ISO 27001:2022 HANDBOOK

Contents

1.PURPOSE OF 'MAINTENANCE HANDBOOK'

The purpose of this handbook is to identify and describe the key management system requirements in relation to:

BS ISO/IEC 27001:2022 Information Security Management Systems Requirements

In addition to providing guidance on the day to day maintenance requirements, further guidance is also provided to assist you with facilitating the Management Review process and preparing for any external audits (surveillance and re-certification) provided by your external certification body.

2.WHAT IS A MANAGEMENT SYSTEM

Every business has three basic challenges that threaten their success if not met:

- Complying with customer requirements or statutory and regulatory requirements
- Protecting business resilience through embedding best practices, quality and compliance of products and services
- Growing the business in line with strategic aspirations, thereby increasing revenue

A management system is a framework of policies, processes, and procedures that your business can use to ensure that it can fulfil all these tasks to achieve its ongoing improvement objectives. When effectively run, a management system can fine-tune your operational performance, manage known risks, and assist to operate in more efficient and sustainable ways.

In addition, a management system can:

- Assign roles and responsibilities, and see exactly where there are bottlenecks,
- Ensure value-adding monitoring, measurement, and analysis of data, that in turn will assist the business to make more informed business decisions,
- Demonstrate compliance to even the most rigid regulations
- Understand where corrective action needs to be taken, and how this can be potentially avoided in future

The level of complexity of a management system will depend on each business's specific context. For some businesses, especially smaller ones, it may simply be in the form of strong leadership from the business owner, providing a clear definition of what is expected from each individual employee and how they contribute to the business's overall objectives, without the need for extensive documentation. whilst larger, more complex businesses operating, for example, in highly regulated sectors, may need extensive documentation and controls to fulfil their legal obligations and meet their high-level strategic objectives.

3.WHY MUST A MANAGEMENT SYSTEM BE MAINTAINED?

A management system needs to reflect the 'reality' of an organisation to remain effective and provide the value-adding benefits noted previously.

As a business grows or diversifies, there is a good chance that processes, and ways of working may change and improve. An example may be when a new technical system (i.e. a CRM system) is implemented – this may not fundamentally change how a process works – but the new system may replace a number of manual records previously maintained as part of the management system. As a result of the new system, reporting may improve which in turn may lead to more effective strategic level decision making. Furthermore, that new system may introduce or mitigate information security risks because the system is now based in 'the Cloud' and not on localised servers.

Therefore, it is important to review any changes as they occur and evaluate what, if any, changes it makes to the documented management system, or to the risk assessments that have conducted previously. This way the management system can be updated to reflect the new way of working.

It is also important to ensure that key records and policies are periodically reviewed to ensure they remain up to date and in alignment with the strategic direction of the company. A good example may be the management system objectives. It is important to review these periodically through the year to ensure that they remain relevant to what the business wants to achieve, otherwise wasted effort may be made progressing an objective that will no longer provide valid improvements.

4. KEY ROLES AND RESPONSIBILITIES

There are several key roles and responsibilities that are integral to the management system:

Top Management

Top Management are required to demonstrate leadership and commitment regarding the Management system. Management involvement must now be demonstrated and cannot be simply confined to annual management reviews or signing the management system policies. Without this demonstratable management commitment, you will struggle to have a successful management system. Therefore, communicating the importance of Leadership commitment and active involvement is essential to the ongoing success of the management system. Areas where this leadership and commitment can be demonstrated is through:

- Taking accountability for the effectiveness of the management system e.g. establishing key metric/measures, system/process performance monitoring and taking action when process performance is not meeting intended results, management review.
- Ensuring regular reviews of risks either through specific risk assessment and treatment activities, allowing the outcomes to inform the direction and use of the management system.
- Establishing and maintaining the policy and objectives and ensuring these are aligned to the strategic direction e.g. context of your organization, external/issues.
- Integrating the management system requirements into the DNA of the business e.g. system architecture, business model, process model, organization footprint, functional alignment (Engineering, Purchasing, IT, Finance, HR etc.)
- Supporting process owners in their process management activities e.g. deployment, governance, process evaluation, process improvement
- Enabling resources, including people, required for an effective management system e.g. resource planning, workload, priorities, constraints, balance, time etc.
- Communicating the importance of conformity to the Management system e.g. meetings, briefs, e-mail, intranet, focused training, consequence of non-conformity etc.
- Fostering an environment for continual improvement, e.g. proactive - product/service/process implementation and improvement initiatives, improvement projects, waste reduction, process re-engineering, cost reduction etc., and reactive - acting on process performance results, audit findings and complaints

4. KEY ROLES AND RESPONSIBILITIES

Management System Champion(s)

The Management system champion(s) will be the individuals who facilitate the day to day management of the system. They will often also act as the 'go to' person for any queries related to the management system for their peers. Typical responsibilities of the champions include:

- set the example for good information security practices
- ensuring that their peers are aware of new security communications
- be able to direct peers to find appropriate policies and procedures related to information security
- feedback opportunities for improvement
- pick up on any information security incidents and ensure they are reported.

Ensuring formal reviews are conducted of the management system to include Management Review, review of objective progress, reviewing the management system with appropriate parties when changes are made in the business or as a result of an issue being raised.

5.OVERVIEW OF THE KEY DOCUMENTS AND THEIR HIGH-LEVEL PURPOSE

5.1. Scope and Boundaries of the Information Security Management System

The scope and boundaries of the Information Security Management System should be maintained as documented information. The scope must include and reflect the context (purpose and marketplace) of the business and the needs and expectation of interested parties that need to be fulfilled by the management system. Any changes to the scope should be documented and made aware to your certification body. By linking the scope to the company's website, keeping the current message of the business up to date is made easier.

5.2 Information Security Policy

The Information Security Policy should be documented and communicated internally and made available to others, as necessary. This may include contractors who are responsible for supporting IT or security, as well as visitors to site so that they may appreciate that information security is central to the company's ethos.

5.OVERVIEW OF THE KEY DOCUMENTS AND THEIR HIGH-LEVEL PURPOSE

5.3. Objectives and KPIs

Information security objectives and KPIs are required documented information in the standard and should be appropriate to the needs of the management system and the organisation to ensure that security is being developed in line with the company's strategy (strategic security objectives) or produced to maintain security requirements in the business (operational objectives or KPIs)

5.4. Risk Assessment and Treatment

Central to the Information Security Management System is the need to conduct an information security risk assessment and take this through to effective risk treatment. This is no longer a one-off activity and should be conducted at planned intervals. Information Security Risk Assessment is not a 'one-off' that only requires regular review as the risk assessment is a living and breathing document that must reflect changes in the business or the unintended consequences of change. Maintenance and updating of the risk assessment are essential to ensure that any new changes to the business are risk assessed and risk treatment plan is in place.

5.OVERVIEW OF THE KEY DOCUMENTS AND THEIR HIGH-LEVEL PURPOSE

5.5. Statement of Applicability

The purpose of the Statement of Applicability is not just to be a list of controls that have been selected or deselected, but should be developed as a guidance document about where to look in the Information Security Management System to find the policies, procedures, activities or records that fulfil the controls within the business.

The Statement of Applicability contains 93 controls across 4 control groups:

- Organisational
- People
- Physical; and
- Technical

The controls have now been developed to enable them to align with other security standards such as Cyber Essentials and NIST. Furthermore, each control is linked to attributes and a sub-attributes which enables organisations to align their auditing to specific subject areas such as:

- Control Type
- Information Security Properties
- Cyber security concepts
- Operational Capabilities and
- Security Domains

6.KEY DOCUMENT MAINTENANCE REQUIREMENTS (DETAILED)

There are key documents that are required by the standard to establish the framework for the Management System. The standard does not necessarily state how this document information should be presented but does define what information should be included. This gives organisations the freedom to present the information in a way that is appropriate to the culture and needs of the company.

The documented information required by the standard includes.

- ISMS Scope
- Security Policy
- Risk Assessment and Treatment
- Statement of Applicability
- Security Objectives
- Competency Records
- Monitoring and Measuring Records
- Internal Audit Programme and Results
- Management Review Results
- Non-Conformities and Corrective Actions
- Policies, Procedures and Records selected in the Statement of Applicability

6.1. Competence

Competency records should be maintained for employees and contractors who can have an impact on information security. This should include any competency required to do a role effectively to ensure that security risks are not introduced through poor job knowledge and expertise. Records of competency should be retained and ready as evidence during internal and external audits.

6.2. Communication / Suggested Improvements

Results of activities aimed at obtaining improvement suggestions should be maintained in either electronic or hard copy form. These might typically be recorded as security weaknesses and are important in preventing security events and incidents.

6.KEY DOCUMENT MAINTENANCE REQUIREMENTS (DETAILED)

6.3. Operational Control - Documented Information

Any implementation of local controls relating to operational control activities should be documented and retained. This can include policies and procedures as well as records of performance. Policies and procedures can be divided into two groups, those that are needed for all staff to follow and those that are specifically for technical staff:

Policies for all staff will include

- Mobile Device and Teleworking Policy
- Access Control Policy (but physical security)
- Clear Desk and Clear Screen Policy
- Acceptable Use policy

Policies for technical staff will include

- Access Control Policy (access to IT systems)
- Encryption Policy
- Back-up Policy
- Secure Development Policy Third Party development
- Information Security Supplier Relationship Policy
- Supplier Services Change Procedures
- Business Continuity Plan
- Business Continuity Testing Reports
- Legal Register
- ...and other policies listed in the Statement of Applicability.

6.4. Monitoring and Measurement

Monitoring and measurement records should include as a minimum the controls selected in Statement of Applicability:

- Information Security Incidents
- Corrective Actions
- Access Rights reviews
- Asset Reviews
- Anti-Virus monitoring
- Back-up Records
- Security Vulnerability testing

6.KEY DOCUMENT MAINTENANCE REQUIREMENTS (DETAILED)

6.5. Results of Analysis and Evaluation

Records gathered from monitoring and measuring must be analysed for trends in types and numbers and an evaluation of whether actions should be taken and what that action might be. Analysis and evaluation are critical parts of the process of continual improvement.

6.6. Audit Programme / Audit Results

Records to confirm that evaluation of compliance activities have been undertaken and evidence in the form of records to demonstrate that the organisation is compliant with applicable compliance obligations identified should be maintained.

6.7. Management Review Results

An audit programme and records to demonstrate that internal audits have been undertaken in accordance with the programme should be maintained and available. Evidence should also be maintained to confirm auditor competency. (See the comment in the statement of applicability section)

6.8. Management Review Results

Evidence to confirm management review has taken place in line with the input requirements and also capturing any actions arising in line with the output requirements should be maintained to confirm management review has taken place at the stated frequency.

Management Review can take the form of either a series of meetings, an individual meeting or a written report to the Board. As long as the agenda requirements of the standard are followed and there is evidence of top management feedback the approach taken must be appropriate to the business.

6.9. Non-Conformities & Corrective actions

Evidence to confirm nonconformities are recorded and actions taken to address them should be maintained. This should include any investigations to confirm root causes of non-conformities, corrective actions taken and verification of the effectiveness of the actions

7. MAKING CHANGES TO THE MANAGEMENT SYSTEM – THINGS TO REMEMBER

Document Control – Changes to documents should be recorded and version control updated. The latest versions should be available where required in hard copy or electronically at the point of use.

Communicate the changes – Those that need to know should be made aware of the change made and obsolete versions removed from use.

Prioritise changed elements for re-audit to review and confirm the changes made were implemented effectively.

8. PREPARING FOR THE MANAGEMENT REVIEW PROCESS

The Management Review is a key leadership tool for understanding the health of the Information Security Management System and, based upon information presented in the review, informed decision making about security improvements can be made. It is important that the Management Review is everyone's responsibility and that those attending might be asked to provide informal update for the meeting; this should be assigned to the best person to obtain the information (or information owner).

8.1. Management Review Agenda

The Management Review agenda is set as a minimum list of subject areas to be covered:

- Changes in external and internal issues that are relevant to the information security management system.
- Feedback on the information security performance, including trends in:
  - -nonconformities and corrective actions;
  - - monitoring and measurement results;
  - - audit results; and
  - - fulfilment of information security objectives;
- Feedback from interested parties;
- Results of risk assessment and status of risk treatment plan; and
- Opportunities for continual improvement.

8. PREPARING FOR THE MANAGEMENT REVIEW PROCESS

8.2. Changes in external and internal issues that are relevant to the information security management system

To maintain your understanding of the changes to external and internal issues it is important that at given intervals you could conduct a new review to determine if there are any new risks to be addressed or opportunities to be exploited. These changes should be presented at the Management Review to ensure that all internal and external issues are understood.

8.3. Nonconformities and corrective actions

You are currently maintaining a log of non-conformities and corrective actions which have come from the risk assessment; internal audits; external assessments and security incidents. This must be maintained and kept up to date to avoid any non-conformities in an external assessment. Any non-conformities or trends should be identified and reported to the Management Review.

8.4. Monitoring and measurement results

You should present to the management review the results of any monitoring, measuring, analysis and evaluation so it can be determined if all the appropriate points of the management system are being monitored

8.5. Audit results

Details on the number of audits planned and those conducted should be presented to the management review. If any have been delayed the reason should be reported because it may require intervention from senior management to provide resources for the audit to take place. Analysis of the number, type, root cause and status of the action should be presented in the meeting.

8.6 Fulfilment of information security objectives

Objectives will have been created from various points in the management system, including the risk assessment and perhaps from the company's strategic planning for information security. The status of the objectives should be reviewed and discussed in the management review, and where appropriate new ones should be raised.

8. PREPARING FOR THE MANAGEMENT REVIEW PROCESS

8.7. Feedback from interested parties

In the scope of your management system you will have identified who your interested parties are which might include:

- Employees
- Clients
- Suppliers

Each of these groups has an interest in making the management system work effectively and they might proffer feedback on how the management system is impacting on them, both positive and negative. Feedback presented in the management review doesn't have to have been previously documented, as it will be recorded in the minutes of the review and can simply be information and knowledge that has been gathered and needs to be shared.

8.8. Results of risk assessment and status of risk treatment plan

The Risk Assessment and Risk Treatment are key to the management system and are living documents that will change as the business changes. The management review should seek to gain information about any new risk assessments conducted, risks identified and status of addressing the treatment of these risks.

Coupled with the Risk Assessment is the need to maintain the Statement of Applicability, including auditing the controls and determining whether the controls that have been excluded are still valid.

8.9. Opportunities for improvement

This is the opportunity for anyone attending the management review to put forward their ideas on how the information security management system can be improved. Ideas should not be limited but discussed openly to determine whether there is any value in pursuing them.

9. PREPARING FOR AN EXTERNAL AUDIT

Once through certification, the general approach to surveillance or recertification audits is the same. Prepare and ensure that evidence is readily available when needed.

Confirm a suitable room / space for the audit to take place also confirm arrangements for lunch (confirm any specific dietary requirements) and refreshments.

Any specific requirements for working on the site such as PPE should be communicated or made available to the auditor particularly when visiting server rooms and data centres.

Any specific emergency arrangements for the site should be established and communicated (e.g. planned fire alarm tests)

The auditor should be directed to report to reception on arrival and should always be accompanied during the audit.

9.1. Surveillance

Review the previous external audit report to:

- Confirm any non-conformities have been effectively addressed. Evidence and examples will be needed to confirm that the non-conformities have been effectively addressed and closed.
- Ensure all opportunities for improvement have been considered for implementation. Ensure that there is good reason when OFI's identified by the external assessor have not been selected for implementation.
- Confirm the audit plan, dates, times, and availability of auditees within your organisation.
- Confirm the auditor name and contact details

9.2. Re-Certification

Recertification audits should take place at least 3 months before certificate expiry. The audit will review the entire management system and are planned in much the same approach as above. It is essential that all outstanding non-conformities are closed at the Recertification to reduce the risk of failing the assessment.

Any Nonconformities raised during recertification audits will need to be responded to via a corrective action plan submitted to the certification body and provision of evidence of actions taken to address them is required before the new certificate can be issued.

10. TYPICAL MONITORING AND MEASUREMENT ACTIVITIES (FOR GUIDANCE PURPOSES)

10.1. What needs to be monitored and measured, including information security processes and controls?

This is key to ensuring that you do not monitor and measure for the sake of it and there are benefits being gained from these activities; benefits that will help to reduce risks and bring about continual improvement of the management system.

There are the mandatory requirements for maintaining certification which are found in the Clause of the standard and there are those requirements which are applicable to the management system you have established; these relate to the controls.

10.2. The methods for monitoring, measurement, analysis, and evaluation, as applicable, to ensure valid results

Monitoring, measuring, analysis and evaluation are essential for demonstrating continual improvement of the management system and the methods you use are entirely up to you so long as they are repeatable and produce consistent results that can be validated.

10.3. When the monitoring and measuring shall be performed

The frequency of monitoring must be based upon risk; what is critical in the business and would constitute as a high risk if it were lost or damaged or would have a high impact of confidentiality, integrity, and availability? See the table below (Pg 19 - 20)

10.4. Who shall monitor and measure?

It is not always the responsibility of the Information Security Manager (or the person responsible for information security) to do all the monitoring and measuring. These activities should be assigned as roles and responsibilities to different employees, or to the risk owners, who might then report it to the Information Security Manager for inclusion in the Management Review.

10. TYPICAL MONITORING AND MEASUREMENT ACTIVITIES (FOR GUIDANCE PURPOSES)

10.5 When the results from monitoring and measurement shall be analysed and evaluated

The analysis and evaluation will take place at different times depending upon the type of information being monitored and measured. Some analysis and evaluation might take place as soon as an activity in completed (such as results from internal audits or back up tests) but others might be done at planned intervals based upon risk, or the amount of data that has been collected (such as security incident trends; review of results in the Management Review). These activities should be scheduled and assigned as responsibilities to ensure that they take place.

10.6. Who shall analyse and evaluate these results?

As with monitoring and measuring the responsibility should not fall to the Information Security Manager (or the person responsible for information security) to analyse and evaluate results. The responsibility should be assigned based upon the competence of the people to be able to do effective analysis and evaluation and then reported to the Information Security Manager for inclusion in the Management Review.

10. TYPICAL MONITORING AND MEASUREMENT ACTIVITIES (FOR GUIDANCE PURPOSES)

10.7. Recommended Areas to monitor and measure

Often, organisations can find it difficult to determine what should be monitored and measured. Below is a list of areas in the Information Security Management System that can be considered (but there is no requirement to monitor all of these):

- Inventory of Authorized and Unauthorized Devices
- Inventory of Authorized and Unauthorized Software
- Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
- Continuous Vulnerability Assessment and Remediation
- Controlled Use of Administrative Privileges
- Maintenance, Monitoring, and Analysis of Audit Logs
- Email and Web Browser Protections
- Malware Defences
- Limitation and Control of Network Ports, Protocols, and Services
- Data Recovery Capability
- Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
- Boundary Defence
- Data Protection
- Controlled Access Based on the Need to Know
- Wireless Access Control
- Account Monitoring and Control
- Security Skills Assessment and Appropriate Training to Fill Gaps
- Application Software Security
- Incident Response and Management
- Penetration Tests and Red Team Exercises

The following table (provided on pages 19 and 20) is for guidance and should not be read a definitive list. Each organisation should monitor what is appropriate to them and use appropriate tools and reporting methods that suit the organisation's needs.

10. TYPICAL MONITORING AND MEASUREMENT ACTIVITIES (FOR GUIDANCE PURPOSES)

DEPT	DAILY	WEEKLY	MONTHLY	QUARTERLY	6 MONTHLY	ANNUALLY
IT Dept	• Dynamic Anti-virus check (2 - 3 days per week) (reported on exception) • Dynamic Back up report check • Dynamic Systems Monitor check (reported on exception) • Server room checks	• AV / Firewall Config • Spiceworks Server • Starters/Leavers (ad-hoc)	• Dynamic Firewall Config • Planned Access reviews (as per schedule)	• Dynamic Vulnerability Scan • BCP tests • Review ISMS Risk Assessment for new risks • Review SOA for updated/changed controls	• Restore Tests • Refresher training (with HR) - Planned Activity • ISMS Risk Assessment Review (with QM)	• PEN Test • Review of IT specific policies
Security Manager	• Ad-hoc support to Business	• Ad-hoc support to Business / Office Manager	• Formal Review of Continual Improvement Log	• Formal report to SIG on objectives/ risks and status of management system • Formal review of Supplier Management records	• Certification Body External Audit • ISMS Risk Assessment Review (with IT) • Aspects & Impacts Review	• Management review (prep & deliver) • Review of policies • SWOT/PESTLE review
Office Manager	• Visitor/ Contractor management			• Review of access system logs for suspicious activity (out of hours and restricted areas) • Review of CCTV for suspicious activity		• Disposal of visitor logs

10. TYPICAL MONITORING AND MEASUREMENT ACTIVITIES (FOR GUIDANCE PURPOSES)

DEPT	DAILY	WEEKLY	MONTHLY	QUARTERLY	6 MONTHLY	ANNUALLY
HR		• Starters/ Leavers (ad-hoc)	• Inductions (as appropriate)	• Review and update staff training records		
Dept Manager						• Formal Access review for systems used (in line with schedule)