ISO/IEC 27001:2022
ISO Gap Analysis

Firm:	Example Org Ltd.
Type:	ISO/IEC 27001:2022 Internal audit
Topic:	ISO Gap Analysis
Location(s):	1
Date Start:	2nd November 2024
Date Finish:	2nd November 2024

Commercial and Confidential
DeepFathom Ltd © 2024

Purpose of this Report

The report outlines key findings from a gap analysis audit, focusing on critical processes surrounding information and security across your management system.

A business management system serves as a structured approach employed by organisations to efficiently oversee operations and achieve specific objectives, resembling a well-organised set of processes guiding company operations.

This structured approach ensures seamless collaboration among various parts of the organisation, ensuring collective efforts are directed towards common objectives.

The evidence presented sheds light on how behaviour directly impacts risk, compliance, and business performance. This insight into your business operations empowers initiative-taking and well-informed decision-making, fostering overall business improvement.

The report visually represents the alignment between people's behaviour and your strategic or operational objectives, highlighting areas of emerging or active risk in achieving these objectives. The employed methodology seamlessly integrates traditional auditing methods with behavioural measurements, resulting in a comprehensive understanding of your business operations.

The results are shown against the following compliance requirements and performance indicators:

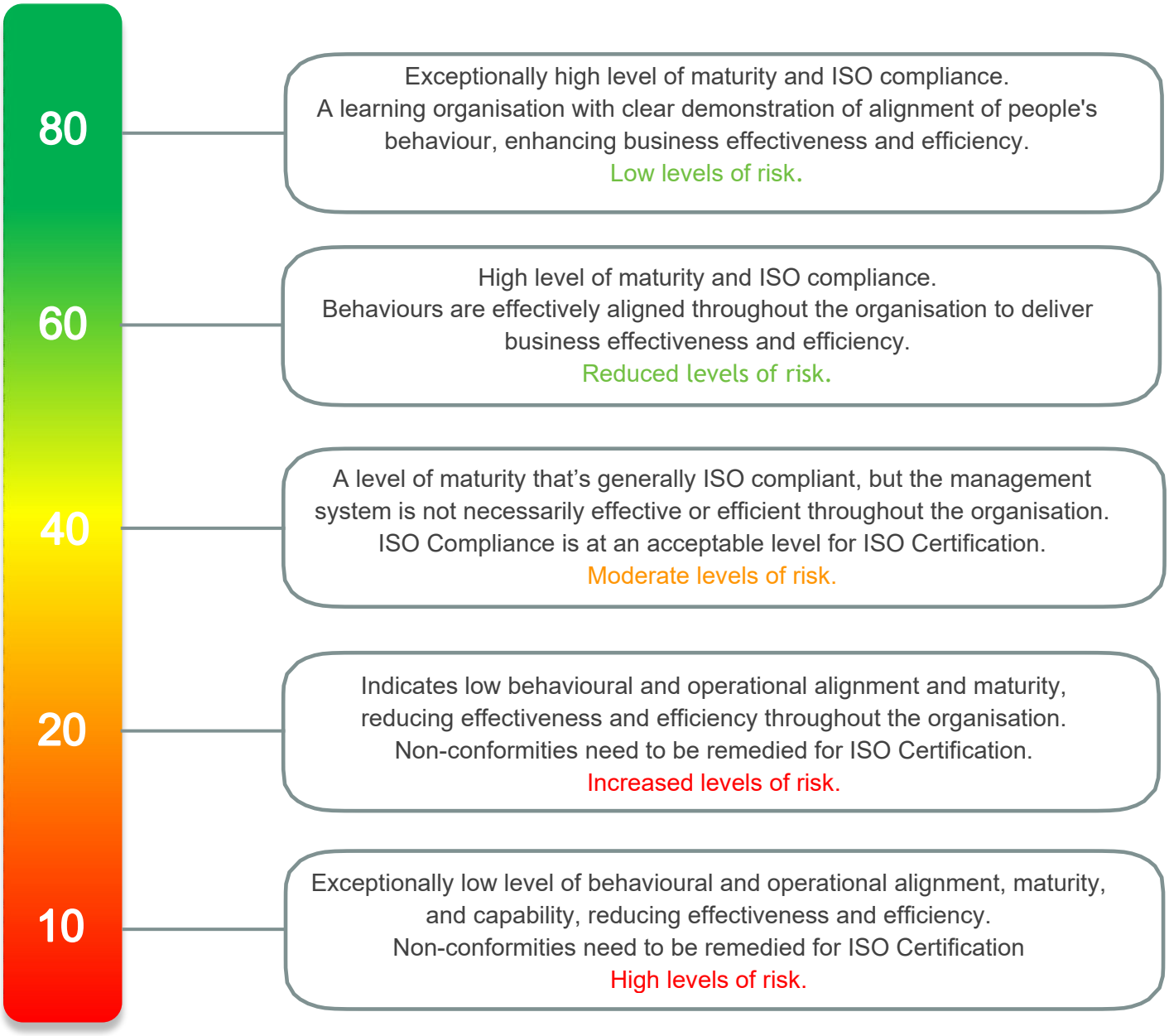
- ISO/IEC 27001:2022 Policies, documents, controls, and behaviours across management system processes.

Performance Risk Maturity Model

The objective evidence provided by participants is evaluated and assigned a score from 0 to 100.

The results are measured against drivers of performance or critical success factors by which the performance of a management system, process, or subject is managed.

By using the maturity risk index below, the report identifies specific areas within the organisation that necessitate attention and improvement. It allows for a targeted and strategic approach to enhance overall performance and stakeholder value.



ISO/IEC 27001:2022

Score Summary

Overall Score

50

The objective evidence provided by each participant/stakeholder is evaluated and assigned scores, these scores collectively form the overall maturity score. The diagram below illustrates the individual scores for each ISO clause requirement specified within the audit scope.

Explanation of ISO/IEC 27001:2022 Clauses

ISO 27001 is organized into a series of clauses that outline the requirements for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS). These clauses are critical for ensuring a structured and effective approach to information security. Here's a breakdown of the main clauses, their importance, and the consequences of low scores in audits:

42

4. Context of the Organisation

This clause focuses on organisation's determining internal and external factors that affect their ability to achieve intended performance and management system outcomes.

Clause 4: Context of the Organization

Importance:

Defines the scope of the ISMS based on the organization's context, including internal and external factors.

Identifies key stakeholders and their expectations for information security.

Ensures the ISMS is aligned with the organization's objectives.

Consequences of Low Scores:

Poorly defined scope can lead to inadequate risk coverage.

Failure to address stakeholder requirements may result in non-compliance with legal or contractual obligations.

Increased vulnerability due to gaps in the ISMS framework.

24

5. Leadership
This clause focuses on top management's commitment and responsibilities in establishing, implementing, and continually improving the management system, including setting policy and objectives.

Clause 5: Leadership

Importance:
Requires top management to demonstrate leadership and commitment to the ISMS.

Ensures clear assignment of roles, responsibilities, and authorities.

Promotes a culture of information security within the organization.

Consequences of Low Scores:
Lack of management buy-in can lead to insufficient resources and support for the ISMS.

Weak leadership may result in poor communication of security objectives and policies.

Employees may lack motivation to comply with security measures.

31

6. Planning
This clause outlines the processes for identifying performance risks and opportunities, setting objectives and targets, and developing action plans to achieve them within the organisation's management system.

Clause 6: Planning

Importance:
Involves identifying risks and opportunities related to information security.

Sets objectives for the ISMS and establishes plans to achieve them.

Aligns risk treatment plans with business needs.

Consequences of Low Scores:
Inadequate risk assessment can leave critical vulnerabilities unaddressed.

Poorly defined objectives may hinder the effectiveness of the ISMS.

Ineffective risk treatment plans can lead to breaches or non-compliance

68

7. Support

This clause addresses the resources, competence, awareness, communication, and documented information necessary to establish, implement, maintain, and continually improve the management system.

Clause 7: Support

Importance:

Focuses on providing necessary resources, training, and awareness for ISMS implementation.

Ensures proper documentation and control of information security policies and procedures.

Highlights the need for effective communication across the organization.

Consequences of Low Scores:

Lack of resources and training may lead to non-compliance and low employee engagement.

Poor documentation can create confusion and inconsistencies in security practices.

Weak communication channels may result in unaddressed security risks.

55

8. Operation

This clause focuses on planning, implementing, and controlling the processes needed to meet performance requirements, including operational controls, design considerations, and procurement of services, products, and equipment.

Clause 8: Operation

Importance:

Involves planning, implementing, and controlling the processes required to meet ISMS objectives.

Includes conducting risk assessments and implementing risk treatment plans.

Consequences of Low Scores:

Ineffective operational controls may fail to protect critical assets.
Poor execution of risk treatment plans can result in security incidents.
Non-compliance with operational requirements may jeopardize certification.

43

9. Performance Evaluation
This clause covers monitoring, measurement, analysis, and evaluation of the organisation's performance and the effectiveness of the management system, including internal audits and management reviews.

Clause 9: Performance Evaluation

Importance:
Requires monitoring, measurement, analysis, and evaluation of the ISMS to ensure effectiveness.

Includes conducting internal audits and management reviews.

Consequences of Low Scores:
Lack of performance monitoring can result in undetected weaknesses in the ISMS.

Inadequate internal audits may fail to identify non-conformities.

Poor management reviews can delay critical improvements.

31

10. Improvement
This clause addresses nonconformities, corrective actions, and continual improvement of the suitability, adequacy, and effectiveness of the management system and performance.

Clause 10: Improvement

Importance:
Focuses on addressing non-conformities and implementing corrective actions.

Encourages continual improvement of the ISMS.

Consequences of Low Scores:
Failure to address non-conformities can lead to recurring issues.

Lack of continuous improvement may result in stagnation and reduced effectiveness of the ISMS.

Poor handling of corrective actions can lead to certification suspension or revocation.

The Gap analysis revealed the following findings across all elements audited:

Major non-compliance. Not meeting mandatory requirements.	Non-compliance. Not meeting mandatory requirements.	Met mandatory requirements. BUT practices regarded as sub-optimal.	Good practices. Practices are effectively formed and mitigate risk	Mature and strong practices. Learning org. High levels of capability.
12	22	0	0	0

Consequences of Low Scores Across Clauses

Increased Risk of Security Breaches:
Inadequate implementation of the clauses can leave an organization vulnerable to cyberattacks and data breaches.

Loss of Certification:
Persistent low scores in audits can lead to the loss of ISO 27001 certification, impacting reputation and customer trust.

Regulatory Non-Compliance:
Low scores may indicate failure to comply with legal and regulatory requirements, resulting in fines or legal action.

Reputational Damage:
Customers and stakeholders may lose confidence in the organization's ability to protect information.

Operational Disruption:
Poor ISMS implementation can lead to inefficiencies and increased downtime during incidents.

Financial Losses:
Security incidents and non-compliance fines can result in significant financial impact.

How to Address Low Scores

Conduct root cause analysis for non-conformities.
Strengthen leadership commitment and allocate necessary resources.
Enhance employee training and awareness programs.
Regularly review and update risk assessments and treatment plans.
Implement a robust internal audit process to identify and correct issues proactively.

By effectively addressing the requirements of each clause, organizations can build a strong ISMS, reduce risks, and ensure compliance with ISO 27001.

ISO/IEC 27001:2022 Controls Review

Disclaimer

This independent audit was conducted on a sampling basis and, therefore, non-conformities and risks may exist outside the evidenced witnessed, viewed, and analysed during this audit.

The data has been collected from the responses from the Client's participants and is consequently a reflection of the auditee not the opinion DeepFathom Ltd.

The descriptive analytics are for guidance only and internal audit review and does not substitute as an external third-party audit.

Use the information provided by DeepFathom Ltd solely at your own risk.

DeepFathom Ltd make no warranties or representations as to the accuracy of information provided herein.

If you have any concerns about your organisation's compliance and remedial actions, please consult a qualified professional.