8

Roles and competencies

This chapter outlines the roles and responsibilities, and supporting competencies, required of staff within an organisation in order to implement and sustain a successful information security management system. It forms part of Stage 1 – Foundations and Stage 2 – Planning, assessment and evaluation, and Stage 3 – Implementation, support and operation in the Toolkit Route map.

Key topics

- **The roles required to deliver effective information security in an organisation**
- **The responsibilities that may be assigned to individuals' roles or functions**
- **The core competencies required of key groups of staff**

8.1 Who does information security?

Information security is the responsibility of all members of an organisation.

Who is responsible for information security in your organisation's top level body?

There are few roles which do not involve interaction with information or information management systems (either paper or IT based). Staff present the greatest risk to information security; although malicious action by individuals cannot be ruled out, there is a greater risk of breaches occurring as a result of ignorance, inconsistent risk tolerances, or carelessness. Roles within the organisation share responsibility for achieving and maintaining appropriate information security.

It is important to distinguish between personal and organisational risk tolerance.

At the top of the organisation, governance and oversight must be the priority; the creation of goals and objectives and the balancing of information risk (see Chapter 2, Information security governance). Top management roles have top-level responsibility for implementation of objectives. Senior information security specialists provide specialist advice and support to executives, along with legal roles and other information management roles (e.g. records managers). Asset owners and technical specialists supply the decisions and expertise to make goals and objectives a reality, while operational staff, students and contractors need to be aware of, and comply with, information security requirements which apply to their roles.

An individual's role in the organisation should dictate their level of responsibility for information security processes and controls. The organisation should ensure that responsibilities are appropriate and fit-for-purpose. These responsibilities should subsequently be reflected formally in the agreements between the organisation and its members – whether these are employment contracts, or any other legal document defining the relationship of a member and the organisation.

Implementing a policy and technical measures goes some way to achieving a good level of information security in an organisation, but should be supplemented by individuals having an understanding of the value of information security and how it relates to their jobs (also see Chapter 9, Awareness raising). Different roles and job functions require different levels of competence, ranging from fairly elementary to a deep understanding of a wide range of topics, and may therefore require different levels of training and awareness.

8.2 Top management – decision makers

Information security decision-makers, or “top management”, manage information security strategy (including Chapter 12, Continual improvement) and governance (see Chapter 2, Information security governance), as these relate to the organisation, its values and its goals. They will have responsibility for determining strategy, policy and, critically, budget. Decisions which they will take include:

- investment in new technologies
- approving a training programme
- authorising a data classification scheme (see Chapter 7, Information management)
- authorising audits to ensure processes and policies remain fit for purpose.

Decision-makers exist at both the organisational and departmental levels within higher and further educational institutions. This leadership should be visible within the organisation.

The risks associated with information need to be owned by a member of top management. In many organisations, this role is known as the Senior Information Risk Owner (SIRO). The role of the SIRO focuses upon ownership of information risk, which is necessary for good information security governance (see Chapter 2, Information security governance).

It is likely that the SIRO will be part of the portfolio of responsibilities of a top level operational manager within the organisation (e.g. the Director of Governance, Risk and Compliance). It is a key decision making role which, in order to be effective, must fit in with any existing risk management hierarchy. The role of the SIRO is an established part of most public sector ISMSs, notably in the NHS.

The SIRO acts as lead and champion for information risk management initiatives and ensures that top management are adequately briefed on strategic level information risk management issues. The SIRO can also authorise acceptance or mitigation of major information security risks that deviate from agreed standards, and determine when (and by whom) breaches of information security will be reported to relevant external authorities.

8.2.1 Competencies of top management

The need to implement an organisation-wide information security management system will be competing with many other initiatives; top management must understand why information security is important to the organisation to ensure that it is adequately funded. Specifically, they need to understand:

- the principles of risk management and the part that information security management plays in mitigating risks
- the potential risk and impact of an information security breach
- that information assets vary in their sensitivity and importance and hence may require different approaches to information security.
- In addition to the above, the Senior Information Risk Owner (SIRO) for the organisation needs to have:
  - the communications skills to ‘sell’ why information security is important to the other members of top management
  - the ability to link information security issues to the overall organisational strategy.

8.3 Asset owners

Do you have a mechanism to establish asset owners in your organisation? Does, for example, the HR Director understand that s/he has this responsibility?

A number of senior staff will have de facto responsibility for the information assets under their control. For example, the HR Director will have responsibility for all the personnel information held within the organisation and will, in part, be responsible for determining how it is used, accessed and stored.

The responsibility may be implicit, for example the post holder will be the senior business owner of processes relating to the given asset. Alternatively, it may be explicitly outlined, for example in the terms and conditions associated with research grant awards for principal investigators.

The responsibility will cover being aware of, and authorising, the uses to which asset(s) are put. It may also extend to ensuring that those that have access to assets are trained and are operating appropriately.

Asset owners must have sufficient seniority to take decisions about the protection of their asset from a strategic perspective. Issues may arise here, as information asset owners may have no direct management control over dispersed instances of those assets. In this case, the focus of the role may be on setting security policy/standards for handling of the asset.

8.3.1 Competencies of asset owners

Organisational asset owners, such as the HR Director, will be members of the organisation's information security group and so should have sufficient understanding in order to be able to inform the decisions made by the group and to understand the impact on their aspect of the organisation's business. Specifically they need to understand:

- the principles of risk management and the part that information security management plays in mitigating risks
- information security principles
- how to classify information assets
- the risk and impact of an information security breach affecting their assets
- the implication of organisational information security policy on the aspect of the business they are responsible for
- the contribution which policies and processes in their business areas make to organisational information security
- the processes relating to the maintenance and use of their information assets.

Understanding the interaction between business functions and information security is particularly critical for those responsible for information relating to people in the organisation.

Maintenance of the information asset may be devolved to departments across the organisation. Consequently some of the responsibility for ensuring that information security policy and principles are applied appropriately to assets may also be devolved to individuals at a departmental level (for example, a departmental administrator). Individuals fulfilling these roles will need the same competencies as the organisational asset owner, albeit applied in a departmental context. Overall responsibility, however, remains with the organisational asset owner.

8.4 Dedicated information security roles

The role of a Chief Information Security Officer (CISO) is a necessary part of information security management. The CISO is the head of the information security function within an organisation, and is usually responsible for establishing and maintaining the enterprise vision, strategy and programme to ensure information assets and technologies are adequately protected.

There will be a number of roles required to support the CISO that are focused on advice, implementation and monitoring. These are often hybrid roles requiring an understanding of legislative requirements and organisational policy and, in IT focused teams, may also require technical knowledge.

Responsibilities may include activities such as conducting risk assessments, monitoring and reporting breaches and monitoring for potentially malicious activity (see Chapter 10, Measurement), and developing processes to ensure that access to systems is removed in a timely fashion from those leaving the organisation. These responsibilities may be vested in an individual or in a team; sample job descriptions are given in the Annex: Example resources to accompany the Toolkit.

The individuals fulfilling the implementation and monitoring roles will often form the core of the team to manage security incidents in the organisation. The team will have responsibility for the monitoring, detection and reporting of security breaches (see Chapter 11, When things go wrong: nonconformities and incidents), for the implementation of centrally mediated measures, and for providing advice and guidance to local areas. The team will also be a focal point for notifications of potential breaches of security and will lead internal investigations. In some instances, there may also be a sub-team with specific responsibility for IT-based information security.

The overall information security team may adopt a collaborative approach to inform decisions and guidance; a case study from UCL included in the Annex illustrates this approach.

Where possible, areas which handle subjects strongly related to information security should be integrated, or work closely together. Relationships should be maintained with areas which influence information security, but which have their own identity (the physical security department may be a good example of this).

Legal professionals will also exist within the specialist information security space, to handle situations relating to Data Protection, Freedom of Information, Information Rights management, Information Governance Toolkit compliance, payment card security, intellectual property and other related areas. Some roles also audit and review activities as part of organisational processes which do not directly or explicitly involve information security or information technology - this can include paper-based information or physical access to organisation facilities.

8.4.1 Competencies of information security professionals

Information security roles within an organisation must have a variety of skills and expertise in order to fulfil their roles. They will need people skills in order to communicate to a wide range of the organisation's staff, process skills to understand how information/data is used and the risks those processes may present, technical skills (knowledge of law, IT skills for those in IT focussed positions), and a high level appreciation of what IT protection can be delivered for those at a CISO level). They will need to:

- understand the nature of threats and risks to the organisation's information
- understand information security legislation and its application within the organisation
- understand organisational policy and its relationship to the organisation's information assets
- be able to communicate at all levels within an organisation to promote the need for information security
- understand the processing of information assets.

There are a wide variety of skills frameworks which can be used to measure and develop information security competence, including:

- The CESG Information Assurance Programme
- IISP Skills Framework
- ISACA qualifications (e.g. CISM)
- ISC2 Common Body of Knowledge and qualifications (e.g. CISSP)
- SANS programmes.

There is no "best" scheme – an organisation should evaluate their requirements and decide which scheme, or schemes (if any) is/are most suited to their needs.

8.4.2 Competencies of legal and compliance professionals

Roles with responsibility for legal advice will require a good appreciation of how their specific field fits into the wider organisation's approach to information risk management. They also have to be able to enable the organisation to be aware of and comply with legal requirements – some of which may vary depending upon the country in which information is being handled. They will need:

- to understand the relevant laws and contracts which relate to the information being handled by the organisation
- to maintain cordial relations with external bodies which impose requirements upon the organisation
- to liaise closely with information security professionals to ensure that policies and advice are legally acceptable
- to be able to negotiate with internal and external parties and achieve a common understanding of ambiguous or conflicting requirements, or agree approaches to handling risk which do not exactly match external requirements
- to be able to liaise with areas across the organisation to advise on and provide approval (as appropriate) for proposed activities.

8.5 Other roles

Almost all individuals in any organisation interact with information in the course of their activities and can therefore impact information security. This can include staff who handle personal information, faculty administrators managing student data, researchers developing intellectual property and managing sensitive data, and students using the organisation's infrastructure to conduct their studies.

Principal investigators, as the lead individuals on research projects, will create information assets during the course of their research. There is, for publicly funded research, growing emphasis on the curation of research data and open access to both research outcomes and the data that informed it.

A significant volume of research is funded by commercial organisations. Such research may be carried out to meet the specific needs of the funder, who may need to protect the commercial value of the research and related data. Research contracts with commercial organisations may well stipulate that the data and outcomes from the research are commercially sensitive and so need to be held securely, and require a data management plan in advance as supporting evidence. In addition, if medical data is being received, additional requirements such as the Information Governance Toolkit may need to be satisfied prior to the provision of data.

Roles which are engaged in the delivery of administrative services will have a greater level of responsibility for security of the information their service holds, by virtue of the fact that they will have higher levels of access than those that merely access the information on a read-only basis.

8.5.1 Competencies of research leads

Responsibility for the security of the assets generated by a research project lies with the grant holder – often the Principal Investigator (PI). This implies that the grant holder also has responsibility for the conduct of any members of the research team involved in their project. PIs (and their teams) will need to understand:

- information security principles
- the sensitivity of the information assets that will be used and/or generated by their research (whether they are commercially confidential, personal, or ethically sensitive)
- how to apply appropriate security measures to sensitive data
- the likely impact of an information security breach (relating to the information they are handling) on their organisation and on their own professional standing.

8.5.2 Competencies of contractors and third party organisations

Third party contractors coming into the organisation are usually specialists or professionals, and it is easy to assume that their expertise also extends to information security. In fact, the converse is true; they are less likely to appreciate local organisational information security arrangements. Those responsible for managing the appointment of contractors should be aware of the risks they pose. Contractors should be required to sign agreements that recognise information security requirements or complete appropriate training before beginning work.

Similarly, whilst adequate security constraints may be in force for employees and contractors, those same levels of safeguard may be overlooked when dealing with third parties, such as hardware and software suppliers, consultants and other service providers. See Chapter 4, Scoping for advice on managing third parties.

8.5.3 Competencies of administrators

Administrative staff need to be able to:

- understand the need to protect information (much of this may be tied to the need to adhere to data protection principles) and the risks of not protecting information
- apply information security principles when dealing with information such as staff and student records
- understand how the information is being used.

8.5.4 Competencies of all staff

The majority of staff will have access to a limited range of systems and will require a clear understanding of relevant information security principles. The relevant competencies are:

- to understand why protecting information is important
- to understand the relationship between the information they maintain and information security and hence their responsibility to maintain data accurately and in a timely fashion
- to be able to distinguish between types of information (and hence, what is important to protect)
- to understand why it is good practice to back up data, change passwords, etc.

How well is responsibility for information security embedded in individual job descriptions in your organisation?

The final point is important to ensuring accurate data – whilst it may be clear that there is a statutory requirement to record staff sickness absences, it may not be apparent to the person entering the data why some details may be required. For example, HR staff may not be aware that entering an end date against an employee's record will trigger the termination of access to IT systems and buildings. Consequently timely entry of that data may mitigate an information security risk. Understanding the use of data and its importance to the organisation assists in ensuring its accuracy; central administrative staff may have a role in educating those maintaining data within departments on how the information is used.

8.6 Students

Although much of the focus of information security policies is on staff responsibilities, students also share responsibility for ensuring the security of information and the systems they use. As with staff, levels of responsibility vary. The majority of taught students will only have read access to data and perhaps the ability to update their own records, but they will still need to adhere to regulations and not place the organisation at risk by introducing malware or other similar activity. However, postgraduate research students may have direct or delegated responsibility for critical information and as such, should be made aware of their responsibilities and good information security practices.

8.6.1 Competencies of students

Students have access to an organisation's systems and may inadvertently present a risk to the organisation. They may also have access to (and the ability to update) their own data. Students like staff, will have consented to the organisation's regulations for the use of IT facilities and these will be linked to student terms and conditions and hence disciplinary measures. However, there is also a need (particularly for new entry undergraduates) to raise awareness of information security and for them to understand the need to protect their own personal data. In short, the majority of taught students will need a basic awareness of sound practice, supplemented by reinforcement of key points from the regulations.

Postgraduate research students may require an additional level of awareness and competency, particularly if they are making use of personal data for their research, or are part of a wider research project (for example, as a research assistant).

Summary

- The organisation's information security policy should define the roles and responsibilities required of staff
- All staff have responsibility for information security; this responsibility will be included in general terms and conditions of employment as well as individual job descriptions
- An information security group should be established at a high level, chaired by a member of top management with specific responsibility for championing information security and including owners (and representatives of owners) of key information assets
- A team to monitor and implement information security measures should be established and should be represented on the information security group
- The information security policy needs to be supported by effective personnel procedures

Resources

Job description template - Information Security Manager

Job description template - Senior Information Security Specialist

Job description template - Information Security Specialist

SFIA competencies

Collaboration between security administrators and academic researchers – UCL, case study

Reading list

No items.