*This chapter describes the external and internal factors which influence an organisation to adopt formal information security management, and which shape an information security management system. It also provides advice on how to balance conflicting drivers. It forms part of Stage 1 – Foundations in the Toolkit Route map.*

### Key topics

- **The levels at which drivers operate**
- **Where drivers come from**
- **How to manage drivers**

## 3.1 Overview

In any academic environment, there will be many different external pressures that may seek to influence how the organisation handles information. These may range from formal contractual and statutory requirements, through industry standards (both formal and informal) and funder expectations, to informal but nonetheless compelling desires to gain competitive advantage by enhancing or maintaining the organisation's reputation as a safe place to conduct research. These can all be seen as "drivers".

There are drivers which might influence an organisation to adopt formal information security management (e.g. ISO/IEC 27001); then there are drivers which might influence and shape an existing formal ISMS. The former include contracts, the need to be competitive, and the desire to use existing "known good" methods to secure information. The latter include those standards (including PCI DSS, the IG Toolkit and the Cyber Essentials scheme) which mandate the adoption of certain controls, or which require the use of detailed processes, such as a particular risk assessment methodology (see Chapter 6, Controls).

Failure to adequately recognise and address drivers can have consequences from adverse headlines to loss of future research contracts, financial loss (e.g. if PCI DSS requirements are not met), fines, or the loss of licences for sensitive areas of research or study.

Unfortunately drivers may conflict with internal requirements, or even with each other. For example there may be opposing requirements between open research and commercial exploitation of results, or between data protection and freedom of information, whose resolution will depend on the organisation's priorities and risk appetite.

A formal ISMS can provide a framework for addressing potential conflicts between drivers in a transparent and coherent way that supports the organisation's objectives. See Chapter 2, Information security governance, for more advice on how to encourage the implementation of an ISMS, and advice on stakeholders.

## 3.2 Identifying drivers

Once all of the stakeholders are known (see Chapter 2, Governance), the organisation should aim to identify the drivers for the ISMS. Organisations should aim to identify relevant drivers early on in the formalisation of their ISMS, so that it is fit for purpose from the beginning.

In any organisation, it is likely that the work of managing the impact of external drivers will be spread across multiple departments. For example, DPA and FOIA compliance may be managed by the Legal department, while Finance handles PCI DSS, the Medical School addresses the IG Toolkit, and the IT department, along with Estates, manages the business continuity plan. See Chapter 8, Roles and competencies, for more on this subject.

The table below provides a sample of different types of drivers, and indicates how specific and granular they are.

**Table 1: Types of Driver**

| Driver | Internal or external? | Issues addressed by driver | Type of driver |
|---|---|---|---|
| Data Protection Act 1998 (DPA) | External | Publication of, or damage to: personal data; inaccurate personal data; personal data used for unapproved purposes; personal data retained for too long | Legislation<br>High-level principles |
| Research contracts | External | Loss, publication, or damage to sensitive research data. | Contractual obligation varies: mostly high level, referencing other standards |
| Business advantage | Internal | Loss of contracts, staff and students to competitors | Business policy<br>High level direction from top management |
| Risk management | Internal | Inconsistent, inappropriate and ineffective controls which waste money and do not protect the organisation | Business policy<br>High level direction from top management |
| Cyber Essentials Standard, Top 20 Cyber-security controls, etc. | External | Compromise of insecure computers through malware or “hacking”, focussing on likely routes and commonly neglected technical measures | Good practice guidance<br>Granular specifications |
| The organisation’s Business Continuity Plan | Internal | Damage to operations during a natural disaster or systems failure | Business policy<br>Granular specifications |
| Information Governance Toolkit (IGT) | External | Insecure storage and use of medical data | Contractual obligation<br>Granular specifications and high level content |
| Anti-terrorism legislation | External | Access by terrorists to certain research areas and equipment | Legislation<br>High level principles |
| Payment Card Industries Data Security Standard (PCI DSS) | External | Fraud through theft of credit and debit card data | Contractual obligation<br>Granular and prescriptive |
| ISO/IEC 27001 | External | Inconsistent approach to security; ineffective measures; recurring incidents; inability to demonstrate due diligence | Good practice standard<br>High level guidance and principles |
| IT Infrastructure Library (ITIL) and ISO/IEC 20000-1 | External | Inconsistent and expensive IT support | Good practice guidance<br>High level guidance and principles |

## 3.3 Identifying requirements

Drivers may determine requirements directly or indirectly. Wherever the requirements come from, it is unlikely that all requirements will apply to all systems. Decisions as to which requirements apply to which systems should be justifiable, and should be based on an assessment of risk against the overall objectives of the organisation and the ISMS (see Chapter 5, Risk assessment). This should be appropriately documented and available for inspection if challenged, e.g. during an audit.

Different stakeholders may have different (possibly conflicting) requirements, in which case the primary stakeholders need to agree which requirements are considered to be in scope.

## 3.4 Continual monitoring of drivers

A common mistake which can be made at the point of setting up an ISMS is to assume that it will be possible to identify all drivers and sources of requirements at an early stage. The organisation may make a huge master list of drivers and requirements, use this to identify controls, implement controls, and then believe that all will be well thereafter. Leaving out the issue that not all of the relevant drivers may be known when the ISMS is set up, it is inevitable that not only will new drivers arise, but that existing drivers may change, or cease to be of relevance (also see Chapter 6, Controls, for more information).

A full lifecycle approach to external drivers is therefore required (see Chapter 12, Continual improvement). This should be linked to organisational change processes (e.g. the project management process, strategic planning process, and research funding process) so that changes to drivers can be identified and assessed in good time i.e. before any formal commitments are made by the organisation. It may be possible to extend existing change management processes to cover the activities described in this chapter.

The organisation should develop a standard process for assessment of requirements provided by a new, changed, or retired driver.

A new driver should be assessed to determine whether it is indeed relevant and appropriate; the correct role in the organisation should provide this verification. This step reduces the risk of inappropriate drivers being included, and of inconsistency within organisations where multiple areas are running semi-independent information security management systems. Equally, changed and retired drivers should be ratified.

## Summary

- Drivers can operate at a very high level (e.g. organisational reputation), or be very granular in their level of detail (e.g. researcher reputation)
- Drivers can be internal (e.g. responsibility to students and staff), but are often external (e.g. the Information Governance Toolkit)
- Managing the impact of drivers is an iterative process

## Resources

**Incidental security improvements from sustainability policies – UCL, case study**

**Information security within the research arena – Loughborough University, case study**

## Reading list

**Criminal Justice Secure Email**
**www.ucisa.ac.uk/ismt12**
http://cjsm.justice.gov.uk/

**Business Impact Levels**
**www.ucisa.ac.uk/ismt13**
http://www.cesg.gov.uk/publications/Documents/business_impact_tables.pdf

**Risk Management and Accreditation Documentation Set (RMADS)**
**www.ucisa.ac.uk/ismt14**
www.gov.uk/service-manual/making-software/information-security.html

**CERT Top 10 List for Winning the Battle Against Insider Threats**
**www.ucisa.ac.uk/ismt15**
www.rsaconference.com/writable/presentations/file_upload/star-203.pdf

**Guide to developing a Data Management Plan**
**www.ucisa.ac.uk/ismt16**
www.dcc.ac.uk/resources/how-guides/develop-data-plan

**PCI DSS and related standards**
**www.ucisa.ac.uk/ismt17**
https://www.pcisecuritystandards.org/