2 Information security governance

The first step in establishing adequate information security management within any organisation is the formulation and approval of an overall information risk governance strategy.

This chapter explains information security governance and gives an overview of the development, implementation and maintenance of a successful ISMS. Lead implementers need to be able to sell the concept of an ISMS to top management (e.g. the governing body of a university) and to the senior operational board in order to get them fully behind the initiative, and this chapter also describes how to do that effectively. It forms part of Stage 1 – Foundations and Stage 2 – Planning, assessment and evaluation in the Toolkit Route map.

Key topics

- **The most critical components in the development, implementation and maintenance of a successful ISMS**
- **How to use your organisational structure to give your ISMS the greatest possible chance of success**
- **How to align your ISMS with your organisation's business strategy**

2.1 What is information security governance?

Information security governance can be defined as:

"the specification of decision rights and an accountability framework to encourage desirable behaviour in the valuation, creation, storage, use, archival and deletion of information. It includes the processes, roles, standards and metrics that ensure the effective and efficient use of information in enabling an organisation to achieve its goals." - Gartner

Governance is the foundation of an ISMS, as it provides both strategic and operational frameworks. Information security governance is an integral part of the organisation's wider governance structures and mechanisms, such as business continuity, risk management, financial planning and research ethics.

2.2 What does information security governance look like?

Information security objectives must support organisational objectives, rather than be an end in themselves.

An ISMS should be part of the organisation's risk management activities, driven by the organisation's risk appetite and implemented to enable the organisation's strategic aims.

From ISO/IEC 27014, the principles of information security governance are to:

- establish an organisational wide information security policy
- adopt a risk based approach
- set the direction of investment
- ensure conformance with requirements
- foster a security-positive environment
- review performance in relation to business outcomes.

Information security governance should be approached holistically and cover people, processes and technology – it is not an IT issue. The security controls that form part of the ISMS must take account of human, environmental and physical factors and cover information in all its forms including paper records. The information security governance framework must encompass policies, processes, procedures, tools and training that are all joined up and designed in relation to each other in order to achieve the organisation's information security objectives.

Policy and objectives - There should be a top level policy which sets out the information security objectives, that in turn support the overall organisational strategy. The policy must be signed off by top management.

Accountability and responsibility - The organisation should define accountabilities and responsibilities at a high level, making top management explicitly accountable for information security but ensuring that personal roles and responsibilities are also defined (see Chapter 8, Roles and competencies).

2.3 Identifying stakeholders and interested parties

Identifying who requires what assurance is one of the critical success factors of implementing any ISMS. This will involve identifying the major stakeholders.

Stakeholders, in this context, may also be referred to as interested parties and could involve any of the following:

- top management
- business/process owners
- third parties setting requirements/standards (such as the NHS, UK Government, merchant banks)
- internal and/or external auditors
- relevant internal professional service departments (IT Services, Legal Services etc.)
- customers and end users (e.g. students and/or staff).

Identifying stakeholders and interested parties will help ascertain the applicable security requirements for the ISMS. The primary stakeholder(s) will be those who ultimately require assurance that any applicable requirements are being implemented appropriately. These stakeholders may also be the sponsor of the ISMS.

2.4 Oversight and audit

However much we wish to believe in our ability to remain impartial, we cannot ignore the natural human tendency toward bias.

One of the most important things to ensure, when designing information security governance, is that there is the capability for oversight. The organisation needs to have confidence that it is investing time, effort and money wisely, and that its activities to manage risk are effective: or, if not, that there is a need for improvement, and in which areas. Accountability for areas and key information assets should be clearly defined (see Chapter 8, Roles and competencies).

In the financial industry, measures are taken to reduce the risk of cognitive bias: the same should exist in the realm of information security.

In order to achieve these two complementary goals, the organisation should ensure that it gives a group or body the formal responsibility for reviewing the effectiveness of the organisation's activities to manage risk. This can be a formal governance body, supported by an executive group made up of staff with responsibility for aspects of risk management. The body with such responsibilities should be independent of the areas upon which it is reporting.

The Audit Committee in an organisation should review the risk register; similarly the internal audit function has a role in reviewing policies and procedures, recommending control systems and monitoring their implementation.

2.5 Identifying and securing adequate resources

Resources are required to establish, maintain and improve an ISMS. The level of investment should be based on risk management considerations (see Chapter 5, Risk assessment).

It is recommended that a project or programme be set up to manage any large scale work involved in creating (or significantly changing) any ISMS, with top level oversight. The programme or project should have a cross organisational focus, and should not be presented or perceived as a piece of work for the IT function alone. It can be quite helpful to have the lead for such a programme or project based, in, for example, a governance or risk management role. Significant input will be required from both the governance and IT departments. In addition, representatives for the Human Resources function and those responsible for physical security should be involved in the programme or project. Finally, requirements, products, outputs and outcomes should be quality checked with the wider stakeholders, including the academic community.

Once the initial work is complete, resources required for the continuing management and maintenance of the ISMS should be made available from the organisation's recurrent (or business as usual) budget. This will ensure that the ISMS can continue to be effective, and can adapt to take account of the needs of the organisation into the future.

2.6 Example governance structure

The organisation could establish an Information Security Governance Group at a senior level within the organisation hierarchy. This Group would include representation from those responsible for key administrative services (for example, HR, student records), representatives of those responsible for other information assets (for example, the Pro-Vice Chancellor for Research) and those responsible for implementing the information security policy, such as the CISO or members of the Information Security Service. The CISO and their team could:

- review the ISMS and play a role in its continual improvement (see Chapter 12, Continual improvement)
- act as the focal point for co-ordination of cross-organisational controls and conflict resolution
- provide regular performance reports (see Chapter 10, Measurement) to the Audit Committee or similar body
- provide advice and expert assistance, including carrying out risk assessments.

Note: This structure contains the risk of conflict of interest, as the CISO team is responsible for advising on controls as well as measuring and reporting on the effectiveness of the ISMS; care should be taken to ensure separation of duties to manage this risk.

2.7 Selling an ISMS to top management

Successful governance depends on buy-in from top management. All organisations operate differently, but one thing which they all have in common is their existence in law. Even the most devolved or federated organisation is still composed of one or more legal entities, each of which is liable to prosecution or criminal charges if found to be breaking the law. Top management are accountable in this respect.

When selling an ISMS to top management, and getting their buy-in, it is important to not use the legal argument as the only, or even the most important, reason for implementing a formal ISMS. For many members of top management, arguments relating to the protection of reputation, safeguarding of intellectual property and maintaining a competitive edge when competing for research grants and contracts are just as persuasive.

Information security should be sold as a business enabler as opposed to a cost. It is imperative to pitch this in terms of the key drivers which align to the organisation's strategic objectives (also see Chapter 3, Drivers). Some examples are given below.

2.7.1 For all organisations

- Protection of reputation – a security breach (and a badly handled aftermath) brings bad publicity, and potential litigation and/or fines, which all damage the corporate reputation and can result in the loss of funds from research and students. An effective ISMS supports the UK's National Security Strategy and its focus on cybercrime and thus can be promoted as a reputation enhancing activity.
- Ensuring continued revenue – most funding councils are now asking for assurances that the information which is to be used in research is to be properly protected.
- Risk management – top management is de facto responsible for information security risk. An ISMS provides them, and their governing body and funding body, with assurance that the risk is being appropriately managed throughout the organisation.
- Effective use of resources - an ISMS can lead to more efficient ways of working and best use of resources as controls are deployed (or relaxed) in a co-ordinated, cross-organisation manner to meet the corporate risk appetite. This can lead to higher staff satisfaction as policies are made clear, training is provided and resources are provided to allow application of controls.
- Customer satisfaction - staff and students can feel assured that their own personal data is held securely and that their identity is safe. In the absence of an ISMS, how confident is top management that their own personal data is safe in the organisation's hands? Are they happy for their own salary details or performance reviews to be held in insecure systems, or potentially accessible by untrained staff in a cyber café?

2.7.2 For research intensive organisations

- Protection of researchers' and the organisation's intellectual property.
- Compliance with research council requirements for data management and availability.
- Assurance to external stakeholders whose data is used for research —the ISMS gives a competitive advantage in winning research grants and framework bids.

2.7.3 Preparing a briefing

Top management will need a concise briefing on what information security is all about, stressing that it as much about availability as it is about confidentiality and integrity, and outlining the concept of an ISMS to deliver information security assurance. The high level briefing should explain the holistic approach of an ISMS (people, processes and technology) and outline why the organisation should pursue an ISMS.

Key points to remember when preparing a briefing to top management include:

- Top management have very little time to spend on any topic: keep your presentations, documents and arguments very brief.
- Explicitly link information security to the organisation's business strategy.
- The main questions to address will be "What are you asking us to do?", "Why?" and "What will this cost?"
- Present positive arguments such as cost savings, improvements in efficiency through process improvement, and the opportunity to really get benefit from information held by the organisation (now it will know what it actually holds).
- Use fear, uncertainty and doubt arguments with great care - only make cases based upon provable fact, e.g. recent and relevant incidents within the organisation.
- Be prepared to "show your working" on any particular statement you make in a document.

2.7.4 Preparing a business case

Visual representations of what you are trying to achieve, and how you plan to get there, can be more effective than lengthy narratives.

In order to secure resources for an ISMS, an initial or outline business case should be presented. It should include relevant drivers as described above and provide an outline of the costs involved in setting up and maintaining an ISMS.

The business case may, if appropriate, explain how the ISMS will provide a return on investment; this is more of a challenge, since an ISMS is largely insurance against loss. It helps to be able to compare the ISMS costs to a published index of costs incurred by similar sized organisations as a result of a major information security breach, such as the annual Information Security Breaches Survey Report commissioned by the Department for Business, Innovation and Skills. An initial outline risk assessment may also be used to support the business case (see Chapter 5, Risk assessment).

Relevant metrics should be identified to show how the information security team will be able to measure and report on the effectiveness of the ISMS.

It is important to continually reinforce that the purpose of an ISMS is to achieve a level of security which is consistent with the organisation's risk appetite and which enables corporate objectives. Once a project or programme to establish an ISMS has been agreed and an initial risk assessment exercise undertaken, it is often the case that the originally agreed risk appetite is modified when the financial cost of the security controls required to meet that appetite is presented to the organisation's executives. It is important, however, to keep reflecting the costs back in terms of the risks mitigated and make it clear that a decision not to spend is in effect a decision to accept a specific risk - and that this is perfectly acceptable as long as it is explicitly understood by top management.

Summary

- A suitable governance framework is a critical component in the development, implementation and maintenance of a successful ISMS
- Top management must endorse and be accountable for information security
- Good governance ensures ownership, scrutiny and accountability

Resources

Template for an information security policy

Responsibilities overview: Information ownership and risk management - Cardiff University

Developing an information security policy – University of York, case study

Bringing information security strategy to senior management – UCL, case study

Key questions for top management

Example of a presentation to sell the concept of an ISMS to top management

Reading list

Gartner article on information governance
www.ucisa.ac.uk/ismt9
http://blogs.gartner.com/debra_logan/2010/01/11/what-is-information-governance-and-why-is-it-so-hard/

ISO/IEC 27014 Information technology – Security techniques – Governance of information security
www.ucisa.ac.uk/ismt10
www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=43754

Annual Information Security Breaches Survey Report commissioned by the Department for Business, Innovation and Skills
www.ucisa.ac.uk/ismt11
http://www.pwc.co.uk/audit-assurance/publications/2014-information-security-breaches-survey.jhtml