ISO Information Security Standards

The International Standards Organisation (ISO) maintains a number of different standards in the area of Information Security. Although the standards are not written to directly address the information security issues of research and education organisations they are nonetheless a useful source of information about good practice. External bodies concerned about information security (for example organisations sharing commercially sensitive or personal data, and regulators) often express requirements or questions in terms of the ISO standards.

Research and education organisations are therefore advised to at least be familiar with how their information security activities relate to the standards (the UCISA Information Security Toolkit may be helpful here); some may choose to base their activities around the standards or, perhaps, to seek certification of their Information Security Management System (ISMS) against ISO/IEC 27001:2005. Certification demonstrates that an independent third party has examined the organisation's ISMS and verified that it conforms to the standard. Certification by an assessor accredited by the relevant national body (e.g. the UK Accreditation Service) may be a requirement of some grants or information sharing agreements.

This factsheet introduces the main ISO standards likely to be relevant to research and education organisations. The standards are available for purchase in both paper and electronic form from ISO or the British Standards Institute (BSI); some libraries have site licences covering ISO or BSI products. The standards are reviewed approximately every five years: revised versions of ISO27001 and ISO27002 are expected to be published in October 2013.

ISO27001 "Information security management systems – Requirements" is the core standard defining what ISO considers that an Information Security Management System (ISMS) should contain. The standard specifies a cyclic process of four steps:

- **Plan**: define the scope of the ISMS, identify information assets and assess risks to their security, select controls to address these risks and obtain management authorisation to implement them;
- **Do**: implement controls to manage the significant risks, including awareness and training programmes and incident detection and response processes;
- **Check**: measure the effect of those controls and review whether the risks have changed;
- **Act**: make necessary changes to the controls, the risk assessment process or the ISMS;
- repeat.

An ISMS can be audited against this standard and certified as meeting its requirements.

Other standards in the ISO27xxx series provide assistance with particular aspects of an Information Security Management System. These include:

ISO27002 "Code of practice for information security management" is a comprehensive list of areas in which information security risks are likely to arise, for example if responsibilities for

security are not included in job descriptions, if computers are not secure against physical or network attack or if the organisation does not have an incident response plan. For each risk the standard suggests controls that may be appropriate to address it. The standard can be used on its own, to highlight areas of risk that the organisation may not have considered, but is best used as input to the risk assessment stage in an ISO27001 ISMS. All risks in ISO27002 should be considered, but it is perfectly acceptable for a risk assessment process to conclude that some of them are currently too low to require or justify treatment measures, or that the organisation's environment requires that different controls to address them.

ISO27011 "Information security management guidelines for telecommunications organizations" supplements ISO27002 by providing a list of information security risks particularly likely to arise in the telecommunications sector. Guidance on the use of cloud computing services is being developed as ISO27017 and 27018.

ISO27005 "Information security risk management" discusses how to perform the risk assessment/management process. An alternative approach is described by the US Government's Risk Management Guide for information technology systems (Special Publication 800-30).

ISO27035 "Information security incident management" describes an approach to managing information security incidents. An alternative approach is described by the US Government's Computer Security Incident Handling Guide (Special Publication 800-61)

ISO27000 provides an overview and standard vocabulary for information security.

References

International Standards Organisation (ISO) www.iso.org [1]

British Standards Institution (BSI) www.bsigroup.com/en/ [2]

UK ISO27001 User Group http://www.iso27001usergroup.co.uk/ [3]

UICISA Toolkit www.ucisa.ac.uk/publications/toolkit.aspx [4]

NIST Risk Assessment http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf [5]

NIST Incident Handling http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf [6]

Links
[1] http://www.iso.org
[2] http://www.bsigroup.com/en/
[3] http://www.iso27001usergroup.co.uk/
[4] http://www.ucisa.ac.uk/publications/toolkit.aspx
[5] http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
[6] http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf