www.adaptaconsulting.co.uk

adapta

processes, people and technology

Adaptive Approach to Information Security

INSTITUTE OF CONSULTING

2016 MemberWise Recognised Supplier

CFG INSPIRING FINANCIAL LEADERSHIP

Adapta Consulting is a CFG Corporate Subscriber

Contents

Published by Adapta Consulting
First published 2015

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 tablets and smartphones, 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. A number of high-profile data security lapses by Government bodies and, more recently, charities 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.

Charities that hold and process "personal data" (i.e. information about identifiable living individual) are required to notify the Information Commissioner and should be aware that Principle 7 of the Data Protection Act requires them to ensure that appropriate technical and organisational measures are taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

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.

There is a wealth of standards and advice available to help organisations put in place appropriate arrangements for information security.

Information security standards

Data Protection Act

Although the Data Protection Act is not prescriptive about what "appropriate technical and organisational measures" means in this context, the Information Commissioner frequently issues guidance on specific areas of the Act, including Principle 7. For example, the Information Commissioner recommends that "portable and mobile devices including magnetic media, used to store and transmit personal information, the loss of which could cause damage or distress to individuals, should be protected using approved encryption software which is designed to guard against the compromise of information".

PCI DSS

Charities that process payment card data are required to comply with the security requirements set out in the Payment Card Industries Data Security Standard ("PCI DSS"). PCI DSS is a worldwide standard that was set up to help businesses process card payments securely and reduce card fraud. The way it does this is through tight controls surrounding the storage, transmission and processing of cardholder data that businesses handle. PCI DSS is intended to protect sensitive cardholder data.

Cyber Essentials

Cyber Essentials is a UK government scheme that provides a clear statement of the basic controls all organisations should implement to mitigate the risk from common internet-based threats.

COBIT 5

COBIT defines a set of generic processes for the management of IT. The framework defines each process together with process inputs and outputs, key process-activities, process objectives, performance measures and an elementary maturity model. The framework supports governance of IT by defining and aligning business goals with IT goals and IT processes.

ISO/IEC 27000 series

The ISO/IEC 27000 series of standards provides a complete framework for the implementation of information security management systems (ISMS).

So where do you start?

Although the other standards listed above may be relevant for many organisations (and are very useful in legal and practical terms), none of them provides the universal “toolkit” that the ISO/IEC 27000 series does. The ISO/IEC 27000 series can be used as a framework for managing information security by any organisation, regardless of its size or its field of operation. The rest of this guide is therefore based on the principles and best practice recommendations set out in the ISO/IEC 27000 series (“the standard”).

Overall approach and framework

The ISO/IEC 27000 series of standards was substantially revised in 2013 to bring it into line with other ISO standards. Although it still mandates a “continuous improvement” approach to information security management, it is agnostic as to which continuous improvement management framework is used (the previous version promoted a ‘Plan–Do–Check–Act’ process model).

In bringing the standard into line with other ISO standards, the ISO 27000 series shares a common document structure, common terms and definitions with them, allowing organisations to operate a single management system that meets the requirements of more than one ISO standard. The new version places more emphasis on measuring and evaluating how well an organisation's ISMS is performing. A section on outsourcing has been added with this release, and additional attention is paid to the organisational context of information security.

The key elements of the 2013 version are:

- Context of the organisation
- Leadership
- Planning
- Support
- Operation
- Performance evaluation
- Improvement

Each of these elements is explained in more detail.

1. The context of the organisation

The organisation can decide the scope of its Information Security Management System ("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. Organisations should also think about the needs and expectations of "interested parties" in relation to information security management. In the case of charities, this can include staff, suppliers, clients/beneficiaries and others.

2. Leadership

The standard places requirements on "top management" (i.e. the person or group of people who directs and controls the organisation at the highest level) to demonstrate leadership and commitment by leading from the top. Particular responsibilities of top management are to assign information security relevant responsibilities and establish an information security policy. The standard defines the characteristics and properties that the policy is to include.

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.

3. Planning

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.

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)

Information security 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

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 software

To prevent loss, modification or misuse of information exchanged between organisations.

Example controls

1 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.

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

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

4 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.

5 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.

6 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.

7 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.

4. Support

The standard requires that organisations shall determine and provide the necessary resources to establish, implement, maintain and continually improve the ISMS.

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

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.

The extent of documented information for an information security management system will differ from one organisation to another but the following documentation would be expected in most cases:

Policies

- Scope of the ISMS
- Information security policy and objectives
- Risk assessment and risk treatment methodology
- Statement of Applicability
- Risk treatment plan
- Risk assessment report
- Definition of security roles and responsibilities
- Inventory of assets
- Acceptable use of assets
- Access control policy
- Operating procedures for IT management
- Secure system engineering principles
- Supplier security policy
- Incident management procedure
- Business continuity procedures
- Statutory, regulatory, and contractual requirements
- Procedure for document control
- Controls for managing records
- Procedure for internal audit
- Procedure for corrective action
- Bring your own device (BYOD) policy
- Mobile device and teleworking policy
- Information classification policy
- Password policy
- Disposal and destruction policy
- Procedures for working in secure areas
- Clear desk and clear screen policy
- Change management policy
- Backup policy
- Information transfer policy
- Business impact analysis
- Exercising and testing plan
- Maintenance and review plan
- Business continuity strategy

Records

- Records of training, skills, experience and qualifications
- Monitoring and measurement results
- Internal audit program
- Results of internal audits
- Results of the management review
- Results of corrective actions
- Logs of user activities, exceptions, and security events

5. Operation

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.

6. Performance evaluation

As a general recommendation, organisations should determine what information is needed to evaluate the information security performance and the effectiveness of the ISMS. Work backwards from this 'information need' to determine what to measure and monitor, when, who and how.

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.

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.

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 the continuous improvement process below.

7. Improvement

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 any continuous improvement process 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.

Conclusion

The ISO/IEC 27000 series provides a convenient framework within which to develop an information security management system. Its 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.

Further information

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

IT governance: a manager's guide to data security and ISO 27001/ISO 27002
Alan Calder
Published by Kogan Page, 2012 (5th edition)
ISBN 978-0-7494648-5-1

Protecting Data, Protecting People: A Guide for Charities
Published by Charity Finance Group (CFG), 2013
ISBN 978-0-9567860-3-6
http://bit.ly/111aNZ7

Security and assurance in the Cloud
Published by the ICAEW Faculty of Information Technology, 2013
ISBN 978-0-85760-654-9

10 steps to Cyber Security
Produced by GCHQ, BIS and CPNI
Published by Crown Copyright, 2012
http://www.bis.gov.uk/assets/BISCore/business-sectors/docs/0-9/12-1120-10-steps-to-cyber-security-executive.pdf

Cyber Essentials
Produced by Department for Business, Innovation and Skills
Published by Crown Copyright, 2014
http://www.cyberstreetwise.com/cyberessentials/

Contact Us

Speak to our team to find out how we can help you take your organisation forward.

T: 020 7250 4788

E: help@adaptaconsulting.co.uk

W: www.adaptaconsulting.co.uk

About Adapta

At Adapta Consulting, we help you meet the challenges of change: processes, people and technology. We work exclusively with not-for-profit organisations, where our consultants bring a combination of deep systems knowledge and wide experience, gained over many years working at senior levels in the sector. We are completely independent and, in all our work, we set the highest professional standards to ensure we provide an objective service, adapted to your needs.

What makes us different?

Our team

Our team consists only of highly experienced consultants, each one a recognised expert in their particular field and all of whom have all worked in and/or are trustees of not-for-profit organisations.

Understanding our clients

Our experience in the not-for-profit sector means we have extensive knowledge of what is realistic and practical in different situations for the organisations we work with.

Supplier independence

We are totally independent of any supplier. We do not receive commissions from any source, and that means we provide unbiased, independent and objective advice that is in your best interests.

Tailored advice and support

All of our advice and support is tailored specifically to you and to your organisation. We assign an appropriately qualified partner to every engagement and their role is to ensure we are always helping you meet your objectives in the most cost-effective way.

Communication

We always keep you informed of progress so you know exactly where, when and how your requirements are being met.

Transparent fees

We know how important it is that our clients get the best value for money. We agree all our fees with you before we start so you always know the cost of the help we provide.

How we can help?

We only offer practical advice – adapted specifically to your needs:
Developing strategies for IT and web
Producing business cases
Improving processes
Selecting package software
Implementing CRM
Managing projects and programmes
Reviewing information security
Coaching and mentoring