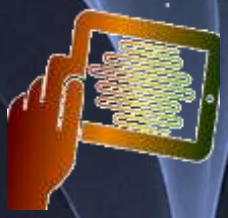

SecAware

Pragmatic ISMS implementation guideline

Putting ISO/IEC 27001
into practice

1 Executive summary 2
2 Introduction 2
3 Scope, purpose, format and structure of this guideline 2
4 Context of the organisation 3
4.1 Understanding the organisation and its context 3
4.2 Understanding the needs and expectations of interested parties 4
4.3 Determining the scope of the ISMS 6
4.4 Information Security Management System 7
5 Leadership 8
5.1 Leadership and commitment 8
5.2 Policy 9
5.3 Organisational rôles, responsibilities and authorities 11
6 Planning 13
6.1 Actions to address risks and opportunities 13
6.2 Information security objectives and planning to achieve them 16
6.3 Planning of changes 17
7 Support 18
7.1 Resources 18
7.2 Competence 19
7.3 Awareness 20
7.4 Communication 21
7.5 Documented information 22
8 Operations 24
8.1 Operational planning and control 24
8.2 Information risk assessment 25
8.3 Information risk treatment 26
9 Performance evaluation 27
9.1 Monitoring, measurement, analysis and evaluation 27
9.2 Internal audit 28
9.3 Management review 29
10 Improvement 32
10.1 Continual improvement 32
10.2 Nonconformity and corrective action 33
Annex A: The information security controls in ISO/IEC 27001 34
Annex B: Documented information 35
Annex C: ISMS implementation project guidance checklist 37

1 Executive summary

This guideline helps information risk and security professionals interpret and apply ISO/IEC 27001 in practice. It offers pragmatic guidance on how to construct and implement an **I**nformation **S**ecurity **M**anagement **S**ystem that satisfies *both* the standard's formal specification *and* the organisation's requirements to manage its information risk and security arrangements cost-effectively.

2 Introduction

ISO/IEC 27001:2022 specifies an ISMS using the ISO/IEC harmonized approach and structure for management system standards from the ISO/IEC Directives (Annex SL and Appendix 2). As a standard specification, it is formal and succinctly worded. It is primarily intended for conformity auditing and certification. *Any* certified ISMS should therefore have the same overall structure and core processes, despite differences between organisations in terms of their sizes, structures, industry sectors, maturity *etc.*

The formalities and precise language can make it difficult to understand and apply ISO/EC 27001 in practice, particularly for people who are unfamiliar with the ISO/IEC approach towards 'management systems'. The standard is meant to be interpreted in a particular narrow way for conformity auditing, with little latitude regarding the management system structure. At the same time, the standard has to be customised or adapted to some extent to fit within the confines of an actual organisation. Using the standard to build, implement, operate and maintain an ISMS within an organisation is a different purpose to conformity auditing, a different perspective.

3 Scope, purpose, format and structure of this guideline

This guideline offers *pragmatic* guidance to help information risk and security professionals interpret and apply ISO/IEC 27001 in their organisations. It is practical in nature, *supplementing* rather than replacing ISO/IEC 27001. It expands upon the standard's concise wording in everyday language more familiar to practitioners, explaining how the standard can be implemented in practice.

However, the standard remains the definitive reference. Certification auditors may interpret the standard differently based on their understanding of its true intent and meaning. In case of discrepancies, certification auditors are constrained by ISO/IEC 27001 as a formal specification, plus other applicable ISO/IEC, corporate and professional standards, policies and procedures concerning conformity or compliance auditing and certification activities. They may dispute or disagree with the guidance provided here … in which case, good luck persuading them that your ISMS substantially satisfies both the standard's formal specification *and* your organisation's requirements.

Likewise, *you* may disagree with this guideline and perhaps even ISO/IEC 27001. Although both are generic and are intended to apply to any organisation, your unique situation and particular circumstances may suggest or dictate a different approach, perhaps differing priorities or objectives.

The remaining sections of this guideline explain and provide guidance on the main clauses of ISO/IEC 27001, following the same sequence and clause numbering for convenience.

4 Context of the organisation

4.1 Understanding the organisation and its context

Requirement[1]

The organisation identifies important factors in the business context, both internally- and externally-driven, affecting achievement of ISMS outcomes.

Explanation

An ISMS is an investment in securing information. As with other business endeavours, management expects the organisation to achieve a net benefit. This means systematically managing information security without incurring excessive costs. A well-designed and effective ISMS aligns with and supports the achievement of business goals, thereby creating value.

Clause 4.1 requires management to identify, consider and discuss relevant issues. This encompasses important topics, potential problems and even valuable opportunities that can affect the business, information, risks and, ultimately, the effectiveness and value of the ISMS. Issues may originate both within the organisation (internal) and in the wider environment (external).

Guidance

The intended ISMS outcomes or objectives are determined by the organisation (see clause 6.2).

The organisation's external context includes its risks, opportunities, constraints and obligations or expectations from outside, such as:

- Laws and regulations concerning privacy, financial reporting, cybersecurity, fraud, safety *etc.*;
- Outside threats *e.g.* hackers, malware, saboteurs, unethical competitors, overzealous authorities, natural disasters (potentially climate-change-induced);
- Disruptions to supply chains or critical infrastructure;
- Stakeholder expectations (*e.g.* financial returns, competitive performance, growth, resilience, compliance, ethical conduct, societal value);
- Cultural factors that differ between industries and locations.

The organisation's internal context involves relevant factors and pressures from within, such as:

- Strategies and plans involving information, knowledge, digital data, intellectual property *etc.*;
- Its **I**nformation **T**echnology and **O**perational **T**echnology, old and new;
- Innovation and creative adaptations to the organisation's particular circumstances;
- Finite resources (competent workers, time and money) and competing priorities;
- Insider threats arising from employees, contractors and other workers;
- Branding and marketing promoting the organisation as ethical, trustworthy and reliable.

[1] This guideline succinctly rephrases the requirements in ISO/IEC 27001:2022 for brevity and readability. Consult ISO/IEC 27001:2022 for the official, formal language.

In addition, there may be further contextual considerations such as:

- Strategic opportunities to adopt diverse approaches, good practices, partnerships or collaborations;
- Volatility and uncertainties requiring short- and long-term perspectives;
- Social and societal influences;
- Changing technological landscape (*e.g*. ubiquitous computing and connectivity, wearable devices, artificial intelligence).

Understanding the organisation's internal and external factors, its strengths and weaknesses, allows management to:

- Target the biggest risks, prioritising the most urgent demands and promising improvements;
- Allocate sufficient financial, human and technological resources;
- Decide on the appropriate risk treatment options (see ISO/IEC 27005);
- Continually improve and adapt to changes and opportunities, making the ISMS agile, responsive and valuable (clause 10.1).

While an ISMS scope may be deliberately constrained, the organisation faces information risks all over. Rather than being an isolated or introspective function, an effective ISMS actively integrates with, supports and influences the entire organisation, enabling and securing information-related business activities throughout.

4.2 Understanding the needs and expectations of interested parties

Requirement

The organisation identifies requirements of interested parties to be addressed by the ISMS.

Explanation

Clause 4.2 involves determining who has interests that are relevant to ISMS, then clarifying the requirements. Understanding their concerns, expectations and needs helps tailor the information security arrangements to both protect and release or realise the value of information.

Guidance

Various stakeholders may have interests in the ISMS, such as:

- Workers, meaning the organisation's employees (management and staff) plus contractors, consultants, student interns, temporary workers *etc.*;
- Other business units, departments, functions and teams, particularly those with obvious concerns in this domain *e.g*. IT, Risk Management, Facilities, Strategy;
- Senior management and governance bodies up to board level, potentially including other business units, headquarters or holding companies in group structures;
- Suppliers, business partners and customers;
- The organisation's owners and investors;
- Regulators, government/supervisory authorities, trade bodies, auditors *etc.* providing guidance, oversight and assurance;

- Trade bodies and professional associations;
- Local, national or global society;
- Adversaries such as competitors, hackers, fraudsters, criminals, terrorists and spies.

Stakeholders' interests in the ISMS can also be varied, such as:

- Confidentiality, integrity or availability of information supplied to, generated and used by, or provided by the organisation;
- Secrecy and privacy in the personal, commercial, governmental or defence contexts;
- Intellectual property protection and exploitation;
- Safety and environmental protection (*e.g*. concerns about the organisation's responses to climate change may raise questions about the integrity of its disclosures and possible 'greenwashing');
- Mandatory obligations and discretionary expectations within applicable laws, regulations, contracts, agreements, codes, treaties, conventions, protocols, standards, permits, licences or other forms of authorisation;
- General business objectives such as cost-effectiveness, efficiency, profitability, trustworthiness, resilience, creativity and innovation;
- Technical objectives such as simplicity, flexibility, dependability or reliability of IT systems, networks *etc.*;
- Service-related objectives such as utility, value, professionalism, quality and credibility;
- Legitimate and illegitimate exploitation of information.

Understanding the perspectives, concerns and priorities of interested parties enables:

- Tailoring the ISMS to address their concerns and expectations, as well as the organisation's own;
- Building trust and confidence with a demonstrable commitment to information security, privacy, compliance, professionalism *etc.*;
- Avoiding misunderstandings through transparency, discussion and agreement on achievable shared goals;
- Improving overall ISMS effectiveness leading to better outcomes.

Although the stakeholder analysis may be worthwhile, too comprehensive and detailed an approach can be overwhelming, costly and slow. Clause 4.2 does not require the comprehensive identification of all the needs and expectations of all interested parties – just those that are relevant to the ISMS. A shortlist of the main stakeholders and their obvious interests may be sufficient to make a start, extending and refining the analysis periodically once the ISMS is fully operational, generating additional information and insight.

Here are some pragmatic suggestions to consider:

- Identify and consult key stakeholders and study relevant documentation such as contracts, laws, regulations, and industry guidance;
- Interested parties' needs and expectations may be identified or validated as a side-effect of other activities such as information and risk inventories, risk assessments, ISMS change management and compliance reviews;
- Prioritising by risk allows the organisation to tackle issues that are obviously crucial and urgent without delay. This can break the cycle of incessant analysis, provide opportunities to learn and improve by doing, and reduce the overall risk profile relative to other approaches;

- Keeping stakeholders informed and actively engaged with the ISMS is a subtle benefit of activities such as this. Productive collaboration with stakeholders can strengthen and transform the ISMS from a compliance activity into a powerful and valuable business tool.

4.3 Determining the scope of the ISMS

Requirement

Senior management[2] determines the ISMS scope by clarifying its boundary and applicability.

Explanation

Information risks are actively managed within the boundary of the ISMS, which may be defined in physical or business terms *e.g.* specific locations, business units or departments, or particular processes and operations.

However, the ISMS may manage information, risks and security controls outside the ISMS boundary, in which case its applicability may exceed the scope.

Guidance

As a management system, the ISMS is not an isolated and remote island but a specialist function that interacts productively with other areas within the organisation and beyond. Information, risks and security arrangements inevitably link the in-scope ISMS with out-of-scope areas. Clarifying the interfaces (points of contact and communication) and dependencies (expectations/demands) helps management understand the broader business context within which the ISMS operates.

Since ISO/IEC 27001 says so little about this, the ISMS may be scoped at management's discretion provided certain matters noted in clause 4.3 are duly 'considered' and the scope is made available as 'documented information' (see Annex B).

Rather than simply replicating the scope of an existing information risk and security management, cybersecurity or similar function, more creative or unconventional scoping approaches are worth considering, for example:

- Designing the ISMS purely as a management unit defining corporate security strategies, policies *etc.*, with interfaces to a range of other (out-of-scope) corporate functions or commercial suppliers providing information risk and security-related services;
- Adapting the scope to respond to and drive changes in the organisational context (*e.g.* reviewing the ISMS scope periodically, using factors such as operational efficiency and effectiveness to determine which information security-related functions fall within or remain outside the ISMS);
- Defining the scope in terms of the significance of risks being managed (*e.g.* "The ISMS only covers critical risks at this stage, extending to lesser risks as it matures") or their nature (*e.g.* "The ISMS is focused on IT risks and data security, excluding other aspects of information security").

[2] ISO/IEC 27001 defines and uses the curious term 'top management' to refer to the most senior managers with responsibility for the ISMS. Top management *may* not be the organisation's most senior (executive) managers if they have delegated management responsibilities for the ISMS. This pragmatic guideline uses the more common term 'senior management' for simplicity.

4.4 Information Security Management System

Requirement

The ISMS is designed, built and operated.

Explanation

Designing and implementing the ISMS is merely the start. Clause 4.4 requires the ISMS to be designed in conformity with clauses 4 to 10 inclusive, and to function as designed in order to claim conformity with ISO/IEC 27001.

Guidance

Once operational, an effective ISMS becomes business-as-usual. It is an integral and valuable part of the organisation's routine management framework, with long-term strategic and governance implications.

There is a risk of an ISMS merely consisting of a suite of fine documentation – good intentions that are not necessarily put into full effect as a functioning management system. Therefore, gathering and evaluating evidence concerning ISMS routine operations is a valuable assurance activity. Records such as written reports, logs, incident record, change requests and approvals demonstrate that the ISMS is operating and improving, systematically.

Further assurance may be appropriate concerning the risk treatments such as the status and effectiveness of security controls and the residual risk levels, as well as confirming that risk identification plus the evaluation and treatment decisions are being performed in accordance with the policies and procedures.

In addition to explicit cross-references to the clauses of ISO/IEC 27001 from this guideline, there are several implicit interrelationships and subtle dependencies both within the ISMS and external to it – not least the rest of the business. It is truly a 'system'.

Regardless of the sequence of clauses in ISO/IEC 27001, there is no requirement to implement an ISMS in the same sequence, nor any sequence in fact. Senior management should decide how best to design and implement the ISMS, using the standard as an overall framework while taking account of relevant factors and creative options such as:

- Business objectives and priorities *e.g*. introducing or improving particular aspects of information risk and security management, reducing incidents, achieving an adequate security baseline across the organisation, adopting good security practices or making a demonstrable commitment to information security;
- Coordination with other priorities plus ongoing and planned initiatives;
- Making optimal use of available and planned resources;
- Gaining experience, knowledge, expertise and momentum through a limited-scope initial phase pilot study or proof-of-concept ISMS, reviewing and deciding how to proceed from there;
- Planning a combination of sequential and parallel activities, perhaps a modular or phased approach, while managing dependencies and the critical path;

- Taking advantage of opportunities that arise through a flexible, responsive approach, within broad bounds and objectives defined on behalf of the business and its stakeholders by senior management;
- Responding positively to incidents through post-incident reviews, driving process improvements;
- Consulting experienced ISMS implementers, project managers, consultants, peers *etc.* for advice and assistance;
- Conducting an initial audit, review or gap analysis to explore the organisation's current information risk and security management status, identify its pressure points, capabilities, resources, options *etc.* before deciding what to do;
- Clarifying key objectives or goals (such as certification, risk optimisation or a material reduction in the number and consequences of security incidents), systematically establishing or improving the contributory processes required to achieve them including process management;
- Focusing on identifying and achieving business goals, objectives, benefits, opportunities, imperatives *etc.* aside from, or in addition to, being certified;
- Clarifying objectives in sufficient detail to develop appropriate metrics that will drive the ISMS implementation phase, leading into routine operations (clause 8).

5 Leadership

5.1 Leadership and commitment

Requirement

Management demonstrates leadership of and commitment to the ISMS.

Explanation

The requirement in clause 5.1 is not merely for senior management to offer their support for the ISMS, but to be actively involved. Senior management should demonstrate leadership and commitment through strategic alignment, decisions, actions, policies, overt communications, resourcing, improvement initiatives *etc.*

Without genuine, visible, proactive and ongoing management support, an ISMS may be or become an irrelevance, sidelined and largely ignored by the rest of the organisation. If starved of resources and insufficiently prioritised relative to other aspects of the business, the ISMS may struggle to achieve all its objectives, ultimately risking failure.

Guidance

Senior management should demonstrate commitment to the ISMS through their personal involvement, particularly in governance matters such as organisational structure, and by ensuring that suitable reporting and assurance arrangements are in place.

Furthermore, senior management may perform or delegate, direct and facilitate activities such as:

- Working with management to clarify the organisation's information risk and security objectives;

- Defining and assigning information security-related rôles, responsibilities, authorities and accountabilities appropriately (clause 5.3);
- Allocating sufficient resources (funds, workers, facilities, technologies *etc.*) to achieve objectives;
- Directing, guiding, motivating, overseeing and generally supporting the ISMS team through conventional personnel management;
- Developing coherent strategies and approaches;
- Expressing the significance of information risk and security, prioritising it accordingly;
- Endorsing, authorising and mandating information risk and security policy;
- Clarifying the criteria for risk treatment decisions, such as risk appetite or risk tolerance;
- Maintaining effective relationships and engagement with the business, collaborating with other functions and teams to identify, work towards and achieve shared objectives;
- Reassuring stakeholders that the ISMS is an integral, valuable and permanent part of the business;
- Requesting and utilising management information such as reports on the status and effectiveness of the ISMS (clause 5.3b), measurements relating to processes and controls (clauses 6.2b and 9.1a), ISMS management review reports (clause 9.3) and ISMS internal audit reports (clause 9.2);
- Actively listening and seeking feedback from the business regarding ISMS performance and value;
- Addressing issues and overcoming obstacles and resistance to change;
- Identifying and pursuing worthwhile ISMS improvement opportunities (clause 10.1).

Leadership and commitment may extend beyond the ISMS and the organisation. Engaging with colleagues, professional and industry peers, senior managers and other stakeholders can present opportunities to share, learn, promote and further good information risk and security practices. Case studies, presentations, articles *etc.* on the ISMS can raise the organisation's profile and motivate the workers involved. Just be careful not to disclose sensitive information inappropriately.

5.2 Policy

Requirement

Senior management establishes an information security policy.

Explanation

Information security policy is an effective mechanism for senior management to formulate and express intentions, providing clear direction.

Guidance

The requirement in clause 5.2 can be interpreted as an overarching, high-level 'corporate' information security policy or strategy for the ISMS. It may include, comprise or be supported by multiple documents forming a structured and coherent policy suite or manual. Any subsidiary policies, procedures, guidelines *etc.* that expand on specific aspects of information risk and security should be aligned with the information security policy and each other, avoiding the confusion of conflicts, gaps and inconsistent language. Document management and change controls help

maintain alignment within the suite and with policies in related areas such as IT, risk, privacy, HR, safety, intellectual property and compliance.

The policy may specify the organisation's information risk and security objectives, or establish a governance framework for setting these objectives, or do both. For example, it might define principles such as protecting information confidentiality, integrity and availability, alongside a management structure and authorisation process for setting more specific objectives within an ISMS.

The organisation's business context, purpose and culture are relevant to the policy.

Given the widespread and significant nature of information and information risks, senior management should determine the appropriate audiences, such as:

- Employees *i.e*. managers and staff in general;
- Contractors, subcontractors, temporary workers and students working for, within or on behalf of the organisation, with access to or control over information;
- Selected external organisations such as business partners, customers, insurers and authorities *i.e*. stakeholders with interests in the ISMS.

While the tone and style may be formal, readability, length, complexity and accessibility are of concern given its intended audiences.

While primarily focused on the ISMS, the policy may also apply to other organisational areas. In large group structures, for instance, group executive management or the board may set high-level objectives for the entire group, allowing individual units some flexibility to interpret them within their local context or ISMS.

An information security policy may comprise part of a policy manual, potentially covering quality, environment, IT and other areas in addition to information risk and security. However, discrete, topic-specific policies offer better visibility and understanding, and easier maintenance when individual policies need to be introduced, updated or withdrawn.

While their format, style and content is for management to determine, policies typically cover:

- Their overall purpose/s, goal/s or objective/s;
- Their applicability or scope;
- Governance aspects such as the associated accountabilities, rôles and responsibilities, plus the formal mandate, imperative, authority or management authorisation that gives them force;
- Assurance arrangements such as conformity assessments, reviews, audits and enforcement options.

Standardising the structure, layout, writing style and branding of policies, procedures, guidelines and other relevant documents (*e.g*. using templates) enhances readability and comprehension, consistency and conformity.

See clause 7.5 and Annex B regarding the definition and interpretation of ‘documented information’.

Policies can be disseminated electronically, with appropriate authorisation, version and access controls reducing risks and environmental impact. Access logs can provide evidence of notification and (if required) acknowledgement or acceptance of the content by workers.

5.3 Organisational rôles, responsibilities and authorities

Requirement

Senior management assigns and communicates important information risk, information security and ISMS-related rôles, responsibilities and authorities to the relevant parties.

Explanation

This governance activity involves management:

- Designing appropriate corporate structures;
- Determining the purposes or functions of various departments, teams and individuals within the ISMS structure;
- Establishing business relationships with other parts of the organisation and specialist functions such as IT and risk management, and with relevant third parties such as the providers of various risk and security-related professional services;
- Deciding how they all work together without inappropriate overlaps and gaps;
- Identifying reporting lines and management information flows;
- Implementing the structure, overseeing its operation and the internal reporting.

In the ISMS context, there may be strategic as well as governance implications to the internal ISMS structure and its external relations. There are important responsibilities for senior management and senior management of the entire organisation (if different) since only they have the requisite authority and purview across the organisation.

Guidance

Rôles are sets of responsibilities and tasks associated with business functions and positions or job titles. As with accountabilities, these vary widely across organisations, depending on the amount and nature of work required, the number and capabilities of the workers involved, and governance decisions. Some typical ISMS-related rôles[3]:

- Backup administrator;
- Business analyst or security analyst;
- Business continuity specialist;
- Change and configuration manager;
- Chief Information Security Officer;
- Crisis manager;
- Cybersecurity specialist;
- Departmental or business unit security representative;
- Forensic analyst;
- Incident management team;
- Help desk operator;
- Information Security Manager;
- IT auditor;
- Penetration tester;
- Policy author;
- Privacy manager or Data Protection Officer;
- Risk owner;
- Security architect;
- Security consultant;
- Security guard;
- Security trainer;
- Supplier relationship manager.

[3] Job titles and rôles vary. These are simply illustrative examples.

In small organisations, information security rôles are often broadly understood rather than formally described, and may be part-time, perhaps combined with other non-security rôles. In larger organisations, the rôles tend to be more specialised, focused and formalised through job descriptions and contracts.

Rôles vary in scope and significance, spanning executive and managerial positions to supervisory, support and operational levels. Rôles may evolve gradually with occasional step changes. Examples include dividing a backup manager rôle into separate duties for data backups and archival, or restructuring a software security team with new rôles to address the risks associated with artificial intelligence.

Well-defined rôles are fundamental to expectations. Engagement, conformity, diligence and motivation are enhanced when workers are clear on their specific responsibilities and understand their contribution to the organisation's goals.

Transparent rôles facilitate effective performance management, enabling the organisation to adapt to changing demands and business needs by modifying or creating new rôles as necessary.

However, poorly conceived and excessively rigid rôle definitions may create gaps, leaving important areas without assigned responsibilities.

Authorities give holders permissions and powers to make decisions within their scope such as:

- Defining objectives, priorities, timescales *etc.*;
- Defining rules and administrative controls;
- Allocating or deploying resources;
- Monitoring and overseeing operations, directing or intervening if appropriate;
- Committing or obliging the organisation through contracts and agreements.

Rôles, responsibilities, authorities and accountabilities are fundamental to the smooth functioning of the organisation, including the ISMS. They form a coherent set, with responsibilities generally cascading down through the organisational structure, becoming more specific at each level. However, key decisions and the associated accountabilities typically reside with managers who possess the authority to make those decisions, set strategies, allocate resources and define rules. Explicitly linking individual rôles to their corresponding accountabilities creates a powerful control mechanism supporting sound governance.

Job descriptions are commonly used to outline the key responsibilities associated with each rôle, according to local practice. They may specify the expected skills, expertise, experience, qualifications, and personal characteristics relevant to the rôle (such as ‘thinking strategically’ for executive rôles, and ‘personable’ for trainers, help desk workers and relationship managers).

The requirements for information security and other types of professional services provided by third parties are generally specified formally in contracts and agreements. Rôles, responsibilities, authorities and accountabilities can be incorporated or referenced separately (*e.g*. conformity with ISO/IEC 27001 and the organisation’s information security policies may be specified, without necessarily elaborating on the details).

When engaging third parties for professional services such as network operations, the rôles, responsibilities, authorities and accountabilities may be included in contracts and agreements or referenced separately. For instance, compliance with applicable laws and regulations, plus

conformity with ISO/IEC 27001 and the organisation's information security policies, may be stipulated briefly without elaborating on the details.

6 Planning

6.1 Actions to address risks and opportunities

6.1.1 General

Requirement

While planning for the ISMS, the organisation uses the internal and external issues (from clause 4.1) and interested parties' requirements (from clause 4.2) to determine risks and opportunities relating to the ISMS.

Explanation

Essentially, management justifies the organisation's adoption of an ISMS, elaborating on the anticipated business benefits and possible risks.

Guidance

Systematically reducing the frequency and severity of costly incidents involving information by improving information security is the main benefit of the ISMS. Other benefits include:

- Streamlined information and information risk management processes boosting cost-effectiveness and productivity;
- Greater assurance and confidence in the organisation's security posture;
- Improved organisational resilience and business continuity;
- Proactive adoption of good security practices such as secure-by-design;
- Competitive advantages due to management's demonstrable commitment to security, enhanced organisational trustworthiness and stronger reputation;
- Additional opportunities for collaboration and innovation.

Risks arise from a combination of factors such as:

- Inherent weaknesses in IT systems, devices and networks or in business activities involving information (*e.g*. using email or social media);
- Malware, hacks or other cyberattacks, natural disasters, legal and regulatory changes or frauds;
- Adverse business consequences (*e.g*. reduced productivity, missed deadlines, penalties, reputational damage or brand devaluation, loss of custom or funding).

Stakeholders (*e.g*. organisation owners, regulatory bodies, business partners, workers) may have different concerns about the risks. Analysing their perspectives helps build a comprehensive picture of the risk landscape.

Diligent analysis of risks and opportunities establishes a sound business foundation for the ISMS, clarifies priorities and identifies the key objectives worth measuring (clause 9.1).

Aside from reducing risks involving information through better information security, the management system has governance advantages. Senior management gains better visibility and control over the information security situation, enabling systematic improvements where justified, and fewer nasty surprises.

6.1.2 Information security risk assessment

Requirement

The organisation documents and follows a process to assess its information risks.

Explanation

The details of the process can vary between organisations and situations, although the guidance in ISO/IC 27005 and ISO 31000 is widely valued. A sequential approach typically involves:

a) Identifying risky situations, occurrences or incidents with the potential to harm the organisation in some way involving information;

b) Analysing the risks to gain insight as to their nature, probability and severity;

c) Quantifying the risks to focus attention, resources and effort accordingly;

d) Evaluating the risks against predetermined criteria to decide on the most appropriate risk treatments in the next stage (see clause 6.1.3).

Guidance

Information risks (risks pertaining to information) are the crux of the ISMS, making this and clauses 6.1.3, 8.2 and 8.3 significant.

ISO/IEC 27005 provides valuable guidance in this area.

Identifying risks before incidents eventuate can make the difference between thriving, surviving, faltering or failing. At the very least, advance warning reduces the shock when incidents occur and gives management and the organisation opportunities to prepare for that eventuality, increasing resilience.

Analysing, quantifying and evaluating identified risks enables rational prioritisation and focus, leading-in to the exploration of risk treatment options.

The requirement to retain documented information about the risk assessment process suggests a procedure plus the associated records such as prioritised lists of risks, and minutes of risk meetings or workshops. The records constitute evidence providing assurance that workers diligently and consistently follow the procedure (clause 8.2). Given the requirement in clause 4.4, even a well-written procedure can be a liability if it is not being followed diligently in practice. The meaning of 'documented information' is explained in Annex B.

6.1.3 Information security risk treatment

Requirement

The organisation develops and documents a process for treating information risks.

Explanation

In this context, treating risks generally means reducing them using information security controls if management decides that they are unacceptably high and the selected controls are cost-effective. It may also mean avoiding them (by not doing some risky activity), sharing them with others (such as insurers, suppliers, partners and customers), or simply accepting them as they are. The risk treatment process brings greater consistency to the related decisions through rational analysis of the risks and treatment options.

The phrase 'necessary controls' in clause 6.1.3 means information security controls that management has decided are appropriate for the organisation. None of the Annex A controls are formally required by the standard. The information security risk assessment process (clause 6.1.2) is the mechanism to determine which controls are necessary.

Guidance

Clause 6.1.3 requires *'documented information about the information security risk treatment process'* but does not elaborate on that specific requirement. In practice, the requirement can be satisfied by a written Statement of Applicability (specified in clause 6.1.3d) and information security risk treatment plan (clause 6.1.3e).

The standard specifies four things in the Statement of Applicability:

1) A list of the information security controls that management has decided are necessary;
2) Justifications for those controls explaining that they are necessary to reduce unacceptable information risks;
3) The implementation status of the controls: to what extent are they implemented?
4) The basis on which management has decided that any or all the Annex A controls are unnecessary.

The standard says nothing about the content or format of the risk treatment plan, giving management full discretion to interpret the requirement as they wish. Options include:

- A programme management plan to implement the necessary controls during the design and build phases of an ISMS implementation project;
- A strategy or general approach to the assessment and treatment of information risks;
- Proposals, business cases *etc.* for management to approve the implementation of information security controls requiring significant investments;
- Target dates or timescales within which the necessary controls are to be fully implemented;
- Details of rôles, responsibilities, accountabilities and expectations for risk owners, project managers, control testers and others involved in the implementation process;
- Other approaches that management determines are valuable for the business or satisfy stakeholders' needs (*e.g.* approved and funded project plans for the implementation of information security, privacy or safety controls demanded by applicable laws, regulations or contractual clauses).

Further documentation may also be retained in connection with clause 6.1.3, such as:

- Notes from meetings to consider the risk assessment results, justify and select necessary controls, approve or authorise them *etc.*;

- Agendas, attendee lists and minutes from regular security committee meetings that review and reconsider the organisation's risks and controls;
- Reports from management reviews (clause 9.3), internal audits (clause 9.2), penetration tests, application security testing, supplier security assessments *etc.* demonstrating that the controls are or are not adequately reducing the risks.

Clause 6.1.3 requires management to check that potentially valuable information security controls have not been overlooked by systematic comparison against Annex A.

Management's tolerance or appetite for risk is subjective and difficult to define, as it depends on both the risks, the context and subjective opinions. Changing economic or business conditions, for example, affect the organisation's ability and willingness to take risks. Strategic initiatives may involve deliberately taking risks that would normally be unacceptable, or conversely the options may be risk-limited. Individual managers may be more or less risk-averse, perhaps selectively willing to accept certain types of risk but not others. Given subjectivity and dynamics, it is difficult to allow management sufficient flexibility to make difficult business decisions in a structured and justifiable manner.

6.2 Information security objectives and planning to achieve them

Requirement

Management determines the organisation's objectives relevant to information risk, security and the ISMS, and makes plans to achieve them.

Explanation

Documented information security objectives or goals clarify what the organisation intends to achieve through the proactive and systematic management of information risks. Strategies and plans explain how the objectives are to be met in practice.

Guidance

Information security objectives may be formulated and stated in various ways and levels, such as:

- Broad, high-level statements *e.g.* "protect the organisation against loss of confidentiality, integrity and availability of information" or "adopt generally-accepted good security practices";
- Strategic statements concerning the organisation's investment in appropriate information security arrangements "for business reasons", elaborating on the anticipated benefits such as increased custom, reduced losses, greater assurance and trustworthiness, or brand enhancement;
- Outcomes or goals *e.g.* "reduce the number and severity of incidents involving information" or "contain risks to information within acceptable bounds";
- Specific targets or thresholds such as "reduce the estimated costs of information security incidents by 10% per year";
- Statements in support of other business strategies, objectives, policies, terminology *etc.*

Clause 6.2 requires objectives to be measurable (if practicable) suggesting a link to clause 9.1. Measuring the rate at which identified objectives are - or are not - being achieved is a powerful

approach addressing points b), d), e) and f) in this clause. Doing so generates information that may be used both to assure management that adequate progress is being made, and to prompt appropriate intervention if things are not going to plan. Either way, management has the information and control mechanisms to drive achievement of the objectives that they have either defined or endorsed.

Clause 6.2 also explicitly links from point c) to the risk assessment process (clause 6.1).

Whereas clause 6.2 does not formally require documentation concerning the associated plans, that is an obvious way to demonstrate conformity with the standard and direct the organisation accordingly. Points h) through k) reflect a typical planning approach, while point l) reinforces the need for measurements and monitoring as noted above.

Defined objectives, goals, targets *etc.* are fundamental to most directed and concerted activities, hence this is another significant clause. The analysis, understanding, insight and intent involved in defining, setting and achieving objectives requires genuine engagement by management, including senior management.

Since clause 6.3 concerns changes to the ISMS itself, the changes covered by clause 6.2 are primarily changes to the information security controls and activities being managed through the ISMS.

6.3 Planning of changes

Requirement

Necessary changes to the ISMS are planned and completed.

Explanation

Having gone to the effort of designing, building and operating an ISMS, it would be risky for it to be changed without a similar degree of management review, authorisation and control.

Guidance

Many situations may prompt changes to the ISMS, such as:

- Evolving standards of good practice, such as updates to ISO/IEC 27001;
- Repeated or significant nonconformities indicating the need for corrective actions to the ISMS to reduce the risk of recurrence (clause 10.2);
- Changes in information security-related requirements, such as new laws, regulations, contracts, or different interpretations or priorities (clauses 4.1 and 4.2);
- Attractive ISMS improvement opportunities involving substantive changes (clause 10.1) such as extending the ISMS scope (clause 4.3);
- Appropriate responses to measurements, audits, reviews *etc.* indicating the need for change (clause 9);
- Changes in the business such as organisational restructuring, evolving relationships and collaborations with other specialist functions or management systems (clauses 4.1 and 4.2);
- Updated strategies, policies, procedures and approaches such as the adoption of quantitative risk assessment methods (clause 6.1.2).

Planning and completing major or significant ISMS changes may involve activities such as:

- Researching and proposing changes, including the scope, objectives, dependencies, risks *etc.*;
- Planning the resources and activities necessary to manage and execute the changes;
- Reviewing and authorising the changes plus strategic aspects, scope, objectives, anticipated benefits, interim reviews, progress reporting, oversight and other change management controls *etc.*;
- Allocating adequate resources to achieve the objectives;
- Addressing risks, barriers and issues during execution;
- Securing the benefits and learning from the experience.

Clause 6.3 does not specify the type or scale of ISMS changes, nor the nature of the planning required. The clause does not necessarily apply to all ISMS changes: only 'significant' changes may require formal authorisation, where 'significance' is organisation and context-specific. Therefore, management may adopt an approach that is suitable and beneficial for the organisation.

Documents such as ISMS change requests, approvals and implementation plans may help stabilise the approach and demonstrate conformity but are not formally required by ISO/IEC 27001. In a small organisation, or for minor changes, management understanding and support for the planning and execution of ISMS changes may be ascertained through interviews or discussion rather than written documentation.

7 Support

7.1 Resources

Requirement

The resources necessary for all phases of the ISMS lifecycle are provided.

Explanation

An ISMS requires the sustained commitment of adequate resources to continue operating and delivering on its objectives, indefinitely.

Senior management can demonstrate its support for the ISMS by providing the resources needed to specify, design, build, implement, operate, maintain and continually improve it. The resources include:

- Sufficient workers with the knowledge and competencies to undertake various rôles and responsibilities associated with each phase or activity (clause 5.3);
- Sufficient budget to procure necessary information security tools, technologies, systems and services (*e.g*. managed security services, security training, penetration testing), plus information such as international standards;
- Senior management's focused attention when required to make key or urgent decisions;
- Sufficient priority and emphasis to make adequate progress alongside other important business activities;
- Access to additional resources if required to assist with specialist tasks and peak workloads;

- Sensible deadlines and expectations re the results that can realistically be achieved within the time and resources available.

Guidance

Once the ISMS is fully implemented and operating routinely, resource needs typically stabilise. The workforce and budgets can be managed in proportion to the business benefits gained (using information obtained from the activities in clause 9), taking account of historical performance and projected workloads as well as resource availability.

Early in the ISMS lifecycle, the situation is more fluid, as with any new business development, project or initiative. The initial stages, characterised by uncertain scope and objectives, pose particular challenges for resource planning. Consulting those already involved in the ISMS, alongside experienced managers and specialists from functions like IT, HR, Risk Management, Compliance, Internal Audit, Procurement, Finance and Project or Programme Management, can prove invaluable.

ISMS resourcing levels can be treated as a risk management activity. The possibility of under-resourcing the ISMS can be reduced through flexibility, such as:

- The use of temporary resources (*e.g*. contractors and consultants, or workers seconded from other functions or business units) for short-term requirements;
- Career-planning, mentoring, training and motivation of suitable workers with a view to securing their job satisfaction and long-term engagement;
- Multi-skilling workers such that they can support each other as required through teamworking;
- Conventional investment management practices such as sound business cases to justify the procurement of expensive security products and services, along with competent project and procurement management;
- Budgeting suitable contingency sums to cover unexpected costs, with the appropriate financial management controls;
- Attentive and responsive management engagement (monitoring, oversight, direction and control).

Conversely, the possibility of over-resourcing the ISMS may be addressed by:

- A strong business focus and clarity around optimising the net value of the ISMS;
- Dynamically updating plans and deadlines to take advantage of opportunities that arise;
- Attentive and responsive management engagement (it works both ways).

Gathering and considering pertinent information, and accumulating experience through practice, helps get the ISMS resourcing just right – an example of continual improvement (clause 10.1).

7.2 Competence

Requirement

The organisation determines the need and acquires workers with the competencies necessary for the ISMS.

Explanation

Determining the need for various competencies, knowledge and skills involves analysing information concerning the ISMS scope (clause 4.3), information security objectives and plans (clause 6.2), and rôles and responsibilities (clause 5.3).

Acquiring suitable workers may involve:

- Assessing the competencies, skills and knowledge of current workers;
- Deploying and tasking current workers appropriately;
- Training and up-skilling workers, motivating and supporting or mentoring them to take up new positions;
- Designing positions that take advantage of available workers;
- Employing, seconding or contracting specialists with the requisite competencies.

Guidance

Effectively and efficiently implementing and operating the ISMS obviously requires workers with the appropriate capabilities and interests. Aside from technical competencies and qualifications, soft skills and personalities can make a significant difference to the function of the team as a whole.

If required, HR specialists can help conduct a job needs analysis.

The requirement in clause 7.2 to retain documented information can be satisfied by evidence of the analysis, the competencies needed (*e.g.* job descriptions, structure charts showing specialist and general rôles), currently available (*e.g.* personnel records) and still required (*e.g.* approved appointments, vacancy notices).

Due to its nature, there may be substantial risks associated with those closely involved with the ISMS. Exemplary levels of personal integrity and trustworthiness are essential for highly trusted security-related rôles, particularly for those working independently in privileged positions. Reducing the risks may involve:

- Strong references plus identity and background checks prior to appointing or promoting people to highly trusted rôles;
- Appropriate management oversight, peer review, monitoring and logging of activities, particularly for newly-appointed people and in situations of heightened risk (*e.g.* special projects, or when there are indications of unethical or inappropriate behaviour or personal problems);
- Clarity and training on the associated expectations and requirements;
- Honest appraisals and guidance;
- Appropriate, timely responses and consequences if the expected high standards are not being met.

7.3 Awareness

Requirement

Workers are made aware of the information security policy and what is expected or required of them.

Explanation

Achieving and maintaining security awareness requires effort to counter the gradual decay of knowledge and reduced conformity caused by ignorance and carelessness.

Guidance

To be effective, security awareness activities need to both inform and motivate. Passively and occasionally providing information may have little effect on decisions and behaviours, whereas a proactive, engaging, persuasive and sustained awareness approach can influence individuals' attitudes and behaviours, gradually strengthening the corporate security culture.

Covering different aspects of information risk and security keeps the information flowing, topical and relevant to the business.

Specialists in awareness, training and marketing may advise or assist with the design, preparation and delivery of awareness content.

The phrase "*persons doing work under the organization's control*" in clause 7.3 is a reminder to include contractors, consultants, temporary workers, student interns *etc.* in the security awareness activities, not just employees (management and staff).

Whereas security awareness tends to be quite general, training can provide more focused, in-depth coverage and tailored guidance or direction to workers with specialist rôles (clause 5.3).

7.4 Communication

Requirement

The organisation determines the need to communicate pertinent information risk and security matters internally and externally.

Explanation

Various parties need to be involved with or informed about information risks, information security, privacy, conformity and compliance, objectives (clause 8.1), performance (clause 9), achievements, improvement opportunities (clause 10.1), change initiatives (clause 6.3) *etc.* Such communications link all the ISMS processes together into a coherent and effective management system, contributing to the organisation's management processes as a whole.

Furthermore, those with relevant, important or urgent information to share need the appropriate mechanisms or contacts to communicate effectively.

Guidance

The audiences and sources of information to be communicated include insiders (the workforce – management and staff) and outsiders (stakeholders such as customers, partners, owners, regulators and auditors).

The topics and messages to be communicated may include:

- Pre-warning of changing obligations and expectations such as anticipated new or updated laws, regulations, policies, procedures and guidelines;

- Timely reminders of current rules, priorities, challenges and focus areas of concern to management and the business;
- Information about risks involving information, data, computer and network systems, intellectual property, proprietary knowledge, trade secrets, personal information *etc.* and the associated risk management activities;
- Technical, physical, procedural and conceptual security matters;
- Disclosures about vulnerabilities, threats, compromises and concerns;
- News of incidents, root causes plus countermeasures;
- News of near-misses and incidents averted or avoided, celebrating success and reinforcing the value of information security;
- ISMS status reports presenting and explaining relevant measures (clause 9.1) along with proposals and action plans to address issues or pursue improvement opportunities (clause 10);
- Follow-ups and progress reports giving additional information;
- Other matters of concern or interest.

Creative approaches involving multiple modes and points of communication (such as emails, seminars, presentations, newsletters and personal conversations) help inform and engage various audiences and individuals with differing interests and concerns.

Since there are risks associated with the information being communicated, controls such as confidential reporting mechanisms (responsible disclosures or whistleblowing), the collection and analysis of evidence to substantiate or refute concerns, and timely escalation paths may be important.

7.5 Documented information

7.5.1 General

Requirement

The ISMS includes documentation required by ISO/IEC 27001 and necessary for the organisation.

Explanation

While ISO/IEC 27001 explicitly requires just 14 types of documentation (see Annex B), the organisation typically requires more for its own business, security and assurance purposes.

Although there are other ways to ensure that the ISMS is properly designed, implemented and operated (clause 4.4), documentation can provide clear evidence to demonstrate that. Documentation is useful for communicating direction, guidance, training and awareness purposes (clauses 7.3 and 7.4). It stabilises and formalises important operational activities (clause 8), facilitating reviews and audits (clauses 9.3 and 9.2), and systematic improvements to the ISMS (clause 10).

Documentation (such as strategies, policies and procedures) can be an important, efficient and effective way to specify information security controls, both manual and automated. Records generated by or associated with controls (such as authorisations and logs of access to information)

provide assurance and historical information that may be used for various purposes, reinforcing the controls.

Guidance

See Annex B.

A minimalist ISMS with only the 14 mandatory types of documentation is unlikely to satisfy the requirements of all stakeholders. However, an ISMS with an inordinate and excessive amount of documentation is likely to be costly and difficult to maintain, increasing the risks. In other words, management needs to strike a balance. Remember, the main purpose of the ISMS is to protect and enable legitimate exploitation of information – and that includes ISMS documentation! Documentation is just part of the mechanism supporting that aim.

7.5.2 Creating and updating

Requirement

The organisation requires structured processes for creating and managing important documentation.

Explanation

Clause 7.5.2 concerns the management processes or activities typically associated with more formal forms of documentation, ensuring for example that information security policies and procedures are suitable and adequate to satisfy the requirements of ISO/IEC 27001 and the organisation.

Guidance

Corporate standards and templates with spaces or fields for the required information or metadata (such as document titles, owners and histories) help document creators conform consistently with the requirements, improve utility and ease review.

Consistent styles, formats and layouts of documentation associated with the ISMS are similar to branding on corporate products, linking disparate items together as part of the whole while emphasising professionalism and quality.

7.5.3 Control of documented information

Requirement

The organisation manages risks relating to documentation.

Explanation

Given confidentiality, integrity and availability concerns for documentation associated with the ISMS (and more generally, information concerning information risk and security), clause 7.5.3 is a further reminder to identify, evaluate and treat the risks.

Guidance

Access and circulation controls reduce the risk of information falling into the wrong hands or failing to reach the intended audiences.

Controlling changes to documents and records may also involve access controls throughout their lifetimes (*i.e*. creation, storage, communication, usage and disposal) plus versioning, reviews and authorisations to facilitate intended and appropriate changes while preventing unintended and inappropriate changes.

Quality assurance (such as structured processes to draft, review, update and approve important documentation) and quality control measures (such as regular plus ad hoc checks or audits of policies and procedures) reduce the risk of integrity failures such as incomplete or inaccurate content, plus inconsistencies across the entire suite.

Further to the note in clause 7.5.1, while insufficient control may fail to address the risks, excessive control over documentation is unnecessary, costly and may be counterproductive (*e.g*. encouraging workers to evade or bypass necessary controls). Implement appropriate controls to reduce unacceptable risks and so achieve information security objectives.

8 Operations

8.1 Operational planning and control

Requirement

ISMS operational processes are planned, implemented and controlled to achieve the information security objectives.

Explanation

Building on clause 4.4, clause 8.1 requires the organisation to design, operate, monitor and manage its processes to satisfy the information security objectives (clause 6.2). This may involve more detailed planning.

Process control in the ISMS context involves the use of performance measurements and assurance (clause 9) and appropriate interventions to direct and guide activities towards the achievement of information risk and security objectives.

Guidance

This requirement is necessarily vague and generic due to the enormous variety of contexts to which it applies. Essentially management institutes whatever information security controls are necessary to reduce (or at least prevent increases in) information risks, including management information. Proactive management ensures that the controls not only operate as planned (requiring assurance) but, in so doing, fulfil the organisation's objectives.

ISMS processes may be supported and enabled by automation, including information systems, tools and services. Although the clause 8.1 requirement does not explicitly refer to them, they should also

be planned, implemented and controlled to achieve the information risk and security objectives, given their close association with the ISMS processes.

Similarly, integration of the ISMS into the wider business implies the need to plan, monitor and control processes, activities and information spanning the ISMS scope boundary. For example, identifying, analysing and evaluating risks to business information requires extensive knowledge about the information, while treating the risks generally involves information security controls that are operated by or involve workers and activities beyond the ISMS. This is why clause 4.3 refers to the applicability as well as the scope of the ISMS.

There may be information risk and security aspects to the supply of processes, products, services or information to the organisation by external providers, including those relating to the ISMS itself such as:

- Threat and vulnerability information services;
- Assurance services such as auditing and certification;
- ISMS support systems, tools, techniques and templates;
- Recruitment, legal and other professional services.

The requirement for documentation in this clause is discretionary. Management determines the need for assurance that the security processes are operating effectively. A blend of documented and undocumented information may provide the necessary assurance *e.g.* direct observation and management oversight of ISMS processes in operation, supplemented by records, measurements, management review reports and audit reports (clause 9).

8.2 Information risk assessment

Requirement

Regular and *ad hoc* information risk assessments are performed in accordance with clause 6.1.2.

Explanation

Since the ISMS hinges on information risks, the systematic identification, analysis and evaluation of such risks, plus their treatment (clause 8.3) are core activities.

Guidance

Risk assessment benefits from strong leadership, policies and responsibilities (clause 5). Workers who understand the associated terms and rationale are more likely to generate valuable and accurate insight. This has implications for:

- Clarity of the associated policies, procedures and guidelines;
- Information security awareness, training and education;
- Engagement and participation of relevant workers in the process;
- Management oversight plus other assurance and conformity measures;
- The quality and management of information relating to risks.

There are inevitably risks associated with risk management, given the inherent uncertainties in predicting or attempting to determine the future based on finite historical and present information.

A key objective of the ISMS is to bring stability, structure and focus, improving management control. However, management should appreciate the possibility of imperfections in the risk management processes and the ISMS, planning accordingly *e.g*. incident and business continuity management, as well as driving continual improvement (clause 10.1).

8.3 Information risk treatment

Requirement

The risk treatment plan is executed.

Explanation

The risk treatment plan (clause 6.1.3 e) may describe how identified and evaluated risks are to be treated (*e.g*. by implementing particular information security controls), or guide the process of treating assessed risks in a more general or strategic sense. Either way, it is clearly important that risks are treated appropriately, hence the associated requirement for documentation.

Guidance

The quantification and evaluation or significance of risks may indicate implementation priorities or sequences, as well as determining the types of risk treatment to be applied (*e.g*. avoid, share, reduce or accept; preventive, detective or corrective controls; organisational, physical or technical controls). However, there are other factors involved in the planning, execution and management of the risk treatment plan, such as:

- The status and adequacy of existing risk treatments, affecting current risk levels;
- Prerequisites and linkages between strategic or operational elements such as information security tools and systems;
- Constraints on resources, including parallel activities and even more important or urgent issues (competing priorities);
- Options and choices to be explored, evaluated or trialled before pressing ahead;
- Detailed analysis and planning of more complicated or involved activities, including coordination with other business functions;
- Stakeholder requirements or objections;
- Creative or opportunistic possibilities such as taking advantage of and supporting other corporate change initiatives.

There are relationships and dependencies involved in planning and executing any complex situation, suggesting the need for iterative and responsive approaches. No matter how well conceived, planned and controlled, in practice things do not always go entirely to plan– in other words, there are risks associated with this clause as well as clause 8.2. Identifying and progressing improvement opportunities in this area can contribute to the maturation and value of the ISMS.

9 Performance evaluation

9.1 Monitoring, measurement, analysis and evaluation

Requirement

The organisation determines requirements for the monitoring, measurement, analysis and evaluation of ISMS performance.

Explanation

The purpose and objectives of the ISMS (as developed and refined in several other clauses) largely determine what needs to be measured. For example, if "reducing the number and severity of information security incidents" is a key ISMS objective, it is clearly worth measuring those parameters in some fashion to ascertain whether the key objective is being met, and at what rate. Subsidiary or supporting objectives may be addressed in the same manner.

The organisation's requirements may involve the acquisition, communication, evaluation and use of management information relating to the ISMS. Internal reporting arrangements, for instance, may include:

- Routine and *ad hoc* reports (including ISMS internal audit and management review reports) and other means of presenting and analysing information such as presentations, briefings and dashboards;
- Escalation paths and mechanisms to pass serious or urgent matters efficiently to senior management;
- Communications mechanisms giving stakeholders opportunities to provide feedback on the ISMS including its performance relative to their objectives.

Guidance

The requirements may be expressed by, determined or surmised for both internal and external stakeholders such as:

- Management from top to bottom;
- Customers, business partners, regulators or other authorities;
- Owners and investors in the organisation;
- Information security and related professionals;
- Other functions or parts of the business with significant interests in protecting and exploiting information plus the associated information security controls such as IT, research and development, risk management, privacy, safety, HR, operations, compliance and internal audit.

The information gained through monitoring, measurement, analysis and evaluation may be of interest and value in different levels or parts of the organisation, both within and outside the ISMS scope. It can support decision-making and drive continual improvement.

The way objectives are formulated (framed and described) can substantially affect their measurability. The predicted need for measurements can help bring clarity and focus to the objectives as they are formulated, for example by considering whether it will be feasible without

excessive costs or complications to determine whether the objectives are or are not being satisfied. Vague objectives that cannot readily be substantiated may be filtered out or refined, avoiding operational, measurement and hence management issues arising later if they had been adopted. Since later practical problems may not be entirely evident at the outset, however, this is another iterative aspect to the ISMS, presenting improvement opportunities as the organisation learns the risks, costs and benefits associated with performance evaluation and assurance.

9.2 Internal audit

9.2.1 General

Requirement

The organisation develops, uses and maintains an ISMS internal audit programme.

Explanation

Internal audits are a powerful assurance mechanism, generating credible, pertinent management information through the independent acquisition, evaluation and analysis of information. The audit objectives or criteria include business objectives for the ISMS plus the requirements specified in ISO/IEC 27001.

Guidance

Clause 9.2.1 specifies that audits are to be conducted at 'planned intervals'. Since the intervals are not specified, they are for management to determine, taking account of the costs and benefits.

In practice, ISMS internal audits can be valuable:

- In the early stages of an ISMS when it is being specified and built, contributing to the strategic planning, definition of objectives *etc.*;
- Prior to certification or surveillance audits, providing opportunities for workers to practice and prepare as well as extra time to address any issues;
- When risks, issues or incidents arise that are exceptional or persistent, suggesting problems within the regular ISMS activities;
- In other situations where the assurance or independent guidance is needed *e.g.* when re-planning the ISMS, integrating it with other management systems, or in response to deteriorating measurements and performance threatening the achievement of objectives.

9.2.2 Internal audit programme

Requirement

The organisation manages a programme of ISMS internal audits.

Explanation

The internal audit programme may:

- Outline a planned sequence of internal audit activities or focus areas over one or more years;
- Describe a general approach to the planning, scoping and execution of internal audits (such as a strategy or policy);
- Record pertinent details of internal audits completed, in progress or planned;
- Take another approach, provided it satisfies the requirements of ISO/IEC 27001. Clause 9.2.2 specifies several requirements concerning the planning, conduct and recording of ISMS internal audits, including documentation (see Annex B).

Guidance

Factors relevant to ISMS internal auding include:

- Auditor independence. Those more closely involved in the ISMS inevitably have preconceptions and interests in it that may limit their perspectives, taint their understanding and cloud their judgment. Auditors gather and examine information objectively, seeing things with fresh eyes.
- Auditor competence and knowledge. ISMS auditors should be familiar with the requirements of ISO/IEC 27001, plus the practice of management system auditing (*e.g.* ISO 19011) and broader considerations such as risk, security, control and governance concepts in the information and IT context. They also need to be skilled analysts and communicators.
- Auditor suitability. Personal characteristics such as diligence, rationality, assertiveness and discretion are relevant.
- Audit processes, techniques and tools, both manual and automated.
- Management understanding and support, for example scoping audits to address areas of concern and provide valuable assurance, allocating suitable resources, authorising auditors' access to pertinent information and workers, and the commitment to consider and respond positively to audit findings.

The following may be helpful:

- ISO/IEC 27006 standards cover certification audits for an ISMS (ISO/IEC 27006-1) or a **P**rivacy **I**nformation **M**anagement **S**ystem (ISO/IEC TS 27006-2).
- ISO/IEC 27007 guides auditors to audit the management system parts of an ISMS.
- ISO/IEC TS 27008 provides guidance on reviewing and assessing the implementation and operation of information security controls.

9.3 Management review

9.3.1 General

Requirement

Senior management reviews the ISMS at planned intervals.

Explanation

Provided the ISMS remains suitable, adequate and effective, it should continue achieving business objectives and generate value for the organisation. It therefore deserves ongoing commitment and support from senior management which should be confirmed from time to time.

Guidance

ISMS management reviews are another form of assurance. As with ISMS internal audits (clause 9.2), the planned intervals and the nature of the planning for ISMS management reviews are not specified in clause 9.3.1. These are for management to determine, given the business context, stakeholder interests and management's requirements or concerns.

ISMS management reviews may:

- Be known by other names such as gap analyses, follow-ups, inspections, focus areas, investigations or re-evaluations;
- Be similar to internal audits, although independence is not an absolute requirement and they may be less formal and less costly;
- Take anything from an hour or so to several weeks, even months to complete;
- Bring significant matters to the attention of senior management or other stakeholders such as the security committee, board or authorities.

Rather than being pre-planned or scheduled in advance, ISMS management reviews may also be triggered by various events or opportunities. Post-incident reviews, for example, present opportunities to gather, analyse, draw conclusions and make recommendations following compromises, breaches, failures, near-misses or other information security incidents, prompting changes to improve the arrangements and prevent recurrences.

9.3.2 Management review inputs

Requirement

Clause 9.3.2 specifies various matters to be taken into consideration by ISMS management reviews.

Explanation

The wording indicates certain areas that should be considered, but does not preclude management from considering other aspects as well. Different approaches or concerns may be pertinent and applicable to the organisation's evolving context.

Guidance

ISMS management reviews can focus on specific topics or be more broadly scoped, for example reviewing:

- The scope and applicability of the ISMS (clause 4.3);
- ISMS resourcing, planning, priorities, policies and leadership (clause 5);
- Information risk and security-related governance arrangements, structure, responsibilities, reporting lines *etc.* (clause 5.3);

- Comparison of risk assessment methods, techniques or approaches (clause 6.1.2);
- The rate at which information risk and security objectives (clause 6.2) are being approached, met or exceeded;
- One or more proposed ISMS changes (clause 6.3);
- Adequacy and suitability of ISMS and information security resourcing levels (clause 7.1);
- Quality and suitability of ISMS plans and management controls (clause 8.1);
- The suitability of the ISMS measurements and other management information (clause 9.1);
- Preparedness for ISMS internal audits (clause 9.2) and certification;
- Persistent themes or issues arising from nonconformity and corrective action reports (clause 10.2);
- What next? Future strategic directions and long-term objectives for information risk and security management;
- Suitability and effectiveness of the organisation's approach to risk management, risk assessment, risk appetite/risk tolerance *etc.*;
- Business continuity management including resilience, redundancy, recovery and contingency preparedness;
- Event, incident and crisis management;
- Identification, authentication and access controls;
- Authorisations and approvals;
- Conformity and compliance, exceptions and exemptions, enforcement and reinforcement;
- Integration of management systems, interoperability and consistency;
- Maturity of the ISMS, benchmarking against peer organisations;
- Supply chain risk management;
- Innovation and creativity in the organisation's management of risks and controls for information;
- And so on. There are many possible areas of interest and concern, plus potential improvement opportunities to explore.

9.3.3 Management review results

Requirement

ISMS management reviews result in decisions on improvements and changes to the ISMS.

Explanation

ISMS management reviews are intended to prompt proactive responses rather than passively describing the situation. There is a requirement for documentation (such as ISMS management review reports) to formalise and substantiate this, providing a record for current and future reference.

Guidance

References to senior management and the management may suggest a high-level governance or strategic perspective for ISMS management reviews. However, lower-level operational issues or

improvement opportunities may be significant or numerous enough to warrant management attention and engagement.

ISMS management reviews can be risk-aligned, business-aligned or take some other approach. Aside from requiring the topics in clause 9.3.2 to be considered, clause 9.3 offers guidance rather than constraining management's options.

10 Improvement

10.1 Continual improvement

Requirement

The ISMS is consistently improved over time.

Explanation

Genuine, substantive improvements in broad areas such as ISMS suitability, adequacy and effectiveness indicates that the ISMS is maturing and adding more value to the business.

Guidance

Expectations or objectives for the ISMS include those relating to or arising from:

- The needs and expectations of interested parties (clause 4.2);
- Strategic direction, policies and responsibilities expressed by senior management (clause 5);
- Information risk and security objectives (clause 6.2);
- Performance measurements (clause 9.1);
- ISMS internal audits (clause 9.2);
- ISMS management reviews (clause 9.3); and
- Nonconformities and corrective actions (clause 10.2).

Significant changes to improve the ISMS should be planned (clause 6.3), defined, resourced and managed, with the approval of senior management. Clear objectives (such as goals and non-goals) may become success criteria and facilitate measurement and management control, ultimately increasing the chances of success.

Maturity involves a gradual process of advancement and improvement, involving a blend of directed and driven changes (innovation) with emergent, evolutionary or cultural changes that occur naturally. The drivers may be internal (*e.g.* reorganising or restructuring the business), external (*e.g.* advances in information security tools and techniques) or both (*e.g.* creative adaptation and innovative exploitation of approaches or ideas from peers, advisors, academia, suppliers or thought-leaders).

ISO/IEC 27001 uses the term 'continual' rather than 'continuous' improvement to indicate changes in the rate and direction over time. Social, economic, market, political or security pressures, for example, can drive, support, interfere with or prevent changes during certain periods. Generally

speaking, the pace and extent of changes both reduce as the ISMS matures, but incidents or opportunities can prompt significant improvements to an otherwise stable and mature ISMS.

10.2 Nonconformity and corrective action

Requirement

The organisation responds actively and positively to nonconformities and the need for corrective actions.

Explanation

Potential ISMS improvement opportunities should be evaluated and progressed if appropriate, meaning they contribute to or facilitate achievement of objectives such as adding value to the organisation.

Guidance

The organisation is required to fulfil its mandatory obligations, and expected to fulfil discretionary requirements to which it has committed. In the ISMS context, the obligations and requirements relevant to information risk, information security, privacy, safety *etc.* may include:

- Applicable laws and regulations;
- Terms in contracts, agreements, industry codes *etc.*;
- ISO/IEC 27001 and other standards;
- Corporate strategies, policies, procedures *etc.*;
- Expectations of various stakeholders such as the organisation's customers and owners;
- Ethical, social, governance and environmental pressures from society.

Where feasible, economic or necessary, root causes of issues and incidents should be identified and addressed, particularly where the issues and incidents are significant or persistent.

Documentation can help capture/describe and record ISMS improvements.

Nonconformities may prompt reconsideration and refinement of discretionary requirements, as well as or instead of simply insisting on conformity.

Although fundamental changes to the ISMS may be costly, disruptive and risky, they may be more valuable than superficial changes which fail to resolve the causes, leading to reoccurrence and, perhaps, a gradual worsening of the situation.

Annex A: The information security controls in ISO/IEC 27001

ISO/IEC 27001 Annex A contains succinct summaries of information security controls that are explained in greater detail in ISO/IEC 27002[4].

The control categories, attributes and wording in Annex A support due consideration of the potential applicability of the listed controls, but are not meant to constrain management's options. Additional, variant, custom or alternative controls may be selected from any source (*e.g.* other standards or bespoke controls) if the Annex A wording is not entirely appropriate.

The information security control descriptions in ISO/IEC 27002 lay out roughly a page of details under the following sections for each control:

- **Attributes** – a table showing the applicable attribute values for each of five control attributes (control type; information security properties; cybersecurity concepts; operational capabilities; and security domains). This can be used to identify specific types of control according to their desired characteristics (*e.g*. preventive controls concerning confidentiality, designed to prevent inappropriate disclosure of sensitive information);
- **Control statement** – a succinct one-sentence summary of the control with almost identical wording to Annex A[5];
- **Purpose** – what the information security control is meant to achieve in terms of mitigating information risks;
- **Guidance** – practical advice concerning what the control entails and how it is normally implemented;
- **Other information** – further points to consider.

[4] Although ISO/IEC 27002 is cited by ISO/IEC 27001, is not normative since the Annex A controls are not mandatory. We recommend studying it for about a page of details expanding on the line or two per control in Annex A.

[5] Whereas ISO/IEC 27002 uses "should" indicating a suggestion or recommendation, Annex A uses "shall" indicating requirements in accordance with the ISO/IEC directives, despite the listed Annex A controls *not* being requirements in fact. Annex A is normative and must be consulted as required by clause 6.1.3, but the listed controls may or may not be selected.

Annex B: Documented information

ISO/IEC 27000 defines 'documented information' as:

> *"information required to be controlled and maintained by an organisation and the medium on which it is contained*
>
> *Note 1 to entry: Documented information can be in any format and media and from any source.*
>
> *Note 2 to entry: Documented information can refer to*
>
> *— the management system, including related processes;*
>
> *— information created in order for the organisation to operate (documentation);*
>
> *— evidence of results achieved (records)."*
>
> *ISO/IEC 27000:2018,*
> *hyperlinked clause references omitted*

Documented information captures knowledge, guides actions, preserves history and facilitates collaboration, fostering clarity, consistency and efficiency.

The following items of documented information are the minimum required for conformity to ISO/IEC 27001:

1. ISMS scope (clause 4.3);
2. Information security policy (clause 5.2);
3. Information risk assessment procedure (clause 6.1.2);
4. Statement of applicability (clause 6.1.3 d);
5. Information risk treatment procedure (clause 6.1.3);
6. Information security objectives (clause 6.2);
7. Personnel records (clause 7.2);
8. ISMS operational information (clause 8.1) – see note ▼
9. Risk assessment reports (clause 8.2);
10. Risk treatment plan (clause 8.3);
11. Security measurements (clause 9.1);
12. ISMS internal audit programme and audit reports (clause 9.2.2);
13. ISMS management review reports (clause 9.3.3);
14. Records of nonconformities and corrective actions (clause 10.1).

Note: the requirement in clause 8.1 reads *"Documented information shall be available to the extent necessary to have confidence that the processes have been carried out as planned."* Strictly speaking, the documentation is discretionary since it is conceivable that someone might gain sufficient confidence without the need for any written records *e.g*. they could simply observe the processes being performed. However, this seems unlikely in practice, particularly if the clause is referring to the confidence of third parties such as certification auditors without ready access to observe activities being performed in real time.

Additional documentation may be valuable or essential for business reasons, such as:

- Information risk and security strategies, proposals, plans, objectives, status reports and deliverables for implementation or change projects *etc.*;
- Topic-specific policies, procedures and guidelines relating to information risk and security;
- Security awareness and training materials, plus the associated attendance records *etc*.;
- Management information such as the agendas, attendee lists, minutes and actions agreed at ISMS management committee meetings;
- Operational records generated routinely in the normal course of business (*e.g*. budgets and expenditure reports, log files, audiovisual security footage, approvals, completed forms, lists and databases) or by exception (*e.g*. post-incident reviews, incident notifications);
- Compliance with applicable laws, regulations and standards, plus the associated business records such as registration or incident reporting details under data protection legislation;
- Contracts and agreements concerning security products and services, including internal service level agreements with corporate functions such as IT, HR, Facilities and Risk;
- Technical materials used for designing, implementing, configuring, training, operating, supporting, monitoring, managing and maintaining systems, including security architectures and designs.

The purposes and uses for documentation include:

- Capturing (recording) important decisions, inputs, activities and consequences;
- Facilitating historical analysis such as tracking performance, identifying trends and improvement opportunities;
- Performance tracking and improvement initiatives;
- Training, knowledge acquisition and skills development;
- Demonstrating and providing assurance of compliance and conformity, or indeed the converse (*e.g*. forensic evidence concerning security incidents; incomplete, inaccurate or false/fabricated documents).

The risks associated with ISMS-related documentation may involve loss of:

- Confidentiality *e.g*. inappropriate disclosure of threats, vulnerabilities, impacts, issues, incidents, concerns, strategies, plans, policies, metrics, reports;
- Integrity *e.g*. incomplete, inaccurate, misleading or fabricated information;
- Availability *e.g*. mandatory or valuable items of information delayed, missing, corrupted, deleted, destroyed, lost;
- Value *e.g*. excessive documentation can be costly to generate, use and maintain, making it counterproductive and inefficient.

Treating such risks can involve:

- Avoidance *e.g*. not documenting activities unnecessarily, in such detail, or in permanent formats;
- Sharing *e.g*. clauses in contracts with security-related suppliers specifying requirements to maintain necessary documents such as records of background checks for new recruits, and evidence that security guards and maintenance workers are regularly inspecting the facilities;
- Reduction using preventive, detective and corrective controls;
- Acceptance *e.g*. where other risk treatments are impractical, inappropriate or too costly, or for risks that are inaccurately, incompletely or ineffectively identified, analysed and treated.

Annex C: ISMS implementation project guidance checklist

These bullet points offer practical advice on how to go about implementing an ISMS.

Project definition, justification, scoping and planning

- ☐ Study the standards, in depth: complete lead implementer training if possible.
- ☐ Study the business, in depth, to understand its objectives, strategies, culture, governance arrangements, existing information risk and security management *etc*.
- ☐ If the organisation has a defined, structured approach for this phase, use it!
- ☐ Build a business case that identifies and promotes the business benefits of the ISMS.
- ☐ Look beyond 'security' and 'compliance' *e.g*. helping management to manage business risks, supporting/enabling other business initiatives and strategies.
- ☐ Identify, explore and elaborate on a broad set of business objectives relating to: information risk and security management; information, cyber, manual and automated security controls; compliance and assurance; resilience; good practice, maturity; efficiency, cost-effectiveness *etc*.
- ☐ Clarify relative priorities for the objectives *e.g*. by ranking them all or grouping them into categories such as 'essential', 'important', 'nice-to-have' and perhaps 'to be avoided'.
- ☐ Be honest about the organisational/governance changes ahead, including the potential disruption, costs and timescales.
- ☐ Be realistic about resourcing, priorities and capabilities.
- ☐ Build-in more than enough slack/contingency to allow for unforeseen difficulties.
- ☐ Offer a do-nothing straw man plus other options as appropriate *e.g*. distinguish essential from important from optional objectives, compare costs *and* benefits of differing ISMS scopes.

Project approval

- ☐ Don't expect the business case to sell itself, no matter how exciting and positive it seems.
- ☐ Hawk it around management, informing them, gathering feedback and amending the proposal.
- ☐ Identify, explore and address genuine concerns, especially blockers.
- ☐ Look for opportunities to align with corporate strategies and other initiatives.
- ☐ Refine the objectives and project proposal, adding explicit details where clarity is needed or helps *e.g*. metrics.
- ☐ While awaiting approval, continue working on the planning and ideally progressing the essential aspects such as information risk assessment.
- ☐ Be crystal clear about those essentials and only compromise in other areas, even if that means the project is refused or deferred.

Implementation activities

- ☐ Aim low, strike high: focus intensely on those essentials, progressing other objectives at lower priority/urgency if resources allow.
- ☐ Where possible, re-use existing content, policies, procedures, controls *etc*., adapting as necessary.
- ☐ Collaborate closely with related teams/functions/organisations/individuals.

- Work to up-skill the core team through training, mentoring and experience on the job.
- Start operating elements of the ISMS as soon as practicable, practising and refining them *and* ideally accounting for the benefits gained (financial or otherwise).
- Look for early wins and promote them: positive feedback is invaluable for motivation and energy.

Project management, oversight, progress reporting and project risk management

- If the organisation has a project management method/approach, use it!
- Work with experienced programme and project managers.
- Establish suitable governance arrangements (*e.g*. structure, reporting, metrics, approvals) for the project as that will evolve into the ISMS governance in due course.
- Play snakes-and-ladders: identify and address risks/issues/setbacks, seizing and promoting opportunities to advance.
- Watch the critical path and anything that does or might consume your contingencies, like a hawk.
- Beware stress and burnout: don't exceed reasonable workloads for long periods, including yours.
- Work hard on clear communications and effective relationships: these will outlast the implementation phase.

Certification and other assurance activities

- Treat certification as an opportunity to improve, more than a hurdle to clear.
- Take time to clarify objectives, identify suppliers and contract with certification bodies.
- Specify experienced and competent certification auditors, anticipating less aggravation and more value-add.
- Line up certification prerequisites such as completed ISMS documentation, records of activities, ISMS internal audits *etc*.
- Line up management to see the purpose and value of assurance regarding the ISMS, information risk and security management, compliance *etc*.
- Line up marketing to promote the certification, enhancing corporate brands, opening new business opportunities *etc*.
- Liaise between the team, management and the certification body closely in the run-up to certification, maintaining alignment and expectations.
- Look beyond the award itself: there is always more to be done, more planning required *e.g*. integrating other management systems.

Transition to business-as-usual

- Plan for a gradual, sequential/piecemeal ISMS build-and-implementation, rather than a big bang.
- Start *using* those policies, procedures, metrics, reports *etc*. as soon as they are available: it inevitably takes time to discover and smooth-off the rough edges, and integrate them all into a coherent, self-sustaining management system, so they constitute 'improvement opportunities'.
- Keep up the communications within and without the team, squeezing more value from metrics through motivational feedback, direction and reprioritisation.
- Become ever more business- and externally-focused as the ISMS settles into a routine, without neglecting the team and individual needs.