ISO 27001:2022 Internal Audit

|  |  |
| --- | --- |
| **Title of Audit** |  |
| **Date of Audit** |  |
| **Audit Author/Lead Auditor** |  |
| **Department/Organisation Unit** |  |
| **Audit Period** |  |
| **Version/Revision Number** |  |
| **Approval (if applicable)** |  |
| **Distribution List** |  |

Contents

[Executive Summary 2](#_Toc156830117)

[Major Observations 2](#_Toc156830118)

[Gaps to ISO 27001:2022 4](#_Toc156830119)

[Recommendations 5](#_Toc156830120)

[Conclusion 5](#_Toc156830121)

[Audit Findings 5](#_Toc156830122)

[Summary of Audit Approach 5](#_Toc156830123)

[Mandatory Documents 6](#_Toc156830124)

[Non-Mandatory Documents 9](#_Toc156830125)

[ISO 27001:2022 Clauses 13](#_Toc156830126)

[Clause 4 – The Context of the Organisation 13](#_Toc156830127)

[Clause 5 – Leadership & Commitment 15](#_Toc156830128)

[Clause 6 – Planning 17](#_Toc156830129)

[Clause 7 – Support 20](#_Toc156830130)

[Clause 8 – Operation 23](#_Toc156830131)

[Clause 9 – Performance Evaluation 25](#_Toc156830132)

[Clause 10 – Improvement 27](#_Toc156830133)

# Executive Summary

The following ISO 27001:2022 Internal Audit was conducted in January 2024. The audit, conducted by [Insert Name] and approved by [Insert Name, Role & Company], aimed to evaluate the effectiveness and compliance of the organisation’s Information Security Management System (ISMS) with ISO 27001:2022 standards.

## Major Observations

The audit revealed a committed approach towards establishing and implementing an ISMS framework aligned with ISO 27001:2022 requirements. Notable strengths include the establishment of a comprehensive information security policy, a risk assessment methodology, documented audits, and management reviews indicating a structured approach to information security management.

However, the audit identified several areas requiring attention to meet ISO 27001:2022 standard fully:

1. **Scope of the ISMS**: A significant gap was noted as the absence of a formally documented ISMS scope detailing the boundaries, applicability, and considerations of internal/external issues and interested parties.
2. **Statement of Applicability (SoA)**: The Statement of Applicability (SOA) is a core document within the ISO 27001:2022 framework that outlines which of the standard’s security controls are relevant and being implemented by an organisation, detailing how each is applied to manage specific security risks. The lack of a completed SoA listing chosen controls, their reasons for selection, and their implementation status presents a gap in demonstrating the ISMS’s comprehensive coverage against the ISO standard.
3. **Information Security Objectives**: The audit found that while objectives are referred to within the Information Security Policy, they are not explicitly defined or linked to specific functions and levels, nor is there clarity on the objectives for 2024.
4. **Monitoring and Measurement**: There is an absence of specific metrics for monitoring and measuring the ISMS’s performance, hindering the ability to evaluate effectiveness comprehensively.
5. **Employee Engagement and Feedback**: Processes for gathering and incorporating employee feedback on information security and channels for reporting security concerns are not adequately detailed.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Clause Group | Yes | No | Partial | Comments |
| 4. Context of the Organisation | 1 | 4 | 3 | Identified gaps in documentation and understanding of internal/external issues. |
| 5. Leadership & Commitment | 6 | 0 | 2 | Strong leadership demonstrated but needs more explicit documentation on integration and communication. |
| 6. Planning | 7 | 3 | 3 | Good risk management but lacks clear objectives and updates on legal compliance processes. |
| 7. Support | 6 | 2 | 6 | Adequate resources and awareness, yet improvements needed in feedback mechanisms and evaluation of resources. |
| 8. Operation | 8 | 0 | 6 | Effective incident management and operational controls, though regular reviews and updates are necessary. |
| 9. Performance Evaluation | 2 | 1 | 4 | Needs clearer metrics for monitoring and a more formal internal audit process. |
| 10. Improvement | 2 | 0 | 4 | Evident commitment to improvement but lacks formalised processes and documentation for continual improvement and corrective actions effectiveness evaluation. |

## Gaps to ISO 27001:2022

The audit identified several gaps in documentation, planning, and engagement that need addressing to fully comply with ISO 27001:2022 standards:

* **Documentation Gaps**: Including the ISMS scope, SoA, and specific metrics for monitoring and measurement.
* **Strategic Planning Improvements**: The clear definition and communication of information security objectives.
* **Engagement and Feedback Mechanisms**: There is a need for structured processes to engage employees and stakeholders in the ISMS’s continual improvement.

## Recommendations

To bridge these gaps, TechSolution.inc is advised to undertake the following actions:

1. **Formalise the ISMS Scope**: Develop and document a clear scope of the ISMS that reflects TechSolution.inc internal and external context, including all applicable requirements from interested parties.
2. **Complete the Statement of Applicability**: Clearly list and justify the inclusion or exclusion of controls within the ISMS and document their implementation status.
3. **Define and Communicate Objectives**: Establish specific, measurable information security objectives at all relevant organisational levels and link them to the ISMS’s overall goals.
4. **Implement Specific Monitoring Metrics**: Develop and document specific metrics to monitor and measure the ISMS’s performance effectively, facilitating targeted improvements.
5. **Enhance Engagement and Feedback Processes**: Establish formal mechanisms for engaging employees and stakeholders, including processes for gathering and acting on feedback and security concerns.

## Conclusion

While TechSolution.inc demonstrates a solid commitment to information security and has made significant progress in aligning with ISO 27001:2022 standards, addressing the identified gaps is essential for achieving full compliance and enhancing the ISMS’s overall effectiveness. Implementing the recommended actions will address current deficiencies and strengthen the organisation’s information security posture and continuous improvement process.

# Audit Findings

## Summary of Audit Approach

This audit is crucial for evaluating the effectiveness of the Information Security Management System (ISMS) and ensuring compliance with the ISO 27001:2022 standard. This comprehensive review will help identify areas of strength and opportunities for improvement in TechSolution.incinformation security practices.

The audit assesses various aspects of the ISMS across the different clauses, ranging from the organisation’s context and leadership commitment to operation, performance evaluation, and continual improvement. Each question in this audit is designed to probe the effectiveness and compliance of the ISMS with the ISO 27001:2022 standard.

For each question, a finding will be recorded using the following categories:

* **Met**: This indicates full compliance with the specific clause or control.
* **Not Met**: Signifies a clear non-compliance or failure to meet the standard’s requirements.
* **Partially Met**: Indicates some level of compliance but with noticeable gaps or inconsistencies.
* **Opportunity for Improvement**: Identifies areas that, while compliant, have potential for further improvement.
* **Not Applicable**: Used when a clause or control is irrelevant to our organisation’s context.
* **Observation**: Notes any significant points that do not constitute non-compliance but are worth recording.

Each finding should be supported with evidence or observations that justify the chosen category with clear, specific, and objective feedback for each finding. This approach ensures transparency and helps the organisation make informed decisions to enhance its information security posture.

The results of this audit will play a vital role in driving continual improvements in the ISMS and maintaining organisational commitment to information security.

## Mandatory Documents

The following documents are considered mandatory within the ISO 27001:2022 standard.

|  |
| --- |
|  |
| **Document** | **Description** | **Clause Reference** | **Present (Yes/No)** | **Notes/Comments** |
| Scope of the ISMS | Defines the scope of the ISMS, including boundaries and applicability. | 4.3 | No | Architecture diagram of the technology stack.  No scoping document clearly articulates the scope of the ISMS, the regulatory needs, interested stakeholders, etc.  **Action**: Create a Scope document before the ISO 27001 application. |
| Information Security Policy | Outlines the organisation’s approach to information security. | 5.2 | Yes | TechSolution.inc\_Information\_Security\_Policy\_20231128 in place. |
| Risk Assessment Methodology | Describes how information security risks are identified, assessed, and prioritised. | 6.1.2 | Yes | TechSolution.inc\_Risk\_Treatment\_Methodology\_20231128 |
| Statement of Applicability (SoA) | Lists the chosen controls, reasons for their selection, and implementation status. | 6.1.3 (d) | No | **Action**: Statement of Applicability to be completed. |
| Information Security Risk Assessment Results | Documents the results of the risk assessments. | 8.2 | Yes | Risk log (TechSolution.inc\_Risk\_Register\_20231120) includes summary of risks, likelihood and impacts. |
| Information Security Risk Treatment Plan | Details how identified risks are managed and mitigated. | 6.1.3 (e) | Yes | Several risk treatment plans for each of the risks TechSolution.inc has identified over a risk threshold.  Examples;  TechSolution.inc\_RTP\_3rd\_Party\_Supply\_Chain\_Disruption\_20231128.docx  TechSolution.inc\_RTP\_Denial\_of\_Service\_Attacks\_20231128.docx  TechSolution.inc\_RTP\_External\_Cyber\_Attack\_20231128.docx |
| Objectives for Information Security | Specifies the information security objectives at relevant functions and levels. | 6.2 | No | Objectives are referred to in the Info Sec Policy (TechSolution.inc\_Information\_Security\_Policy\_20231128), but the link is missing.  The December steering group meeting minutes have actions, but the objectives for 2024 are unclear.  **Action**: Define the 2024 Objectives for Information Security. |
| Evidence of Competence | Records of skills, education, training, and experience of personnel. | 7.2 | Yes | * TechSolution.inc\_Onboarding\_Training\_Matrix\_20231010.xlsx * HR Breathe system is used to track training and awareness.   **Action**: (OFI) Ensure a clear register of who has had GDPR training & when and who has had system training. Evidence should support that staff have been trained to access secured tools, equipment, areas, pipeline deployment, routers, etc. |
| Monitoring and Measurement Results | Documentation of monitoring and measurement of ISMS performance. | 9.1 | No | **Action**: TechSolution.inc should implement key KPIs around the ISMS and report them to the Information Steering Group, demonstrating how the ISMS is performing. E.g.   * % Staff employees who have undertaken GDPR training. * # Security-related incidents in the period. * # Of attempted breaches identified by an intruder detection system (IDS) |
| Internal Audit Program | Details about the audit program, including plans, schedules, and methods. | 9.2 | Yes | It is clear that auditing is taking place, both internally and externally, but TechSolution.inc needs to define the frequency, method, etc, of their internal audit programme in the future.  Action : (OFI) TechSolution.inc to define an internal audit methodology and schedule that routinely takes place at least annually to ensure standards are maintained and areas of addressment are identified. |
| Internal Audit Reports | Reports from conducted internal audits. | 9.2 | Yes | This document, along with other audit documents from January 2023, is evidence of an audit procedure.  1\_18\_**Audit\_BRS** - Information Security Assessment REPORT - FINAL v1.0 **18012023**.pdf  1\_18\_**Audit\_BRS** - Information Security EXEC REPORT - FINAL v1.0 **18012023**.pdf  1\_8\_Bulletproof - TechSolution.inc Penetration Test Report v1.0\_2019.pdf (**audit from 2019)**  1\_5\_Penetration Testing Report 2023 - PT50589-5219.pdf (**audit from 2023** – showing progression) |
| Results of the Management Review | Documentation of the management reviews of the ISMS. | 9.3 | Yes | 1\_6\_Information Security Steering Group **Meeting\_Minutes**\_20231130.pdf |
| Results of Corrective Actions | Evidence and results of corrective actions taken. | 10.1 | Yes | Evidence of addressing security vulnerabilities.  This will be developed as TechSolution.inc matures and has operational data to feed into the Plan–Do–Check–Act process.  **Action**: (OFI) TechSolution.inc to ensure it maintains a clear log of nonconformities and corrective actions taken (e.g. the findings from this audit and how any gaps were addressed). |

## Non-Mandatory Documents

The following documents are not considered mandatory within the ISO 27001:2022 standard but provide additional benefits and are common ways to address some clauses.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Document** | **Description** | **Benefit** | **Clause Reference** | **Present (Yes/No)** | **Notes/Comments** |
| Information Security Roles and Responsibilities | Detailed roles and responsibilities related to information security. | Clarifies accountability and ensures responsibilities are understood. | 5.3, 7.1, 7.2 | Yes | **Action**: OFI - TechSolution.inc should document ISMS roles & responsibilities in more detail than is outlined in the Info Sec Policy, as per the defined action in the Risk Treatment Plan for Information Security Governance. |
| Information Security Procedures | Specific procedures for managing and maintaining security controls. | Provides clear instructions for consistent implementation of controls. | 6.1.2, 8.1, A.12.1.1 | Yes | **Action**: OFI - TechSolution.inc should maintain a log of procedures for easy reference. |
| Asset Inventory | Comprehensive list of information assets under the ISMS scope. | Helps in risk assessment and management by identifying critical assets. | 8.2, A.8.1.1 | Yes | **Action**: OFI – TechSolution.inc should define the assets they are protecting as part of the ISMS scoping and then maintain a log of all assets, which in turn states where the live list of assets can be found. For example, the log might direct the reader to an asset management tool for identifying all laptops and desktops in scope. |
| Access Control Policies | Policies regarding access to information and systems. | Ensures appropriate access levels and protects against unauthorised access. | A.9 | Yes | Related policies / documents;   * TechSolution.inc\_Access\_Control\_Policy\_20231201.docx * TechSolution.inc\_Access\_Control\_Matrix\_20231120.xlsx * TechSolution.inc\_Admin\_Access\_Policy\_20231109.docx * TechSolution.inc\_Data\_Access\_Policy\_20231120.docx |
| Operational Procedures and Guidelines | Step-by-step guidelines for daily operations. | Facilitates consistency and efficiency in operational tasks. | 8.1, A.12.1.1 | OFI | Guidelines for handling data breaches seen.  Examples: Procedures for configuring and maintaining secure systems, steps for performing regular security checks, and protocols for updating software and systems.  Evidence:   * Step-by-step process documents and checklists for specific operational tasks. * Logs or records showing these procedures being carried out. * Training materials and records are specific to operational tasks. * Incident response records demonstrate the application of these procedures. |
| Incident Response Plan | Detailed plan for managing information security incidents. | Ensures a structured and efficient response to security incidents. | A.16.1.1, A.16.1.4 | Yes | * **Incident & Major Incident Processes**: Presented in a PowerPoint document (**TechSolution.inc\_Incident\_&\_Major\_Incident\_Processes\_20231128.pptx**), which likely outlines the steps to be followed in case of an incident, indicating a structured plan for incident response. * **Major Incident Report Template**: Available in a Word document (**TechSolution.inc\_Major\_Incident\_Report\_Template\_20231128.docx**), providing a format for reporting major incidents, which is crucial for documentation and further analysis. * **Cyber Security Incident Response Plan**: Referenced as part of the evidence provided (**TechSolution.inc\_Cyber\_Security\_Incident\_Response\_Plan\_20231128**), directly indicating that there is a specific plan dedicated to responding to cyber security incidents. * **Insurance Documents**: Including an invoice from CFC Underwriting Ltd (**1\_15\_Insurance\_CFC\_Underwriting\_Ltd\_Invoice\_20230831.pdf**), a policy document (**1\_15\_Insurance\_CFC\_Underwriting\_Ltd\_Policy\_20230831.pdf**), and technology key facts (**1\_15\_Insurance\_CFC\_Underwriting\_Ltd\_Technology\_Key\_Facts\_20230831.pdf**). These documents suggest that TechSolution.inc has also prepared for incident response through insurance that likely includes coverage for incident response services. * **Incident Response & Forensics Document**: By Bulletproof (**1\_15\_Incident Response & Forensics (BP UK).pdf**), indicating that they have external support for incident response and forensics, which is a critical part of handling incidents effectively. |
| Business Continuity Plans | Plans for maintaining and restoring business processes in the event of a disruption. | Critical for business resilience and continuity in adverse situations. | A.17.1.1, A.17.1.2 | Yes | While not a BCP, there is a solid disaster recovery plan;  TechSolution.inc\_Disaster\_Recovery\_Plan\_20231109 |
| Supplier Security Agreements | Agreements outlining security requirements for suppliers and third parties. | Secures the supply chain and extends security practices beyond the organisation. | A.15.1.1, A.15.1.2 | OFI | There is a Supplier Security Policy evidenced, but it is recommended that the next step is to collate supplier agreements and track any obligations with regard to information security (e.g., GDPR handling).  TechSolution.inc\_Supplier\_Security\_Policy\_20231128 |
| Information Classification and Handling Policies | Guidelines on classifying, handling, and securing information based on its sensitivity. | Helps in the appropriate protection of data according to its classification. | A.8.2.1, A.8.2.2, A.8.2.3 | Yes | * **Information Security Policy**: Mention of the Information Security Policy (**TechSolution.inc\_Information\_Security\_Policy\_20231128.docx**) suggests a framework for managing and protecting information assets, which typically includes guidelines for information classification and handling. * **Data Access Policy**: The Data Access Policy (**TechSolution.inc\_Data\_Access\_Policy\_20231120.docx**) likely covers aspects of how data is accessed and handled within TechSolution.inc. This would inherently involve some level of classification to determine who has access to what types of information. * **Data Retention Policy**: The Data Retention Policy (**TechSolution.inc\_Data\_Retention\_Policy\_20231120.docx**) addresses how long different types of data should be kept, which implies a need for classifying data to apply appropriate retention schedules. Data classification is crucial for understanding the value and sensitivity of data, thereby informing its retention. |
| Privacy Policies | Documents detailing how personal data is collected, used, and protected. | Ensures compliance with data protection regulations and respects privacy rights. | A.18.1.4 | OFI | There is a privacy policy for data collected via the Website ([https://TechSolution.inc.co.uk/privacy-policy/](https://helpthemove.co.uk/privacy-policy/)).  However, a more comprehensive Data Protection Policy is recommended.  **Action**: Draft and confirm a Data Protection Policy. |
| Training and Awareness Records | Records of security training and awareness programs for employees. | Demonstrates commitment to staff education and security awareness. | 7.2, A.7.2.2 | OFI | TechSolution.inc\_Onboarding\_Training\_Matrix\_20231010.xlsx  **Action**: Maintain accurate records for each staff member and their most recent training & awareness session. |
| Audit Trails and Logs | Records of system and user activities for monitoring and investigation purposes. | Facilitates the detection of anomalies and supports forensic activities. | A.12.4.1, A.12.4.3 | Yes | **Protective Monitoring Framework**: TechSolution.inc utilises Google Workspace Admin and Security Centre to detect and alert malicious threats and incidents.  **Use of Rollbar and AWS Services**: The mention of using Rollbar for log monitoring, along with AWS CloudWatch and AWS CloudTrail, indicates that TechSolution.inc has implemented tools specifically designed for logging and monitoring systems and user activities. Rollbar is a cloud-based error monitoring service that captures and aggregates errors, providing insights into issues occurring in real time. AWS CloudWatch and CloudTrail enable the monitoring of AWS environments, with CloudTrail focused explicitly on logging and retaining account activity related to actions across the AWS infrastructure.  **Incident Management Processes**: The detailed incident management processes, which likely involve investigating security incidents, would require audit trails and logs to trace the actions leading up to an incident, understand its scope, and remediate effectively. |
| Change Management Documentation | Records of changes to the ISMS, including impact assessments. | Ensures controlled and reviewed changes to the system, minimising risks. | A.12.1.2 | Yes | There is evidence of a Jira Change Management Process. |

## ISO 27001:2022 Clauses

### Clause 4 – The Context of the Organisation

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Clause Ref | Heading | Question | Finding | Evidence / Comments |
| 4.1 | Understanding the Organisation and Its Context | What external and internal issues relevant to information security are identified, and how are they documented and reviewed? | Partial | No specific documentation on external and internal issues. TechSolution.inc needs to document and review these as part of their ISMS. |
| 4.1 | Understanding the Organisation and Its Context | How does the organisation determine the impact of these issues on its information security management system (ISMS)? | Partial | The impact of external and internal issues on the ISMS is not explicitly documented. TechSolution.inc should assess and document how these issues affect their ISMS. |
| 4.2 | Understanding the Needs and Expectations of Interested Parties | Has the organisation identified and documented interested parties relevant to the ISMS and their requirements? | No | No evidence was provided regarding the identification and documentation of interested parties and their requirements. This needs to be addressed. |
| 4.2 | Understanding the Needs and Expectations of Interested Parties | How does the organisation monitor and review information about these interested parties and their requirements? | No | There is no information on how TechSolution.inc monitors and reviews the needs and expectations of interested parties. This process must be established and documented as part of the organisational ISMS context. |
| 4.3 | Determining the Scope of the Information Security Management System | Is the scope of the ISMS defined, documented, and justified in terms of external/internal issues and requirements of interested parties? | No | The scope document is missing. The organisation needs to create a document defining the ISMS scope, considering internal/external issues and interested parties’ requirements. |
| 4.3 | Determining the Scope of the Information Security Management System | Does the scope consider all physical and digital boundaries and information security attributes? | No | Without a documented ISMS scope, it’s unclear if all physical and digital boundaries and information security attributes are considered. This needs to be explicitly addressed in the scope document. |
| 4.4 | Information Security Management System | Has the organisation established, implemented, maintained, and continually improved an ISMS per the requirements of ISO 27001:2022? | Yes | TechSolution.inc has taken steps towards establishing and implementing an ISMS, as evidenced by the various policies, risk assessments, and treatment plans provided. Continual improvement processes need to be more clearly documented. |
| 4.4 | Information Security Management System | How does the organisation evaluate the performance and effectiveness of the ISMS? | Partial | Some monitoring and measurement tools are in place (e.g., Google Workspace Admin and Security Centre, AWS CloudWatch), but a comprehensive evaluation of the ISMS’s performance and effectiveness, including defined KPIs and regular management reviews, is not clearly documented. |

|  |  |
| --- | --- |
|  | Recommendations  * **Context of the ISMS**: Develop and document a process for identifying and reviewing external and internal issues and the needs and expectations of interested parties. This should be a part of the ISMS documentation and reviewed regularly. * **Scope Definition**: Create a comprehensive scope document for the ISMS that includes all physical and digital boundaries and considers the information security attributes relevant to TechSolution.inc. * **Performance**: Enhance the documentation on the continual improvement process and evaluation of the ISMS’s performance. Define KPIs and schedule regular management reviews to assess the ISMS’s effectiveness and identify areas for improvement. |

### Clause 5 – Leadership & Commitment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Clause Ref | Heading | Question | Finding | Evidence / Comments |
| 5.1 | Leadership and Commitment | How does top management demonstrate leadership and commitment to the ISMS? | Yes | Top management’s commitment is inferred through the initiation of ISO 27001:2022 preparation, including developing various policies and establishing an Information Security Steering Group. |
| 5.1 | Leadership and Commitment | What evidence is there of top management ensuring the integration of the ISMS requirements into business processes? | Partial | Evidence of integration is seen in the creation of information security policies and procedures that are part of business operations. However, detailed documentation on the integration process is not explicitly mentioned. |
| 5.1 | Leadership and Commitment | How does top management ensure that the resources needed for the ISMS are available? | Yes | The hiring of skilled personnel (e.g., Head of Engineering, Ruby Developers) and investment in security technologies (e.g., Digital Ocean, AWS) indicate that resources are allocated for the ISMS. Specific budget allocations or resource planning documents were not provided. |
| 5.1 | Leadership and Commitment | What actions are taken by top management to communicate the importance of effective information security management? | Yes | The establishment of an Information Security Steering Group and the documentation of security policies suggest communication efforts. However, examples of communication from top management (e.g., memos meetings) are not detailed. |
| 5.2 | Policy | Has the organisation established an information security policy that is appropriate to the purpose of the organisation? | Yes | The “TechSolution.inc\_Information\_Security\_Policy\_20231128” document evidences that an information security policy has been established and is aligned with the organisation’s objectives. |
| 5.2 | Policy | How is the information security policy communicated within the organisation and to interested parties? | Yes | The Info Sec policy is shared via the HR system, which evidences that staff have read the policy. |
| 5.3 | Organisational Roles, Responsibilities, and Authorities | Are information security roles, responsibilities, and authorities clearly defined, documented, and communicated? | Yes | Documentation and the establishment of the Information Security Steering Group suggest roles and responsibilities are defined and documented.  Policies reviewed outlined R&Rs, but a centralised summary of key roles has already been acknowledged as an improvement area. |
| 5.3 | Organisational Roles, Responsibilities, and Authorities | How does top management ensure that the responsibilities and authorities for roles relevant to information security are assigned and communicated? | Partial | While roles are assigned, as evidenced by the various documented responsibilities and TechSolution.inc structure, explicit evidence on how top management ensures and communicates these assignments is not detailed. |

|  |  |
| --- | --- |
|  | Recommendations  * **Leadership Commitment**: Enhance documentation and provide explicit evidence of how top management demonstrates leadership and commitment beyond policy development. This could include records of meetings, communications, and decisions related to the ISMS. * **Communication of Policies**: Ensure the information security policy is actively communicated both internally and externally, with records of how and when this communication takes place. * **Explicit Documentation**: Provide detailed documentation on integrating ISMS requirements into business processes and how the effectiveness of these integrations is measured and improved over time. * **Clarify Communication Methods**: Detail the methods used to communicate roles, responsibilities, and authorities for information security within the organisation to ensure clarity and understanding among all stakeholders. |

### Clause 6 – Planning

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Clause Ref | Heading | Question | Finding | Evidence / Comments |
| 6.1 | Actions to Address Risks and Opportunities | How does the organisation identify and assess information security risks and opportunities? | Yes | TechSolution.inc has a risk assessment framework as evidenced by “TechSolution.inc\_Risk\_Treatment\_Methodology\_20231128”, indicating a process for identifying and assessing risks. Opportunities identification was not explicitly mentioned. |
| 6.1 | Actions to Address Risks and Opportunities | What methods are used to plan and implement actions to address these risks and opportunities? | Yes | Risk treatment plans such as “TechSolution.inc\_RTP\_3rd\_Party\_Supply\_Chain\_Disruption\_20231128.docx” evidence methods for planning and implementing actions to address risks. No specific methods for addressing opportunities are documented, e.g. a SWOT analysis. |
| 6.1.1 | Information Security Risk Assessment | Is there a documented process for information security risk assessment? | Yes | The risk assessment methodology document indicates a structured process for assessing information security risks. |
| 6.1.1 | Information Security Risk Assessment | How does the organisation ensure the information security risk assessment is consistent, valid, and comparable? | Yes | The documented risk treatment methodology implies a consistent approach, though specific validation and comparison methods are not detailed. |
| 6.1.2 | Information Security Risk Treatment | Has the organisation established and applied an information security risk treatment process? | Yes | The existence of risk treatment plans for various identified risks demonstrates that a risk treatment process is in place. |
| 6.1.2 | Information Security Risk Treatment | How are decisions regarding risk treatment options documented and implemented? | Yes | Risk treatment plans document decisions on risk treatment options. Implementation details are indicated in the plans, but evidence of the actual implementation process is not provided. |
| 6.1.2 | Information Security Risk Treatment | Is there a method for monitoring the effectiveness of the risk treatment plan? | Partial | Risk treatment plans are in place and methods for monitoring their effectiveness are detailed in the provided information. However, time is required to demonstrate progress against the plans. |
| 6.1.3 | Information Security Risk Management | How does the organisation ensure ongoing monitoring and re-evaluation of information security risks? | Partial | Ongoing monitoring and re-evaluation are documented through the risk management framework. |
| 6.1.3 | Information Security Risk Management | Are there processes in place for adapting the risk treatment plan in response to changes in the risk landscape? | Partial | The documentation suggests an awareness of the need to adapt risk treatment plans, but explicit processes for responding to changing risks are not described. |
| 6.1.3 | Compliance with Legal and Regulatory | How does the organisation ensure compliance with applicable legal, regulatory, and contractual requirements in information security? | Yes | The information security policy and GDPR training indicate efforts to ensure compliance, but a comprehensive compliance process is not detailed. |
| 6.1.3 | Compliance with Legal and Regulatory | Are there processes to stay updated with changes in relevant laws and regulations? | No | There are no specific processes for staying updated with legal and regulatory changes. |
| 6.2 | Information Security Objectives and Planning to Achieve Them | Are information security objectives established at relevant functions and levels? | No | Information security objectives are referred to in the policy document but not explicitly defined or linked to specific functions and levels. |
| 6.2 | Information Security Objectives and Planning to Achieve Them | How are these objectives measured, monitored, communicated, and updated? | No | There is no evidence of how information security objectives are measured, monitored, communicated, and updated. |

|  |  |
| --- | --- |
|  | Recommendations  * **Identify and Document Opportunities**: Alongside risks, opportunities for improvement in information security should also be identified, assessed, and documented. * **Validate and Compare Risk Assessments**: Implement and document specific methods to validate and compare risk assessments to ensure consistency and accuracy. * **Monitor Effectiveness of Risk Treatment Plans**: Establish and document methods for regularly monitoring the effectiveness of risk treatment plans, including specific metrics and review intervals. * **Update Risk Management Processes**: Document processes for the ongoing monitoring, re-evaluation, and adaptation of risk treatment plans in response to the changing risk landscape. * **Legal and Regulatory Compliance**: Develop a documented process to regularly review and stay updated with changes in applicable legal, regulatory, and contractual requirements. * **Define and Communicate Objectives**: Clearly define information security objectives at relevant functions and levels and document how these objectives are measured, monitored, communicated, and updated. |

### Clause 7 – Support

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Clause Ref | Heading | Question | Finding | Evidence / Comments |
| 7.1 | Resources | Has the organisation determined and provided the resources to establish, implement, maintain, and continually improve the ISMS? | Yes | The hiring of specialised personnel and investment in security technologies suggest that TechSolution.inc has determined and allocated resources for the ISMS. Details on the exact resource allocation process were not provided. |
| 7 | Technology and Process Alignment | How are information security technologies and processes aligned with the ISMS? | Yes | Digital Ocean, AWS, and security practices like penetration testing indicate alignment of technologies and processes with the ISMS objectives. |
| 7 | Technology and Process Alignment | Are security technologies and processes reviewed and updated in accordance with the ISMS? | Partial | While there is evidence of the use of security technologies, explicit documentation on the periodic review and updating of these technologies and processes in line with ISMS objectives is not available. |
| 7.1 | Resources | How are these resources evaluated and adjusted as necessary? | Partial | The documentation suggests resource allocation for the ISMS, but there’s no detailed evidence yet on how resources are evaluated and adjusted over time. |
| 7.2 | Competence | How does the organisation ensure that personnel performing work affecting the ISMS are competent? | Yes | The provision of CVs for key personnel and references to specific training (e.g., GDPR training) indicate efforts to ensure competence. However, a systematic process for ensuring competence across all personnel affecting the ISMS is not detailed. |
| 7.2 | Competence | What actions are taken to acquire the necessary competencies and evaluate the effectiveness of these actions? | Partial | The hiring of experienced personnel and conducting training sessions are actions taken, but the evaluation of the effectiveness of these actions is not documented. |
| 7.3 | Awareness | Are employees aware of the information security policy, their roles and responsibilities, and the importance of information security? | Yes | Documentation of policies and references to training sessions suggest employee awareness. However, specifics on how this awareness is measured are not provided. |
| 7.3 | Awareness | How is this awareness maintained and updated? | Partial | Training sessions indicate an effort to maintain awareness, but there’s no evidence of how this awareness is systematically updated or measured over time. |
| 7.3 | Awareness | How does the organisation gather and incorporate employee feedback regarding information security? | No | There is no mentioned process for gathering or incorporating employee feedback on information security within the provided documentation. |
| 7.3 | Awareness | Are there channels for employees to report security concerns or suggestions? | Partial | While security incident management processes suggest channels for reporting, specific mechanisms for employee feedback on security concerns or suggestions are not documented. |
| 7.4 | Communication | What processes are in place for internal and external communication relevant to the ISMS? | Partial | Internal communication is inferred through training and policy dissemination, but processes for external communication relevant to the ISMS are not clearly documented. |
| 7.4 | Communication | How is the effectiveness of these communication processes evaluated? | No | No evidence or methodology for evaluating the effectiveness of communication processes was provided. |
| 7.5 | Documented Information | How does the organisation create, update, and control documented information required for the ISMS? | Yes | Various policies and documented processes suggest mechanisms for creating, updating, and controlling documentation, though specifics on control mechanisms are not detailed. |
| 7.5 | Documented Information | Are there procedures for managing records (creation, storage, transmission, protection, etc.)? | Yes | Documented policies imply procedures for managing records, including storage and protection, but the details on creation, transmission, and specific control procedures could be more explicitly mentioned. |

|  |  |
| --- | --- |
|  | Recommendations  * **Systematic Review of Security Technologies:** Implement and document a periodic review process for security technologies and processes to ensure they remain aligned with ISMS objectives and current threats. * **Evaluation of Resource Allocation**: Develop a formal process for evaluating and adjusting resources dedicated to the ISMS to ensure they remain adequate over time. * **Effectiveness of Competence Measures**: Establish and document methods for evaluating the effectiveness of training and competence-building activities. * **Employee Feedback Mechanisms**: Create formal channels for employees to provide feedback on information security matters and document how this feedback is incorporated into the ISMS. * **Communication Effectiveness**: Develop and document processes for evaluating the effectiveness of both internal and external communication related to the ISMS. * **Document Control**: Enhance documentation around the creation, update, and control of documented information, including specific procedures for managing records throughout their lifecycle. |

### Clause 8 – Operation

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Clause Ref | Heading | Question | Finding | Evidence / Comments |
| 8 | Incident Management | How does the organisation manage and respond to information security incidents? | Yes | TechSolution.inc has an Incident Response Plan as outlined in the provided documents (e.g., TechSolution.inc\_Incident\_&\_Major\_Incident\_Processes\_20231128.pptx), indicating structured management and response to information security incidents. |
| 8 | Incident Management | Are incident response procedures regularly tested and updated? | Partial | There is evidence of an incident response plan, but explicit details on the regular testing and updating of these procedures are not provided. |
| 8.1 | Operational Planning and Control | How does the organisation plan, implement, and control the processes needed to meet information security requirements? | Yes | TechSolution.inc demonstrates planning, implementation, and control through documented policies and procedures, including access control and risk treatment plans. |
| 8.1 | Operational Planning and Control | Are these processes evaluated for effectiveness and efficiency? | Partial | There is an awareness of the need for evaluation, but explicit evidence or methodology for evaluating effectiveness and efficiency is not detailed. |
| 8.1 | Operational Planning and Control | How does the organisation manage information security within the supply chain? | Yes | Supplier security (e.g., TechSolution.inc\_Supplier\_Security\_Policy\_20231128), |
| 8.1 | Operational Planning and Control | Are suppliers and third-party service providers evaluated and monitored for information security? | Yes | The presence of a Supplier Security Policy suggests that suppliers and third-party service providers are evaluated and monitored, but the depth of these evaluations and monitoring processes is not fully detailed. |
| 8.2 | Information Security Risk Assessment | How are information security risks assessed in ongoing operations? | Yes | Ongoing risk assessments are indicated through the documentation of risk assessment methodologies and risk registers, suggesting a structured approach to assessing risks in operations. |
| 8.2 | Information Security Risk Assessment | What procedures are in place for periodic and event-driven reassessment of risks? | Yes | Risk reassessment procedures are documented. |
| 8.2 | Operation of Information Security | How are information security technologies and processes aligned with the ISMS? | Yes | Information security technologies and processes are aligned with the ISMS as indicated by the use of security technologies (AWS, Digital Ocean) and documented security procedures. |
| 8.2 | Operation of Information Security | Are security technologies and processes reviewed and updated in accordance with the ISMS? | Partial | There’s evidence of the use of security technologies and processes, but details on their regular review and updates in accordance with the ISMS are not explicitly mentioned. |
| 8.2 | Information Security Incident Management | How does the organisation manage and respond to information security incidents? | Yes | The organisation’s approach to managing and responding to incidents is documented in the Incident & Major Incident Processes, indicating structured incident management. |
| 8.2 | Information Security Incident Management | Are incident response procedures regularly tested and updated? | Partial | The presence of an incident response plan is noted, but the frequency and methodology for testing and updating these procedures are not explicitly documented. |
| 8.3 | Information Security Risk Treatment | How is the effectiveness of information security risk treatments monitored and reviewed? | Partial | TechSolution.inc has risk treatment plans, but specific details on how the effectiveness of these treatments is monitored and reviewed are not provided. |
| 8.3 | Information Security Risk Treatment | Are there processes in place for updating the risk treatment plan as necessary? | Partial | Risk treatment plans suggest a mechanism for updates, but the process for regularly updating these plans in response to changes or effectiveness evaluations is not detailed. |

|  |  |
| --- | --- |
|  | Recommendations  * **Incident Management:** Ensure regular testing and updates of incident response procedures are documented, including logs of drills or real incident analyses. * **Operational Control Evaluation:** Develop and document specific methods for evaluating the effectiveness and efficiency of operational planning and control processes. * **Supply Chain Security Management:** Enhance documentation on information security management within the supply chain, including detailed evaluation and monitoring processes for suppliers and third parties. * **Risk Assessment Procedures:** Clearly document the procedures for periodic and event-driven reassessment of risks to ensure they remain comprehensive and up-to-date. * **Technology and Process Reviews:** Establish and document regular review schedules for security technologies and processes to ensure alignment with the evolving ISMS and threat landscape. * **Risk Treatment Monitoring:** Implement and document methods for monitoring the effectiveness of risk treatments, including criteria for success and periodic review schedules. * **Risk Treatment Plan Updates:** Clearly define and document the process for regularly updating risk treatment plans, ensuring they adapt to changes in the risk landscape or effectiveness feedback. |

### Clause 9 – Performance Evaluation

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Clause Ref | Heading | Question | Finding | Evidence / Comments |
| 9.1 | Monitoring, Measurement, Analysis and Evaluation | How does the organisation monitor, measure, analyse, and evaluate information security performance and the effectiveness of the ISMS? | Partial | While specific metrics or methods were not detailed, TechSolution.incuse of various security tools (e.g., Google Workspace Admin, AWS CloudWatch) and documented policies suggest a framework for monitoring and evaluation exists. Explicit methods and metrics need to be clearly documented. |
| 9.1 | Monitoring, Measurement, Analysis and Evaluation | What metrics are used to measure the effectiveness of controls and the ISMS? | No | TechSolution.inc should define and document specific metrics for evaluating the effectiveness of controls and the overall ISMS. |
| 9.1 | Monitoring, Measurement, Analysis and Evaluation | How are these evaluation results documented and used to drive continual improvement? | Partial | The process of documentation and utilisation of evaluation results for continual improvement is implied through the presence of various policies and plans. However, explicit evidence of how these results drive continual improvement was not provided. |
| 9.2 | Internal Audit | Is an internal audit program established to verify conformity to ISO 27001:2022 requirements and the effectiveness of the ISMS? | Partial | TechSolution.inc has conducted internal audits, as evidenced by the audit reports provided (e.g., penetration testing reports, and information security assessment reports). This suggests an established audit program, but should be formalised and tracked. |
| 9.2 | Internal Audit | How does the organisation ensure the objectivity and impartiality of the audit process? | Partial | Using external parties for penetration testing implies an effort towards objectivity and impartiality in some audit activities. However, specifics on how internal audit objectivity is maintained are not detailed. |
| 9.2 | Internal Audit | Are internal audit results reported to relevant management, and are follow-up actions taken? | Yes | Audit reports and documented evidence of corrective actions suggest that results are reported to management and follow-up actions are implemented. Detailed processes or evidence of these actions’ effectiveness were not provided. |
| 9.3 | Management Review | Does top management periodically review the ISMS’s performance, including assessing opportunities for improvement and the need for changes? | Yes | The Information Security Steering Group’s involvement suggests a mechanism for top management review. |

|  |  |
| --- | --- |
|  | Recommendations  * **Define and Document Metrics:** Clearly define and document specific metrics for monitoring and measuring the effectiveness of information security controls and the ISMS. These metrics should be relevant, measurable, and aligned with TechSolution.incinformation security objectives. * **Systematic Evaluation Documentation:** Enhance the documentation process for evaluation results, explicitly linking these results to actions taken for continual improvement. This should include a structured approach for recording findings, decisions made, and tracking the implementation and effectiveness of improvement actions. * **Audit Objectivity and Impartiality:** Establish and document formal procedures to ensure the objectivity and impartiality of internal audits. This may include criteria for auditor selection, auditor independence, and handling conflicts of interest. |

### Clause 10 – Improvement

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Clause Ref | Heading | Question | Finding | Evidence / Comments |
| 10.1 | Continual Improvement of the ISMS | How does the organisation continually improve the ISMS’s suitability, adequacy, and effectiveness? | Partial | While specific strategies for continual improvement were not detailed, documented policies, risk treatment plans, and the implementation of an Information Security Steering Group suggest a framework is in place. Detailed processes or mechanisms for ensuring continual improvement are not explicitly documented. |
| 10.1 | Continual Improvement of the ISMS | What processes are in place to identify and implement opportunities for improvement? | Partial | TechSolution.inc shows evidence of identifying risks and implementing risk treatment plans, which could lead to improvement. However, a formalised process for identifying and implementing opportunities for continual improvement across the ISMS is not clearly outlined. |
| 10.2 | Nonconformity and Corrective Action | How are information security nonconformities identified, assessed, and managed? | Yes | An Incident & Major Incident Processes document indicates a process for managing nonconformities. However, outside of incident management, the specific process for identifying and assessing these is not detailed. |
| 10.2 | Nonconformity and Corrective Action | What is the process for implementing corrective actions and preventing recurrence? | Yes | Documentation of corrective actions in response to incidents and audit findings suggests a process is in place. The exact steps for implementing these actions and ensuring non-recurrence are implied but not explicitly outlined. |
| 10.2 | Nonconformity and Corrective Action | How does the organisation evaluate the effectiveness of corrective actions taken? | Partial | While corrective actions are mentioned, there’s no detailed evidence on how the effectiveness of these actions is evaluated post-implementation. This process needs to be documented and demonstrated. |
| 10.3 | Continual Improvement of the Information Security Management System | What strategies or mechanisms are in place for continually improving information security? | Partial | TechSolution.inc has engaged in activities such as risk assessments, internal audits, and policy updates, indicating a commitment to improvement. Specific strategies or mechanisms for continual improvement, such as feedback loops, performance metrics, or regular review cycles, are not clearly described. |

|  |  |
| --- | --- |
|  | Recommendations  * **Formalise Continual Improvement Processes:** Establish and document formal processes for the continual improvement of the ISMS, including how improvements are identified, prioritised, implemented, and reviewed for effectiveness. * **Document Nonconformity Management:** Clearly document the entire process for managing nonconformities, from identification and assessment to implementing corrective actions and preventing recurrence. Include roles, responsibilities, and timelines. * **Evaluate Corrective Actions:** Develop a method for evaluating the effectiveness of corrective actions, ensuring that these evaluations are documented and the findings are used to inform future actions. * **Strategies for Continual Improvement:** Define and document specific strategies or mechanisms for continual improvement of information security within TechSolution.inc. This could include setting specific improvement objectives, utilising feedback from internal and external audits, and leveraging technology or process innovations. * **Engagement and Feedback Mechanisms:** Enhance engagement with employees and other stakeholders to gather feedback on information security practices and the ISMS’s performance. Use this feedback as a basis for identifying and implementing improvements. |