Information security management made simple

CFDG

sayer vincent
consultants and auditors

Acknowledgements

This guide was produced with help from the partners and staff at Sayer Vincent, as well as support from staff and trustees of CFDG.

CFDG (Charity Finance Directors' Group) is the professional body for finance directors within the sector, and has nearly 1,500 members. CFDG provides assistance to charities on a range of issues, such as accounting, taxation, audit and other finance-related functions. CFDG's mission is to deliver services that are valued by members and enable those with financial responsibility in the charity sector to develop and adopt best practice.

For more information go to **www.cfdg.org.uk**

Sayer Vincent only works with charities and not-for-profit organisations. With five partners and over 35 professional staff we are one of the largest teams of charity specialists. Our work focuses on making charities more effective through improved infrastructure, reporting and governance. We help charities with mergers, systems implementations and training. Charities appoint us as consultants, internal auditors or external auditors. Working with a diverse portfolio of charities, we deliver rapid insights into your issues and problems and help you to find effective solutions to them.

For more information, go to **www.sayervincent.co.uk**

Published by CFDG
First published 2009

CFDG and Sayer Vincent shall not be liable for loss or damage arising out of or in connection with the use of this publication. This is a comprehensive limitation of liability that applies to all damages of any kind, including, (without limitation), compensatory, direct, indirect or consequential damages, loss of data, income or profit, loss of or damage to property and claims of third parties.

Introduction

Charities have a legal duty to look after their information properly, and would face significant damage to their reputation if any data about their supporters or beneficiaries were to be lost or stolen. In addition, like any organisation, charities depend on their information systems to run their businesses properly and efficiently.

Dependence on information systems has grown in all areas of life, and to a great extent this has meant increasing dependence on computerised information systems. Recent trends of working, such as the greater availability and use of laptop computers and other mobile devices, bring with them new risks not faced previously, such as being able to lose or have stolen prodigious quantities of data, some of which may be confidential or sensitive. The recent spate of government data security lapses has brought these issues to the forefront of people's minds.

The growth of the internet and increased inter-networking within organisations (as well as wireless networking) has meant that our information systems are now much more vulnerable to attack, potentially from anywhere in the world. This includes the threat of 'hacking' (i.e. unauthorised access to computer systems), damage by computer viruses, and computer-assisted fraud. In addition, damage can be caused to computerised information systems as a result of malfunction, and accidental damage such as flood or fire.

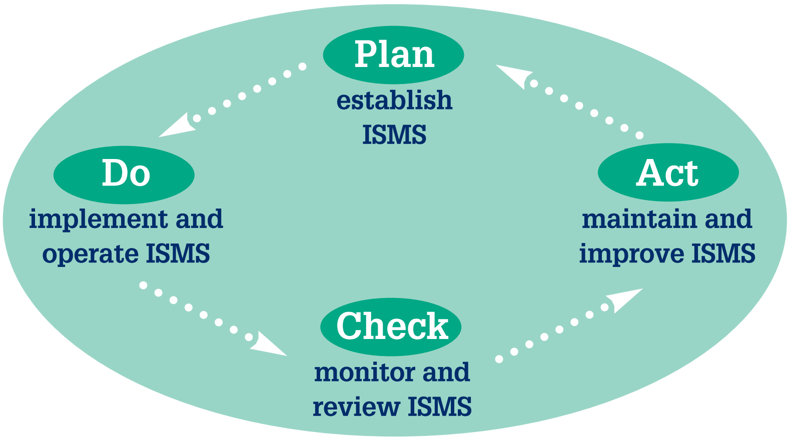
Managing information security is therefore vital and should pervade all aspects of an organisation's operations. It should be remembered that information security is a management issue not an IT issue.

So where do you start? Fortunately, there is a wealth of advice available to help organisations put in place appropriate arrangements for information security. In particular, the ISO/IEC 27000 series of standards provides a complete framework for the implementation of information security management systems ('ISMS').

This guide is based on the principles and best practice recommendations set out in the ISO/IEC 27000 series.

Overall approach and framework

The ISO/IEC 27000 series promotes a 'Plan–Do–Check–Act' process model for establishing an ISMS.



The four stages of this process can be broken down further, to give a ten-step plan:

Plan (establish the ISMS)

1 Define the scope of the ISMS

2 Establish an ISMS policy

3 Carry out an information security risk assessment

4 Decide on risk treatment and controls

Do (implement and operate the ISMS)

5 Implement the chosen controls

6 Provide awareness training for staff and others

7 Establish incident detection and response procedures

Check (monitor and review the ISMS)

8 Carry out an internal ISMS audit

9 Carry out a management review

Act (maintain and improve the ISMS)

10 Take corrective and preventative actions to achieve continual improvement of the ISMS

Each of these ten steps is explained in more detail below.

plan

Step 1 Define the scope of the ISMS

The organisation can decide the scope of its ISMS. The scope is normally the whole organisation, but it could be restricted to a particular department or perhaps the charity's trading subsidiary. This decision will determine the ownership and responsibilities for the ISMS (e.g. the trustees, department head). If a restricted scope is chosen, care will be needed to ensure that any policies required by the ISMS are compatible with any over-arching organisational policies.

Step 2 Establish an ISMS policy

An information security policy should be approved by management, published and communicated as appropriate to all employees. It should set out:

- The organisation's approach to managing information security
- A definition of information security, objectives, principles and scope
- An explanation of security policies, principles, standards and compliance requirements of particular importance to the organisation
- A definition of responsibilities and reporting arrangements
- References to supporting documentation, rules and procedures

The characteristics of an effective information security policy include:

- An approach to implementing, maintaining, monitoring and improving information security that is consistent with organisational culture.
- Visible support and commitment from all levels of management.
- Providing appropriate awareness, training and education.
- Distribution of specific guidance on information security policy and standards to all managers, employees and other parties.

Step 3 Carry out an information security risk assessment

Once the scope of the ISMS has been decided, and an ISMS policy is in place the next step is for the organisation to carry out an information security risk assessment. This should involve an assessment of organisational risks generally and specifically in relation to information processes developed by the organisation to meet its own operational requirements, as well as consideration of legal, statutory, regulatory and contractual requirements.

For more guidance on carrying out risk assessments, see our **Risk Assessment Made Simple** guide.

Each organisation will have a different risk profile, depending on the types of activities that they carry out, and the way in which they are organised. In general, the risk assessment should cover (for example):

- Physical and environmental security. This would include consideration of:
  - The organisation's security perimeters (barriers such as walls, windows, doors, receptions desks, intruder alarms etc.)
  - Physical entry controls (swipecard entry systems, visitors book, visitors badges)
  - Equipment security (equipment siting and protection, emergency power supplies, equipment maintenance procedures, security of equipment off-premises, secure disposal, or re-use of equipment)

- Personnel security (threats to/from staff or ex-staff). This would include consideration of:
  - Security roles (to ensure that staff understand their roles and responsibilities in relation to information security)
  - Screening (obtaining references, confirmation of claimed qualifications, independent identity checks, etc.)
  - Terms and conditions of employment (legal responsibilities under copyright and data protection laws, non-disclosure agreements where appropriate, actions to be taken if the employee disregards the organisation's information security policies and procedures)
  - Awareness training (see *Step 6* below)
  - Termination responsibilities (e.g. return of assets and removal of access rights)

- Communications and operations management. This would include consideration of:
  - Operational procedures and responsibilities (to ensure the correct and secure operation of information processing facilities)
  - Segregation of duties (e.g. separation of development, test and operational facilities, system administration rights)
  - Management of third parties (such as computer maintenance companies)
  - System planning and acceptance (to minimise the risks of systems failures and to define acceptance criteria for implementing new systems)
  - Protection against viruses and malicious code (detection, prevention and recovery)
  - Information backup (including testing and rehearsing backup and restore systems and procedures)
  - Network security management (including design of data access rights, firewalls, service levels, intrusion detection systems)
  - Media handling (see example in *Step 4* below)
  - Exchanges of information and software (see example in *Step 4* below)

  - E-commerce (including encryption and security of websites, security of online transaction details, etc.)
  - Monitoring (system audit trails, routine system monitoring, protection of audit trail log files, fault logging, system clock synchronisation)

- Asset management (*NB* assets can include physical assets and non-physical assets such as information, software, services, people and reputation). This would include consideration of:
  - An asset inventory (this should include all the information necessary to recover from a disaster, including type of asset, ownership, location, backup information, and business value)
  - Ownership (i.e. responsibility for ensuring the appropriate access restrictions of information assets)
  - Acceptable use of assets (including email and internet acceptable use policies, and guidelines for use of mobile devices)
  - Classification of assets (to indicate the need, priorities and expected degree of protection when handling the information)

- Access controls. This would include consideration of:
  - The business requirements for access control (including user access control policies governing different types of users)
  - User access management (including user registration and de-registration, password management, periodic review of access rights, session timeouts)
  - User access policies (including password policies, clear desk policy, policies on unattended equipment, mobile computing and working from home)

- Information systems acquisition, development and maintenance. This would include consideration of:
  - Security requirements of information systems (to ensure that security requirements are identified and agreed prior to the development and/or implementation of information systems)
  - Correct processing in applications (including the validation of input data, internal processing and output data)
  - Cryptographic controls (encryption of data where appropriate in mobile devices, websites and in email transmission, etc.)
  - Security in system files and software development processes (including controls over the installation of software and upgrades)
  - Technical vulnerability management (including correct application of operating system 'patches', penetration testing)

Step 4 Decide on risk treatment and controls

Having identified those risks that require further action, the organisation needs to decide how to treat them. The choices are to avoid the risk, accept it, transfer it or mitigate it.

Example

Risk that confidential information held on web-based membership database is lost or compromised

Avoid	Do not provide web access to database
Accept	Do nothing and accept the consequences
Transfer	Outsource the operation of the database and hold operator liable for its security
Mitigate	Identify controls that will reduce the likelihood or impact of particular threats to the data

Specific controls will need to be designed for each risk identified in the risk assessment.

Examples of controls

Category
Communications and operations management

Control objective Media handling and security
Objective To prevent damage to assets and interruptions to business activities.

Example controls
1 *Management of removable, computer media.*
The management of removable computer media, such as tapes, disks, cassettes and printed reports shall be controlled.

2 *Disposal of media*
Media shall be disposed of securely and safely when no longer required.

3 *Information handling procedures*
Procedures for the handling and storage of information shall be established in order to protect such information from unauthorised disclosure or misuse.

4 *Security of system documentation*
System documentation shall be protected from unauthorised access.

Control objective Exchanges of information and software
Objective To prevent loss, modification or misuse of information exchanged between organisations.

5 *Information and software exchange agreements*
Agreements, some of which may be formal, shall be established for the electronic or manual exchange of information and software between organisations.

6 *Security of media in transit*
Media being transported shall be protected from unauthorised access, misuse or corruption.

7 *Electronic commerce security*
Electronic commerce shall be protected against fraudulent activity, contract dispute and disclosure or modification of information.

8 *Security of electronic mail*
A policy for the use of electronic mail shall be developed and controls put in place to reduce security risks created by electronic mail.

9 *Security of electronic office systems*
Policies and guidelines shall be prepared and implemented to control the business and security risks associated with electronic office systems.

10 *Publicly available systems*
There shall be a formal authorisation process before information is made publicly available and the integrity of such information shall be protected to prevent unauthorised modification.

11 *Other forms of information exchange*
Procedures and controls shall be in place to protect the exchange of information through the use of voice, facsimile and video communications facilities.

do

Step 5 Implement the chosen controls

Once the control framework has been designed, resources need to be put in place to ensure that it can be implemented.

This should include a comprehensive and balanced system of measurement which is used to evaluate performance in information security management and feed back suggestions for improvement. There should be provision to fund information security management activities.

Step 6 Provide awareness training for staff and others

As with any new policy, the organisation's management has a responsibility to ensure that staff (and other stakeholders such as volunteers, business partners and suppliers) are aware of the policies and understand them.

Different staff will have different training requirements, depending on their role in relation to the ISMS – for example technical staff may need training in configuring a firewall, whilst ordinary users only need to be aware that there is a firewall and what it does. In general, all staff need to understand:

- What the policies are, and how they are expected to carry out their responsibilities within the policies
- The different kinds of threat that could prejudice the organisation's information systems (e.g. email viruses, 'phishing', password theft, hacking, identify theft)
- The possible impact that these threats could have on the organisation's operations and reputation
- What to do if they suspect something is wrong

Step 7 Establish incident detection and response procedures

Following on from the above, the organisation needs to put in place incident detection and management procedures so that any information security breaches are dealt with properly. These can range from the simple implementation of automatic virus signature updates to a whole set of procedures outlining what to do in the event of a major incident such as a fire.

Indeed, this process will help to develop a business continuity plan, setting out procedures for maintaining essential business activities during any period of disruption.

check

Step 8 Carry out an internal ISMS audit

Ideally, the information security controls that have been put in place will be effective, and provide the protection intended. The purpose of an internal ISMS audit is to test whether or not this is the case, and should be carried out by an independent person (which need not necessarily be a formally qualified internal auditor). The internal ISMS audit provides an opportunity to review and enhance the ISMS by examining what actually happens across a sample of events and processes and comparing this with what the documented management system describes. Identifying any mismatches allows the organisation to put things right either by enhancing working practices or by changing the documentation of what happens.

In principle, an internal audit programme should be devised that aims to review the entire ISMS and associated controls over a period such as a year. In addition to checking whether the chosen controls are operating as they should, the internal ISMS audit should consider whether they are indeed the right ones.

Step 9 Carry out a management review

Following the internal ISMS audit and periodically (at least annually), the organisation's management should review the effectiveness of the ISMS in relation to its current situation. This should include a review of the risks and controls in the light of current circumstances and business requirements.

The management review should take account of:

- Results of ISMS audits
- Incident reports
- Suggestions and feedback
- New techniques, products and procedures
- Preventative and corrective actions already taken
- Risk assessments
- Results from effectiveness measurements (i.e. the effectiveness of the implementation of existing controls)
- Previous management review actions implemented
- Changes affecting the ISMS
- Recommendations for improvement

The outcomes of the management review will feed into *Step 10* below.

Certification

Organisations may consider whether to seek external validation of their ISMS. 'Certification' is the process by which an organisation's ISMS is assessed for conformance with the ISO/IEC 27001 standard. Certification can only be carried out by a 'Certification Body' (such as the British Standards Institute). A certification audit is carried out in two stages – a review of the ISMS documentation, followed by testing of the procedures and controls specified in the ISMS. As with other international standards, the process of certification is likely to prove time consuming and expensive. At the time of writing, fewer than 350 UK organisations in the UK have received certification of which only a handful appear to be charities.

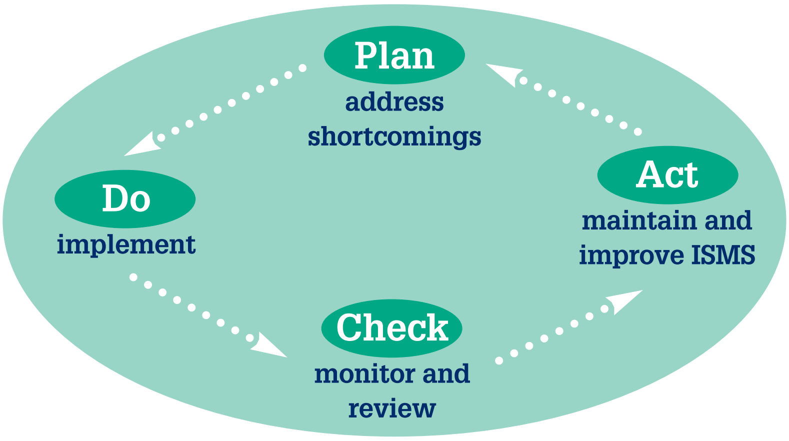
act

Step 10 Take corrective and preventative actions to achieve continual improvement of the ISMS

The outcomes of the management review could include:

- Proposed improvements to the ISMS
- An updated risk assessment
- Modified controls and procedures
- Additional resource requirements
- Better ways of measuring the effectiveness of existing controls

The final stage of the 'Plan–Do–Check–Act' cycle is the development of a plan to act on the outcomes of the previous stages to address any shortcomings found. Thus, the initial cycle of continuous improvements continues indefinitely. In subsequent iterations, the stages would become:



Conclusion

The ISO/IEC 27000 series provides a convenient framework within which to develop an information security management system. The Plan-Do-Check-Act approach promotes a cycle of continuous improvements.

Risk management techniques are used to identify information security risks and select appropriate controls.

It remains to be seen whether certification will become a widely used benchmark for charities or non-profit organisations. However the development of an ISMS based on the ISO/IEC 27000 series can provide assurance to trustees, funders and other stakeholders that appropriate information security measures are in place.

References and further information

Dealing with internet security threats
Ian Kilpatrick
Published by the ICAEW Faculty of Information Technology, 2008
ISBN 9781841525570

Information security – an essential today: a guide to ISO/IEC 27001 and ISO/IEC 17799 for business managers
William List
Published by the ICAEW Faculty of Information Technology, 2006
ISBN 9781841524672

Information security standards kit
Published by British Standards Institution, 2005
ISBN 0 580 37804 7
http://www.bsi-global.com/en/Shop/Publication-Detail/?pid=000000000030140674

The standard of good practice
Published by the Internet Security Forum, 2007
https://www.isfsecuritystandard.com/SOGP07/index.htm

Information security – business advice
Department for Business Enterprise and Regulatory Reform
http://www.berr.gov.uk/whatwedo/sectors/infosec/infosecadvice/page10059.html

IT governance: a manager's guide to data security and ISO 27001/ ISO 27002
A. Calder
Published by Kogan Page, 2008 (4th edition)
ISBN 9780749452711

made simple guides

Made Simple guides are aimed at finance professionals and other managers working in charities. They cover technical areas such as tax and VAT treatments as well as information management areas and aim to provide practical guidance to busy managers and trustees in charities.

The content of guides is correct at the time of going to print, but inevitably legal changes, case law and new financial reporting standards will change. You are therefore advised to check any particular actions you plan to take with the appropriate authority before committing yourself. No responsibility is accepted by the authors for reliance placed on the content of this guide.

Other guides in the series

Risk assessment made simple

Reserves policies made simple

Trading issues made simple

Subsidiaries made simple

VAT made simple

Grants and contracts made simple

Pricing made simple

Gift aid made simple

Tax effective giving made simple

Employee and volunteer taxation made simple

Accounting software made simple

Mergers made simple