigned a "Share" treatment, indicating non-compliance

with the standard. These inconsistencies should be rectified to ensure the process's integrity and effectiveness.

4. **Statement of Applicability (Case Study Document D14):**
   The Statement of Applicability in the case study determines and justifies the necessary controls to address information security risks, as required by ISO/IEC 27001:2022, Clause 6.1.3. It clearly outlines the selected controls and their applicability to the organization's context. While the document appears comprehensive, it should be regularly reviewed and updated to align with changes in the risk landscape and the organization's objectives. However, the case study reveals instances of non-compliance, such as the exclusion of control "A10 Phones - Desk" without providing a clear rationale, which does not fully adhere to the standard's requirements.

5. **Backup Log (Case Study Document D24):**
   The backup log in the case study provides evidence of the organization's implementation and maintenance of a backup process, aligning with ISO/IEC 27001:2022, Clause 8.1, and ISO/IEC 27002:2022, Control 8.13. It serves as a record of backup activities, demonstrating the organization's commitment to ensuring the availability and integrity of its information assets. While the backup log appears well-maintained, with all systems marked as "Complete" for the week of 01/09/20XX, there is no evidence of regular testing of the backup process's effectiveness. To ensure reliability and full compliance with the standards, the organization should focus on regularly testing the backup process.

References

Berry, V. (2022, March 11). *The Three-Year ISO certification cycle explained*. british-assessment.co.uk. https://www.british-assessment.co.uk/insights/the-3-year-certification-cycle-explained/

ISO 19011:2018. (2018, July). ISO. https://www.iso.org/standard/70017.html

ISO/IEC 17021-1:2015. (2016, December 1). ISO. https://www.iso.org/standard/61651.html

ISO/IEC 27001:2022. (2022, October). ISO. https://www.iso.org/standard/27001

ISO/IEC 27002:2022. (2022, March 1). ISO. https://www.iso.org/standard/75652.html

ISOQAR. (2024, January 24). ISO *9001 Audit Process explained | ISOQAR*. https://isoqar.com/iso-standards/iso-9001/audit/

LDCC Case Study. (n.d.). Mimeo Digital. Retrieved May 16, 2024, from https://bsi.mimeo.digital/BSI/a9b74f73-b20a-42d0-b22f-dffafdbc4157/content

RiskOptics. (2023, October 30). *What is an ISO Surveillance Audit?* https://reciprocity.com/resources/what-is-an-iso-surveillance-audit/