Conclusion

This Toolkit has been designed to enable organisations in the educational sector to design, establish, maintain and improve an information security management system. From getting a clear picture of the organisation is, to achieving buy-in, to selecting controls, implementing business changes and ensuring that these changes are properly embedded by the use of awareness materials, measurement and reporting, each step builds on the previous one to create something which is genuinely worth having and which continues to be relevant and cost-effective.

A well-managed ISMS is a powerful business enabler.

In summary, it is vital for everyone in the organisation to understand that this is not a finite project that can be implemented and forgotten about. Continual improvement is crucial, for a successful ISMS will require ongoing investment. Analysis of information security threats and incidents over the years shows that there is no room for complacency, as threats and risks are ever-changing.

The battle for hearts and minds is a key one. At all times, organisations must ensure that their ISMS is as user-friendly as possible. Information security professionals should work closely with colleagues across the organisation to maintain an holistic approach. The way to ensure the continued relevance of an ISMS is to keep it closely and visibly linked to the organisation's strategic objectives and risk appetite.

The summaries for each chapter are collected below. Readers are also encouraged to review and use the resources the material referenced in the reading lists at the end of each chapter and in the Annex: Example resources to accompany the Toolkit.

Overall summary

1 What is information security?

- Information security applies to all forms of information
- Threats are becoming more sophisticated and revenue-led
- Information security is the responsibility of all members of an organisation

2 Information security governance

- 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

3 Drivers

- 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

4 Scoping

- Successfully defining and agreeing the scope of an ISMS from the beginning is a critical success factor in the implementation of any ISMS – if the scope is wrong you will not know where you are going or when you got there!
- There are different scopes involved in implementing information security in an organisation from high-level scopes covering the entire organisation to the scope of a particular project.
- Start small with your scope, demonstrate success and build from there.
- Monitor and review, and if your scope is wrong then change it accordingly

5 Risk assessment

- Information risk management is a systematic, consistent, iterative process where risks are identified and assessed before being treated and monitored
- Information risk treatment options should not cost more to deploy and manage than the cost of the risk itself
- Information risk management should not be done in a vacuum, but as part of the overall organisational risk management process

6 Controls

- 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

7 Information management

- An information management scheme should comprise of: a classification scheme, a labelling scheme, handling rules and processes to define how these all interact
- A classification scheme describes how information should be classified
- A handling scheme describes how information given a particular classification should be treated
- Do not have more classification levels than necessary, or practical
- Labelling can indicate both the classification and who should (and should not) see the information
- Handling rules must provide consistent protection across different media

8 Roles and competencies

- 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

9 Awareness raising

- For greatest impact, target content to match identified risks and roles within the organisation, in response to changes in the organisation environment and threat landscape
- Target learning through media, practical instruction, or theoretical instruction, using physical hand-outs such as flyers, electronic communications, fixed-place messaging like posters, and persistent messaging (such as screensavers and online training)
- Consider that security is supporting the individual to do their job well, and that there is competition for their attention – security needs to be there to help develop skills that will be applied in targeted roles

10 Measurement

- Measurements may be used to measure the performance of an ISMS, the effectiveness of controls, to track threat levels, and as part of controls themselves (see Chapter 6, Controls).
- Every measurement must have a purpose: to direct action, and/or to support decision making
- Suitable presentation of measures is critical to their effectiveness

11 When things go wrong – nonconformities and incidents

- The ISMS should aim to manage the level and severity of adverse events, not to eliminate them
- The ISMS should contain plans to respond to, and learn from, these events
- Incident response requires trusted cooperation both within and outside the organisation; trust must be established in advance

12 Continual improvement

- The goal of continual improvement is to iteratively identify and implement ways to make an established ISMS more cost effective and appropriate
- Improvement activities are also necessary during the creation of an ISMS
- Continual improvement can include adapting to the current environment, or improving the efficiency of controls and/or processes
- Continual improvement should be an objective from the outset when implementing any ISMS

13 Policies

- The information security policy should not stand alone; it should be part of an organisation's risk management strategy and must be approved by the highest governance body in the organisation
- The organisation's policy for information security defines responsibility for delivery and risk ownership