6 Controls

This chapter describes how to approach security measures, or controls, and how to make them work in practice. It forms part of Stage 2 – Planning, assessment and evaluation and Stage 3 – Implementation, support and operation in the Toolkit Route map.

Key topics

- **Definition of a control**
- **How to pick and assess controls**
- **What to do about "ready-made" sets of security controls**

6.1 What is a control?

A control is a tool for treating risk. Controls can reduce the impact or likelihood of a risk, thus decreasing its overall rating. Many controls can be applied to treat a single risk, and, equally, one control can treat multiple risks. Controls can be selected by the organisation's risk assessment (see Chapter 5, Risk assessment) or imposed by internal or external requirements (e.g. PCI DSS).

Some controls can be applied to the whole organisation (e.g. the authentication scheme, or retention schedules), while some can be specific to a particular scope (e.g. password lifespans, or patching policies).

The organisation should first consolidate its business and compliance requirements, and only then design and consolidate controls. This minimises duplication and redundancy.

6.2 Types of controls

Controls can be roughly grouped into three categories, as follows.

Table 2 - Types of Controls

Category	Examples	Reduces likelihood?	Reduces impact?
Preventative/ Deterrent	Training	Y	N
	Pre-employment screening	Y	N
	Segregation of duties	Y	Y
	Secure media disposal	Y	Y
Detective	Intrusion Detection System	N	Y
	Review of user access rights	Y	Y
Reactive	Burglar alarm	Y	Y
	Back-ups	Y	Y

Controls can fall into more than one category. For example, anti-malware software both prevents infection and acts to remove existing malware.

Controls can also be technical (such as anti-malware) or non-technical (such as keeping documents in a drawer overnight, rather than on a desk). Non-technical controls often involve changes to business processes, which

may require more involvement from different parts of the organisation to implement, but which are more cost-effective. When selecting technical controls, the organisation must always ask itself the question, "Why is this control the best or only option? Is there a non-technical approach which is more effective?".

Different cultures may have very different attitudes to acceptable behaviour, which should be taken into account when designing controls (see Chapter 5, Risk assessment). For example, in some cultures, it is considered unacceptable to let a door close in the face of someone walking behind you – in this case, the organisation should consider alternative controls to pass-opened doors, such as turnstiles.

6.3 Control sets

There is no "perfect control set", any more than there is a "perfect diet".

There are many sets of controls available, some backed by government, others produced by professional bodies, and still more developed by community organisations (see the reading list for this chapter for a few examples).

Control sets are like diets – everyone is looking for a "quick fix". Some approaches are faddish and incomplete and require huge lifestyle changes. Others require you to pay a third party to make all of the difficult decisions for you. Others start with good advice based upon fact, and expect you to interpret it to suit your situation. Unfortunately, just as there is no one menu which will suit us all, there is no one control set which will sufficiently protect every organisation.

Using governmental advice can be a good start, if there is a clear message.

The crucial point of difference between a control set and a diet, where the analogy breaks down, and which explains the fluidity in the information security sector (which far exceeds the confusion even in the nutrition sector) is the rapidly changing and volatile state of technology. Human biology is relatively static. Imagine if a person born thirty years ago was unrecognisable to anyone born twenty years ago, and could not eat the same food or even talk to them.

The more specific and technology-focused a control set is, the more effort it will take to keep it up to date – which is why managing people and business processes can be a better way to manage a risk.

Any organisation seeking to identify a control set to implement should assess it for stability (given the changing nature of technology), suitability for their needs, and other side benefits (e.g. will it make it easy to get government funding?). The control set chosen will almost certainly need to be augmented to fill in the areas where organisational risk tolerance differs from the tolerance of the authors of the control set.

Governmental control sets can be used to improve top level buy-in, as top management may have been contacted by governmental bodies asking for feedback on compliance with the currently popular control set. An example of an initial risk assessment which helped an organisation to raise awareness, gain support from governance and executive bodies and make the case for increased investment in information security controls was to take the CPNI 20 controls and assess: current organisational compliance (rated as red, amber or green), priority for action, actions recommended with cost, timescales and responsibilities.

6.3.1 A note on the ISO/IEC 27001 Statement of Applicability

The Statement of Applicability is one of the documents required to certify to ISO/IEC 27001. It consists of a mapping of the organisation's list of selected controls to the list of controls in Annex A of ISO/IEC 27001 (which is the same as the controls in ISO/IEC 27002). Every information security control which is used by the organisation (in the environment being certified) should be in this list, even if they do not appear in Annex A of 27001. Justification should be given (briefly) for the inclusion of all implemented controls; and where a control listed in 27001 is not implemented, justification for its omission should also be given.

The purpose of the SOA is mainly to ensure that an organisation has not missed anything. The Annex is not intended to be a control set, or a means of bypassing a risk assessment. A good way to think of it is as a supermarket containing all the foods you can imagine – your list of controls is your shopping list. Going to this supermarket without a list and buying everything on the shelves will bankrupt you, and leave you with many foods you don't need or want. Equally, implementing all controls in Annex A of ISO/IEC 27001 will be too expensive for the organisation, and will not meet its needs. That is why the list of controls in Annex A is best ignored until after the organisation has sorted out its list of required controls.

6.4 Implementing controls

Controls are only effective when completely defined, and implemented in the correct context.

For example, a policy developed by a small group, published on a website and left to the ravages of chance will

be unlikely to have its desired effect. Log files, as another example, in and of themselves have no protective or preventative capability. They need to be part of a detective control, and linked to incident response, in order to reduce the impact of incidents.

An effective control should be:

- developed through consultation with affected parties, transcending any internal "silos"
- designed to address a risk
- proportionate
- supported by top management
- tested
- implemented with appropriate awareness work to ensure that all impacted users understand what to do and have support in any transitional period
- managed, with non-compliance detected, followed up, reported on, and persistent issues handled effectively.

To put this another way, controls are a component of an ISMS; they do not replace it.

Implementation of a control should be managed as any other business change, using the techniques which the organisation finds most effective, and the management channels which are in place already.

6.5 Assessing and managing change

Business changes may change risk levels, introduce new sources of risk or new external requirements, which then cause controls to be revised. The impact of any new/changed/retired driver (see Chapter 3, Drivers) on existing controls should also be assessed (i.e. change or removal).

The impact on the organisation of each control introduction/change/retirement should then be assessed, so that any changes which are not feasible can be identified. As previously noted, this assessment should be done as early as possible, ideally before the organisation commits to a project or new service which brings with it changes which are not feasible to implement. For example, taking payment card data may result in specialist security software being required (file integrity monitoring), and hence a much higher cost for software licenses.

Using this information, the appropriate level in the organisation should then make a decision on the business change: should it go ahead?

Assuming that the business change will go ahead, once the changes to controls are clear, a plan should be agreed which leads to their implementation/alteration/removal (as relevant) in a suitable time frame.

6.6 Documenting controls

Controls deriving from requirements, either via risk assessment (see Chapter 5, Risk assessment) or via other drivers (see Chapter 3, Drivers), should be compiled into a single list, along with internally defined controls, to reduce the chances of unnecessary duplication and accidental omission. The source(s) of each given control should be recorded, so that changes in a driver can easily be propagated into policies, technical measures etc. Equally, should a question arise as to the necessity of a control, it will be easy to understand why it exists and the consequences of removing it.

In many cases, especially where legislation is concerned, an external requirement will not specify exact controls. In this situation, the organisation should use the driver to inform its risk assessment and control selection processes, with reference to its own risk appetite and legal counsel as appropriate. This ensures that legislation is not over- or under-interpreted.

In order to relate controls derived from external drivers to controls derived from risk assessment, the organisation should decide how to treat externally derived controls. They may be seen in one of two ways:

- as a way to address the risk of non-compliance (e.g. with the DPA)
- as a way to treat a specific information security risk (e.g. the risk of a user deliberately or accidentally leaking information).

Of these two options, the first is the easiest to do initially, but leaves externally derived requirements in a separate group, and does not, perhaps, encourage all controls to be treated equally. The second approach requires each control to be "deconstructed" to identify what risk (or risks) it is actually going to be addressing. This takes more time, but is a much more effective (and satisfying) approach.

Summary

- Controls reduce the impact and/or likelihood of incidents
- Ready-made control sets should be considered carefully
- Controls form part of an ISMS – they do not replace it
- Controls should be traceable to the requirements/risks which they are intended to address

Resources

Evaluating software security patches – Loughborough University, case study

Hacking before and after: How Certified Ethical Hacking (CEH) training changed my perspective on hacking – UCL, case study

Technical vulnerability management

Penetration testing

Reading list

CPNI 20 Controls
www.ucisa.ac.uk/ismt27
www.cpni.gov.uk/advice/cyber/critical-controls/

10 steps to cyber security
www.ucisa.ac.uk/ismt28
www.gov.uk/government/publications/10-steps-to-cyber-security-advice-sheets

Educause IT Governance, Risk and Compliance Programme
www.ucisa.ac.uk/ismt29
www.educause.edu/library/resources/it-governance-risk-and-compliance-higher-education

Cyber Security Essentials scheme
www.ucisa.ac.uk/ismt30
www.gov.uk/government/uploads/system/uploads/attachment_data/file/317481/Cyber_Essentials_Requirements.pdf