Introduction

Information is the lifeblood of successful organisations. Without it, they cannot operate. Equally, if it is untrustworthy, every activity is suspect, and no-one can make a reliable decision. This is especially important in research, where data accuracy is vital. Finally, some information, such as commercial research findings, personnel records and medical data, is so sensitive that even knowledge of it by the wrong people is dangerous to the organisation.

Information is not the sole domain of the IT department— it is a cross-institutional concern.

Because everyone in any organisation needs to create, access and use information, everyone is responsible for protecting it and using it appropriately. This protection requires a culture where information is seen as being valuable and worth protecting, where effective data management is established, and where student and staff privacy are respected.

In order to achieve and maintain a good approach to information risk management, or information security, organisations can benefit from the well-developed international standards in this area.

ISO/IEC 27001 is the international standard describing the creation and maintenance of an information security management system (ISMS). It can be used by any size of organisation, and is flexible enough to fit any sector. It has been in existence for over twenty years, and is used by many universities in the UK and abroad.

The UCISA Information Security Management Toolkit has been constructed for use by information security/governance professionals wishing to put in place an ISMS in their organisation. It also addresses how to convey the importance of information security to the organisation, since the need for an ISMS is based upon the acceptance that information security is worth investing in. This edition of the Toolkit outlines an approach to successfully implement an ISMS based on ISO/IEC 27001:2013 (Information technology — Security techniques — Information security management systems — Requirements). It is intended as a practical resource, providing an overview of the key aspects of a successful ISMS and guidance on how to implement them. It also includes case studies, as well as templates and example resources which organisations can tailor to suit their needs.

The Toolkit has evolved from edition three of the UCISA Information Security Toolkit, which was based upon the 2005 version of ISO/IEC 27002 (Information technology — Security techniques — Code of practice for information security management), and included sample policies for all the Standard's controls, grouped according to the internal functions of the organisation.

The different approach taken this time reflects the need of organisations for advice and guidance upon setting up and maintaining the organisational infrastructure (including top level policies, processes, and governance) which enables policies and other security measures (controls) to be appropriate, well maintained, and effectively implemented. Information on how to implement controls is not included.

The document has also been revised to reflect the changing trends in the workplace, such as: the growth of the use of personal devices to access organisational systems and services; the increase in off-site working; and the complexities of the research agenda (e.g. protecting intellectual property in an open environment).

The UCISA Information Security Management Toolkit will:

- assist those who have responsibility for implementing information security across the organisation by providing advice and guidance to them;
- help them to provide senior university management with an understanding of why information security is an important, organisation-wide issue.

The structure of this document

Good information security requires a proportionate, risk-based response.

The Toolkit is arranged in chapters, each one covering a key aspect of an ISMS and providing advice, instructions and examples to aid implementation. At the end of each chapter is a summary of key points and references. At the end of the document, in the Conclusion, is a collection of all the chapters' summary points.

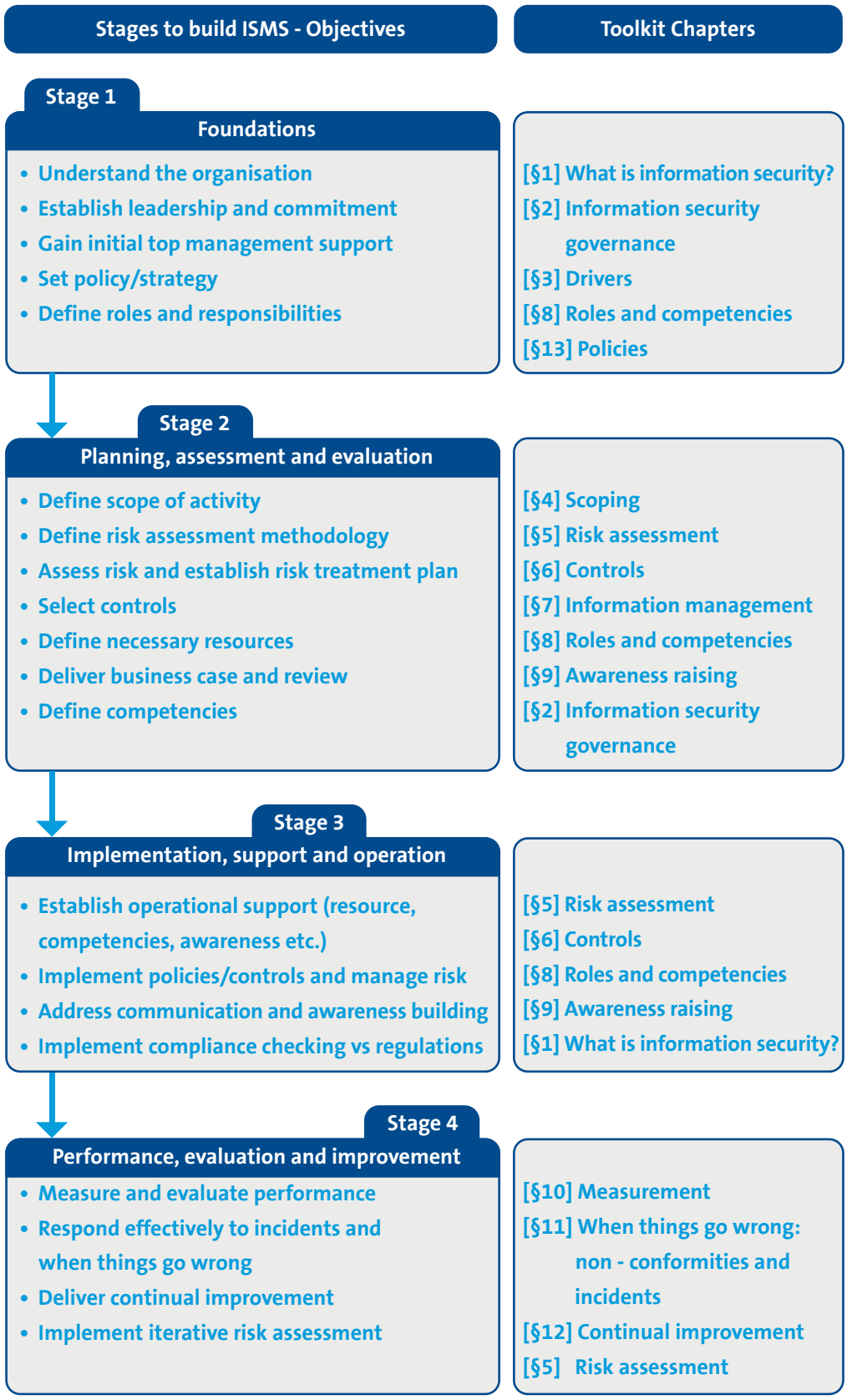
Definitions and standards

Please note that this document uses the definitions in ISO/IEC 27000 Information technology — Security techniques — Information security management systems — Overview and vocabulary. These definitions may differ from standard dictionary definitions.

It is also strongly recommended that readers read this document in conjunction with the standards ISO/IEC 27001 and ISO/IEC 27002.

Route map for using the UCISA Information Security Management Toolkit

Toolkit Route Map



Resources

Different elements of an Information Security Management System - Cardiff University

Stages for implementing an Information Security Framework (ISF) programme - Cardiff University

Reading list

ISO/IEC 27000:2014 Information technology — Security techniques — Information security management systems — Overview and vocabulary
www.ucisa.ac.uk/ismt1
http://standards.iso.org/ittf/PubliclyAvailableStandards/

ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements
www.ucisa.ac.uk/ismt2
www.iso.org/iso/home/standards/management-standards/iso27001.htm

ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls
www.ucisa.ac.uk/ismt3
www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54533

The Business Dictionary
www.ucisa.ac.uk/ismt4
www.businessdictionary.com