ISO 27001 CONTROLS

A guide to implementing and auditing

Bridget Kenyon

ISO 27001 Controls

A guide to implementing and auditing

ISO 27001 Controls

A guide to implementing and auditing

BRIDGET KENYON

IT Governance Publishing

Every possible effort has been made to ensure that the information contained in this book is accurate at the time of going to press, and the publisher and the author cannot accept responsibility for any errors or omissions, however caused. Any opinions expressed in this book are those of the author, not the publisher. Websites identified are for reference only, not endorsement, and any website visits are at the reader's own risk. No responsibility for loss or damage occasioned to any person acting, or refraining from action, as a result of the material in this publication can be accepted by the publisher or the author.

IT Governance Publishing Ltd
Unit 3, Clive Court
Bartholomew's Walk
Cambridgeshire Business Park
Ely, Cambridgeshire
CB7 4EA
United Kingdom

www.itgovernancepublishing.co.uk

Formerly published as *Guide to the Implementation and Auditing of ISMS Controls based on ISO/IEC 27001* by BSI.

First published in the United Kingdom in 2019 by IT Governance Publishing.

ISBN 978-1-78778-146-7

FOREWORD

Information is one of your organisation's most valuable assets. The objectives of information security are to protect the confidentiality, integrity and availability of information. These basic elements of information security help to ensure that an organisation can protect against:

- sensitive or confidential information being given away, leaked or otherwise exposed, both accidentally or deliberately;
- personally identifiable information being compromised;
- critical information being accidentally or intentionally modified without the organisation's knowledge;
- important business information being lost without a trace or hope of recovery; and
- important business information being unavailable when needed.

It should be the responsibility of all managers, information system owners or custodians, and users in general, to ensure that their information is properly managed and protected from the variety of risks and threats faced by every organisation. The two standards ISO/IEC 27001:2017, Information security management systems – Requirements, and ISO/IEC 27002:2017, Security techniques – Code of practice for information security controls, together provide a basis for organisations to develop an effective information security management framework for managing and protecting their important business assets, while minimising their risks, maximising investment and business opportunities, and ensuring their information systems continue to be available and operational.

ISO/IEC 27001 is a requirements standard that can be used for accredited third-party information security management system (ISMS) certifications. Organisations going through the accredited certification route have their ISMS audited by an accredited certification body. This ensures that they have appropriate management processes and systems in place, and that these conform to the requirements specified in ISO/IEC 27001.

ISO/IEC 27002, a guidance document, provides a comprehensive set of best practice controls for information security and implementation guidance. Organisations can adopt these controls as part of the risk treatment process specified in the standard ISO/IEC 27001, in order to manage the risks they face to their information assets.

This guide is designed to provide you with assistance in establishing, implementing and maintaining your ISMS to help you prepare for ISMS certification. This is the fifth edition of this guide, and it has been updated to reflect the publication of the latest versions of ISO/IEC 27001 and 27002.

Bridget Kenyon

ABOUT THE AUTHOR

Bridget Kenyon (CISSP) is Global CISO for Thales eSecurity. Her experience in information security started in 2000 with a role in network vulnerabilities at DERA. Following this, she took hands-on roles as a network administrator and a systems administrator, before returning to her chosen field as Information Security Officer for the University of Warwick.

In 2007, Bridget moved into consulting, guiding many of the major UK banks to compliance with payment card security standards (PCI DSS), as well as advising clients in the educational, retail, telecommunications and hospitality sectors. During this period, she also started to participate in the development of ISO/IEC 27001 and related standards. At University College London, she devised and implemented a complete information security management scheme ab initio.

In addition to her current role, Bridget is a member of BSI Panel 1 (for development of ISO/IEC 27001 and related standards), and is an editor for ISO/IEC 27014. Bridget has co-authored three textbooks on information security, most recently as lead author for the UCISA Information Security Management Toolkit (Part 1). In 2018, she was named as one of the top 25 Women in Tech by UK publication PCR.

Bridget is a CISSP and Associate Member of the Institute of Information Security Professionals. She strongly believes that “information security is fundamental to reliable business operations, not a nice-to-have”.

ACKNOWLEDGEMENTS

I would like to thank Vitalis Nkwenti, Andrew Pattison, Marc van Delft and Christopher Wright, for their time and helpful comments during the review process.

DISCLAIMER

A document such as this is provided with the best of intentions. It reflects publicly available common best practice, which is derived from a consensus among international experts with a wide variety of skills, knowledge and experience in the subject. This guide makes no claim to be exhaustive or definitive, and users may need to seek further guidance in implementing the requirements of ISO/IEC 27001 or the use of the guidance found in ISO/IEC 27002. Furthermore, there will always be other aspects where additional guidance is required relevant to the organisational, operational, legal and environmental context of the business, including specific threats, controls, regulatory compliance, governance and good practice.

The author of this guide cannot be held liable by organisations, users or third parties for the execution or implementation of this information. It has been assumed in drafting the information and advice given in this guide that the execution of this information by organisations and users is entrusted to appropriately qualified and experienced people.

Unless stated otherwise, all quotations are from ISO/IEC 27001:2017.

CONTENTS

CHAPTER 1: GENERAL

1.1 Scope of this guide

This guide provides instructions on the implementation of ISMS control requirements and on auditing existing control implementations to help organisations prepare for certification in accordance with ISO/IEC 27001.

The contents of this guide include the ISMS control requirements that should be addressed by organisations considering certification. Part 2 of this guide discusses each of the controls in Annex A of ISO/IEC 27001 from two different viewpoints:

•implementation guidance – what needs to be considered to fulfil the control requirements when implementing the controls from ISO/IEC 27001, Annex A. This guidance is aligned with ISO/IEC 27002, which gives advice on the implementation of the controls;
•auditing guidance – what should be checked, and how, when examining the implementation of ISO/IEC 27001 controls to ensure that the implementation covers the essential ISMS control requirements.

It is important to emphasise that this guide does not cover the implementation or auditing of the ISMS process requirements (the main body of ISO/IEC 27001). This is discussed in more detail in 1.3, Meeting ISO/IEC 27001 requirements.

1.2 Field of application

1.2.1 Usage

This guide is intended to be used by those involved in:

- designing, implementing and/or maintaining an ISMS;
- preparing for ISMS audits and assessments;
- carrying out internal ISMS audits and and
- carrying out ISMS audits and assessments of other organisations.

This guide makes reference to the following standards:

- ISO/IEC 27001 – the requirements specification for an ISMS. This International Standard is used as the basis for accredited certification.
- ISO/IEC 27002 – a reference for selecting controls as part of the implementation of an ISMS, and a guidance document for organisations implementing commonly accepted security controls.

This guide will be updated following any changes to these standards. Organisations should therefore ensure that the correct version is being used for compliance checks related to pre-certification, certification and post-certification purposes.

1.2.2 Compliance

To claim compliance with the requirements of ISO/IEC 27001, the organisation needs to demonstrate that it has all the processes in place and provides appropriate objective evidence to support such claims. Any exclusion of controls found to be necessary to satisfy the risk acceptance criteria needs to be justified. Evidence also needs to be provided that the associated risks have been knowingly and objectively accepted by those in management who have the executive responsibility and are accountable for making such decisions.

Excluding any of the requirements specified in ISO/IEC 27001, Clauses 4–10 is not

The implementation of ISMS processes results in the organisation deploying a system of controls based on a risk management approach to manage its risks. The organisation should have implemented an effective system of management controls and processes as part of its ISMS, and should be able to demonstrate this by providing evidence to the ISMS auditor (whether it be a first-, second- or third-party audit).

This guide can be used by those who might not have an immediate need for an audit, but require a specification for establishing and implementing an ISMS based on industry accepted best practice processes. However, claiming compliance with ISO/IEC 27001 does require the organisation to have at least an internal ISMS audit in place, whether or not it goes for a third-party audit at a later stage. The organisation may not have a business case for a third-party audit, but in order to be compliant with ISO/IEC 27001, an internal ISMS audit process is mandatory. This guide can, of course, also be used by those preparing for a second-party or third-party audit.

1.3 Meeting ISO/IEC 27001 requirements

ISO/IEC 27001 has two main parts:

- the requirements for processes in an ISMS, which are described in Clauses 4–10 (the main body of the text); and
- a list of ISMS controls, which is given in Annex A. These controls are described in more detail in ISO/IEC 27002.

The ISMS process requirements address how an organisation should establish and maintain its ISMS. An organisation that wants to achieve ISO/IEC 27001 certification needs to comply with all of these requirements – exclusions are not acceptable.

The ISMS controls listed in ISO/IEC 27001, Annex A are not mandatory. They are expected to be used as an aide-memoire to assist the organisation in identifying where it might have missed a risk or relevant security control in its risk assessment and creation of its risk treatment plan. This is stated in ISO/IEC 27001 as follows:

"The organisation shall… produce a Statement of Applicability that contains the necessary controls… and justification for inclusions, whether they are implemented or not, and the justification for exclusions of controls from Annex A."

[1] Auditors deployed by the organisation to carry out an internal ISMS audit, auditors from certification bodies and assessors from accreditation bodies engaged in assessing certification bodies.

[2] See ISO/IEC 27001, 1.

CHAPTER 2: IMPLEMENTING AND AUDITING ISMS CONTROL OBJECTIVES AND CONTROLS

In this section, each of the control objectives and control requirements in ISO/IEC 27001, Annex A are discussed from implementation and auditing viewpoints, taking into account the implementation advice given for each control in ISO/IEC 27002, the code of practice for information security management. The complete control objectives from ISO/IEC 27002 are included in this document to clarify the requirements.

Readers are encouraged to read both the implementing and auditing sections to obtain a clear view of what is required and how it might be tested.

2.1 Information security policies (ISO/IEC 27001, A.5)

2.1.1 Management direction for information security (ISO/IEC 27001, A.5.1)

“Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.”

2.1.1.1 Policies for information security (ISO/IEC 27001, A.5.1.1)

“A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties.”

Implementation guidance

Guidance on what an information security policy should contain can be found in ISO/IEC 27002, 5.1.1.

Organisational policies should be simple and to the point. It may not be appropriate to combine every level of policy into one document. In this case, the top level information security policy can easily refer to more detailed policies, e.g., using hyperlinks. Indeed, the top level policy should normally be capable of expression within a single piece of paper. It might also be part of a more general policy document. The top level information security policy should be distributed and communicated to all staff, and to all relevant external parties, e.g., others regularly working on the organisation's premises.

The lower level policies should be available to appropriate staff as needed, dependent on their job function and the associated security requirements, and classified accordingly. The top level information security policy and several, or all, of the lower level policies could be delivered to staff within a security policy manual.

The information security policies should be subject to version control, and should be part of the ISMS documentation. It should be ensured that all those with responsibilities for information security have access to all necessary policies. Information security policies should also be made available to anyone with appropriate authorisation on request, and they should be protected from tampering and unintentional damage.

When an information security policy is distributed outside the organisation, it should be redacted, with any sensitive information that might have been contained in it removed before such distribution.

Auditing guidance

The top level information security policy does not need to be extensive, but should clearly state senior management's commitment to information security, be under change and version control, and be signed by the appropriate senior manager. The policy should at least address the following topics:

- a comprehensible definition of information security, its overall scope and objectives;
- the reasons why information security is important to the organisation;

- a statement of top management's support for information security;
- a summary of the practical framework for risk assessment, risk management and for selecting control objectives and controls;
- a summary of the security policies, principles, standards and compliance requirements;
- a definition of all relevant information security responsibilities (see also 2.2.1.1 below);
- reference to supporting documentation, e.g. more detailed policies; and
- how non-compliances and exceptions will be handled.

The auditor should confirm that the policy is readily accessible to all employees and all relevant external parties, and that it is communicated to all relevant persons, checking that they are aware of its existence and understand its contents. The policy may be a stand-alone statement or part of more extensive documentation (e.g. a security policy manual) that defines how the information security policy is implemented in the organisation. In general, most, if not all, employees covered by the ISMS scope will have some responsibility for information security, and auditors should review any declarations to the contrary with care.

The auditor should also confirm that the policy has an owner who is responsible for its maintenance (see also 2.1.1.2), and that it is updated appropriately following any changes affecting the information security requirements of the organisation, such as changes in the original risk assessment.

Topic-specific policies that underpin the top level policy should be clearly linked to the needs of their target group(s), and cover all topics that are necessary to provide a foundation for other security controls.

2.1.1.2 Review of the policies for information security (ISO/IEC 27001, A.5.1.2)

"The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness."

Implementation guidance

This control forms an important part of the continuous maintenance, review and updating of the ISMS, which is also addressed in Clause 9 of ISO/IEC 27001 'Performance evaluation'.

This maintenance process should detect all changes that affect the ISMS, and update the information security policy if appropriate, to keep it current and to ensure that it accurately reflects how the organisation is managing its risks.

Scheduled periodic reviews and defined review procedures are also essential to ensure that any changes which have gone undetected thus far are taken into account. Appointing an owner for the information security policy, with responsibility for its review, helps to ensure that a periodic review does take place.

Staff should also be made aware of policy changes that may affect their role (see 2.1.1.1).

Auditing guidance

This control is necessary to ensure that information security policies are current and effective. Information security policies play an important role in the establishment and maintenance of an ISMS.

Auditors should confirm that the organisation has appointed an owner for its information security policy with responsibility for its review, or, if this has not taken place, ensured that other clear responsibilities are in place for the review.

Auditors should also confirm that the organisation has developed procedures to react to any incidents, new vulnerabilities or threats, changes in technology, or anything else that is related to the ISMS and might make a review of the policy necessary.

There should also be scheduled periodic reviews to ensure that the policy remains appropriate and is cost-effective to implement in relation to the protection achieved. The auditor should confirm that the time schedule for such reviews is appropriate for the overall risk context of the organisation.

Auditors should also check the organisation's plans for distributing updated policies and verify that all employees are made aware of the changes.

2.2 Organization of information security (ISO/IEC 27001, A.6)

2.2.1 Internal organization (ISO/IEC 27001, A.6.1)

“Objective: To establish a management framework to initiate and control the implementation and operation of information security within the organization.”

2.2.1.1 Information security roles and responsibilities (ISO/IEC 27001, A.6.1.1)

“All information security responsibilities shall be defined and allocated.”

Implementation guidance

The organisation will be vulnerable if employees, contractors and third parties are not aware of what rules they must comply with, and what behaviour is expected of them. All employees, contractors and third-party users should have their roles and responsibilities relating to information security defined and clearly communicated to them. These roles and responsibilities should also be consistent with the organisation’s security policies.

Responsibility for the protection of individual assets and for carrying out specific security processes should be clearly defined and documented in accordance with information security policies (see 2.4.1.2). This is not a trivial task, and should encompass every employee. It is fundamental that management and staff should be told what is expected of them, especially where information security is not likely to be their first interest. In general, all staff should have a basic responsibility for security noted in their job description (see also 2.3.1.2), and they should understand their security responsibilities to be an integral part of their job function. Those employees, contractors and third-party users with substantial and complex security responsibilities should have these detailed in a document, for example in their job description or in the terms and conditions of employment (see 2.3.1.2). This document could be signed by the employee, contractor and third-party user, and their manager, to indicate acceptance and understanding. All employees, contractors and third-party users should be given a personal copy.

When information security responsibilities change, those affected should be made aware of the change in a timely fashion and provided with appropriate training to ensure that they can fulfil their changed responsibilities (see 2.3.2.2).

Information security responsibilities may also be delegated to others during work processes. In such cases, it is important that the persons delegating their responsibilities are aware that they remain accountable, and that it is part of their role to determine that any delegated tasks and responsibilities have been performed correctly. This also applies when an organisation outsources activities to another entity (see 2.11.1.3). A member of the organisation should be responsible for managing the relationship and ensuring that the third party carries out their part of the activities that support the ISMS.

Auditing guidance

Auditors should confirm that somebody with overall responsibility for information security has been appointed (e.g. an information security manager).

The information security policy, and/or the risk treatment plan, is normally used to define the higher level responsibilities and reporting structure, but the explicit detail of information security responsibilities is normally contained in job descriptions or some other format based on the individual. All employees having specific roles and responsibilities for information security should therefore have a document, e.g. the job description that defines these security roles and responsibilities. Auditors should check that this is available to the relevant employees, and that the employee is fully aware of their roles and responsibilities. One way of demonstrating this is to check whether the document has been signed by both the employee and appropriate manager, to signify understanding and acceptance. Another aspect for the auditor to check is the date of the document, and whether it contains correct and consistent details relating to information security functions. A check of the security responsibilities defined in policy statements and individual procedures should provide full consistency with the individual roles and responsibilities. Where security roles have changed since the individual took on their current role, the auditor should look for either a reissued document or an addendum to the original one, again signed by the employee and relevant manager.

Organisations may vary in terms of where documents describing roles and responsibilities are held; some may be with the individual, others with personnel/HR departments. In the latter case, it should be checked that the individual has ready access to this information – they should have their own copy, as a person is unlikely to comply with a document last seen perhaps over a year ago. Where individuals have jobs with specific security requirements, such as a network administrator, ensure that the job description or an additional document fully reflects this – general statements covering all employees are not acceptable in such cases. Auditors should confirm that all documentation of this nature is current and properly controlled.

It is particularly important that those who are new to their jobs fully understand their responsibilities. The relevant paperwork should be completed at the time of appointment, before the new hire can accidentally contravene policy or act inconsistently with their responsibilities, not at the next convenient review. Auditors should pay particular attention to temporary employees, contractors and third-party users. The same rules should apply to them; exceptions are not acceptable. There should be adequate descriptions of security roles and responsibilities for everyone working within the scope of the ISMS.

The clear definition and allocation of information security roles and responsibilities should be carefully investigated, as this can be a potential weak link in many situations. Overlaps in responsibility without a specific person being designated as lead, can result in no one taking responsibility; conversely, if no one has been allocated a specific responsibility, it cannot be verified that it will be carried out.

2.2.1.2 Segregation of duties (ISO/IEC 27001, A.6.1.2)

"Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorised or unintentional modification or misuse of the organisation's assets."

Implementation guidance

Segregation of duties is a traditional business control used to reduce vulnerability to human error and deliberate misuse. Although most of the people employed in an organisation are essentially honest, there might be some who are not. Equally, honest people may be placed in a position where they will behave uncharacteristically (e.g. if under duress). A proportion of people may also become increasingly negligent over the course of time if their activities are not limited. This can lead to problems with integrity (of people as well as information), loss of confidentiality and resources becoming unavailable for their proper purpose. Ensure that risk assessments properly identify the risks of unsegregated activities.

Dividing a process up between two or more staff provides a check at the point of handover, as one person can see that another has done what they were supposed to do. In sensitive areas, for example, the use of two keys or passwords by separate staff can ensure that no one obtains access to a resource without a second person either authorising or confirming their authority.

Many fraud and accounting deceptions are committed by people who have been given access to too many functions within an accounting system, and/or not needing separate authorisation for their activities. A well-known disaster of this type was the Barings Bank incident. In 1995, a single trader, Nick Leeson, made a loss of £827m before being detected. This resulted in the collapse of the entire business. The subsequent Bank of England indicated that this was caused by "serious problems of controls and management failings within the Barings group".

Segregation prevents staff from operating on their own to create such incidents. Although the possibility of collusion remains, it is very rare that more than two people will take the personal risk.

In small organisations, where segregation can be difficult to implement, the principle should be applied as far as possible with additional controls, such as increased monitoring, being implemented to compensate for any lack of segregation. If segregation of duties cannot be achieved, it can at least help to record all activities and to have procedures in place for independent review of these records to identify any suspicious or unauthorised activity.

Auditing guidance

As noted in ISO/IEC 27002, 6.1.2 small organisations may find it difficult to implement this control. This may be due to a lack of resources. At least for critical roles, some provisions should be in place – if nothing else is possible, at least crucial activities should be logged and the logs reviewed. The auditor should ask to see these logs and evidence of the review process. It should also be shown that the individuals whose activities are being logged cannot alter or delete these logs, perhaps by the logs being stored in an unalterable format, numbered sequentially by someone other than the subject of the logs and checked for missing entries as part of internal audit activities (see ISO 27001 9.2).

For larger organisations, this principle should be an established fact and properly demonstrated in their procedures. Of those procedures that should be considered for independent operations, security administration and audit are possibly the most critical and should be considered first.

The auditor should look at what independent verification of data and results is carried out between processing stages or before release. As part of its risk assessment, the organisation should have considered critical processes and whether any one person is responsible for carrying out too many of the checks and balances. Look at work arrangements for critical tasks: how are periods of sickness or holidays covered? Does this compromise independence? The organisation might need to enforce mandatory minimum holiday periods to achieve effective segregation. This approach is standard in some financial sector organisations.

2.2.1.3 Contact with authorities (ISO/IEC 27001, A.6.1.3)

“Appropriate contacts with relevant authorities shall be maintained.”

Implementation guidance

The organisation should have procedures in place to identify and establish all appropriate liaisons that must be in place with external regulatory bodies, service providers and any other organisation important for information security. In addition, the necessary approvals, non-disclosure agreements, reporting procedures and formats should be defined and approved to ensure that as much relevant information as possible can be exchanged.

It might be helpful to establish the function of a liaison officer who is responsible for contacting and liaising with authorities. This person can receive information from the authorities that might be helpful to guard against certain events, and to prepare for upcoming new legislation or regulations. They may also manage communications with authorities in the case of an incident (see

Auditing guidance

This control requires appropriate relationships to be in place with external regulatory bodies, service providers and others who may have a crucial role in either preventing security incidents or in mitigating their effects. The auditor should therefore look for evidence regarding the existence of the necessary contacts in business continuity and contingency plans, and infrastructure support documents. Contact details should be checked and updated on a periodic basis to ensure they are correct. For each contact, the purpose of the contact should be clear. Depending on the context, the auditor may ask the relevant liaison to make contact, to show that a chain of communication is established and to check that the contact details are accurate. The auditor can also check whether contacts are event-driven (e.g. following an incident) or time-driven (e.g. every quarter). Depending on the purpose of a contact, both types of relationship may be appropriate, but if contacts are really in use, the liaison should be very clear on how they are initiated and by whom.

The auditor should also look for evidence that legal, industrial, operational and technical requirements are being monitored for conformity as appropriate. The auditor should ensure that the organisation is able to demonstrate that it knows and has documented all applicable legal requirements, and that all contacts necessary to conform to these requirements are in place and up to date. Agreements and approvals should also be reviewed by the auditor to ensure that information being provided to relevant authorities is suitable, timely and authorised.

2.2.1.4 Contact with special interest groups (ISO/IEC 27001, A.6.1.4)

"Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained."

Implementation guidance

Good ideas can be acquired from a meeting of information security professionals from different organisations and sectors, many of whom have long and valuable experience in the subject, as well as from joining specialist groups, standards committees, etc. Although some bodies involve a membership fee, they will usually give you a taste of what they have to offer before you need to make up your mind. Other bodies do not have members as such, but are useful sources of information. Many of them communicate via the Internet, which can be a useful source of security information. Try a search on a keyword or organisation using one of the many search tools available. Various individuals have made a name for themselves based on the provision of interesting, accurate and timely information online. Following their activity is an excellent way to maintain awareness of new threats, opportunities and trends.

Exchanges of security information should be controlled to ensure that confidential information is not passed to unauthorised persons. Some bodies operate on a strict non-disclosure basis to enable confidential discussion.

Auditing guidance

It is usually very helpful for an organisation to participate in discussions on best practice and share knowledge on threats being promulgated across the industry. A large organisation can be involved in security specialist groups, standards committees or similar activities outside its own environment. Smaller organisations are unlikely to be able to support extensive involvement, but attendance at appropriate free conferences and seminars would partly address this. In either case, auditors should check that procedures are in place to share and distribute any information received from such participation within the organisation in the most beneficial way. These procedures should also be designed to ensure that no confidential information is exchanged without proper authorisation.

2.2.1.5 Information security in project management (ISO/IEC 27001, A.6.1.5)

"Information security shall be addressed in project management, regardless of the type of the project."

Implementation guidance

Projects are a major component of any organisation's work. Inappropriately controlled security during the delivery of a project can expose the organisation to uncontrolled business risks, resulting in information security incidents. Equally, the products and services that the project intends to deliver must also be suitably secure. A deliverable that provides what the customer asked for, but which also provides a route for compromise of an environment, is not fit for purpose. The chances of this outcome can be managed by integrating information security appropriately into project delivery.

In order to ensure that a project preserves security during its lifespan, and produces secure deliverables, two types of risk assessment should be carried out at the beginning of the project. One type of risk assessment should consider risks relating to the activities of the project itself, and the other should consider risks relating to its deliverable(s). They should both produce security controls, which should be combined into one list and documented as part of project requirements. These requirements should then be prioritised according to the risks that the controls are intended to counter, and implemented as part of standard project activities.

Care should be taken to distinguish between the concept of 'project risk' and information security risk. The project may have a risk register that lists the risks to the delivery of the project, but this may not be a suitable vehicle within which to record and manage information security risk. Consider having an information security risk register, which integrates with the organisation's ISMS and is referenced explicitly from the project risk register. The information security risk register will then be less subject to the drivers that can overwhelm local project requirements. For example, a project may choose to remove operational requirements to improve its chances of delivering on time. Proposed changes to information security controls should be raised at the appropriate organisational level so that the risk to the organisation may be managed suitably.

Since projects inevitably change during their lifespans, information security should be reassessed as part of any project change process, to ensure that risk mitigations are still suitable. There should also be consideration of information security at all key stages in the project's lifespan.

Finally, the transition phase of deliverables should be very carefully managed to ensure that project security requirements are realised appropriately in the deliverables that survive the project.

Auditing guidance

The auditor should firstly check the documentation for the project methodology in use, and check that it contains a requirement for identification of information security objectives, risks (as distinct from project risks) and controls. The methodology should also contain checkpoints throughout the project lifecycle to ensure that information security is addressed regularly. Any changes in the project should automatically initiate a review of existing information security risk assessment work, to ascertain whether it needs to be revised. Changes should be made as appropriate to existing controls, new controls added and/or controls removed. There should be a statement to the effect that responsibilities for information security must be defined and associated with particular roles.

In terms of what should be documented for each project, the auditor should seek to find evidence that there is a record of information security objectives and an information risk assessment for each project. Evidence should also be obtained to show that information security risks can be traced to specific controls. Responsibilities for information security during each phase of the project should be defined, and roles should be associated with these responsibilities.

2.2.2 Mobile devices and teleworking (ISO/IEC 27001, A.6.2)

“Objective: To ensure the security of teleworking and use of mobile devices.”

2.2.2.1 Mobile device policy (ISO/IEC 27001, A.6.2.1)

“A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices.”

Implementation guidance

In most cases, the use of mobile computing and communication facilities takes place outside the organisation, e.g. in airports, or on planes or trains when travelling; during conferences and meetings; or with customers at their organisation or home. There are many additional risks to mobile equipment that result from this way of working. This is particularly important where users are allowed to use their own personal devices.

Employees using mobile equipment should be aware of these risks and should adapt their behaviour accordingly. The organisation should develop a mobile computing policy describing the controls that should be in place, and employees should only be allowed to use mobile devices after they receive the policy and have had sufficient training and awareness education. Mobile devices should be required to meet an appropriate standard of security (e.g. be promptly updated to remove security vulnerabilities), and users should have clear guidance on what to do and who to inform should a device be lost or stolen, especially if it is a personal device.

Other security risks when using mobile computing facilities are related to information exchange. Backups should be made regularly, and effective and frequently updated malware protection should be used (as available – some devices do not require this protection) if any information transfer takes place. In the case of remote connections to the organisation's site, authentication not only for the machine, but also for the authorised user, should be in place, to avoid such connections being exploited, e.g. by somebody who has stolen a laptop or mobile phone.

ISO/IEC 27002 describes in 6.2.1 some controls that can be applied to protect information and facilities used in mobile computing and communications.

Auditing guidance

The auditor should confirm that the use of all mobile computing and communication devices and equipment has been identified by the organisation. This includes the use of personal and work-owned mobile phones, laptops or other mobile devices outside the organisation's premises (e.g. at home, customer sites, hotels, during travel or at conference venues), and any remote connections to the organisation's internal information processing facilities using such devices. As mobile computing and communication activities normally take place outside the organisation, their use will normally be difficult to audit directly.

It is therefore particularly important that the auditor looks closely at the controls, rules and procedures that the organisation has in place to ensure that such devices are used securely. This includes the controls that should be implemented to protect such devices. User training and awareness, authorisation processes and security arrangements for using such devices can be reviewed against the list in ISO/IEC 27002, 6.2.1.

As is feasible, audit evidence should be collected to check that all these controls are implemented correctly. Audit checks for controls should also include what the policy says about password and malware protection on mobile computers, what is permitted to be stored locally, the use of cloud services for backups, and what additional software must be present to separate personal and work-related data. Check that there are sufficient controls in place to secure remote access, and that strong cryptographic controls are applied where necessary.

2.2.2.2 Teleworking (ISO/IEC 27001, A.6.2.2)

"A policy and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking sites."

Implementation guidance

As in the mobile computing environment, the main security problems with remote working from a fixed address (similarly to working from a mobile or temporary location) arise from the location where this work is taking place. The user's home does not normally have the same level of physical security, and their work area is often easily accessible by family members and visitors. To reduce these risks, teleworking should only take place after the organisation has developed appropriate policies and procedures, has put in place physical controls to secure the work area and has raised the awareness of the employees doing teleworking sufficiently to control the physical and logical access to the information processing facilities used for teleworking activities.

Connections between the organisation's site and teleworking facilities should be secured to ensure that information cannot be destroyed, damaged, compromised or modified. Information that is accessible remotely should be restricted to a minimum.

ISO/IEC 27002, 6.2.2 contains a detailed list of actions the organisation should consider before authorising any teleworking activities.

Auditing guidance

A list of users who are authorised to carry out teleworking should be recorded, along with what level(s) of activities are authorised (e.g. what classifications of data they are allowed access to) and what controls should be in place. It should be possible for the organisation to show how it verifies that these controls are in place, perhaps via a register, along with a generic or specific risk assessment for teleworking activity. It should be clear who is responsible for implementing and maintaining which of the controls (the user or the organisation). Teleworking activities should only be authorised if sufficient controls are in place, including physical controls, access controls and security of the remote connection. The remote working equipment should be included in the asset register. There should also be some mechanism for establishing and controlling what information is transmitted to, from and used at home, or other teleworking environment.

There should be a defined policy on the use of the equipment for non-work related activities, such as games software, accessing the Internet, etc., any of which can introduce problems when allowed to interfere with sensitive data. ISO/IEC 27002, 6.2.2 provides a useful list of measures that describe what the auditor can review to determine whether the organisation has adequately secured their teleworking environment.

2.3 Human resource security (ISO/IEC 27001, A.7)

2.3.1 Prior to employment (ISO/IEC 27001, A.7.1)

"Objective: To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered."

2.3.1.1 Screening (ISO/IEC 27001, A.7.1.1)

"Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations and ethics and shall be proportional to the business requirements, the classification of the information to be accessed and the perceived risks."

Implementation guidance

Screening is an essential control that can prevent the organisation employing the wrong person but legal restraints may put a limit on the checks that the organisation may consider. Whatever screening and data collection take place, care should be taken to ensure that all applicable legislations and regulations are complied with. Identification checks, CV reviews and checks of qualifications and character references should be made. Where the proposed position provides access to sensitive, critical and/or personally identifiable information, it is essential to get details of the applicant's responsibilities in previous positions and get them confirmed by previous employers. Although one should be wary of very cursory references, remember that some organisations will not, as a matter of policy, offer any detail or opinion other than confirmation of the period employed and the last position held. Gaps or irregularities in employment should be questioned.

All exchanges and interviews should be fully documented and retained on file throughout employment and for a reasonable period after it ceases, or after rejection of an application pending any possible appeal by the applicant. The required screening processes should take place for all people working within the scope of the ISMS, irrespective of whether these are employees, contractors or third-party users.

Auditing guidance

The auditor needs to collect relevant evidence that screening procedures for personnel recruitment (including contractors, third-party users and temporary staff) are being enforced and include appropriate verification checks. ISO/IEC 27002, 7.1.1 lists the items to be covered. In particular, organisations should not rely solely on employee-supplied CVs, endorsement letters or qualifications without suitable verification of the claims made. The auditor needs to check any follow-up actions, such as conversations with referees, which should be documented. It should be checked that managers are aware of their responsibilities for evaluating and reviewing the background checks for staff in their area of responsibility. The auditor should also check that all information related to personnel verification checks is handled in accordance with all relevant regulations and legislation (e.g. data protection).

2.3.1.2 Terms and conditions of employment (ISO/IEC 27001, A.7.1.2)

“The contractual agreements with employees and contractors shall state their and the organization’s responsibilities for information security.”

Implementation guidance

It is important that employees, contractors and third-party users are aware of their security and legal responsibilities regarding the handling of information, the classifications and use of information processing facilities and the consequences of not complying with security or legal requirements. This also extends to any contractual obligations that the organisation has entered into that might affect the employee’s, contractor’s or third-party user’s scope of work. Any such responsibilities should be included in terms and conditions of employment.

It is also important that employees, contractors and third-party users sign a confidentiality agreement (see also 2.9.2.4) before starting work, and that they understand that such responsibilities may extend beyond their normal working environment and working hours, as well as home working, working on customer’s sites and any other form of remote working. Some confidentiality agreements may persist beyond the termination of the individual’s employment with the organisation, if legally permitted (see 2.3.3.1).

In addition, the organisation's responsibilities for handling the personal data of employees, contractors and third-party users should be stated, for example compliance with data protection legislation (see also 2.14.1.4).

Auditing guidance

Auditors should check whether the terms and conditions of employment accurately describe both the employer's and the employee's, contractor's or third-party user's responsibilities for information security. These descriptions should cover all security-relevant aspects of the employee's job, including responsibilities applicable to legal requirements, responsibilities related to classified information, working outside the organisation or outside normal working hours, and those responsibilities that might extend beyond the employee's contract. The terms and conditions should also describe the actions that will be taken if employees do not fulfil their security responsibilities. The auditor should check that agreement to, and signing of, the terms and conditions of employment is a necessary requirement before any work starts. Employees, contractors and third-party users should also be required to sign a confidentiality agreement (see also 2.9.2.4) before accessing any confidential information. The auditor should confirm that procedures are in place to ensure that the terms and conditions of employment are updated if the employee's security responsibilities change in any way, e.g. taking on new roles or using new or different information processing facilities.

The auditor should also check that the organisation's responsibilities for handling personal data are clearly stated, e.g. compliance with data protection legislation (see also 2.14.1.4).

2.3.2 During employment (ISO/IEC 27001, A.7.2)

"Objective: To ensure that employees and contractors are aware of and fulfil their information security responsibilities."

2.3.2.1 Management responsibilities (ISO/IEC 27001, A.7.2.1)

"Management shall require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization."

Implementation guidance

A key success factor for all security programmes is support from management. Part of this support is that management are aware of their duty to ensure that everybody in their area of responsibility (including themselves) is acting in compliance with approved policies and procedures, and is supporting/applying implemented controls. A list of typical management responsibilities is given in the implementation guidance of ISO/IEC 27002, 7.2.1. An important part of these responsibilities, in addition to the usual management functions, is to give employees, contractors and third-party users the message that their information security activities are recognised, valued and as important as other elements of their job function. The other key aspect is to execute the control function, and check compliance with controls, policies and procedures during day-to-day work. This might not need complicated policing exercises – if management is aware of the correct application of controls, policies and procedures, they will easily detect if people in their area of responsibility are varying from them.

Auditing guidance

The first thing auditors should check is that managers are aware of their responsibilities and understand their duty to ensure that employees, contractors and third-party users comply with controls, policies and procedures. The next step is to look for evidence that managers take this responsibility seriously – there could be several indications, such as mentioning information security in standing agendas for a meeting, or the reaction of employees when asked about management messaging regarding information security. Records of previous awareness evaluations (such as phishing tests) are also encouraging indicators. Another high-value indicator is whether employees feel that management is leading by example. Do individuals in senior roles comply with the same rules as apply to general staff (e.g. locking their computer when leaving their desk), or do they appear to have special dispensation to ignore the rules?

It can also help to ask about remedial training programmes for employees, contractors or third-party users whom management have identified as not complying with controls, policies or procedures, and what initiates such programmes. Another topic is what management does to motivate their personnel, whether there are reward programmes for good suggestions, or other ways of actively encouraging personnel to support information security.

2.3.2.2 Information security awareness, education and training (ISO/IEC 27001, A.7.2.2)

“All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.”

Implementation guidance

The organisation is vulnerable to the activities of untrained employees, contractors and third-party users. There is a risk of them producing incorrect and corrupted information or losing it completely. Untrained personnel can take wrong actions and make mistakes through ignorance.

All personnel should be trained in the relevant policies and procedures, including security requirements and other business controls. They should also be trained to use all the IT products and packages required of their position, as well as in the relevant security procedures. The organisation should consider when training should be repeated and updated.

Training might be required at different levels as follows.

security awareness: every employee, and where relevant, contractor and third-party user, should be given a foundational level of security awareness training. A course should convey to them the organisation's security policy, objectives and framework within which they are expected to work. Essential procedures should be provided and described. The material supporting this training (including procedures and policies) should be made readily available to employees, and updates circulated whenever any changes are made, ideally to only those affected by the changes. Awareness should be refreshed as necessary and through ongoing action.

security training: staff with special responsibilities for security (not only security-dedicated roles) should, in addition to basic training, be provided with relevant, specialist training. A training plan should be developed for each individual according to the specific knowledge and skill required for their role. The general development of security knowledge can benefit significantly from employees attending suitable conferences and carefully selected events, which are frequently free. All training and relevant event attendance should be recorded in the individual's training record. Training should be available to employees, agency staff and third-party users as appropriate. Ensure that training suppliers use appropriately qualified staff, and that the syllabus is clear and consistent with the organisation's requirements.

Generic training will not be retained nearly so well as training that reflects the ethos and culture of an organisation.

Auditing guidance

This control is applicable to all employees, including users of information processing facilities such as system administrators, managers and application users, as well as senior management and those processing any form of information (e.g. paper based, telephone, etc.). It is also applicable to contractors and third-party users, and anyone else with access to information or services within the ISMS.

The first point to check is the appropriateness of the training. This should be consistent with the job and the related security responsibilities. How is it provided, internally or externally? If internal, is it a formal course or general 'on-the-job' type training? Who is providing the training, and are they suitably qualified? If the training is informal, is there some definition of what has been covered? If the training is external, who has approved the supplier? Is the supplier an accredited or industry-recognised provider of training? What records exist and do they reflect the nature and depth of training given?

At a minimum, organisations should have some form of induction training that is given to all employees, contractors and third-party users. This should cover the general principles of security, the information security policy, areas of applicability, etc. This should be formally recorded in individual records. In addition, it should be ensured that sufficient training for those with more complex security responsibilities is in place, all training material is up to date and the training is provided in time for the job to be carried out. Check the records for different types of job function to ensure that sufficient training is provided, and that it is provided before access to information or services is given.

Training should be being repeated as appropriate to ensure that it is current and reinforced, and when the information that people should know, or the skills they need, change.

There will be situations, particularly with technical aspects, where experience or previously acquired qualifications are claimed in lieu of formal training. Auditors need to take a pragmatic approach on this and view the effective result of formal training, qualifications and experience when looking at the skills of individuals and how they fit with their roles. If previously acquired experience is claimed, make sure it is current and relevant. Also check what environment the experience was gained in, and whether it has been verified in a suitable fashion. Many organisations rely too heavily on what individuals claim in CVs – an inadequately trained or inexperienced individual in a key position can cause major damage to vital assets, so it is important that the organisation treats training verification seriously. This also relates to the checks that should be made on recruitment (see 2.3.1.1).

The auditor should confirm that the organisation provides appropriate training and keeps records of employee training activities. The auditor needs verification that staff are aware of the content of the information security policy, how they contribute to the effectiveness of the ISMS and the implications of not conforming with the ISMS requirements (ISO/IEC 27001 7.3). This can be obtained by interviewing staff members that the auditor randomly selects.

2.3.2.3 Disciplinary process (ISO/IEC 27001, A.7.2.3)

"There shall be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach."

Implementation guidance

Any non-compliance with the security policy or controls by employees needs to be properly dealt with or there will be a decline in standards and an increase in insecurity. The disciplinary process should be shaped by the organisation's culture and management practices. It should be documented and staff should be aware of how it works. To avoid demotivated employees, amongst other issues, the disciplinary process should ensure consistent and fair treatment. It should only be initiated after there is sufficient evidence that a security breach or a non-compliance with controls, policies or procedures has taken place. The actual process should match that which is documented. Different levels of non-compliance should be considered in the disciplinary process, to be able to react accordingly to the grade and severity of the incident. Compliance incentives (which can be included in training programmes) can act as an excellent foil to sanctions for non-compliance.

Auditing guidance

This might be a sensitive issue in organisations, but it is important that such a process is in place to be able to react properly to any security breaches, and to deter or correct non-compliance. Auditors should check that all employees are aware of the disciplinary process, that it is initiated following an appropriate trigger and that it provides fair treatment to all involved. If the disciplinary process is not implemented correctly, the organisation may be liable to potential claims of unfair dismissal or other personal infringements.

Auditors should also check recorded security incidents, look at the criteria for disciplinary action and verify that it has been initiated when criteria had been met. Auditors should also verify that procedures are in place to ensure that the disciplinary process is only used if there is sufficient evidence that a security breach or non-compliance has occurred.

2.3.3 Termination and change of employment (ISO/IEC 27001, A.7.3)

"Objective: To protect the organization's interests as part of the process of changing or terminating employment."

2.3.3.1 Termination or change of employment responsibilities (ISO/IEC 27001, A.7.3.1)

"Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor and enforced."

Implementation guidance

Many problems can occur if termination or change of employment is not handled appropriately (see also 2.4.1.4 and 2.5.2.6). This could include excess permissions being granted to an individual who changes roles, resulting in a loss of segregation of duties. This could also include an individual retaining access to sensitive staff records after they have left the organisation, which breaches data protection laws.

There should be processes in place to ensure that all rights for logical and physical access are removed as and when the job function terminates. A specific role within the organisation should be responsible for making this happen, ensuring that the necessary communications between departments takes place in case of termination or change of employment. On termination, all equipment and information belonging to the organisation or its customers should be returned as per company policy.

The responsibilities for termination or change of employment should also include any ongoing security or legal requirements that need to persist after any business relationship has ended. The most typical example is the confidentiality agreement. All such responsibilities and duties should be covered in the employee's, contractor's or third-party user's contract.

Another important point that is sometimes overlooked is that these controls should be applied not only in the case of employment termination, but also when an employee, contractor or third-party user changes role. A change of role should be handled as a termination of one role and the beginning of another. All logical and physical access rights and all assets related to the old role need to be returned.

Auditing guidance

The auditor should confirm that the organisation has procedures in place for the termination and change of employment. The auditor should look for records that provide evidence that these procedures and responsibilities are clearly assigned and executed, and that responsibilities have been appointed for the termination of logical and physical access rights and the return of assets (see also 2.4.1.4). There should be procedures in place to ensure that all parties involved in these actions are notified if a termination or change of employment takes place, as well as other parties who need to be aware of the event.

Another aspect for the auditor to consider is the handling of responsibilities or duties that continue for a period after employment has terminated. The auditor should check whether such responsibilities have been included in the contract.

Finally, it should be confirmed that the responsibilities, controls and procedures applied in case of employment termination are also applied when an employee's or contractor's role changes.

2.4 Asset management (ISO/IEC 27001, A.8)

2.4.1 Responsibility for assets (ISO/IEC 27001, A.8.1)

"Objective: To identify organizational assets and define appropriate protection responsibilities."

2.4.1.1 Inventory of assets (ISO/IEC 27001, A.8.1.1)

"Information, other assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained."

Implementation guidance

An inventory of physical assets is required by accounting standards. For this reason, as well as for information security reasons, all organisations should have such an inventory. For information security purposes, the information assets that the organisation holds should also be included in an inventory. This may be in the same system or a separate one, as long as they are correlated appropriately (for example, enabling one to identify which servers hold which information). Appropriate protection can be applied to assets if it is known that the organisation has them, as then their information security, business and legal requirements can then be assessed. The level of granularity of the asset inventory should take into account the requirements of the organisation, and the level of detail that will be necessary to support an effective risk assessment. Information can be grouped by business purpose, for example, perhaps as a list of databases or file names.

It is important to note that some 'assets' may need to be retained by the organisation, and can actually constitute more of a liability than an asset. For example, identity documents which are required to be retained to prove that staff are authorised to work in the country. These assets cannot be used to generate revenue or positive value for the organisation. They should be treated as for other assets unless they are not actually required, in which case they should be disposed of.

For each instance of information and each physical asset, the inventory should contain information about its business value and classification (see also 2.4.2), and its backup and disaster recovery arrangements.

The inventory of physical assets should also contain full details of equipment identity, including owner (see also 2.4.1.2), location, maker, model, generic type (e.g. printer, PC), serial number, date of acquisition and inventory tag.

A record of disposals – when and how/who to – also needs to be kept, and the asset inventory should be updated whenever an item is disposed of. Organisational inventory tags (logo, inventory number) should be fixed to all items that appear in the inventory. It should be ensured that all documentation (including system documentation), contracts, procedures and business recovery plans are included in the inventory; indicate the owner and those with operational responsibility. Information stored in non-technical formats (e.g. on paper) should be recorded, as well as that in technical formats (e.g. on CD).

All software products should also be listed in the asset inventory, including where they are used and where the original media are kept, together with the relevant licensing information. Adequate procedures should be in place to maintain accuracy of the inventory, including updating the inventory as part of change management and project activities, and a stock check should be carried out at least annually.

Auditing guidance

The auditor should confirm that the organisation maintains a complete and accurate asset inventory (or correlated physical asset and information inventories). This should include all major information (in whatever form, including software), physical assets, services and processes to be protected. The assessment will first need to determine that assets have been properly identified and classified (see also 2.4.2.1). The auditor should evaluate the inventory's adequacy:

•is it complete and accurate?
•does it contain all necessary detail, and when and how is it updated?
•are disposals recorded, when and to whom?

The auditor should check that a role has been assigned responsibility for the asset inventory, and for its development and maintenance. They should also check how the inventory is protected. If the inventory is computer based, what about access control and backup? If paper based, where is it kept, how is it protected against loss, and what happens when the record is replaced? Are old copies kept? If yes, how long for and where? The asset inventory should identify:

- the item, format and, where applicable, its unique serial number, date, etc.;
- its business value and security classification;
- any special characteristics that may attract requirements (e.g. if personal data is involved);
- owner;
- location(s);
- media (if information);
- licence (software);
- retention period/lifespan;
- information about backups and disaster recovery; and
- date of entry and/or audit check.

2.4.1.2 Ownership of assets (ISO/IEC 27001, A.8.1.2)

"Assets maintained in the inventory shall be owned."

Implementation guidance

Possibly the most important concept regarding responsibility for and protection of assets, is to assign asset ownership. It is necessary to appoint an asset owner for all major assets or assets to which special requirements are attached (e.g. personal data). This asset owner is responsible for the asset itself, and its protection. This includes:

•determining the classification of the asset (see 2.4.2.1);
•supporting risk assessments by giving input about the asset's business value and its importance for the organisation's business activities;

•ensuring appropriate protection in the day-to-day use of the asset; and
•keeping security classifications and control arrangements up to date.

It might be the case that the asset owner is not working with the asset on a day-to-day basis. In such cases, it is best that the asset owner appoints a custodian that works with the asset and looks after the asset on the asset owner's behalf. This custodian then looks after the protection of the asset in day-to-day business. It is important to note that the owner remains ultimately accountable and needs to check that the custodian is taking their responsibilities seriously. As most organisations have many assets and/or complex systems, it can help to group several assets together, for example all assets involved in a particular process or in the provision of a particular service. The owner of that process or service could then be responsible for all of the assets involved in the process or service, and for their correct functioning and protection.

Auditing guidance

The auditor should confirm that owners have been assigned for all important assets, and that each owner is aware of the tasks and duties that come with asset ownership. It might be helpful to review the records for asset classification and risk assessments, to verify that the asset owner has actually participated in these activities to an appropriate level.

The auditor should also check the procedures in place to delegate routine tasks or the day-to-day use and protection of the asset to a custodian, and how, in case of such delegation, the owner checks that all tasks are carried out correctly.

As an asset inventory is only useful if it is up to date, the auditor should check the procedures in place to update the asset inventory, and how the introduction of new assets and the disposal of assets is reflected in the asset inventory. Project management and change management processes should be checked to see if they contain a step to update the asset inventory when changes occur which affect it.

2.4.1.3 Acceptable use of assets (ISO/IEC 27001, A.8.1.3)

"Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented and implemented."

Implementation guidance

Every organisation is vulnerable to staff, and others, misusing assets, i.e. using them in a way that varies from their authorised business purpose. This may be unintentional or deliberate. In either case, misuse can impact the integrity of data and systems, threaten availability and expose confidential information. Additionally, information processing systems can be misused to attack other organisations.

A typical example is the Internet. This can be used for casual browsing during working time (which is possibly not an authorised business use), or can be used to launch an attack from the organisation's network into other networks – an action the organisation could be held liable for.

In some circumstances, misuse of computers can be a criminal offence, for example in the UK under the Computer Misuse Act 1990. Similar legislation is in place in many other countries. The details of the applicable legislation should be checked out to inform control selection.

To ensure that assets are only used for their intended business purpose, the organisation should identify, develop and implement rules, procedures and guidelines describing their acceptable use. These rules can vary considerably depending on the asset considered. The intended business use, past incidents and the owner of the asset can give valuable input when developing the rules for acceptable use. Any different use should be considered as improper use, and all staff should be aware of that.

It is important that everyone using the asset signs up to these rules, including not only the organisation's employees, but also any contractors, third-party users or anyone else using the asset.

Auditing guidance

The auditor should confirm that acceptable use rules clearly describe the intended use of the assets, and also the boundaries of this intended use.

The organisation should apply controls to detect misuse. Disciplinary procedures should deal with actions on discovering intentional misuse (see also 2.3.2.3) and inadvertent non-compliance. Investigate the use of other, peripheral or associated equipment such as printers, copiers, etc. What is the policy here? Is a suitably brief and readable warning message displayed at log-on, making the user aware of the fact that unauthorised use of information processing facilities is not permitted?

The auditor should also confirm that asset users are aware of these rules. Evidence could be that the rules have been signed before access to the asset has been given. It is also important to talk to users to see if they retain an awareness of what constitutes inappropriate use. The auditor should review incident reports to see if they identify where the rules of acceptable use have not been followed, or have not functioned as intended. The reports should also lead to changes in the rules of methods for circulating them, as appropriate. If the organisation has no rules in place for the acceptable use of assets, there should be valid reasons for not doing so, and this should be supported by the findings of the risk assessment. Again, it might be helpful to look at incident reports to identify areas where rules for acceptable use would be helpful.

2.4.1.4 Return of assets (ISO/IEC 27001, A.8.1.4)

"All employees and external party users shall return all of the organizational assets in their possession upon termination of their employment, contract or agreement."

Implementation guidance

The organisation should have procedures in place to ensure that all assets in the possession of employees, contractors and third-party users are returned when their employment terminates or changes (see also 2.3.3). It is important that this covers all assets, not only equipment and software, but also all of the organisation's documents and any information stored on media. Depending on the organisation, its business and the particular job function, there might also be other assets, e.g. credit cards, access cards, manuals and mobile devices.

All of the organisation's information that might have been stored on non-organisational assets, such as private equipment, or equipment of a third-party organisation or of a contractor, should also be returned and securely erased from that equipment. The return of assets should be part of the contract.

Auditing guidance

Auditors should examine the procedures the organisation has in place to ensure the return of assets. There are several issues that these procedures should address:

•they should cover all assets, ranging from hardware and equipment to information in any form (electronic, paper, on storage media, slides, films, etc.), and should also cover keys or cards that are used for access control purposes;
•they should also cover the transfer of any information stored or processed on non-organisational equipment or media, and the secure erasure of the information from the equipment or media; and
•they should be applicable to employees, contractors and third-party users.

The auditor should also check that these procedures are not only applied upon termination, but are also applied if employment changes and the assets are no longer required in a new job function. Records for each leaving or moving employee, contractor and third-party user should verify the return of assets.

2.4.2 Information classification (ISO/IEC 27001, A.8.2)

“Objective: To ensure that information receives an appropriate level of protection in accordance with its importance to the organization.”

2.4.2.1 Classification of information (ISO/IEC 27001, A.8.2.1)

"Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification."

Implementation guidance

Information with different requirements for protection of confidentiality, integrity and availability will require differing levels of protection and handling procedures to enable this protection. A method of labelling called 'classification' should be used to indicate the required protection level for information.

There should be a clear decision as to whether all information must be classified, or whether unclassified assets are permitted, and what handling is permitted for these.

The classification scheme should be in writing and available to all those with authority to apply it, i.e. all those who originate documents and data. It should also be available to those who need to understand what the classification means when applied to a document. The classification scheme should also be easy to understand and clearly differentiate between levels to support the correct assignment of classification levels. Too many levels will lead to inconsistency as staff cannot differentiate between definitions. Too few levels, and staff will find that they need to over- or under-classify.

There is no international standard for the classification of information. Most large organisations and government bodies have a formal scheme, which can vary considerably. Similar labels may be used (confidential, restricted, etc.), but their meaning, in terms of their value, criticality and sensitivity, can be very different – often because the organisations' business needs are different.

The handling, storage and disposal requirements of each classification should be specified, and supporting procedures created. Allowance should be made for the need to periodically review classifications, and change the level of classification when/if the sensitivity changes. Provide change and expiry dates to record these. The asset owner should be responsible for classifying their asset(s), ensuring that handling rules are complied with and updating the classification as appropriate (see also 2.4.1.2).

Auditing guidance

Auditors should confirm that the organisation has developed or selected, and implemented, an adequate and consistent classification scheme, supported by training and handling rules. For assets to be properly protected, there should be some form of grading based upon their individual requirements for confidentiality, integrity and availability. The classification that is assigned to an asset, and the associated handling requirements, should take account of business requirements for exchanging and sharing information, as well as the security requirements of the asset. The classification scheme should be applied to all assets considered in the scope of the ISMS. Without clear classification, assets may not be properly protected. The scheme should not be too complex and should be supported by arrangements with other organisations to ensure that the interactions between different classification schemes are understood. Do the procedures account for how the correct classification is to be checked? Does a procedure to review and upgrade or downgrade the classification level exist?

The auditor should confirm that the classification and handling scheme is readily accessible, understood by all staff and regularly reviewed. The owner of an asset should be responsible for assigning its classification, applying/supervising appropriate handling and for updating the classification if anything changes.

2.4.2.2 Labelling of information (ISO/IEC 27001, A.8.2.2)

"An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization."

Implementation guidance

There is a risk of unauthorised disclosure, modification or destruction of classified material. All information assets can be prominently labelled in a manner suiting their form to ensure that they can be associated with the necessary handling in use, storage and transport. All printed items should contain the appropriate classification label (unless unclassified), and unbound documents should carry it on every page.

Information held in information systems should also be classified, although it is sometimes challenging to label it. Its classification should be maintained in the system or application documentation. Handling requirements should be reflected in the system by the use of appropriate technical controls, such as access levels and the range of users who can access it and at what level (read-only, write, delete). Some security systems may include a security labelling facility. In any case, it should be ensured that the outputs (e.g. print-outs) carry the label with them.

Transmitted information also requires classification. Low sensitivity information might be sent in an open email message, but information of higher sensitivity may require encryption. The classification should be indicated in the text of the message. To maintain the security of information transferred within an organisation or between organisations, appropriate controls need to be considered such as that defined in ISO/IEC 27002 13.1.

One consideration that may significantly affect this advice is where it is inadvisable to make it obvious which information is the most valuable or sensitive, as this essentially provides a shopping list for an attacker. In this case, only roles that need to know of the most sensitive information should be aware of its existence, and labelling may be disguised. This, of course, may lead to the risk of inadvertent mis-handling should the information fall into the wrong hands, so the control of distribution of this information, and the thorough training of roles which handle it, is vital.

Care should be taken in interpreting classification labels on documents from other organisations because different organisations may have different definitions for the same (or similar sounding) label. Equally, ensure that your classifications will be properly respected when sent to other organisations.

Information may cease to be sensitive after a certain period of time, for example when it has been made public. In such cases, provide an expiry date to avoid unnecessary protection expense.

Auditing guidance

The auditor should confirm that the organisation has procedures for the labelling of classified information, compatible with the classification scheme. Auditors should also confirm that the marking suitably represents the most sensitive item in the entity (e.g. an information processing system or a database).

Labelling physical items, such as documents, tapes, hardware, etc., is straightforward, but what about information held in information systems, and correspondence electronically transferred? The auditor should confirm that the solutions the organisation has chosen for labelling electronic formats have been checked for adequacy. Is this clear and understandable? Does it convey the correct label to the receiver of the information, and does this subsequently lead to sufficiently secure access, use or storage of that information? Are the labels of physical assets appropriate? Labels may be hard to find where they should be prominent; adhesive labels can become detached and leave the item unmarked and unprotected.

2.4.2.3 Handling of assets (ISO/IEC 27001, A.8.2.3)

"Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organization."

Implementation guidance

There is risk of a breach of confidentiality whenever sensitive information is handled, for example, invoices, cheques and financial transaction data. Additionally, breaches of integrity and availability may need consideration depending on an asset's classification. Procedures for the storage, processing (including destruction) and transmission of sensitive information, together with roles assigned responsibility for each procedure, appropriate authorisation and records, are required.

The procedures should be adequate for the sensitivity level of the information handled, in line with the classification applied. It is also important that these procedures cover all sensitive information, regardless of the form it takes.

Auditing guidance

The auditor should confirm that, for each classification label, there are procedures in place supporting information assigned that classification, such as procedures for secure processing, storage and transmission.

The auditor should confirm that procedures are in place to protect sensitive information – regardless of which form it takes – in line with the classification scheme used by the organisation. Is it recorded? Who is responsible for this information? Who authorises its release? Who has received the information, and who is authorised to access it? Is clear labelling applied? Is distribution of sensitive information only taking place if there is a need to know?

Where information is being handled by persons unknown to staff – such as couriers – what additional identity checks are made? Are access restrictions in place, and if so, which ones? Check that agreements with external parties support the classification and handling procedures that internal staff are required to follow, and that they provide appropriate interpretations for the classifications. Checks on confidentiality or non-disclosure agreements also need to be made (see 2.9.2.4).

Observe how people in the organisation are handling sensitive, critical and personally identifiable information, and how easy or difficult it might be to circumvent or disregard the procedures.

2.4.3 Media handling (ISO/IEC 27001, A.8.3)

“Objective: To prevent unauthorized disclosure, modification, removal or destruction of information stored on media.”

2.4.3.1 Management of removable media (ISO/IEC 27001, A.8.3.1)

“Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.”

Implementation guidance

Removable media containing the organisation’s data presents risks of loss of availability and confidentiality. Controls are required for the management of media items, including backup tapes, disks, USB sticks, removable hard drives, CDs, DVDs and printed media. Procedures should be developed and implemented to ensure that authorised media are used, maintained and transported in a safe and controlled manner that is consistent with the classification of the information stored on the media. The supplier’s recommendations on storage conditions should also be followed, and the issues of media deterioration and obsolescence should be considered.

Authorisation should be required for the removal of any item from the premises for transport (see 2.4.2.3). The authorisation process and which roles may authorise what should be documented. Any risk assessment should recognise that the effectiveness of controls is limited by the ease with which small media items (e.g. USB sticks) can be brought into and removed from the premises.

Auditing guidance

The auditor should review the organisation's policies describing which media should be used. For media handling, check records to verify that these procedures are followed and interview random staff to establish that everybody is aware of them. The handling and storage should be appropriate to the classification of the information stored on the media, and the media should also be stored and disposed of in accordance with manufacturer recommendations. Media should also be replaced before it is obsolete, and included in an asset inventory (see 2.4.1.1).

Another aspect the auditor should check is how media is removed from the site. This might be for transfer to secure archive storage, by personnel for business use or for destruction. There should be a well-defined procedure and logging mechanism in place, as well as authorisation required, in each case as appropriate. The procedure should ensure that removable media, if no longer needed, are erased to ensure that no information is leaked. If media contain sensitive information, the auditor should check how they are labelled and handled, and confirm that there are procedures for them to be destroyed or erased before being reused or discarded.

The auditor should also confirm that the transport arrangements for various media afford sufficient protection. Whatever controls are in place, this is a difficult area to police. Check that organisations have properly identified this in their risk assessments, and what compensating controls have been applied.

2.4.3.2 Disposal of media (ISO/IEC 27001, A.8.3.2)

“Media shall be disposed of securely when no longer required, using formal procedures.”

Implementation guidance

An item no longer required is often regarded as worthless. But if it contains information, it may well be of interest and value to others. Serious breaches of confidentiality occur when apparently worthless drives, disks, tapes, paper files and printers are dumped without proper regard to their destruction. The return of damaged devices or media to the manufacturer for repair or disposal may also create a risk – the organisation may not be able to retrieve data, but this does not mean that others cannot.

The procedures for the handling of media containing classified information should specify appropriate means for its destruction and disposal (see also 2.4.2.3), and there should be formal procedures in place governing the disposal of any media no longer required. Control 8.3.2 of ISO/IEC 27002 describes what such procedures could address, and these controls should be applied as required by the importance and sensitivity of the information on the media. A record of sensitive items should be maintained at the point of destruction.

Auditing guidance

The problems related to removal of media from the site are covered above (see 2.4.3.1), but the auditor still needs to look at the disposal procedures, for example those items listed in ISO/IEC 27002, 8.3.2.

The auditor should confirm that formal procedures are in place. What general disposal arrangements are there? How do external contractors handle them? Check that the organisation has carried out proper security and process checks, and that the most sensitive level of information handled in this way is known and verified. It should be checked that – whatever the specific arrangements are – sensitive information cannot be compromised through the disposal process, because it has already been erased or destroyed. There should be a logging process for the disposed-of media, and what has been done to them prior to disposal. Check that this provides a satisfactory audit trail.

There should also be a process to govern the handling of damaged media containing classified data, which includes a risk assessment and determines whether the media will be destroyed rather than sent for repair.

2.4.3.3 Physical media transfer (ISO/IEC 27001, A.8.3.3)

"Media containing information shall be protected against unauthorised access, misuse or corruption during transportation."

Implementation guidance

Media transport carries a risk of loss, unauthorised access and misuse. This has consequent impacts to confidentiality, integrity and availability of the information or software contained on the media. A risk assessment should be used to help select the right transport method and the controls applied to it (e.g. by post with recorded delivery, secure parcel delivery, personal delivery by trustworthy couriers). Appropriate courier services and packaging should be selected, including locked containers or tamper-evident packaging for sensitive or valuable items. It may even be appropriate to divide some consignments into two deliveries. To significantly mitigate the risk of breach of confidentiality if media is lost or stolen, consider data encryption. If encrypting, never ship the encryption key and/or password with the encrypted data.

All despatches should be recorded and, where appropriate, authorised.

Auditing guidance

The auditor should confirm that whenever information is physically transported, the organisation has considered what protection is in place to protect the media holding the information. What are the transport arrangements? If couriers, do they have secure and tamper-proof containers? Have they been identified as trustworthy couriers? Data might be transmitted by staff on disks or tapes or perhaps on mobile devices – are these devices secure enough for the information carried? Who determines the method of transportation? What criteria do they use? Where couriers are employed, the methods of transportation might be the carrier's default methods: are these sufficient? Consider also postal services: are these secure?

The auditor should check for evidence of a risk assessment of sensitive or critical information, which should identify whether either encryption or other additional protections, such as digital signatures for critical information, are to be applied.

In all cases where there is a requirement for secure transport of information, there should be formal procedures defining the arrangements, and the authority for release should be specified and recorded. Records should be kept of all deliveries, including details of what was delivered, when the courier picked it up and when the delivery arrived at its destination.

2.5 Access control (ISO/IEC 27001, A.9)

2.5.1 Business requirements of access control (ISO/IEC 27001, A.9.1)

“Objective: To limit access to information and information processing facilities.”

2.5.1.1 Access control policy (ISO/IEC 27001, A.9.1.1)

“An access control policy shall be established, documented and reviewed based on business and information security requirements.”

Implementation guidance

Access control is a fundamental prerequisite to securing information or services on information processing systems, and is also necessary to protect physical premises containing information in all forms. The confidentiality, integrity and availability of the organisation’s business information, services and processes, together with other business assets, are at stake.

Allocation of user access permissions should be driven by business requirements, approved and regularly reviewed by asset owners, and clearly stated in the access control policy. Any access not necessary for the activities assigned to a role should be denied. This approach is known as ‘least privilege’.

The organisation should develop, document and implement an access control policy that defines user access rights based on business needs, taking into account the classification and handling requirements of the information, services, networks and/or applications accessed, and any legal or regulatory requirements. Standard user access profiles for specific roles are a useful way of managing access where many users are involved (this is known as 'role-based access'). It is important to review the access control policy regularly and remove any access rights that are no longer necessary. Note that business information repositories such as calendaring systems should also be taken into account.

Auditing guidance

Auditors should confirm that access control rights and rules are clearly defined in the access control policy, and that they are consistent with the classification and handling requirements for the information. Suitable mechanisms for enforcement of this policy should be in place and implemented. An access right to an asset should be traceable to a risk assessment and authorised by the correct asset owner. Any access to sensitive information, or to information processing facilities, should be based on the 'need to know' and 'need to use' principles, i.e. justified by business requirements and necessary for the task at hand. Role-based access should be implemented where possible.

Auditors should be prepared to question why certain roles, especially senior ones, have access to certain information if this access is not sufficiently justified. Check also that access to sensitive information takes place in line with the classification given, and that the access permissions given have been checked to ensure that they are consistent with applicable legislation and regulations. Also check that personnel with access to sensitive or confidential information have been properly trained, since unrestricted use of such information by untrained staff can have disastrous consequences.

The auditor should also check that the organisation has procedures in place to review the access control policy, taking account of employees leaving the organisation, job functions and requirements changing, etc. These procedures should include that any access rights that are found to be no longer necessary are removed immediately. Records should exist to show that this is the case.

2.5.1.2 Access to networks and network services (ISO/IEC 27001, A.9.1.2)

“Users shall only be provided with access to the network and network services that they have been specifically authorized to use.”

Implementation guidance

Business networks can provide a lot of individual services to thousands of users undertaking a wide variety of activities. Each user might only require a few of these services (e.g. email, purchasing applications and the intranet). Users should only have access to networks and network services that they are actually authorised to use, in line with the access control policy (see also 2.5.1.1).

Additional control can be provided by restricting the visibility of services. Where every user can see the full range of services, the organisation can be vulnerable to unauthorised access attempts, with the attendant risks of breach of confidentiality and loss of data integrity. Where restricting the use and views of services is not possible, alternative controls should be considered, such as preventing authentication from outside the organisational area that needs to use a particular service. Particularly sensitive services may have to be implemented on a separate network domain or a separate system to be fully segregated. It is, however, wise to be aware that making a service invisible does not prevent people from talking to each other about it; security through obscurity is not effective in the long term.

Several network access controls, such as port-based security, can be used to limit access to network services, and these controls should be implemented to support the organisation's policy on the use of network services. Good change control and management is essential to keep the accesses correct, and regular monitoring is required to provide assurance.

Auditing guidance

Users logging on to a network, computer or application should be provided with access only to the information and services required for their business function and that they have been authorised to use. What access is provided to which users needs to be explicitly defined and authorised. For some network services, total availability of the service and all information might not be a problem, for others it could be critical. The auditor should verify that the necessary access restrictions have been defined and documented in a policy on the use of network services which is in line with the access control policy (see also 2.5.1.1). The auditor should also check that network security controls have been implemented to support the policy on the use of network services, including access controls.

2.5.2 User access management (ISO/IEC 27001, A.9.2)

“Objective: To ensure authorized user access and to prevent unauthorized access to systems and services.”

2.5.2.1 User registration and de-registration (ISO/IEC 27001, A.9.2.1)

“A formal user registration and de-registration process shall be implemented to enable assignment of access rights.”

Implementation guidance

Every user should be formally and uniquely registered by the organisation, and a record maintained of each information system, network or service which he/she has a business requirement to access. Failure to control registration can result in breach of confidentiality, unauthorised modification and/or loss.

The sharing of user IDs almost guarantees loss of accountability, as actions cannot be unambiguously traced to individuals. This can then lead to loss of confidentiality, integrity and availability. Users should therefore each have a unique identifier for every system they have authorisation to access.

In those few cases where it is not possible to have individual IDs (e.g. because the system does not have the required functionality), the organisation should implement a manual process to track who is using the ID at any given time, ensure that it cannot be used by more than one person at any time and change authentication credentials whenever the ID is passed to a new custodian.

Auditing guidance

The auditor should collect and check relevant evidence to be assured that the user registration and de-registration process functions effectively. This may include records of starters, movers and leavers, process documentation and lists of authorisations for systems. The auditor should also check that actual system privileges match documented authorisations, and that user IDs on the systems match registered users.

The term ‘user’ should be taken to include all users of information processing facilities, including system administrators, managers, application users, technical support personnel and programmers.

The process for creating and removing user IDs should be documented and logged, and the process for employees leaving the organisation should include prompt removal of user IDs. There should also be a process for auditing live IDs on a regular basis, to catch any that may have been inadvertently left live when they are no longer required. Redundant user IDs should not be reissued to other users because of the risk of inadvertently giving excessive and unauthorised access to resources.

The auditor should check whether user IDs are unique or shared. If shared, why is this necessary? Look at risk assessments, and the management and authorisation for this. Are additional controls applied to provide accountability, and are these additional controls sufficient?

2.5.2.2 User access provisioning (ISO/IEC 27001, A.9.2.2)

“A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services.”

Implementation guidance

The unjustified allocation of access rights increases the organisation’s vulnerability to breaches of confidentiality, loss of data integrity and availability through misuse.

A user registration form should be prepared, upon which the information system, network, service or application(s) required is described, as well as the conditions of access. This should be signed by the applicant to document their acceptance of the conditions, and by the system owner or custodian to document their authorisation for the applicant to be registered. This form should have the user ID added to it and then be archived.

It is equally important that user access to resources is promptly disabled when someone ceases to have a business reason to access the resources, for example termination of employment or internal job move. Procedures should be put in place to ensure this. There should be notification procedures, and clearly defined responsibilities and actions if employees leave the organisation or change their employment.

Role-based access should be considered, as this can be easier to manage, and reduces the chances of 'special cases'; or, if they do appear, it makes them more visible and therefore harder to authorise without adequate justification.

Auditing guidance

The auditor needs to collect and check records of registrations and authorisations to be assured that user access levels are based on formal registration and authorisation of the users, and that the access taking place is recorded. The auditor should check that these records are consistent with actual implementation. Have staff who have moved away or changed to other responsibilities had their authorisations immediately removed from the appropriate systems? Interview staff who have changed role – have they retained previous privileges that they no longer need? Those interviewed should include staff members who have been with the organisation longest, and those who have been promoted within the same function.

Another aspect that the auditor should check is whether users who change role are promptly granted any necessary additional access. If this is not done, users will tend to start sharing IDs to enable them to get their jobs done. Where the addition of required privileges is frequently delayed, this temporary credential sharing may be a widely accepted workaround which has not been risk assessed.

Auditors should spend some time with the system administrators looking at operating system settings for access control of specific groups and individuals, ensuring that access can only take place for registered and authorised users. ISO/IEC 27002, 9.2.1 gives further information on managing user IDs. It is also worthwhile checking that users are aware of their access rights and restrictions, and understand that they should not try to circumvent access controls.

2.5.2.3 Management of privileged access rights (ISO/IEC 27001, A.9.2.3)

"The allocation and use of privileged access rights shall be restricted and controlled."

Implementation guidance

Privileges are any features or facilities of information processing systems that enable the user to carry out system management activities or override access controls, such as maintaining the security system or the data management system. If privileges are uncontrolled, an increasing number of users will be using privileges, rendering pointless the carefully implemented access controls. The unnecessary allocation and use of privileges is often found to be a major contributing factor to the vulnerability of systems that have been breached. Loss of confidentiality through exposure, loss of integrity through modification of data and unavailability of data are typical consequences.

Privileged access to systems might be a politically challenging aspect to control. Systems engineers might try to persuade systems owners to authorise a privilege that is not really required. Privilege tends to be seen as a means to shortcut controls, and as a prize to be won and then held on to; a bit like getting to a higher level in a computer game. The fact is that most systems require very little use of privilege to manage them in a perfectly efficient manner.

Risk assessment should address not only the risk of providing privileges but also the consequences of not having them. Authorisation should be provided to staff, including those at a senior level, on the basis of sufficient business justification, which, in some cases, might need an independent expert opinion.

An important situation in which special privilege can be required is in the event of system failure. Fast recovery may require the skilled attention of a system engineer who might need to access the internals of a system and make changes that not only require elevated privilege, but also bypass controls that have been put in place to protect the system. Such occasions require their own controls, which will often be implemented after the event. It is essential that all the actions that are taken are properly logged, assessed and reviewed, and that further checks of the system are made to ensure that its security controls have been re-established.

If strong authentication techniques are required (including two-factor), the different techniques available (e.g. cryptographic means, smart cards, tokens or biometric means) should be considered, and a risk assessment used to determine the best solution to meet the requirements of the organisation.

What happens when the privileged person is not available? An emergency arrangement is required, such as a procedure to enable another systems engineer to obtain privilege out of hours. A user ID and password can be held in a safe under strict procedures for issue. This procedure should ensure that management will find out at the earliest appropriate opportunity that the emergency arrangement has been used, and should be followed up by review, as described above.

Auditing guidance

By definition, privileged access provides access to system features that are normally unavailable. The auditor should pay particular attention to system administrators, systems engineers and supplier's engineers, and others who have 'super user' access to facilities. The auditor should check that the level of access provided is appropriate to the business purpose. Full administrative access should not be used as the default approach to providing elevated privilege unless the system cannot provide any intermediate levels between standard user and full access. The auditor should also verify that more than one person has monitoring access and the ability to supervise activities.

For critical functions, such as system administration, there should be a special ID assigned to each user solely for this purpose, in addition to their standard user account on the system. Logging of usage of the account should also be in place. Interview users who have been granted elevated privileges and establish when they have used their accounts. Look at logs to ascertain that usage is being recorded. How long are these logs kept? Can they be modified? When and under what circumstances are they reviewed? If the application does not provide this traceability, look at the risk assessment relating to this, and ask what additional controls are in place to mitigate this issue.

Also check what is happening in cases of service incidents, such as system failures. Are privileges allocated without due care and attention? Are controls violated? Check the records and logs that are created during such incidents. Check that all privilege activities are monitored and logged, and that someone is responsible for reviewing these logs. Check for each incident reviewed that there is evidence that post-incident restoration of security has occurred, and that a review of actions taken to resolve the incident has taken place.

Access to secure information may also include access to codes for safes and other secure areas. These also need to be recorded and regularly changed. It should also be verified that privileges are allocated on a 'need to use' and 'event by event' basis, are immediately removed when they are no longer necessary and use a different user identity than the one used for normal job functions.

Consider whether the authentication procedures used by the organisation provide sufficient security for the information, systems and applications they are supposed to protect. The use of passwords alone is not generally appropriate for high-risk situations. Two-factor authentication (two of 'something you know, something you have and something you are') should be in place in these cases. Be particularly aware that repeated single-factor authentication (e.g. a password followed by another password or PIN) does not provide additional security. A risk assessment should have been used to identify the appropriate user identification and authentication mechanisms and procedures.

2.5.2.4 Management of secret authentication information of users (ISO/IEC 27001, A.9.2.4)

"The allocation of secret authentication information shall be controlled through a formal management process."

Implementation guidance

User identification and authentication goes hand in hand with access control, user registration and allocation of privileges. This is very often done through passwords, which remain a common, but not the only, mechanism for user authentication.

Whatever process is used for the allocation of secret authentication information, it should be based on the positive identification of the user, and apply a formal process enforcing users to change initial temporary passwords. The user should acknowledge receipt of their credentials.

A procedure is required to ensure that user IDs and passwords are issued only to those with a business need for access, and are authorised properly by the owner of the resource being accessed. Where other methods of user authentication are being used, similar controls will be required but potentially with additional controls suitable for the method employed.

Auditing guidance

The auditor should check how secret authentication information is allocated and controlled; sometimes this is under the personal control of the user, but at other times the system administrator might issue it. If centrally controlled, where is the information held? Is this secure? Who has access? If it is under user control, are they aware of their responsibilities (see also 2.2.1.1)? Are procedures in place to ensure that temporary or default vendor passwords are changed immediately?

Auditors need to review records to verify that users have signed a statement to keep their secret authentication information confidential, and interview a randomly selected group of users to check that they are aware of and understand this responsibility. This awareness should be tested at different levels of the organisation. There should also be a record of how each user's identity was verified at the time of provision of the information, as well as a list of acceptable forms of ID. Look for records showing that initial secret authentication information has been changed by the user on first use. Ask users what happens when they forget their passwords. How are new passwords provided? Is there an additional route for resetting passwords if the matter is deemed urgent? Are there follow-up processes to review the use of an urgent password reset (see 2.5.2.3 re service incidents)?

2.5.2.5 Review of user access rights (ISO/IEC27001, A.9.2.5)

"Asset owners shall review users' access rights at regular intervals."

Implementation guidance

Access rights should always be based on business needs – when the need is no longer present, then the access should be cancelled. However, with the best will in the world, it is possible that a mistake may be made, and access inappropriately retained when a user leaves or changes role. The continued need for access should therefore be reviewed periodically, and access rights should be withdrawn at that point if it is found that they are no longer needed. This is particularly important where users have access to sensitive information or have elevated privileges.

Auditing guidance

The auditor should check that procedures for regular review of all kinds of user access rights and privileges are in place and are being followed. These procedures might be a formal audit to check compliance, followed by a management level review to check for consistency with business and policy requirements. Changes should be reviewed on a periodic basis.

Access control procedures should include periodic reviews of allocated access rights. The auditor should check that reviews are logged, that actual access has been compared to authorised access and that the authoriser for the system has verified that authorised access is appropriate.

2.5.2.6 Removal or adjustment of access rights (ISO/IEC 27001, A.9.2.6)

"The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change."

Implementation guidance

If a user’s employment terminates (i.e. for an employee, contractor or third-party user), all access rights associated with their employment should be reviewed for removal. This includes physical access rights (i.e. returning of access control cards, keys, identification cards, etc., see also 2.4.3.2), as well as rights to log in to the organisation’s network, user accounts, passwords, email addresses and any other form of permitted access. Unless there are clearly identified reasons why particular access arrangements need to remain, all of these access rights should be removed immediately. It will also be necessary to review and update the documentation listing the individuals that have access rights, are assigned to a role, any subscriptions that are tied to them and memberships in interest groups.

All forms of access should be reconsidered when employment changes, and any access that is not necessary for the new job role should be removed. This might seem to be excessive, as the relationship with the organisation is maintained, but it is appropriate. The main purpose of access controls should be to allow only the access necessary for the job function (following the principle of ‘least privilege’). Any other access that is not explicitly allowed should be forbidden.

Special procedures might be required if termination of employment is initiated by management and/or relates to disaffected employees, contractors or third-party users, to avoid information collection and disclosure, modification or destruction of information or services in the period between the individual becoming aware that their employment is terminating, and the point at which they lose access to information and information systems.

Auditing guidance

The auditor should check that the organisation has procedures in place that define all actions to be taken to remove access rights in case of employment termination. These procedures should be applied in case of any termination, irrespective of whether this relates to an employee, contractor, third-party user or anyone else having had access to the organisation's premises or assets. The access rights considered for removal should include all physical and logical access, access to services and involvement in user or interest groups. They should cover the notification of staff and other relevant parties of the departure of the user, with instructions to cease to share information with the user which the user should no longer have access to.

It is important that these procedures are also applied in case of employment changes, and the auditor should look for evidence that access rights are always removed if there is no defined business purpose for having them. The auditor should also check that employment termination or change initiates a review of all related user access rights (see also 2.5.2.5), and that all shared passwords the person had access to are changed.

2.5.3 User responsibilities (ISO/IEC 27001, A.9.3)

“Objective: To make users accountable for safeguarding their authentication information.”

2.5.3.1 Use of secret authentication information (ISO/IEC 27001, A.9.3.1)

“Users shall be required to follow the organization’s practices in the use of secret authentication information.”

Implementation guidance

Secret authentication information includes things such as passwords, biometric data and PINs, but not user IDs or email addresses (as these are not secret). It also includes the answers to questions that are commonly used to allow a person to do a self-service reset of their password. Exposed (written down) secret authentication information, or obvious and easily guessed passwords, can lead to misuse of systems by unauthorised persons, with the attendant risks of loss of confidentiality, integrity and availability. ISO/IEC 27002, 9.3.1 contains guidelines for users for choosing their passwords, and for managing all forms of secret authentication data.

Users should also be made aware if they may be held accountable for actions carried out by someone else having used their sensitive authentication information.

Auditing guidance

The auditor should check that the policy on sensitive authentication information, including matters such as password lifespan, length and content, is sufficient for the security requirements of the organisation and the information protected. Some systems enforce rules of this type, others do not. Check what other measures are in place if the system does not automatically enforce such rules. If necessary, ask staff to show you how they change their sensitive authentication information (as relevant). Do they know the criteria? Are the sensitive authentication information rules currently in place consistent with policy?

The auditor should also note any instances of sensitive authentication information being written down on memos, stuck to monitors, etc. It is also instructive to ask for the results of password cracking tools that the organisation might have used to check the quality of user passwords. ISO/IEC 27002, 9.3.1 gives examples of good practice. Check also the relation to other sensitive authentication information management controls, such as 9.2.3 and 9.4.3, and ensure that all these controls together build a good sensitive authentication information management system. Auditors should ensure that proper management authority is obtained when investigating the use of sensitive authentication information.

2.5.4 System and application access control (ISO/IEC 27001, A.9.4)

"Objective: To prevent unauthorized access to systems and applications."

2.5.4.1 Information access restriction (ISO/IEC 27001, A.9.4.1)

“Access to information and application system functions shall be restricted in accordance with the access control policy.”

Implementation guidance

The owner of the information held in each application should specify the access rights and rules for that application, in accordance with business requirements and the access control policy (see 2.5.1.1). These rights and rules should define who will have access and, in the case of information, at what level, e.g. create, read, modify, delete. Without this there is a high probability that users will be given access to too much information. This creates the risk of a breach of confidentiality and loss of integrity or availability. Over-accessibility can also lead to the risk of fraud in financial applications, and theft of intellectual property.

Be particularly cautious where a shared database is used. Ensure that each role can only access the data meeting the role’s requirements, and that applications cannot be used to circumvent the access controls in place.

Auditing guidance

Auditors should collect and check relevant evidence to be assured that access to information provided by individual applications is actively managed, matches business requirements and is in line with the access control policy (see also 2.5.1.1). For example, different applications might access the same database. Can sensitive information be accessed from one program but not from another? Does this allow the same role different levels of access inappropriately? The access rules in place should also match the handling requirements of the classification scheme (see 2.4.2.3).

Users should not generally be presented with lists of information or application functions that they are not allowed to access. Menu options that are not accessible for security reasons should be removed, likewise information in user manuals relating to sensitive functionality. Pay particular attention to little used parts of applications, such as maintenance utilities. Are these properly controlled?

Auditors also need to check what happens to information that is authorised and accessible. Are there restrictions to what can be extracted as files or in print? How are these extracts then controlled? They should be subject to the same rules regardless of format.

2.5.4.2 Secure log-on procedures (ISO/IEC 27001, A.9.4.2)

“Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure.”

Implementation guidance

While a log-on process should be easy for authorised users to follow, it should not disclose unnecessary information about the operating system, service or application the user is trying to access (e.g. the version number, whether a specific user account exists in the system and error messages revealing database structure). Any information provided might assist an unauthorised person trying to obtain access, so the less information given away, the better.

Some systems do not have the facility to control or modify the level of information they present, and the organisation has to accept the system as provided. In such cases, other mitigating controls should be used. The organisation should implement what features are available, and add further compensating controls where necessary.

ISO/IEC 27002, 9.4.2 provides more examples of what a secure log-on procedure should provide. As many aspects of that list as possible should be implemented in the organisation's systems and applications.

Auditing guidance

Log-on procedures can be more involved than simply typing the correct name and password. The auditor should obtain evidence relating to the design and implementation of the log-on procedures. Does the user need to carry out a sequence of log-on activities? What happens if the wrong information is entered? Is there a delay period, and is a lockout imposed after repeated false attempts? If so, what is the recovery mechanism? Is the password displayed or hidden? Is it obvious how many characters the password should have? Do error messages reveal how the system operates behind the scenes?

ISO/IEC 27002, 9.4.2 provides a helpful list of properties for a secure log-on procedure. Sometimes an application might not provide the necessary level of log-on protection, e.g. if the number of unsuccessful log-ons is not restricted. In this situation, determine if any other controls have been added, e.g. by physically restricting access to the operating system, enforcing a delay between log-on attempts or steps in a log-on sequence or raising an alert. Verify that the risk assessment has considered each operating system and application in scope, their access methods and log-on procedures, and whether these are considered adequate.

2.5.4.3 Password management system (ISO/IEC 27001, A.9.4.3)

"Password management systems shall be interactive and should ensure quality passwords."

Implementation guidance

Weak password management leads to the risk of misuse of systems by unauthorised persons, with the consequent risks of breaches of confidentiality, integrity and availability of information. Where systems can be used to enforce password quality, lifespan and frequency of change, these should be used. If this is not the case, compensating controls and monitoring may be required. Use risk assessment to determine whether this is necessary.

ISO/IEC 27002 lists guidelines for good password management systems in control 9.4.3, and further guidance about password management and related user responsibilities in controls 9.2.4 and 9.3.1.

Auditing guidance

The auditor should check that there is a policy covering the use of passwords throughout the organisation, including ensuring that a suitably secure password management system is used. Any requirements for particularly sensitive areas should be additional to, and consistent with, this policy. Aspects that auditors should check for include:

- length and content of passwords;
- frequency of changing passwords (both maximum and minimum limits);
- use of individual user IDs;

- use of common passwords between individuals and/or by the same individual across different applications;
- secure handling and storage of passwords; and
- changing of default passwords.

Additional desirable attributes of a password management system are given in ISO/IEC 27002, 9.4.3.

Look also at the process for changing passwords. What logs are kept? Are previously used passwords disallowed, and if so, how many previous passwords are retained for comparison? Does the application require successful authentication before accepting a password change request? If necessary, get users to demonstrate how passwords are changed.

2.5.4.4 Use of privileged utility programs (ISO/IEC 27001, A.9.4.4)

"The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled."

Implementation guidance

System utilities provide an opportunity for misuse, which can damage the integrity of the security controls of an operating system or application. As these utilities may be necessary to resolve control problems, their use should be tightly controlled and only take place after sufficient authorisation and justification.

It is essential that all system utilities are identified, that the associated risks are assessed and that controls such as those described in ISO/IEC 27002, control 9.4.4 are applied.

Auditing guidance

System utilities may allow access to parts of the system that applications do not, and may also allow overriding of system controls. Auditors should collect and check relevant evidence to establish that the organisation has overall control of the utilities installed. Check that they are catalogued and authorised, and that appropriate access control and user restrictions are applied. Check on individual systems that no additional or modified utilities are in existence.

In less well-regulated environments, unauthorised utilities may have been installed that could have consequences not only for the confidentiality of information but also its integrity and availability. The auditor should check that no forgotten utilities are still resident on systems. Finally, the auditor should check that no one without appropriate authorisation can access or use system utilities. Further controls to secure the use of system utilities are listed in ISO/IEC 27002, control 9.4.4.

2.5.4.5 Access control to program source code (ISO/IEC 27001, A.9.4.5)

“Access to program source code shall be restricted.”

Implementation guidance

Program source code may contain details of the system, other applications and implemented controls. It provides an attacker with a perfect starting point for understanding and performing the unauthorised modification of a system. Serious security problems can result from unauthorised access to, and modification of, source code.

Clear and effective procedures are required to ensure proper maintenance and protection of source code. One method is to use central storage of code, e.g. in a library. Such libraries should not be held in, and should not be accessible from, production systems, and there should be controls and procedures in place to manage access to libraries and source code. Other controls include logging of copies sent, after authorisation, to maintenance staff, logging of updates, strict change control procedures and digital signatures to enable all modifications to be identified.

Auditing guidance

The auditor needs to check that access to any program source code is protected, ideally by not holding it on production systems and by strictly controlling access to it. Access to such code and the means to modify and re-compile it, can effectively bypass all of the security features within the application. Highly secure applications should include some means of verifying code check sums (or digital signatures). These should be used to identify if unauthorised changes have been made.

The auditor should also check any macros and database report programs. These can be much easier to change and could cause loss of integrity, or make information unavailable. Normal updates of application source code should also be properly controlled to prevent installation of the wrong code, and to ensure recording and testing of changes before access to live data is permitted. The auditor should look for documented procedures and records relating to these activities.

ISO/IEC 27002, 9.4.5 provides additional guidelines that can be applied to secure access to program source code and the libraries in which this code might be held. The auditor should also ask about other standards that are, or have been, used to secure code.

2.6 Cryptography (ISO/IEC 27001, A.10)

2.6.1 Cryptographic controls (ISO/IEC 27001, A.10.1)

“Objective: To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.”

2.6.1.1 Policy on the use of cryptographic controls (ISO/IEC 27001, A.10.1.1)

“A policy on the use of cryptographic controls for protection of information shall be developed and implemented.”

Implementation guidance

The effective use of cryptographic techniques is only possible if basic principles are identified, agreed and applied. For example, the algorithms used should be suitable for the business processes and services they are supporting, the key length should be appropriate for the security requirements of the information that will be protected, and the solutions implemented should be consistent throughout the part of the organisation where cryptographic controls are applied. The organisation should avoid designing its own cryptographic algorithms unless that is its only activity; it is easy to create a weak but apparently strong algorithm. Relevant legislation on what algorithms are permitted should also be taken into account (see 2.14.1.5).

In order to achieve this, a risk assessment should be used to determine the requirements for confidentiality, integrity, authenticity and non-repudiation, and the most suitable cryptographic solutions and a policy on the use of cryptographic controls should be communicated to all users of such controls prior to any application. This policy should take into account the relevant key management activities (see also 2.6.1.2) and legal issues involved in the use of cryptographic techniques.

Auditing guidance

An important aspect of the secure and effective use of cryptographic controls is to make sure that the requirements have been identified, and that the correct decisions have been made about what cryptographic controls to use. A policy should be in place supporting the day-to-day use of these controls. This policy should cover the key management approach applied (see ISO/IEC 27002, 10.1.2 and below for examples), the roles and responsibilities related to the use of cryptographic controls, and the information and circumstances for which cryptographic controls should be applied.

If the organisation applies cryptographic controls, auditors should check that a policy on the use of cryptographic controls has been developed, communicated and is known and followed by employees. The auditor should verify that the decisions shaping the policy are traceable to a risk assessment, and that the controls actually implemented are commensurate with the policy.

The strength of cryptographic controls does vary, and is related to the algorithms employed and the key sizes and parameters used. A factor to be taken into account is the environment and application in which cryptographic controls are applied. Some application environments might require the use of stronger cryptographic controls. Equally, as the implementation of stronger cryptographic controls may have an impact on performance, it is necessary to also consider this aspect when reviewing policy decisions.

The auditor will need to have at least a general knowledge of cryptographic techniques and mechanisms, key management and their implementation to assess whether what the organisation is using is adequate and appropriate. The use of specialist technical expertise may also be necessary to support the auditor in this area. A useful rule of thumb is that all algorithms must be industry-standard and not known to have been broken. Internally devised cryptographic algorithms are almost without exception fatally flawed.

2.6.1.2 Key management (ISO/IEC 27001, A.10.1.2)

"A policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented through their whole lifecycle."

Implementation guidance

The key management system used should provide protection of the cryptographic keys according to their use, and management methods that support the handling and use of keys as required by the business processes for which the cryptographic controls will be used.

The requirements for key management will be different depending on which cryptographic technique, secret or public key technique will be used, and what type of key, public or private, is considered. The protection of secret and private cryptographic keys is different from the protection necessary for public keys. When defining a key management system, these protection requirements should be analysed with the help of a risk assessment, and appropriate protection should be in place before the first production keys are generated and used.

A set of standards and procedures for the key management activities as described in ISO/IEC 27002, control 10.1.2 should be agreed and implemented before using cryptographic controls. The lifetime of cryptographic keys should be defined for each application in relation to the risks of possible damage if they are compromised, and the deactivation of keys should take place immediately when they reach this age.

The organisation should also consider its needs for keeping copies of keys or parts of keys used for cryptographic controls, either for its own use or to satisfy legal requirements. It might be necessary to agree public key management processes with certification authorities, and the organisation might also want to consider the use of other services such as key generation, distribution and revocation, directory services or time stamping, which may be offered by third-party organisations.

Finally, the organisation may choose to retain copies of the employees' keys to avoid any misuse, such as the unauthorised distribution of the organisation's information, or a disgruntled employee first encrypting information and then destroying their private key.

Auditing guidance

Key management is an essential prerequisite for the secure use of cryptographic controls, and no cryptography should be used without a secure key management system in place. The whole lifecycle should be considered (see ISO/IEC 27002, 10.1.2 for a list of stages in the life of a key).

Auditors should check that the organisation has implemented adequate controls to protect:

- secret and private keys against replacement, disclosure, modification and destruction; and
- public keys and public key certificates against replacement, unauthorised modification and destruction.

If the organisation is using a certification authority (public or internal) for the management of its public keys, it should be able to show how it has verified that the authority is trustworthy and suitably managed.

The protection of cryptographic keys should encompass both logical and physical protection. Auditors should review the physical and logical access controls that are being applied to protect cryptographic keys. Where keys are managed by, or in combination with, third parties, the organisation should have agreements in place that cover key protection.

In addition, auditors should check that other relevant key management procedures, for example as described in ISO/IEC 27002, 10.1.2 are in place. If a key escrow arrangement (or other provision for emergency recovery) is in place to protect cryptographic keys, it should be ensured that the appropriate employees are aware of it, and that there are no possibilities to circumvent key escrow or to inject an unauthorised key.

2.7 Physical and environmental security (ISO/IEC 27001, A.11)

2.7.1 Secure areas (ISO/IEC 27001, A.11.1)

“Objective: To prevent unauthorized physical access, damage and interference to the organization’s information and information processing facilities.”

2.7.1.1 Physical security perimeter (ISO/IEC 27001, A.11.1.1)

“Security perimeters shall be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.”

Implementation guidance

Premises that contain business processes, information, services, IT and other assets are vulnerable to unauthorised access and undesirable activities. Persons attempting such activities might work for the organisation, so internal protection is required as well as perimeter protection (think pomegranate instead of melon).

Small premises might comprise a single physical location with just one perimeter. Larger premises might need to use several perimeters, and hence be divided into multiple zones. It is important to specify and describe the perimeter of each zone properly.

The objective is to be able to control entry into (and possibly exit from) every zone, and additionally to record entry to, and exit from, sensitive areas. A security model can be prepared showing, perhaps schematically, the various zones and the connections between them. A risk assessment should be used to identify appropriate perimeters, and to select controls to give adequate protection. Procedures should be defined to control the management of physical security, access control and its monitoring. Give due consideration to out-of-hours working, lone working and any necessary authorisation, supervision and monitoring. The implementation guidance of ISO/IEC 27002, 11.1.1 contains a list of guidelines and controls for physical security perimeters.

Auditing guidance

All organisations must be able to demonstrate the physical protection of their assets to auditors. Security procedures should describe what measures are taken, how this is monitored and who has access. To assess the physical protection in place, auditors will need to look for opportunities for access. Unlocked fire escapes, open fire doors, unattended reception areas, shared security passes and unlocked cabinets are all security threats and should be noted. A foundational part(s) of the physical protection in place is/are the actual physical perimeter(s). The organisation should be able to explain what perimeters are in place, and what protection is achieved with them (this should be supported by a risk assessment). Auditors should also check how access into the building is controlled and monitored, and whether the controls in place are sufficient for the needs of the organisation, or whether there are possibilities to circumvent the protection. The implementation guidance of ISO/IEC 27002, 11.1.1 describes several different issues that should be considered and implemented for the security perimeters of an organisation.

2.7.1.2 Physical entry controls (ISO/IEC 27001, A.11.1.2)

“Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.”

Implementation guidance

A secure area, in this context, is any area that the organisation identifies as requiring access control to limit the roles that can enter. Such areas can include the entire premises, but certainly server rooms, network equipment rooms and plant rooms (power, air conditioning). A clerical area handling sensitive data (such as sales calls, customer service or banking) might also fall into this category. Different secure areas will possibly need different levels of security and access control. Secure areas, and the protection to be provided by the controls within such areas, should be determined by a risk assessment. Decisions on these matters should be treated as equivalent to protecting access to electronic systems via login. The physical access route should not be the ‘weakest link’.

Potential threats may include breaches of confidentiality, unauthorised tampering with equipment (causing loss of integrity) and equipment theft (resulting in loss of availability).

Appropriate entry controls might include a check of staff ID cards, the use of biometric verification (e.g. via fingerprint) and/or the entry of a password or PIN. All those accessing secure areas should be appropriately checked, and badges should be consistently used to identify authorised personnel. It should also be ensured that visitors are registered and escorted, and that any person not wearing an identification badge is reported to security personnel. If staff habitually do not wear passes, then a visitor may 'become' a member of staff simply by removing their visitor badge. Further specific controls are listed in the implementation guidance of ISO/IEC 27002, 11.1.2.

Auditing guidance

Auditors should check the entry controls in place, ensuring that these are actually in existence, and restrict physical access to authorised people only. Do employees wear badges and is this mandatory? What about visitors – are badges issued, is their entry and exit logged, what restrictions are placed on their movements? Are persons not wearing badges challenged? Auditors, invariably being visitors to the organisation, can determine this from their own treatment (e.g. by quietly removing their badge and awaiting developments).

Auditors should also check the audit trails of access that has taken place in the past, and ensure that procedures for the review and update of physical access rights are in place. Authorisation, in terms of access rights and restrictions, might be in a variety of forms. It could be described in job descriptions, it could be written into procedures or it could be listed at the point where the restrictions apply, such as on a label affixed to a door. Auditors should take a view on the appropriateness of each approach in the specific organisational context.

2.7.1.3 Securing offices, rooms and facilities (ISO/IEC 27001, A.11.1.3)

“Physical security for offices, rooms, and facilities shall be designed and applied.”

Implementation guidance

The organisation should identify the controls required to secure offices, rooms and facilities. These controls should be appropriate to the value, liability and importance of the information and related assets within the areas. A risk assessment should support the decisions made. In addition, care should be being taken to make sure that all applicable health and safety regulations and standards are complied with.

It may be appropriate to avoid giving clues about the location of potential targets, for example by using signs pointing to the server room or indicating the purpose of rooms or buildings. For the same reason, directories and internal phone books should not be accessible by anyone outside the organisation.

The risks of loss of confidentiality, integrity and availability all increase as more of the organisation’s key information is centralised. These concentrated repositories become critical to the organisation. Effective security is then especially vital, both outside and inside, to ensure that losses are not experienced.

Auditing guidance

The level of protection provided for a secure area should be consistent with the most sensitive and critical information held in that area, and consistent with the documented procedures for the handling of classified information. There is a clear link here to risk assessment. Auditors should confirm that the information security requirements have been identified, and that the protection in place is adequate for this. A list of security controls that might be applicable to protect secure areas is given in the implementation guidance of ISO/IEC 27002, 11.1.3. Auditors should also try to identify the use and purpose of rooms where information is processed, or try to get access to internal telephone directories/lists, to test these controls. Phone lists are commonly left next to phones on reception.

2.7.1.4 Protecting against external and environmental threats (ISO/IEC 27001, A.11.1.4)

"Physical protection against natural disasters, malicious attack or accidents shall be designed and applied."

Implementation guidance

Organisations are always vulnerable to problems outside their control. The selection and design of the site and the controls applied should take account of the possibility of damage from fire, flooding, explosion, civil unrest and other forms of natural or man-made disasters. Consideration should also be given to any threats presented by neighbouring accommodation. For example, are hazardous materials being handled? Do any neighbours carry out business that may attract hostile attention?

The selection of controls should be carried out in consultation with specialists in the relevant areas, documented as required in ISO/IEC 27001 Clause 6.1.3, and the necessary training recorded in staff training records. The fall-back arrangements and backups taken should conform to the business continuity plan (see also 2.13.1).

Auditing guidance

Auditors should check the provisions the organisation has in place to react to natural and man-made disasters, and the physical protections in place to limit the damage. Records should exist of specialist advice pertaining to the main hazards that are likely in the circumstances, and should identify measures that are to be taken in the event of a hazard being realised. Secondary effects should have been taken into account, for example the ability of a server room to retain adequate climate control in the event of a power failure.

Have any reasonably predictable sources of hazard been omitted? For example, if a neighbouring site poses a threat to the organisation, has this been considered? The auditor should also investigate whether these arrangements link in with, and conform to, the business continuity arrangements the organisation has implemented (see also 2.13.1.2). Another issue to consider is the emergency support and environmental protection in place. Has the organisation assessed whether there is a fire hazard, or whether the site could be flooded – and what is there to prevent or mitigate these dangers?

Auditors should check if measures have been implemented as described. It might be helpful to walk through the site to identify weaknesses, such as large quantities of paper stored in an aisle without specific protection, not easily accessible fire extinguishers, a computer room in the basement, etc. Some measures may be eroded by time (e.g. fire extinguishers being used to prop fire doors open on hot days).

2.7.1.5 Working in secure areas (ISO/IEC 27001, A.11.1.5)

"Procedures for working in secure areas shall be designed and applied."

Implementation guidance

In addition to setting up physical perimeters, applying entry controls and securing offices, rooms and facilities for day-to-day operations, the specific security requirements of areas involving sensitive work need to be considered. For example, an organisation could be working on a new product, the design of which has high commercial value and is ahead of its competitors. Another example might involve a project or process that is sensitive and needs to be protected from damage, loss, modification or disclosure.

The work in secure areas should be protected and supervised as described in the implementation guidance of ISO/IEC 27002, 11.1.5. Which controls exactly are applied, and the degree of protection they will afford when used in concert, should be determined by a risk assessment, based on the work going on in the secure areas, and the protection requirements of the assets in these areas.

Auditing guidance

Personnel working in secure areas should be subject to specific controls that ensure sufficient security is implemented for the sensitivity and criticality of the information that is processed in such areas. Auditors should check:

- that entry controls are in place to ensure that only authorised personnel have access to secure areas;
- to what extent the work going on in such areas is generally known, and whether this exceeds any rules on ‘need to know’;
- how easy or difficult it is to take information (e.g. in the form of paper or electronic media) in or out of such areas;
- whether it is possible to take mobile phones, or other photographic, video, audio or recording equipment inside such areas, and to use it, or leave such equipment there to record;
- whether the work in such areas is sufficiently supervised; and
- whether mechanisms are in place to ensure that dual controls (where the presence and simultaneous activity of two individuals are required to authorise an action) are applied where appropriate.

The auditor should also check that the procedures for working in secure areas are applied consistently to everyone in those areas, including employees, contractors and third parties.

2.7.1.6 Delivery and loading areas (ISO/IEC 27001, A.11.1.6)

"Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access."

Implementation guidance

Breaches of confidentiality, integrity and availability can occur through uncontrolled public access to the organisation's premises, or uncontrolled delivery and despatch. There are threats from unauthorised access, malicious delivery (e.g. letter bomb), and unauthorised despatch, which frequently involve theft.

A busy organisation will experience many deliveries and collections. No one will be surprised to see packages being delivered or collected by strangers (delivery staff). It is therefore essential to control this activity to ensure that deliveries are expected, that collections are of only properly authorised despatches and that delivery staff are properly controlled with respect to access. In addition, the delivery and loading areas might be easily accessible by the public, and as there are people coming and going, someone might use the chance to sneak into the organisation's premises.

In order to control these problems, physical zoning with access controls is recommended to isolate delivery and loading from the most secure areas, and restrict access from outside to identified and authorised personnel. Internal procedures should be used to ensure that the transfer of goods between the loading bay and secure area is controlled, and that the incoming goods are inspected for potential threats. Complete records of all deliveries and despatches should be kept, and the ingoing and outgoing material should be reflected in updates of the asset inventory (see also 2.4.1.1). The names of all delivery drivers and vehicle numbers should be recorded.

Auditing guidance

This control is to help prevent security incidents by public access, delivery and loading operations. Deliveries may involve outside personnel on the premises and their movements need to be restricted, as well as the public access that might take place via the delivery and loading area. Products received could cause a hazard if not properly inspected, tested or stored as appropriate. Items leaving the premises could inadvertently contain sensitive information.

The auditor should check that the risks relevant to loading and delivery areas have been identified by the risk assessment and security procedures, and that adequate measures have been taken to both prevent and mitigate potential security breaches. For example, who receives goods: the person requiring the goods, a stores employee, or a general receptionist? What happens to the goods after receipt: are they sent directly into the secure area? Are they held in a store? Are they left on someone's desk? How are goods added to the asset inventory (see also 2.4.1.1) upon receipt, and is the asset inventory also updated when goods leave the organisation? How is access to the delivery and loading area controlled? Is it possible for the public to gain access, and what controls are in place between the delivery and loading area, and other parts of the organisation? Do staff know what to look for (e.g. evidence of tampering) and how to react? Ask them.

2.7.2 Equipment (ISO/IEC 27001, A.11.2)

"Objective: To prevent loss, damage, theft or compromise of assets and interruption to the organisation's operations."

2.7.2.1 Equipment siting and protection (ISO/IEC 27001, A.11.2.1)

"Equipment shall be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access."

Implementation guidance

Equipment can be vulnerable to damage and interference, with a resultant loss of integrity and availability. Inappropriate accessibility can lead to unauthorised use and/or breach of confidentiality of the information available.

Physical damage can arise from poor environmental conditions, particularly in industrial situations where moisture, vibration, heat, dust and chemicals can all take their toll. Electrical and electromagnetic interference can also be significant in some environments, and should be tested to identify possible problems resulting from interference. It is relatively easy to protect equipment such as communications devices and connection panels from inappropriate access – simply lock them in an appropriate small room or equipment cupboard with appropriate cooling services. Equipment required by operating staff should be available in their workspace and special protection, such as keyboard covers, can help to protect it. Ensure that the risk assessment covers this kind of situation and identifies solutions for equipment requiring special protection.

Other problems relate to the people working with the equipment; for example, equipment can be damaged if eating, drinking or smoking takes place too close to the equipment. There should be a policy in place to prevent this. In addition, there are risks associated with equipment displaying confidential information. There are different ways to handle this, including a clear desk and clear screen policy (see also 2.7.2.9), rules for unattended equipment (see also 2.7.2.8) and restriction of viewing angle to avoid information being viewed by unauthorised people, for example when walking past.

Where networked equipment is considered, remember that remotely accessible equipment probably requires more security attention than in-house equipment. Clearly establish the extent of the organisation's responsibilities for the network, and apply appropriate protection at the boundaries. Ensure that remote equipment is accounted for in inventories, security scope and risk assessments.

A list of guidelines is provided in ISO/IEC 27001, A.11.2.1.

Auditing guidance

During the audit, the organisation needs to demonstrate how its equipment is protected from environmental threats and hazards, and opportunities for unauthorised access. Equipment should be sited away from potential risk areas, such as windows that could be easily broken during a burglary without setting off an alarm. Consider also that terminal screens might be viewed from outside the protected area, and information can be leaked through electromagnetic or other emanation (e.g. the sound of keystrokes).

In some environments it may be appropriate to secure computer equipment to desks. As well as malicious damage, equipment needs to be protected from accidental damage from a very untidy or poorly managed environment, unrestricted access, unstable racks, spilt coffee, etc., and from environmental hazards such as water, chemicals and fire, and electromagnetic interference. Check that such measures have been considered, a risk assessment has taken place and that adequate protection is implemented.

Looking beyond the immediate computer area, does a fire or water hazard exist in adjacent areas? A large organisation will probably have a site layout plan. Look for this, and find out how it was developed.

2.7.2.2 Supporting utilities (ISO/IEC 27001, A.11.2.2)

"Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities."

Implementation guidance

Supporting utilities, such as electricity, water, heating/ventilation and air conditioning are an essential prerequisite to ensure business continuity and for the use of any computing and communications equipment. While many organisations tend to take a reliable public supply of electricity or water for granted, they are still at risk of disruption resulting from incidents, such as the activities of someone with a digger – no supporting utilities usually means no availability.

The need for supporting utilities should be identified. The utilities should be regularly inspected and tested to ensure their reliable functioning. The water supply should be sufficient to guarantee air conditioning as necessary, as well as sufficient fire protection. A problem with any of the essential supporting utilities should be identified by an alarm system.

The risk assessment should highlight those facilities that require redundant power supplies, especially for computer services supporting critical business operations. The selected option, such as an uninterruptible power supply (UPS) or generator, should be capable of sustaining sufficient power for the maximum potential period of a power cut, or at least for the time identified in the business continuity plan(s). Some equipment requires a very stable electrical power supply, free of peaks and troughs (spikes) in power. If this requirement is not met, power spikes can lead to a loss of availability through equipment damage or failure.

Building management systems in the scope of the organisation should be treated as for other IT systems with regard to malware, backups, vulnerability management and audit (see ISO/IEC 27002, Clause 12).

Auditing guidance

The level of protection that should be provided to protect an organisation from disturbances in its supporting utilities depends on the security requirements of the information held in each environment. For example, information with high availability requirements should be protected by controls designed to ensure sufficient supporting utilities. Auditors should check that the organisation has considered all necessary supporting utilities, and has implemented controls to ensure adequate levels of service, both technically, and via agreements with external service providers (e.g. telecommunications providers). Auditors should also check that there are procedures in place to inspect and test all supporting utilities regularly, for example by asking to review the records of those tests.

For higher power requirements, check that sufficient facilities such as standby generators, UPS units, redundant disk (RAID) units, etc., are in place. If this is the case, look more closely at the power supply support. Does it have sufficient capacity to cover air conditioning requirements? What is the extended operating period? Does it match the documented requirements? How is this verified? Is equipment maintained and tested in accordance with the manufacturer's recommendations? What actions are taken to detect malfunctions? The auditor should also check that emergency lighting is provided in case of a power failure.

The auditor should also check that there are redundant connections to key utility providers, to prevent failure of one connection resulting in the loss of a critical service.

2.7.2.3 Cabling security (ISO/IEC 27001, A.11.2.3)

“Power and telecommunications cabling carrying data or supporting information services shall be protected from interception, interference or damage.”

Implementation guidance

Unless properly installed, it can be very easy to damage such cables, especially their connectors, leading to a loss of availability. It can sometimes be difficult to trace the fault. Cables left on floors and hanging loose around walls are a safety hazard and will suffer excessive wear or pulling, leading to damage. In addition, unclearly marked cables might be subject to inaccurate connection. Finally, including power and data cables in the same conduit may result in interference affecting the data cables.

In sensitive organisations, communications cables might be at risk of interception and consequent loss of confidentiality of the information they carry. In this case, they should be protected by conduits, with all connections made in locked equipment rooms or boxes. While physical protection will be the principal safeguard to consider, there are also data transmission controls, such as encryption, that can be employed. The risk assessment should determine where this is necessary.

Public access to roadside telecommunications junction boxes might also pose a risk in some places, both from physical damage and tampering. Discuss this with your network service provider with a view, perhaps, to relocating the box underground beneath a secure lid. The implementation guidance in ISO/IEC 27001, 11.2.3 provides further guidance on cabling security, especially on how to protect sensitive or critical systems.

Auditing guidance

During the audit, the organisation should be able to demonstrate that interconnecting plugs and cables are adequately protected from interception, interference or damage. Are they correctly fitted and properly routed, or are they badly put together and placed where they could be damaged or cause an accident? ISO/IEC 27002, 11.2.3 provides a list of guidelines that should be considered for power and telecommunication cables.

A good indication of the status of the cables is the documentation describing the power and communication lines, and the cable markings used. Routing of communications links could be critical for some users. Auditors should check that the organisation has considered the communication risks and looked for potential weak points regarding network cabling routed between departments or buildings, unprotected or unsegregated telecommunication and power lines or cabling accessible to interruption or eavesdropping.

2.7.2.4 Equipment maintenance (ISO/IEC 27001, A.11.2.4)

“Equipment shall be correctly maintained to ensure its continued availability and integrity.”

Implementation guidance

The correct operation of computing and communication equipment can lead to a false sense of security. The sudden failure of equipment that has worked faultlessly for years can have a profound effect on the integrity and availability of business processes and services – especially if the equipment cannot readily be replaced.

Most equipment is supplied with maintenance instructions and these need to be built into operating procedures. Ensure that maintainers are authorised and qualified, and that they are accompanied when carrying out their maintenance work. Keep records of faults and maintenance – monitoring these will help in the judgement of when equipment should be replaced and so avoid the sudden failure. Also ensure (either by deleting confidential information prior to maintenance activities or protecting it in other ways) that no confidential information is disclosed.

Auditing guidance

The auditor should confirm that the organisation has controls in place to ensure equipment maintenance in accordance with suppliers' recommended service intervals and specifications. In addition, simple maintenance processes such as regular cleaning of air filters, tape drive mechanisms and printers can save considerable disruption. Even mundane activities such as regular disk defragmenting on computers with spinning hard disk storage can extend the usable lifespan of equipment.

Look to see what maintenance activities are identified in the procedures, determine whether they are sufficient and check the records to ensure that maintenance activities in the past have taken place as specified in the procedures. There needs to be a formal fault reporting mechanism. Check for this, and for logs of defects and their rectification. It should be verified that only authorised personnel can carry out maintenance activities, that external personnel carrying out maintenance are always accompanied and that no confidential information is accessed. As far as is possible, equipment should be checked after repairs and maintenance for evidence of tampering and unauthorised modification (e.g. the installation of a wireless access point to permit future remote access).

2.7.2.5 Removal of assets (ISO/IEC 27001, A.11.2.5)

“Equipment, information or software shall not be taken off-site without prior authorization.”

Implementation guidance

In many organisations, staff can regularly be expected to take equipment, data and documents away from the premises. This might be to work at home, or to attend meetings at other premises. There are three main alternatives that an organisation may consider to address the risk of theft or misuse, as follows.

of all assets containing sensitive information is prohibited. On the face of it, this is the simplest approach, but difficult to implement for most organisations. Highly restricted environments might need to use this approach.
of assets containing sensitive information is permitted with appropriate controls. The organisation needs to be very clear what information is involved and what controls are needed.
of assets containing sensitive information is permitted without controls. This can be very dangerous, and should always be accompanied with additional controls regulating the handling of sensitive information when it is outside the organisation's premises.

Assets removed without authorisation might also be in the process of being stolen. This can lead to non-availability, and loss of confidentiality where items contain sensitive information or software in a readable format. In a technology-rich environment, the likelihood of loss can be very high, especially among items that can be useful at home or sold online for profit. Also consider the possibility of the unauthorised removal of information via the Internet for later retrieval at home.

Equipment, information and software, etc., should not be taken (or transmitted) off-site without formal authorisation. It is essential that the organisation knows where its assets are and who has responsibility for them. All items of equipment should, where possible, be marked to indicate their ownership.

Those carrying items such as laptops, other mobile devices and sensitive business information (in digital form or on paper) in and out on a regular basis, should be provided with documentation verifying their authority to carry this equipment with them, which should be produced on demand. Additional verification and authorisation should be considered where an individual needs to carry information, or devices capable of accessing information, to another jurisdiction which has different laws on information access and protection.

Where items are on long-term loan, for instance to home workers, the individual should be required to attest periodically that the items are still in their possession, in good condition and necessary for their work. Procedures should be implemented to ensure that those leaving employment return all company assets before departure. Alternatively, where the organisation allows staff to retain or buy their equipment, procedures should be followed to permanently erase any stored organisational information prior to the individual being given ownership of the device (see 2.4.3.2 and ISO 27002, 8.3.2).

Those bringing property into secured areas should be required to log the property on entry so that they can leave with it without difficulty. Appropriate documentation should be kept regarding procedures, authorisations, off-site inventory and returns.

Auditing guidance

The auditor should check which approach is taken by the organisation to the removal of sensitive information, and then look at the documented procedures for managing the risk of this removal (if it is permitted at all). Is a booking in/out system in use? What authorisation is needed and recorded? Is this for all items or only a restricted range? How does management monitor compliance? Are spot checks carried out? Does the confidentiality agreement (see 2.3.1.2 and ISO/IEC 27002, 7.1.2) cover responsibility for information held while off-premises? Many employees use notebook computers or mobile phones. What controls exist for these or any sensitive data held? Information held on notebook computers or storage media could be disguised by changing the file names. Are search tools needed to combat this? If so, when are they employed?

Information can also be removed from premises via the network. Auditors should also check what export transfer control mechanisms exist when staff access the Internet. Are cloud services allowed or blocked? Is clear advice present on the use of personal email accounts to handle work information (also see 2.9.2.3)?

2.7.2.6 Security of equipment and assets off-premises (ISO/IEC 27001, A.11.2.6)

"Security shall be applied to off-site assets taking into account the different risks of working outside the organization's premises."

Implementation guidance

The use of equipment outside the secure environment of the organisation yields many security problems and added threats. For some organisations, this will not be an issue, depending on the business carried out, but for most organisations this could be a significant area of concern.

The security of equipment off-site should be subject to a risk assessment, and appropriate controls should be used to ensure that it remains in place, in operation and does not provide an uncontrolled risk, for example through its links to central networks. The risk assessment should ensure that the security provided off-site is equivalent to the security arrangements on-site, and the appropriate insurance arrangements should be implemented for equipment when off-site.

Be especially careful to identify all the risks inherent in portable equipment. Portable/mobile devices are particularly vulnerable to theft when in public places, leading to breaches of confidentiality as well as the loss of the device. The security of mobile equipment is also discussed in 2.2.2.1.

Auditing guidance

The auditor should look for evidence that the risks posed by off-premises equipment have been assessed, where this is applicable to the organisation. The auditor should then check that the controls implemented for the physical protection of equipment outside the premises provides security comparable with what is implemented on-site. Procedures and guidelines should be in place to ensure that equipment off-premises is not left unattended. Where relevant, sufficient insurance should have been taken out. Verify the excess payable and the requirements on the organisation to ensure that the insurance will pay out when required.

Additional protection mechanisms are also described in 2.2.2, where 2.2.2.1 addresses mobile computing and 2.2.2.2 the security issues related to home workers and their environment.

2.7.2.7 Secure disposal or re-use of equipment (ISO/IEC 27001, A.11.2.7)

"All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use."

Implementation guidance

Serious breaches of confidentiality can occur when discarded storage media, such as disk drives, are accessed by unauthorised persons, for example after being sold on the second-hand market or left in a skip. Although files may have been deleted from media, they may remain accessible to anyone with the right tools. Copies can also be made of the organisation's software if it is not permanently deleted, laying the organisation open to charges of unauthorised distribution of copyright material. The organisation should use controls to ensure that any equipment to be disposed of or reused no longer contains sensitive information.

It should be noted that certain storage devices (such as magnetic hard drives) may be adequately wiped using suitable programs, but that other types of devices (such as solid-state disks) may retain data indefinitely. Many types of storage device are relatively cheap. The organisation should consider complete destruction as a method of disposal for unwanted storage devices containing sensitive data. Magnetic storage is relatively cheap – much cheaper than the impact of theft or compromise of sensitive data.

Encrypted data may not be retrievable from discarded media in any reasonable time if the keys are suitably chosen and not stored on or with the media, but, as computing power increases, the risk of successful brute-force decryption also rises. The lifetime of sensitivity of the data can be considered to determine the level of encryption required, or to decide whether encryption is an adequate control.

Auditing guidance

The auditor should check that the organisation has an effective process in place to ensure that any sensitive information is removed from equipment that is disposed of or otherwise taken outside of its control. The auditor should also check user awareness of the potential dangers. The organisation should understand that erasing files from magnetic media is not necessarily secure. The information is often still accessible. Overwriting tools should be utilised to reduce the chance of data recovery.

Where encryption is used to mitigate the risk of data leakage, the auditor should check that the level of encryption is adequately matched to the sensitivity of the information to be protected, taking into account the likely future increase in computing power available to an attacker over the usable lifespan of the information.

For magnetic media holding very sensitive information, specialist equipment (e.g. degaussing tools) should be employed to minimise residual data. The policy should extend to all media if labels on items holding sensitive data could be removed or modified before disposal, making positive identification difficult.

Depending on the risks involved, the organisation may apply physical destruction of media, and this should also extend to hard disks inside computers.

Consider also items sent for repair. Are there any checks to ensure that sensitive information cannot be accessed or interfered with, or is there a policy that all items sent for repair should have storage media removed or destroyed before dispatch? See also, 2.4.3.2.

2.7.2.8 Unattended user equipment (ISO/IEC 27001, A.11.2.8)

"Users shall ensure that unattended equipment has appropriate protection."

Implementation guidance

An unattended system left logged on to a service is vulnerable to misuse, providing concerns for confidentiality, integrity and availability. Other equipment that is accessible by unauthorised people is also vulnerable to disclosure, misuse, tampering and theft, leading to loss of confidentiality, integrity and/or availability.

Sensitive equipment, such as communications panels and controllers, should be locked away in equipment rooms or purpose-built cupboards. Desktop equipment such as computers should be locked or shut down when unattended. Risk assessment should determine the maximum time a session can be left open before it is automatically disabled or terminated. Keyboard and mouse use should be protected by a password while the computer is unattended. Screensavers with passwords should be used to hide the screen contents while unattended. Ensure that the strength of the password system is matched to the confidentiality and integrity requirements of the resources being protected.

Auditing guidance

The auditor should check that appropriate procedures to secure all unattended equipment are in place, that staff are aware of the requirements and dangers, and that the procedures are followed and are effective. Look for instances of unattended terminals without password protection or left logged on. Screen savers on PCs should have password protection – check. Ask to turn on any terminals switched off and ensure access to information is not possible.

Timeouts from sessions (via the connection to the resource being terminated, and/or the local computer screen saver) should be in place. Look at where this has been implemented, and determine whether the timeout periods are sufficient given the access level, the vulnerability and the operational needs. Determine what the time-out is based on: specific use of the application, or simply movements of a mouse cursor. Check that this timeout is employed consistently at all high-risk locations. Where timeouts rely on operating system features such as a screen saver, check that the facility has not been disabled (e.g. by the user, if they have the relevant access rights).

High-security equipment such as servers, communications equipment, etc., which are normally left unattended, should be in a protected environment – check for this and whether it is properly secured.

2.7.2.9 Clear desk and clear screen policy (ISO/IEC 27001, A.11.2.9)

"A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted."

Implementation guidance

Offices, especially open plan offices, provide good opportunities for people to walk around and read documents or information on screens that they are not authorised to view. Such people might include other staff or other individuals, such as visitors, air conditioning engineers and cleaners. The ubiquity of technology means that most people have a camera in their pocket (as part of their mobile phone), so photographing documents on paper or on a screen is very easy and unobtrusive. If access to computers is not protected, this might lead to unauthorised persons obtaining sensitive information. In addition, individuals might steal documents, or even throw them away thinking they are part of the recycling.

A disorderly desk may lead to loss of documents due to misfiling, or even putting them in the wastepaper bin by mistake, which could cause sensitive information to be viewed by unauthorised persons (such as recycling contractors). Information left out on desks is also more likely to be damaged or destroyed in a disaster such as a fire, flood or explosion. In addition, paper, being flammable, may contribute to a fire hazard.

Printers and faxes may also pose a risk, and the use of 'pull printing' (where the user has to authenticate to the printer before their job is printed) may be appropriate, as long as users know not to wander off while a particularly long document is being printed. Faxes expected to receive sensitive data should be suitably located in a secure location, and regularly checked for messages.

Organisations should adopt a clear desk policy for papers and computer media, and a clear screen policy for information processing facilities, in order to reduce these risks. Staff usually see this as an onerous control, so training should emphasise the benefits of working in an organised and tidy environment, and mandate that screen savers with passwords are used, or equipment is switched off when leaving the office. Compliance should be monitored and rewarded, persistent offenders noted, and training and/or sanctions applied.

Auditing guidance

The objective of this control is both to ensure that sensitive information in any form (processed electronically, on paper or media, etc.) is not left unattended, and also that information is not lost or made available to unauthorised people. This should apply to both working and non-working hours. Controls applied should be matched to the classification of information (see also 2.4.2).

The auditor should confirm that the organisation has a policy in place to prevent sensitive information being accessed by external individuals, e.g. cleaning staff. The auditor should also check what happens when desks, filing cabinets and safes are left unattended during the day, and when cleaning staff or other visitors (such as the auditor) enter the office. Furthermore, is there a process for warning staff who may be working on sensitive data, so that they can clear their screens and/or desks before the visitor enters? The auditor should check the risk of access to computers while staff are absent (irrespective of the duration of this absence): password-protected screen savers, switching the computer off or any other form of clear screen control should be applied.

Are faxes and printers suitably located, is there a pile of printouts on the printer and/or fax machine? Is the fax machine in a secure location if it is intended to receive sensitive material? Is pull printing in place or available for use for sensitive documents? Do staff know how to invoke it if it is optional?

Where necessary, additional access controls should also be in place. If the whole area is covered by an appropriate level of security, and all staff are appropriately authorised, then additional measures might not be needed. Check that the overall policy is clear, and that staff are aware of and follow the appropriate procedures. Sanctions for non-compliance should be simple, fair and consistently applied.

2.8 Operations security (ISO/IEC 27001, A.12)

2.8.1 Operational procedures and responsibilities (ISO/IEC 27001, A.12.1)

“Objective: To ensure correct and secure operations of information processing facilities.”

2.8.1.1 Documented operating procedures (ISO/IEC 27001, A.12.1.1)

“Operating procedures shall be documented and made available to all users who need them.”

Implementation guidance

As with all the controls in this standard, the scale of procedures should be appropriate to the size and complexity of the particular organisation. A large organisation with many staff might require more comprehensive and detailed procedures than a small organisation, where a few thoroughly experienced staff cover the whole operation. The documentation requirements for these procedures might also vary. In any case, the organisation should ensure that sufficient documentation is available to address typical activities in the day-to-day working environment, e.g. computer start-up and shutdown procedures, backup, equipment maintenance, mobile working, media handling, computer room and mail handling management, and safety. Typical instructions that operating procedures should include are described in ISO/IEC 27002, 12.1.1.

Inadequate or incorrectly documented procedures can result in system or application failures, causing loss of availability, failure of data integrity and breach of confidentiality. Complicated or infrequently used procedures provide opportunities for mistakes and should be avoided where possible. Operating procedures should be treated as formal documents, changes to which may only be approved by authorised persons.

Many organisations outsource the management of their computers and communications to a specialist facilities management organisation. One way of ensuring that appropriate security is in place, is to use sufficiently detailed contracts, and to check whether the other organisation is ISO/IEC 27001 compliant (see 2.11.2 for more about working with service providers).

Auditing guidance

Auditors should check the organisation's operating procedures and confirm that these are appropriately documented and are being applied throughout the relevant parts of the organisation. In order to be able to check procedures for completeness, auditors should have a general understanding of the various operational processes and workings of the organisation.

In addition, the handling and management of these procedures should be checked. A check should be made to ensure that it is not possible to modify the procedures without appropriate authorisation, that proper version control is in place and that the latest version is accessible to all those that need to have access to it.

Another aspect to check is the level of compliance with these procedures. Is it possible to circumvent these procedures or any associated controls? Are they commonly circumvented? Are the employees aware of these procedures, and do they know which procedure to use and where to find it, if needed? Are they using the latest version?

Responsibility for network service operation and administration is often held by a separate department, or even a separate organisation. The auditor therefore needs to understand the arrangement in place, and confirm that the necessary levels of service and procedures are properly documented. In some areas, detailed work instructions will be needed. There is likely to be considerable use made of supplier documentation, so this should also be checked for relevance and availability. This issue is also addressed in more detail in 2.11.2.

2.8.1.2 Change management (ISO/IEC 27001, A.12.1.2)

"Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled."

Implementation guidance

Uncontrolled changes to the organisation, its processes, information processing facilities and systems can cause major interruptions to business processes. Changes that might cause problems include the installation of new software, changes to a business process or operational environment, acquisition of a new business or the introduction of new connections between information processing facilities and systems.

In order to avoid interruption to business activities, any changes to operational systems should only take place after the necessary testing has taken place and formal approval has been given. The procedures for such an approval should take into account the potential impacts, including on security controls in place.

The change procedure should also allow for failback arrangements, for stopping changes, if necessary, and defining what action is needed to recover from unsuccessful changes. All changes that are made need to be fully documented, for example in an audit log that contains all relevant information.

Care should also be taken to control changes to applications (see also 2.10.2.2), since these changes are likely to have an impact on the operational systems in which these applications are running.

Auditing guidance

The auditor should check that management responsibility and formal procedures are in place to control changes to operational information processing facilities. All such changes should be monitored, and logs should exist describing exactly which changes have been made. It should be confirmed that no changes can take place without first assessing the possible information security impact that such changes may have, and obtaining appropriate approval for the proposed change.

The auditor should check that procedures are in place describing how to monitor a change for issues while it is being carried out and how to react if something goes wrong. It should be confirmed that no change can take place without appropriate fallback procedures allowing a return to the original state. The auditor should also confirm that the procedures cover informing all relevant personnel when a change has taken place. A good indication can be obtained by not only looking at the change control procedures, but also at records of previous changes, to check that these records contain all necessary information and support the evidence that the change control procedures have been complied with. If operational changes also yield changes to the applications, the changes should be integrated (see also 2.10.2.2). Changes should also result in changes to associated process or specification documents, and tests should include tests for vulnerabilities that may have been introduced.

2.8.1.3 Capacity management (ISO/IEC 27001, A.12.1.3)

“The use of resources shall be monitored, tuned, and projections made of future capacity requirements to ensure the required system performance.”

Implementation guidance

With growing requirements for the use of information processing facilities, an organisation may be vulnerable to loss of service because of inadequate resources, both facilities and staff. This risk should be reduced by system tuning and monitoring the use of present resources and, with the support of user planning input, projecting future requirements. Controls detecting problems in capacity can ensure timely corrective action. This is especially important for communications networks where changes in load can be very sudden, resulting in poor performance and unproductive users.

Capacity should also be managed by managing demand wherever possible, to smooth out peaks and troughs. Alternatively, if using externally provided services, it may be possible to arrange for on-the-fly increases and decreases in capacity to match demand.

The capacity management process is likely to be cyclical, and evidence of requirements should be obtained and documented in a standard manner that enables reliable repeat capacity calculations to be made. Critical systems, such as network gateways and main database servers, should be prioritised, and a capacity management plan documented for them.

Auditing guidance

Forward planning of basic operational needs is often overlooked, and auditors should check the organisation's ability to handle this.

The first question could be, “What is being monitored?” This would typically include disk capacity, transmission throughput, printer utilisation and other potential bottlenecks. Other appropriate questions could be, “What do you use for system tuning?” “Where are the logs from the detection controls put in place to identify capacity problems?” “How do you manage demand?” Examples of methods for managing demand are given in ISO/IEC 27002, 12.1.3.

The auditor should enquire how the information received from the capacity monitoring is used to identify future capacity requirements. Trending information and extrapolation of future requirements should be being used to plan upgrades. This should include capacity figures, trended as appropriate, reviews and identification of needs and upgrade plans. Look also at staff planning: inadequate human resources at critical times can often compromise security.

2.8.1.4 Separation of development, test and operational environments (ISO/IEC 27001, A.12.1.4)

“Development, test, and operational environments shall be separated to reduce the risks of unauthorised access or changes to the operational environment.”

Implementation guidance

Operational systems demand the utmost integrity and reliability. Using the same equipment and software to develop and test new systems makes the organisation's operational systems vulnerable to failures of integrity and loss of availability. Risks are particularly high where new operational software, communications equipment or services are being developed or tested. Errors and omissions can lead to unauthorised access, introduction of malicious code and other security problems.

Equally, it is highly inappropriate to put sensitive data into a test environment unless this is as secure as the live environment, taking into account the fact that, since you are testing something, it may have security flaws. Hence any security controls that are part of the application or other entity being tested should not form part of the controls implemented by the test environment.

Measures such as strong access control should be applied to separate development, test and operational facilities. The easiest way is to use entirely separate systems, or at least separate domains that are completely segregated from each other. Where such a separation cannot be completely achieved, separate log-on procedures, supporting access control and good monitoring can be implemented to achieve similar effects. Finalised and fully tested developments should be fed into the change control procedure in readiness for operational acceptance (see also 2.8.1.2 and 2.8.5.1).

Auditing guidance

It is important that appropriate separation between test, development and live environments is achieved to avoid disruptions in the operational process. The auditor should check how such separation is implemented, and what authorisation processes ensure that development and untested application software is not used on operational systems. The auditor should also review the risk assessment to verify that this issue has been given appropriate consideration, and that the controls in place are adequate to protect against the identified risks.

If operational applications software and information are held on the same system as those under development and in test, then the auditor should check that they are at least held in separate domains, and that strong access controls are in place to ensure that no merging of development, test and operational facilities takes place.

Different logins with different passwords should be implemented for operational and development environments. Test systems and compliers, system utilities, facilities to edit programmes, etc., should not be accessible from operational systems. The auditor should check how new software is introduced (see also 2.8.1.2), and verify that this software is no longer in the development or testing state.

If sensitive data is present in the test environment, the security measures there should be at least as good as those in the live environment, neglecting any measures that are part of the system/software being tested. Additional security controls may be needed for the test environment to take account of this.

2.8.2 Protection from malware (ISO/IEC 27001, A.12.2)

“Objective: To ensure that information and information processing facilities are protected against malware.”

2.8.2.1 Controls against malware (ISO/IEC 27001, A.12.2.1)

“Detection, prevention, and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.”

Implementation guidance

Most (if not all) operating systems are vulnerable to the threat of malware (e.g. viruses, worms, Trojans, etc.). It is very easy for malware to install itself on a vulnerable system, but it can be difficult and costly to get rid of. Prevention can only be achieved to a certain level (relatively new viruses, for example, are often not detected by anti-malware software), but it is still necessary that this control is strictly applied and followed. Malicious code in a networked system can have a devastating impact on the confidentiality, integrity and availability of all files on it, and potentially on any data that its user has a right to access. Traditionally, malware has affected only executable programs. However, macro viruses in word processing and spreadsheet files are a cause of significant difficulty because such files are quite commonly passed from user to user; and other forms of malicious code can spread themselves to any file in the system.

One of the keys to prevention is user awareness. If staff understand the risks, they will apply the controls and will be wary about what to download, what emails to open and which websites to visit. It is advisable to also use technical controls that run independently in the background, carrying out checks automatically. A check for malware using a different anti-virus program should also be implemented where appropriate, such as on file servers supporting a large number of users.

Another key to success is to ensure that the protection against malware is up to date. It is recommended that dynamic updates be used to ensure that protection remains effective, and that relevant information sources are reviewed for news about the latest threats. Updates should be done manually if dynamic updates are not possible for technical reasons.

Auditing guidance

Malware is a problem on almost all operating systems; therefore the auditor should confirm that implemented controls are adequate. The guidance in ISO/IEC 27002, 12.2.1 can be applied to ensure optimum protection.

A number of options are available when installing software protecting against malicious code. Sometimes it is held on a central server covering all client systems that are logged on. Other systems may require protection software to be installed on each system. Sometimes the installation updates the entire software package, and at other times only libraries are involved, so auditors need to know how to determine the correct versions. Another important item for the auditor to check is that the updating is done whenever it is necessary, for example through an automatic update or some other form of notification of necessary updates. Handling of portable systems can involve particular problems: how are regular updates assured? Is malware protection available, or necessary, for the device in question?

For systems handling sensitive information, the use of more than one vendor's anti-virus software is advisable, to improve detection rates.

If checks are not constantly running in the background (very often a good option, but not always possible), procedures should be explicit about regular checking. There should be a clear policy on incoming software, emails and websites. The auditor can also check user awareness of this issue, and look at training records to ensure that users have been provided with information describing correct behaviour.

The actions in the event of virus infection should be covered. Check that automatic removal is implemented where possible. Occurrences of malicious code infections should be properly recorded. Look at the type of software used. Is it adequate and properly supported?

Free applications might not give the necessary protection and could cause additional damage. Some malware imitates protection software in order to extort money from the user. The auditor should confirm whether users know and use the correct methods of interfacing with applications, operating systems, etc. An unexpected request for password information, for example, could be an attempt by an attacker to obtain a password and access vital data.

2.8.3 Backup (ISO/IEC 27001, A.12.3)

“Objective: To protect against loss of data.”

2.8.3.1 Information backup (ISO/IEC 27001, A.12.3.1)

“Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy.”

Implementation guidance

Every organisation is vulnerable to a crashed disk or failed tape, and to other problems that can cause loss or corruption of information or software. Integrity and availability of all important information and software should be maintained by making regular copies to other media. The regularity will depend on the criticality of the data. Some systems can justify real-time backup – writing the copy at the same time as the original. If this is not possible, other copying should be used, be it automated or user initiated. A backup cycle should be designed to ensure that all information and software is copied at appropriate intervals, while maintaining at least two copies of each file. This can, for instance, be satisfied with a three-tape cycle. Risk assessment should be used to identify the most critical data, which may justify more frequent copying.

Copies should be stored in a safe place. Full copies of data should be kept off-site or at least in a fireproof safe. The protection applied to the backups should be equivalent to that used for the original. It is important to regularly test the ability to restore data from backup, and to replace media at end of life. Old media should be adequately disposed of (see 2.4.3.2 and ISO/IEC 27002, 8.3.2).

Some data will be being kept in a long-term archive for legal or other reasons. It is essential to maintain the means to recover data that has been archived. This requires the appropriate computer; media reading device; the software to read the data format, e.g. database manager; and the correct version of the application programs to interpret the data fields. Failure to recover data could leave the organisation in breach of statutory requirements to maintain records. Comprehensive records of tape contents and program/data relationships should be maintained. Alternatively, the data could be transferred to currently supported media when the media it is on is deprecated, if permissible.

Auditing guidance

Backups are a key component in maintaining information integrity and availability. The organisation should have well-defined procedures for dealing with backup. Initially, look at the backup sequence, which should be consistent with the organisation and its security requirements, and compatible with recovery and business continuity plans.

In a typical network environment, this is based on full server backup plus a number of incremental updates defined at a frequency appropriate for the requirements for integrity and availability, for example, daily, weekly or monthly cycles. The auditor should confirm that there are appropriate backup arrangements in place according to the results of the risk assessment, and check that this includes full coverage of items within the scope of the ISMS.

How and where the backup media is labelled and stored is also important. The auditor should check that each item can be uniquely identified, is logged correctly and is held securely. Backup media should be held in separate locations to the systems they back up, and sufficient controls should be in place to give the same level of protection the backed-up information normally has.

The auditor should confirm what the long-term storage requirements of critical data are, and how the organisation validates this. Backup media can deteriorate and may need to be refreshed. Look also in the procedures for backup. What corrective actions are required if the backup fails? What arrangements exist for restoring the data? How often is this exercised? What records are kept? Are backup media tested to ensure they are working properly? Test restores of backup files should not compromise data integrity: check that this is adequately addressed. The auditor should check that requirements for business continuity planning (see also 2.13) are met by the backup arrangements in place in terms of frequency, format and availability.

2.8.4 Logging and monitoring (ISO/IEC 27001, A.12.4)

“Objective: To record events and generate evidence.”

2.8.4.1 Event logging (ISO/IEC 27001, A.12.4.1)

“Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.”

Implementation guidance

Audit trails are an essential prerequisite to investigating what went wrong. They are often necessary to establish the events leading up to an incident, as well as to determine the accountability for an incident.

The policy for event logging should be determined by an appropriate level of management. Some systems can produce very large logs covering a wide range of activities, exceptions and events within the system. Generally, such a quantity of data is difficult to use to identify possible misuse. The level, type and frequency of monitoring required will depend on the sensitivities of the system and should be established by the risk assessment. It is as important as the creation of monitoring logs to assign responsibilities and sufficient time to review/process these logs; information important for system processing might require more frequent reviews than others.

Monitoring of all relevant information can easily create large quantities of information to be evaluated. Automated procedures and appropriate tools are vital to distinguish truly significant items from the overall noise of logging information. An analysis of monitoring requirements should be made, and the results from this analysis used to manage the log information to be collected. Data may need to be cross-correlated between systems to derive actionable intelligence: for example, to trace an IP address to the system using that IP address at the time the event was logged, and then to the user account on that system that owned the process responsible for initiating the event.

Logs of user activities should record the items listed in ISO/IEC 27002, 12.4.1. Logs should be kept for a sufficient period in case they are needed for an investigation. They should also be protected in their own right, particularly against unauthorised modification designed to cover up other unauthorised activity (see also 2.8.4.2).

As with all types of incident, system faults can expose vulnerability to loss of service integrity and availability. All faults should be logged to enable orderly corrective action to be taken. In the longer term, logs should be analysed to identify unacceptably unreliable equipment and fault trends in individual devices. The process for handling reported faults should include a review of fault logs, and the identification and implementation of the appropriate corrective action. The effectiveness of corrective actions should also be verified.

Special care should be taken where a fault, or its correction, may have compromised security.

Auditing guidance

For all systems processing information, there should be an event log kept that is independent of, and not accessible by, the user (even if they have full access to the system itself). Auditors need to confirm whether the logging arrangements are appropriate for the security requirements of the organisation, and should check the organisation's approach to logging. The auditor should check that all records that are required to be kept because of record retention policy, or in order to collect evidence, are suitably archived (see also 2.8.3). What is recorded, and are the records holding sufficient contextual information? How can it be shown that the records have not been altered in the archive?

As a minimum, the log information should identify the event, the person causing the event, any changes made, the date and the time. In addition, transaction codes, terminal ID, network addresses and actions carried out (such as use of privileges or system utilities, changes to the configuration of the system, etc.) may also be recorded. The auditor needs to check what constitutes a loggable event, and also needs to confirm how long this information is required to be held, in what form and under what protection. Example events include changes made by system administrators and failed logins or access attempts. Ask for examples of such event logs.

Event logs need to be reviewed and, where necessary, suitable and effective corrective actions should have been taken. The auditor needs to check how often the logs are reviewed – the higher the related security risks are, the more frequently the logs should be reviewed. This check should also confirm whether the review process itself is effective and efficient. The principle of separation of duties should be employed in assigning responsibility for reviewing log files. The roles whose activities are being reviewed should not be performing the review.

The logs produced by system monitoring or event logging processes will result in large volumes of data. This might result in important information related to security relevant incidents getting lost in other less important data. Tools such as security incident and event monitoring software (SIEM) should be in use to automatically process audit logs, with rules designed to ensure that all relevant incidents and activities are identified, prioritised and highlighted. The auditor should enquire about the use and coverage of such tools, and review how these tools are applied in practice to detect and alert on incidents.

Part of the process for reviewing an alert should be to determine whether security has been compromised. If so, the process should lead to the incident management process. Check that this is defined in the procedures and understood by management. It should be verified that all faults have been satisfactorily resolved, or are in the process of being handled. Auditors should also check that only sufficiently authorised personnel are able to carry out corrective actions, and that these are designed to avoid recurrence of the faults in the future, and/or sufficiently limit the damage.

2.8.4.2 Protection of log information (ISO/IEC 27001, A.12.4.2)

“Logging facilities and log information shall be protected against tampering and unauthorized access.”

Implementation guidance

The information contained in audit logs, administrator logs, fault logs and in logs resulting from monitoring activities is only valuable if its integrity can be relied upon. It is therefore essential to give log information sufficient protection. This is especially important when investigating incidents, or when evidence needs to be provided (see 2.12 and 2.12.1.7).

The organisation should ensure that it is not possible to:

- edit log files, except with explicit authorisation;
- delete log files, except with explicit authorisation and the creation of a record to document the erasure;
- modify the type of information (e.g. level of event) being recorded in the logs;
- stop logging, except with explicit authorisation;
- redirect log files to an unauthorised destination; and
- overwrite logs (e.g. by using the fact that storage capacity is limited) without generating an alert to an appropriate recipient.

Auditing guidance

Auditors should check the provisions the organisation has in place to protect its log information, to ensure that the logging and monitoring controls provide reliable evidence of what is going on in the organisation. Check how the logs are stored and maintained, and confirm that they cannot be maliciously modified or deleted. Check also who determines what exactly is logged, and confirm that nobody can maliciously alter the types of information recorded in the logs or overwrite logs.

2.8.4.3 Administrator and operator logs (ISO/IEC 27001, A.12.4.3)

"System administrator and system operator activities shall be logged and the logs protected and regularly reviewed."

Implementation guidance

Both automatically and manually generated logs of administrator and user activity are important for providing assurance of the integrity of systems. They are often a very useful aid to incident investigation, and consequently should be protected against alteration by privileged users, ideally by promptly removing them to a log server that is not under the control of the users of the systems generating the log data. Separate detection systems, such as an intrusion detection system, can also be used to monitor user activities.

Log data should be retained for a reasonable period of time and be subject to regular, independent reviews against operating procedures. The logs should identify the time when an event occurred, provide relevant and useful information about the event, and identify the person(s) and processes that were involved in the event.

Auditing guidance

The system operating procedures should identify the administrator and user logs that need to be kept, both for normal operations and fault detection. There should be evidence that these logs are independently reviewed as part of internal monitoring. The auditor should check that the logs contain sufficient information, and that they are protected from tampering and deletion, especially by privileged users of the systems creating the logs.

When checking operating logs for context, the auditor could check how shift changes are recorded, the occurrence of carry-over operations and special requirements, etc. Look also at the archiving of logs, both manually and automatically recorded. Are logs identified? Can they be retrieved? Are they protected from unauthorised changes and viewing?

2.8.4.4 Clock synchronisation (ISO/IEC 27001, A.12.4.4)

"The clocks of all relevant information processing systems within an organisation or security domain shall be synchronised to a single reference time source."

Implementation guidance

Most output from computers and communications equipment is time and date stamped. This information forms part of the audit trail for transactions moving between computers. It might also be required in investigations or to resolve disputes, and should therefore be entirely consistent between all devices within the scope of the ISMS (see also 2.12.1.7). An internal reference time source should be identified, documented and implemented. The use of an external reference time source should be considered, and the decision on this matter clearly documented. Radio receivers are available that will provide a computer with a signal from an atomic clock which maintains accuracy to the second.

Auditing guidance

The organisation needs to establish what its base time shall be. For most this will be local time, but for international organisations some other base may be used, e.g. GMT/UMT. Without proper timing across all systems, audit and monitoring logs can be inaccurate and misleading. Any system audit trails and monitoring investigations rely on accurate system clocks. The auditor needs to verify that access to the configuration of system clocks is restricted to avoid tampering. There should also be some facility to monitor system clocks, and correct them if necessary. Also check what is done to ensure the consistency of wall clocks that may be used for manual logging, e.g. goods received and incident reports. Ensure that these are used, rather than user's wristwatches; are they in the right place? Can system clocks be used instead?

The auditor needs to check how the transition to and from British Summer Time (BST) is controlled. What arrangements are made to correlate the time for systems that are located in different time zones? Are any additional checks carried out when portable/mobile devices log in to the network?

Finally, the auditor should confirm that other systems, such as CCTV systems, are using the same reference time source as other systems.

2.8.5 Control of operational software (ISO/IEC 27001, A.12.5)

"Objective: To ensure the integrity of operational systems."

2.8.5.1 Installation of software on operational systems (ISO/IEC 27001, A.12.5.1)

"Procedures shall be implemented to control the installation of software on operational systems."

Implementation guidance

Operational systems are vulnerable to the installation of unauthorised software and unauthorised changes to operational software, with a resulting loss of system and data integrity. Controls are necessary to reduce the risk of system failure, the introduction of any unauthorised software and the possibility of fraud. All software updates should be subjected to change control and authorised and tested prior to implementation, and all changes should be logged. Backups of old configurations should be retained, and a fallback strategy should be in place for the case of failure of the new system.

New products should be obtained against a business requirement and appropriately authorised. Ensure that valid licences are provided to cover the extent of use intended. For vendor-supplied software, it should be ensured that support is available at the level needed by the organisation, and that this support does not cease for as long as the organisation uses the software.

Auditing guidance

Auditors should check the controls applied for the implementation of software on operational systems. How is the code held on the system? Is source code included? How are new versions introduced? How are system files and libraries protected? What records are kept of changes? Are changes only made if there are business requirements to do so and after security considerations have been made? Developers and maintenance staff need to be aware of the potential dangers of introducing untested code or of allowing unauthorised code onto operational systems. Check that this awareness exists.

The auditor should check implementation. What protection is applied to source and object code? What testing stages have to be completed before new or modified code is introduced? Is regression testing adequate? Can previous issues of code be reinstalled? Are full data backups performed before changes, and are fallback arrangements in place for where changes have not been successful (see 2.8.1.2 and ISO/IEC 27002, 12.1.2).

The auditor should check records of changes to operational code. Are they complete, sufficiently descriptive and showing proper authorisation? Complex or critical operations can require carefully thought-out and detailed plans for the introduction of new or modified code. Look for examples of this.

2.8.6 Technical vulnerability management (ISO/IEC 27001, A.12.6)

“Objective: To prevent exploitation of technical vulnerabilities.”

2.8.6.1 Management of technical vulnerabilities (ISO/IEC 27001, A.12.6.1)

“Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization’s exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk.”

Implementation guidance

More and more attacks on organisations’ information systems are based on the exploitation of published technical vulnerabilities, and the lead time for these attacks gets shorter and shorter. The organisation should have procedures in place to identify any technical vulnerabilities of its information systems in a timely way, and to identify and implement the appropriate response to such vulnerabilities. Vulnerability scanning tools are widely available and should be considered. Manual penetration testing may also be appropriate for more sensitive or critical systems.

The necessary roles and responsibilities for this process should be identified, as well as a timeline for actions, to ensure that appropriate actions are taken within a suitable period.

If a vulnerability has been identified, the organisation should identify the risks related to this particular vulnerability, and the suitable action to be taken, for example to install or not to install a patch to protect against the vulnerability. If the decision is that a patch should be installed, the organisation should ensure that it is tested prior to installation, and there should be rollback procedures in place to go back to the previous state if the patch causes unforeseen problems after being installed. Control 12.6.1 of ISO/IEC 27002 describes the management process for technical vulnerabilities that organisations should consider.

How an organisation approaches the problem of technical vulnerabilities is dependent on its need for robust information processing systems, and the resources and technical expertise the organisation has in place to evaluate patches before installation. Small organisations may restrict their actions to being aware of all relevant patches and installing them in a timely way (possibly taking account of the experiences other organisations have had), whereas larger organisations might include extensive testing before the patches are installed. Whatever approach the organisation takes, it should be based on a risk assessment that takes account of the requirements for resilience to attacks, and the resources the organisation has available to address this problem.

Auditing guidance

The auditor should check how the organisation is addressing the issues of published technical vulnerabilities. The organisation should have assessed the risks associated with published technical vulnerabilities, identified their requirements to protect against attacks exploiting technical vulnerabilities and put an appropriate management process for technical vulnerabilities in place.

The detection process for technical vulnerabilities should include testing procedures, which may include the use of automated vulnerability scanning tools and manual penetration testing engagements for more sensitive environments. The procedures should be clearly defined and repeatable, and tools should be configured to test all relevant systems, not just a sample. Reports from testing should be available, as well as reports from re-tests which verify that vulnerabilities identified in the previous test have been remediated.

Depending on the requirements of the organisation and the resources available, the auditor should check that a sound management process for technical vulnerabilities has been implemented. ISO/IEC 27002, 12.6.1 describes components of such a management process.

The correct operation of this process should be monitored, and the organisation should have procedures in place to evaluate the effectiveness of its technical vulnerability management. Whatever is done in response to identified technical vulnerabilities needs to link in with the change control process that is in place (see 2.10.2.2), and there should always be the option to uninstall a patch and return to the previous state.

2.8.6.2 Restrictions on software installation (ISO/IEC 27001, A.12.6.2)

"Rules governing the installation of software by users shall be established and implemented."

Implementation guidance

It is now common for certain groups of users to have increased privileges, allowing them to install or alter software necessary for their role. For example, some users may be developing software, and need to install both it and other tools on development systems. Equally, certain software requires users to have the right to install applications in order to update it. In all cases, the use of these privileges should be strictly controlled and appropriate uses documented and monitored.

Auditing guidance

The auditor should ask for and check documentation relating to the authorisation of users to install programs (this should apply to administrative users if not to other users), and acceptable uses for these privileges. Permitted categories of software that specific roles are allowed to install (e.g. patches) should be documented, as well as forbidden categories (e.g. software from dubious sources, games and vulnerability analysis tools).

2.8.7 Information systems audit considerations (ISO/IEC 27001, A.12.7)

"Objective: To minimise the impact of audit activities on operational systems."

2.8.7.1 Information systems audit controls (ISO/IEC 27001, A.12.7.1)

"Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimise to business processes."

Implementation guidance

Before any audit of information systems takes place, the audit requirements should be assessed and, if an audit is required, it should be carefully planned and a schedule agreed. Audit activity on operational systems may require the use of special programs that access data files used by the system or its applications. Such use should be planned to avoid causing problems and disruption in operational systems. Audit plans should be documented and authorised. ISO/IEC 27002, 12.7.1 gives further guidance on conducting information systems audits.

Auditing guidance

Information system audit controls and tools used in the audit should not compromise either the information or operations being checked. Where audits are planned, check that the requirements have been identified and appropriate authorisation has been obtained from operational management. No information should be changed for the purpose of these activities, and access to information should be logged as for any other operation.

The auditor should also check that the interruptions to business activities are minimised. Make sure the audit results are kept and that use of any tools is properly recorded. A check can also be made that any tools are themselves formally validated before use. This includes checking that the person carrying out the audit is independent of the activities being audited.

2.9 Communications security (ISO/IEC 27001, A.13)

2.9.1 Network security management (ISO/IEC 27001, A.13.1)

“Objective: To ensure the protection of information in networks and its supporting information processing facilities.”

2.9.1.1 Network controls (ISO/IEC 27001, A.13.1.1)

“Networks shall be managed and controlled to protect information in systems and applications.”

Implementation guidance

Networks are especially vulnerable to misuse and abuse, as well as unauthorised access or the unintentional failings of technology. They are complex, and it is easy to make mistakes in their configuration, control and protection.

As a result, network integrity can be impaired and availability lost. The confidentiality and integrity of information passing over public networks should also be considered, with the implementation of appropriate controls to protect the information and the organisation’s connected networks and systems, and the information held in these systems.

The only way to reduce these risks is to put in place effective management and security controls, together with sound procedures. Good network security begins with network architecture, and security should be considered throughout the design, implementation, operation, problem management and monitoring. The management of network information security has become a significant part of the overall security management activity within an organisation, with specialist knowledge being required for each communications technology. There are also many security controls available to protect the network in different ways, and their use should be properly planned:

- remote control of network equipment and user workstations for problem solving and software management.
- network monitors (also known as 'sniffers' or 'taps') to detect attacks and analyse traffic.
- encryption of transmitted data to retain confidentiality.
- restricted routing per user or network address.
- access control techniques to allow only authorised users.

Many of these controls require policies and procedures to be established at the organisational level. All these techniques require comprehensive authorised documentation for network designs, implementation, operation, and changes and monitoring. Constant monitoring of the activities in the network and security status is essential, with appropriate records being kept of faults, problems and corrective actions.

Auditing guidance

Network topology and operating environments, particularly where sensitive traffic is involved, should be properly planned and managed. The auditor needs to confirm that the organisation has done this, and that formal records of these activities are available. Have due consideration and protective mechanisms been employed where networks have access to or use public networks?

For large, complex operations, the use of external experts may be appropriate. If not, look carefully at the qualifications of internal network designers. Have the most exposed aspects of network operations been identified? Has zoning been adequately implemented? What protective measures have been adopted? Security breaches on networks are not always immediately obvious. Data may be intercepted, copied or modified without any obvious trace.

The auditor needs to check what monitoring activities are used to identify and alert on potential breaches, and to confirm that incident reporting procedures cover this (see also 2.12). Network technology, data encryption and digital signatures are all areas of rapid technological change. The auditor should check how the organisation is monitoring developments in these areas and identifying new opportunities and threats to existing protection mechanisms.

2.9.1.2 Security of network services (ISO/IEC 27001, A.13.1.2)

"Security mechanisms, service levels, and management requirements of all network services shall be identified and included in any network services agreements, whether these services are provided in-house or outsourced.”

Implementation guidance

The use of third-party supplied network services can increase the opportunities for unauthorised access by other parties, leading to losses of confidentiality and integrity. Availability should also be given special attention, checking on the resilience of the supplier’s failover provisions in the event of power, connection or equipment failure The organisation should establish security standards that will be maintained when the supplier is experiencing or recovering from a failure, and which should identify the security features, service levels and controls required by the services being consumed. This is best done via a risk assessment. The organisation should ensure that the identified security features are provided, and specify them in the agreement with the service provider (see also 2.11.1.2). Additional controls may be needed in some circumstances to offset any identified weakness.

Auditing guidance

Where the organisation is dependent on external suppliers for any networked services, it is essential that the full extent of all available security features, services levels, controls and management requirements are understood. The auditor needs to confirm that the organisation has assessed the risks and the needs for security services, that it has obtained information about the security features from the service provider, and that it has verified that these security features are actually being provided, and are sufficient and relevant to the identified needs.

The auditor should also check that these security features have been incorporated into operational procedures and security controls, and that there are procedures in place to review and verify security features regularly. The auditor needs to confirm that the organisation has covered all relevant aspects of information security, including confidentiality, integrity and availability, in their considerations.

2.9.1.3 Segregation in networks (ISO/IEC 27001, A.13.1.3)

"Groups of information services, users, and information systems shall be segregated on networks."

Implementation guidance

Networks are always vulnerable to unauthorised access attempts, which can result in breaches of confidentiality and loss of integrity for the network or its attached systems. The bigger the network, the greater the risk. Security is easier to manage if the network is divided up into physical or logical domains. Tight security can then be provided to manage the gateways or firewalls between the domains. A firewall can also be used to protect the organisation's networks from unauthorised external access, while still allowing public access to the organisation's web server, and allowing staff to receive email from other organisations.

Network modelling should be used to define the individual network zones required by the organisation, and risk assessment will determine the level of security needed to be applied to each domain. Network connection and routing controls should then be implemented to achieve sufficient segregation of networks.

The zones and their relationships should be carefully documented. The network security plan should be specific about which systems and network devices are in which zone. It is possible for different parts of a single system to be in more than one zone, for example by department or business unit. Provided that the security system can logically segregate them, this may be acceptable.

Auditing guidance

The larger a zone, the more difficult it can be to secure. This is true of networks, as much as of any other structure. It is highly likely that secure networks will need access to wider aspects of corporate operations – email, intranet web pages, networks of other organisations, etc. – so separation of particularly sensitive areas is needed.

Appropriate segregation in networks can be achieved by physically segmenting networks or by applying network connection and routing controls, e.g. via bridges, routers, firewalls, etc.

The auditor should:

•enumerate what network zones have been put in place by the organisation;
•establish that they are appropriate for the organisation's security requirements;
•determine how they are defined and incorporated into network operations; and
•verify how the connection from one network zone to another is controlled.

Considering that security zones can impose restrictions in operational performance, the auditor should also investigate whether performance-related modifications, especially to the implemented environment, have led to any security compromises.

Where wireless networks are part of the scope of the ISMS, the auditor should check that a risk assessment has been carried out to determine whether direct connection between the wireless network and the main network is appropriate, and whether this assessment has identified and implemented all relevant controls to manage the risks. The organisation should implement known good security standards when configuring any wireless network, especially if it is directly connected to the main network.

2.9.2 Information transfer (ISO/IEC 27001, A.13.2)

"Objective: To maintain the security of information transferred within an organization and with any external entity."

2.9.2.1 Information transfer policies and procedures (ISO/IEC 27001, A.13.2.1)

“Formal transfer policies, procedures, and controls shall be in place to protect the transfer of information through the use of all types of communication facilities.”

Implementation guidance

The exchange of information using electronic communication facilities, such as networks, landline or mobile phones, answering machines, video or faxes carries a lot of risks of compromise. The organisation should have an information exchange policy and supporting procedures in place describing the rules to be applied when exchanging information. When developing this policy and the supporting procedures, the items listed in control 13.2.1 of ISO/IEC 27002 should be considered.

An appropriate policy dealing with these issues should be communicated to all employees, and awareness training with real-life examples should be used to illustrate the risks involved.

All personnel should be aware of this policy and the related procedures, and when exchanging information they should also be aware of the possibilities of:

- information being leaked if sent to the wrong email address;
- information being intercepted by unauthorised people if being sent unprotected;

•information being compromised when left unattended in printers or fax machines;
•staff being overheard when using mobile phones in public places such as trains;
•messages and faxes being received by the wrong person through misdialling; and
•the wrong person picking up a fax or listening to an answer machine message, despite the right number being dialled.

Auditing guidance

The auditor should check that the organisation has a policy for information exchange and supporting procedures, and that this policy and supporting procedures address the different types of exchange that are used by the organisation. It should be checked, either through reviewing procedures or through technical means, that information exchange violating the policy is not permitted. It should also be checked that the policy and supporting procedures cover all forms of communication facilities, including networks, mobile computing devices, telephones and mobiles, fax machines and answering machines.

Auditors review procedures against the items described in ISO/IEC 27002, 13.2.1. The organisation should be logging information exchanges that are taking place. A specified role should have the responsibility to review these logs, and they should be doing so regularly.

The auditor should confirm that employees are aware of these procedures, for example, by asking them about their use of email, wireless communications, mobile phones, answer machines or fax machines, to find out whether they are aware of the risks involved and the appropriate way to mitigate these risks.

2.9.2.2 Agreements on information transfer (ISO/IEC 27001, A.13.2.2)

"Agreements shall address the secure transfer of business information between the organization and external parties."

Implementation guidance

When sending information to another organisation, there is always the risk that it might be compromised in transit or at the receiving end. The other organisation might have different standards, or different interpretations of the same labels and protections they may require. This can lead to unauthorised data leaks, and other impacts, including bad publicity for the sending and/or receiving organisation.

Agreements or contracts with a third party should explicitly specify the controls to be applied by the organisation and the third party when exchanging sensitive information (see ISO/IEC 27002, 13.2.2 for more detail on items to be considered).

Agreements should be authorised at an appropriate level in the organisation and periodically reviewed. Changes in practice should always be change controlled and reflected where necessary in the agreement.

Auditing guidance

Auditors should:

- check which third party organisations are involved in the transfer of sensitive information;
- confirm that the necessary contractual documents exist; and
- verify that these documents address the correct treatment of sensitive and confidential information in transit.

This covers not only information but also software. For example, where a software house has developed an application on which the organisation is entirely dependent, the organisation needs to ensure continued access to that software in the case of failure of the software house, perhaps via escrow.

The auditor should check what the organisation has done to investigate the controls which its suppliers, customers and partners use when sending and receiving information to/from it, and investigate how the organisation has addressed situations where protection requirements and controls vary from that which the organisation has implemented internally. The auditor should also verify that agreements between organisations exchanging sensitive information or software are in place. A list of relevant items that can be included is given in ISO/IEC 27002, 13.2.2.

2.9.2.3 Electronic messaging (ISO/IEC 27001, A.13.2.3)

“Information involved in electronic messaging shall be appropriately protected.”

Implementation guidance

Email and other electronic messaging (including texting and the use of instant messaging (IM)) provide a wide variety of information security risks to any organisation if used without appropriate controls. Case history shows that organisations can be open to libel writs as a result of what their staff have written in a message, often informally and supposedly for internal distribution only. Messages may also be covered by freedom of information and data protection legislation. Staff may use their personal and work messaging accounts interchangeably, leading to leaks of sensitive data should a personal account be compromised.

Organisations should have a clear communications policy and approval processes in place regarding the use of electronic messaging that explicitly covers all forms of electronic messaging, not just email. The legal implications of both internal and external messages should be properly understood. The exposure of even an internal message that is critical of another organisation or person could result in legal action. An external message may be found to constitute an unintended contract between the parties. Deleted messages can remain for years in backup systems, from whence they could be retrieved if required. The courts and statutory regulators have the power to demand extensive disclosure from archives.

Email and some forms of IM can be a major source of infection with malware, via attachments or via links to websites which install malware without the knowledge of the user by taking advantage of vulnerabilities in web browsers. Appropriate controls should be applied to protect against these threats (see also 2.8.6.1). Additionally, an out of date email program can permit infection simply via the receipt of a maliciously crafted email, without the user even opening the email or any attachments.

Electronic messaging is also commonly used in attempted financial fraud, which employees can fall victim to.

All these aspects make email and other forms of messaging relatively high-risk services, so it is essential that staff are properly trained in the organisation's requirements and control mechanisms.

Auditing guidance

Electronic messaging is now ubiquitous in all organisations. As this form of communication is extremely vulnerable, the controls in place to protect it should be carefully considered. The auditor should check the organisation's security arrangements for electronic messaging, asking questions such as: How is information included in and attached to electronic messages controlled? How is correct receipt verified? How is incoming data verified as to source and integrity? If applicable, what encryption methods are applied? If encryption and digital signatures are used, are the controls discussed in 2.6.1 applied to ensure sufficient security? Is information received from electronic messages checked for virus infection before use? Does an electronic message within the organisation have a different integrity status from that sent externally, and if so, how is this defined and monitored? What services are allowed to be used for what sort of data? How is the use of personal messaging services controlled or prevented?

There are considerable legal risks in the use of electronic messaging, and organisations should have a clear and implemented policy on this issue. Internal messages could inadvertently be sent to external parties, contracts can be implied, and messages and attachments could be retained on backups past their authorised retention period. Standard disclaimers attached to electronic messages might help, but their legal status as protection is not clear.

Auditors should check the organisation's security arrangements if access to external messaging services is permitted, and verify that an appropriate risk assessment has been performed and managed. For example, it might be appropriate to restrict access to message transmission to a limited number of individuals. If so, how is this enforced?

2.9.2.4 Confidentiality or non-disclosure agreements (ISO/IEC 27001, A.13.2.4)

"Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, regularly reviewed and documented."

Implementation guidance

Suitable confidentiality agreements should be in place before giving anyone access to confidential information. This should be ensured for all employees of the organisation, as well as any relevant external personnel, and any other organisation with which information is exchanged. The organisation should develop confidentiality agreements that address its particular requirements. Examples of what might be included in the confidentiality agreements are given in ISO/IEC 27002, 13.2.4. This is not a definitive list, but can be used as a starting point.

Requirements for confidentiality agreements can be identified by looking at the following:

•identified legal, regulatory and contractual requirements – if these requirements impose confidentiality, e.g. as data protection legislation does for personal data, a confidentiality agreement(s) might be useful.
•information exchanged with other organisations – confidentiality agreements with these organisations should be in place to ensure that the confidentiality of the information exchanged is not compromised.
•asset valuation – whenever the results of the asset valuation have shown that an asset has higher confidentiality requirements, all people having access to the asset should sign a confidentiality agreement.

•unplanned access to confidential information – it might be the case that people have unplanned access to confidential information, such as cleaning personnel in an office where desks have not been cleared. As the requirements for confidentiality agreements may change, it is important that a review process is in place that identifies new requirements and ensures that these requirements are addressed in the relevant confidentiality agreements.

Auditing guidance

Auditors should confirm that confidentiality (or non-disclosure) agreement(s) are in place, and check whether they address the identified business, legal and contractual and information security requirements. It might be helpful to consult the risk assessment results and see how these relate to the different clauses of the confidentiality agreement(s).

Auditors should also check that any confidentiality agreement uses legally enforceable terms, so that it is valid in disputes that might arise, and that the organisation has carried out due diligence to ensure that confidentiality agreements are not in conflict with any existing applicable legislations and regulations. Specialist expertise might be required to review legal documents.

The auditor needs to confirm that there are defined review and updating procedures in place for each of the confidentiality agreements, and there should be processes in place that ensure that appropriate agreements are signed before access to any confidential information is given (see also 2.3.1.2).

2.10 System acquisition, development and maintenance (ISO/IEC 27001, A.14)

2.10.1 Security requirements of information systems (ISO/IEC 27001, A.14.1)

“Objective: To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems that provide services over public networks.”

2.10.1.1 Information security requirements analysis and specification (ISO/IEC 27001, A.14.1.1)

“The information security related requirements shall be included in the requirements for new information systems or enhancements to existing information systems.”

Implementation guidance

Information security requirements and vulnerabilities should be recognised from the first stages of information systems acquisition or development, and all relevant requirements for information security should be specified along with the functional requirements. The development or acquisition of information systems should follow a well-specified and documented procedure that ensures that all identified security requirements are suitably addressed. The requirements analysis should refer to the results of risk assessments, and testing should be used to validate that the developed or purchased information system satisfies the identified requirements. ISO/IEC 27002, 14.1.1 contains a useful list of specific subjects to consider.

Auditing guidance

An organisation should be able to demonstrate to the auditor that information security requirements for the existing and new information systems have been identified and taken into account in the development and acquisition of applications, new systems, enhancements and upgrades to systems. This falls into two categories:

bespoke applications software is developed specifically for or by the organisation; and
commercial off-the-shelf (COTS) software is acquired for use by the organisation. (Note that an insecure add-on component or customisation might compromise the entire application.)

The organisation's analysis of requirements should identify appropriate information security requirements for new systems (e.g. preservation of integrity within a given application), and these should be incorporated into their requirements documents. It is vital that this process takes place for all developed and purchased information systems. Having confirmed that this is the case, the auditor should check how these requirements are tracked, monitored and reviewed during system development or acquisition, testing, configuration and installation. The auditor should confirm that testing of the information system takes place, where necessary, to check that the requirements are met. Any identified deficiencies should be analysed, raised at the appropriate management level and satisfactorily resolved.

2.10.1.2 Securing application services on public networks (ISO/IEC 27001, A.14.1.2)

“Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute, and unauthorized disclosure and modification.”

Implementation guidance

Controls should be implemented to protect the information involved in applications that use public networks, e.g. for electronic commerce.

ISO/IEC 27002, 14.1.2 provides a range of controls that are applicable, and the organisation should consider them and identify those applicable to its way of doing business. For example, the application of cryptographic controls (see also 2.6.1) can achieve protection in several ways:

- encryption can be applied to ensure the confidentiality of information such as billing details, customer information and personal information;
- digital signatures can be applied to ensure the integrity of electronic transactions and to authenticate the partners involved in

transactions; and
•encryption and digital signatures can be used to achieve non-repudiation that helps to resolve disputes regarding the occurrence or non-occurrence of events.

When using cryptographic controls, care should be taken to ensure that an appropriate policy and key management system is in place, and that these controls conform to any legal requirements (see also 2.14.1) that might be applicable.

Any organisation providing or using application services over public networks should have a policy in place that describes who is allowed to carry out electronic commerce activities, what each of these employees is authorised to do and what controls are in place to protect and monitor such activities.

Auditing guidance

Auditors should enquire about the current and future activities within the organisation. All activities related to the organisation's public use or provision of application services should be reviewed for any security-related aspects. This includes a check of the following:

•Is an authorisation process in place? Can only those employees within the organisation that are authorised carry out activities?
•Is there suitable segregation of duties? Are activities that, in combination, can be used to commit fraud or otherwise compromise legitimate communications segregated or supervised?

•Are appropriate cryptographic controls in place (see also 2.6.1) to ensure the authenticity, integrity and confidentiality of information processed in relation to non-repudiation of actions and events, and is a policy in place to regulate the application of such controls?
•Are appropriate network security controls in place to protect the organisation's network and the host used for public application services from attacks that can result from the interconnection with other networks (see also 2.9.1.1)?

•Are procedures applied to achieve appropriate verification of actions, payments, etc.?
•Have actions been taken to arrange sufficient insurance?
•Is sufficient protection given to guard against risks from other security problems that might relate to information involved in the provision of public application services (see also ISO/IEC 27002, 14.1.2)?

2.10.1.3 Protecting application services transactions (ISO/IEC 27001, A.14.1.3)

"Information involved in application service transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay."

Implementation guidance

If the organisation is using application services transactions (e.g. for online payments), controls should be put in place to protect against the risks associated with them, as listed in the control statement above. The organisation should use a risk assessment to identify the level of protection required for information involved in transactions. Control 14.1.3 of ISO/IEC 27002 describes items that should be considered for application services transactions, depending on the concerns of the organisation.

As described above in 2.10.1.2, the use of cryptographic controls (encryption for confidentiality and digital signatures for integrity and/or authenticity, see also 2.6.1) can help to achieve the desired level of protection. Particular consideration should be given to compliance with any applicable legal or regulatory requirements in the jurisdiction where the transactions take place.

Auditing guidance

The auditor should check how the organisation – if it is using application services transactions – has addressed the issue of identifying and implementing the appropriate level of protection for these transactions. Has the organisation carried out a risk assessment? Has this assessment taken account of at least the following issues?

- The use of cryptographic means, i.e. electronic signatures to ensure the integrity and/or authenticity, and encryption to ensure the confidentiality of information involved in transactions;
- The secure use of, and communication with, authorities managing certificates for digital signatures;
- Verification of who is involved in the transactions and of user credentials;
- The use of secure communication protocols;

•The secure storage of the information involved in transactions; and

•Compliance with applicable legislation and/or regulations, depending on the jurisdiction(s) that might be involved in the transaction.

2.10.2 Security in development and support processes (ISO/IEC 27001, A.14.2)

“Objective: To ensure that information security is designed and implemented within the development lifecycle of information systems.”

2.10.2.1 Secure development policy (ISO/IEC 27001, A.14.2.1)

“Rules for the development of software and systems shall be established and applied to developments within the organization.”

Implementation guidance

Where software, services, networks or whole environments are being developed, it is necessary for the organisation to consider the information security of these environments to prevent the deliberate or accidental inclusion of inappropriate functionality (or of vulnerabilities) that could be used later in the live system to compromise it, and also to protect the intellectual property of the organisation, both embodied in the materials being developed, and in the tools and systems being used in the development. The compromise of a development environment itself may impact the confidentiality, integrity and availability not only of that environment, but of the production environment in the future.

A policy should be implemented to ensure that development is carried out to standards that are suitable to the organisation's risk profile. ISO/IEC 27001, A.14.2.1 contains a checklist of what should be contained in the secure development policy.

Auditing guidance

The auditor should look for evidence of the use of secure coding or other relevant standards in the development environment, and ask to see documentation supporting a consistent and suitable approach to the identification and resolution of vulnerabilities. Developers should have training and competence in secure practices, which can usually be ascertained via interview. The auditor should confirm that information security standards are not only used, but that adherence to them is mandated and checked. Third parties (e.g. external organisations or contractors) should be required to meet the same rules as internal employees. The auditor should confirm that compliance is formally verified by the organisation on a routine basis, and non-compliances by any party followed up and resolved satisfactorily. The auditor could look for records of secure coding audits, both against standards and to find actual vulnerabilities. Check that these were not performed by the staff who wrote the code in question, and that they were performed by appropriately competent individuals. Automated code audit tools will find many issues, but should not be relied upon where coding standards are inconsistently applied.

2.10.2.2 System change control procedures (ISO/IEC 27001, A.14.2.2)

"Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures."

Implementation guidance

A system is always more vulnerable when undergoing changes – even fully authorised changes can have damaging effects. There are risks of loss of data integrity, application unavailability and possibly exposure of confidential information. Any changes should only take place in accordance with well-defined procedures and after appropriate authorisation has taken place.

Formal control and coordination of all changes should be implemented, together with business and technical authorisation, for each change at all stages of development – requirements capture, design, code, test and transition to operational status. Changes should be planned and prepared with appropriate testing and review, and the application and operational change control procedures should be integrated and linked as much as possible. Final testing should be signed off by the organisation before operational implementation. Control 14.2.2 of ISO/IEC 27002 provides further information about the change control procedures that should be applied.

Auditing guidance

The auditor should check that formal change control procedures are in place for all changes made to applications in the operating and system environment. These procedures might need to be in quality plans rather than standard procedures. The auditor should also check that similar procedures exist within support and that, where necessary, they provide for changes to design and requirements documents.

In particular, the auditor should check how changes to online operational (and often critical) systems are handled. These often need to be very carefully and extensively planned. Are sufficient fallback arrangements provided if things go wrong? Support staff's access to sensitive parts of the system should be restricted to only that which is necessary – investigate how this is implemented.

The auditor should check that all changes are properly authorised (i.e. that the authorisation is from the correct level of management and is suitably informed), that changes are correctly reviewed and tested, and that formal authorisation is always given before changes are incorporated.

Changes will often be grouped together and incorporated into a release rather than introduced separately. In this situation, the auditor should look to see that release records correctly identify each of the changes made, that proper configuration control is applied during all changes and that correct records of the implemented release are in place.

It is likely that an emergency change procedure is also employed to correct operational system failure situations. Check that this also meets all of the above criteria.

2.10.2.3 Technical review of applications after operating platform changes (ISO/IEC 27001, A.14.2.3)

“When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.”

Implementation guidance

Changes to operating system software should be under control (see also 2.10.2.2). However, the impact of operating platform (e.g. operating system) changes on security in general and on the applications should also be assessed. Where new operating software has been installed, the applications should be reviewed and the whole system should be properly tested to ensure there is no vulnerability to breakdowns, leading to non-availability of service, loss of integrity and compromise of information. Organisations should have procedures in place for the review of applications after any changes have been made to the operational system, and these procedures should include the identification of any applicable vulnerabilities (see also 2.8.6) and the appropriate reaction to such vulnerabilities.

Auditing guidance

The auditor should confirm whether the organisation has a review procedure covering operating system changes and their impact on the applications installed on the operational system. This should occur before the planned installation. If possible, a test installation should be evaluated. This review should include an assessment of the controls planned to be in place after the change – check that they are sufficient for the security requirements.

The auditor should look at the inputs to such reviews, such as manufacturers' data sheets and release notes, evaluation data if available, identified software changes that will be needed, for example where a 'workaround' has been applied to operating system defects and support arrangements.

Outputs from these reviews should include any necessary application changes and a plan for installation of the new operating system version. The version of operating system (plus any patches) should be specified in the configuration records. In some situations, organisations may decide not to upgrade the operating system. The auditor should check whether, under these situations, they still have access to the necessary levels of support, and, if not, that this is identified and reacted to in the risk assessment.

2.10.2.4 Restrictions on changes to software packages (ISO/IEC 27001, A.14.2.4)

"Modifications to software packages should be discouraged, limited to necessary changes and all changes shall be strictly controlled."

Implementation guidance

Modern software can be immensely complex and is subjected to control and testing during its development. There is considerable risk in making modifications within the user organisation, as such changes can introduce vulnerabilities that lead to a breakdown in internal controls. Loss of confidentiality, integrity and availability can result from such changes.

Changes to software packages, especially vendor-supplied software packages, should only be made if there is a convincing business requirement for such changes. Where changes appear to be essential, a risk assessment should identify the potential sources of vulnerabilities, and compensating controls should be selected. Such changes should be authorised at an appropriate level and subjected to change control procedures. If changes are made, a copy of the original software should be kept, and all changes should be fully documented and tested.

When deciding on changes to vendor-supplied software packages, it should also be taken into account that making such changes may mean that vendor support ceases and that the organisation then becomes fully responsible for the maintenance, curation and further development of the software. It may also violate copyright agreements.

Auditing guidance

The auditor should check that all changes to software follow a properly documented and authorised change control procedure. Any changes should be introduced in a controlled fashion, ensuring that they are fully justified and authorised before implementation. Software packages should only be modified if there is a clear business requirement to do so.

Sometimes changes to code can be made as patches, to be incorporated later into future releases. Where this is done, ensure that the patch is correctly removed after the future release is installed, and that all necessary documentation is updated (see also 2.8.6). Sometimes organisations may have access to the source code but are not the design authority. Rights to make modifications should then be documented in contracts. Such modifications must also be properly incorporated since, due to not having full access to design records, they might unintentionally impact the security of the overall application.

The auditor could also look at how previously applied changes are handled when new releases of the program are issued – they might need to be re-applied.

The auditor should confirm that there is a complete history of all changes made and that these records are retained for as long as is required, as well as a copy of the original software. The application should have a defined suite of regression tests that can be used to validate the performance of modified code – look at the control of this. Has the organisation considered the use of an external specialist testing body, where appropriate?

2.10.2.5 Secure system engineering principles (ISO/IEC 27001, A.14.2.5)

"Principles for engineering secure systems shall be established, documented, maintained and applied to any information system implementation efforts."

Implementation guidance

The discipline of security engineering is a relatively mature one, and provides a whole raft of principles and tools which can usefully be applied to the implementation of any information system. It enables security to be designed in from the beginning, which makes information security cheaper and more likely to be viable (retro-fitted security is never the best plan). It also integrates information security into standard development and implementation activities, which is critically important.

However, security engineering approaches must be tailored to the environment and to the organisational culture. They should also be regularly reviewed to ensure that they are up to date and achieving the desired goal of making information security intrinsic to information system engineering activities.

Auditing guidance

The auditor should check what security engineering principles the organisation uses when designing and creating an information system, where it obtained them and how it keeps them up to date. What assessment has been done to verify that the principles are suitable, and are they implemented as described? How are they promulgated to contractors and external parties? There is likely to be a role with responsibility for security engineering. Interview staff assigned this role to ascertain their level of competence in the field.

2.10.2.6 Secure development environment (ISO/IEC 27001, A.14.2.6)

"Organisations shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle."

Implementation guidance

Where an organisation is carrying out development activities, it must not only have policies to support suitable processes (see 2.10.2.1), but also a suitably secure development environment. As with any environment, the risks may come from not only the technology being inappropriately selected and configured, but also from the actions of people with access to the environment. It should also be noted that multiple development environments may be required to separate more sensitive work from less sensitive work. The organisation may indeed choose to have an entirely segregated environment for every development activity it carries out, to reduce the risks of cross-contamination. In this case, there may be a common set of requirements for each category of environment, to simplify the set-up process. Where the work involves integration of separate systems, other issues come into play, since the scope of the work, and hence the risks, are inevitably higher. Considerations that should be taken into account are listed in ISO/IEC 27002, 14.2.6.

Auditing guidance

The auditor should ask to see documentation describing the secure development environments in use. They should also ask about principles used to determine appropriate controls to apply to each environment, and what (if any) connections may exist between environments. A revealing subject to explore is that of administration. Does the design of the development environment take into account the risks posed by any common administration back-end, such as a private administrative network or authentication service?

The auditor can review designs and implementations against the items in ISO/IEC 27002, 14.2.6. Interview users of the environment(s) to see if they are aware of the measures that should be in place, and any behaviours that they are expected to exhibit. What background checks are carried out on staff working in the secure development environment(s)?

2.10.2.7 Outsourced development (ISO/IEC 27001, A.14.2.7)

"The organisation shall supervise and monitor the activity of outsourced system development."

Implementation guidance

Outsourcing software development carries many risks because of the lack of control during the development process. These risks include inappropriately low quality products, as well as unwanted software, such as covert channels or Trojan code being integrated into the product. Clear contractual agreements should be used to protect against these risks, to ensure the timely delivery, sufficient quality and reliable functioning of the software, and to identify the intellectual property rights of the work carried out. In addition, checks should be devised (as appropriate and possible) to verify that the development carried out is as specified. This may include testing of deliverables, auditing of the outsourcer's environment and obtaining evidence to support the outsourcer's compliance with the organisation's requirements (e.g. outputs of testing, lists of flaws identified and addressed, and certificates to confirm training of developers in secure development).

Auditing guidance

The auditor should confirm that the risks of outsourcing software development are being considered and assessed on an ongoing basis. Ideally, the development environment and processes involved should be inspected and reviewed by the organisation. The results can then be checked by the auditor.

The auditor should also check that risks associated with such developments are periodically reviewed, and that changes to security requirements, controls and responsibilities of both parties relating to such developments and any changed or new risks are covered by contract. The auditor should check that contracts cover:

•conditions to measure the timeliness and quality of developed software and requirements for the quality of code;
•access rights in case an audit is necessary to ensure quality of work done;
•regulations and agreements defining intellectual property rights and ownership of developed software;
•sufficient testing of the functionality of developed code, including checks for viruses, covert channels and Trojan code; and
•training requirements for developers.

2.10.2.8 System security testing (ISO/IEC 27001, A.14.2.8)

"Testing of security functionality shall be carried out during development."

Implementation guidance

Security testing should, of course, be carried out prior to deployment (see 2.10.2.9). In order to ensure that vulnerabilities and inappropriate functionality (e.g. Trojans) are removed from code as soon as possible, and not left until the end of the development process, systems should also be tested on an ongoing basis. Testing may include vulnerability scanning, penetration testing, automated source code testing, formal methods analysis and manual code review, as relevant and appropriate.

Auditing guidance

The auditor should check whether system testing records exist of testing of systems throughout their development. The frequency of testing should have been determined by a risk assessment during the design phase, and should be revisited if there are issues found resulting from insufficient testing. Tests may be performed by the team carrying out development, in the early stages of work.

2.10.2.9 System acceptance testing (ISO/IEC 27001, A.14.2.9)

"Acceptance testing programs and related criteria shall be established for new information systems, upgrades and new versions."

Implementation guidance

The introduction of new systems, upgrades and new versions of software needs to be carefully managed to ensure no service loss or data compromise occurs where operational systems are concerned.

New systems can bring in unrecognised vulnerabilities. It is important that acceptance criteria are established, and that these criteria are checked and that testing is carried out before the new system is introduced to ensure that vulnerabilities are identified and eliminated. This control is also applicable where new subsystems and devices are being introduced, and where changes are being made to existing systems.

In particular, any adverse effects on existing systems should be identified and brought under control before acceptance into operational service. It is especially important that new facilities connected to the communications network are properly secured before connection. All levels of acceptance testing should be documented and signed off by an appropriate role.

For major new developments, the operations function of the organisation and other relevant stakeholders should be consulted at all stages in the development process to ensure the practicality of the proposed security design. Involving users is important, as they need to operate the system securely as part of their work. Appropriate tests should be carried out to confirm that all acceptance criteria are fully satisfied.

Auditing guidance

The auditor should look for clear acceptance criteria for security that need to be fulfilled before implementing new or upgraded systems. New systems or processes need to be thoroughly tested before operational use. What plans are there? Have they been reviewed for adequacy? How have the results been recorded?

Adequate testing usually means more than just testing new functionality. Has sufficient consideration been given to regression tests? Has the system response to defective data or false user input been covered? Are access controls fully secure? What about other security controls?

Training may need to accompany system acceptance, to ensure that the system is used securely. Has this been catered for? Who has determined its adequacy? Have all necessary personnel been involved, both in the preparation and receipt of training? Who authorises final acceptance before operational use? Check this is defined and recorded.

Has user testing investigated whether, and how, users may seek to bypass security measures?

2.10.3 Test data (ISO/IEC 27001, A.14.3)

"Objective: To ensure the protection of data used for testing."

2.10.3.1 Protection of test data (ISO/IEC 27001, A.14.3.1)

"Test data shall be selected carefully, protected and controlled."

Implementation guidance

Test data should normally be fictitious, but there are occasions when operational, tokenised or anonymised operational data needs to be used. The organisation is vulnerable to breaches of confidentiality when such data is used and it should avoid such use as far as possible, and control and protect the data to at least the same extent as operational data in an operational system if its use in tests cannot be avoided.

The use of operational data in testing should be recognised in risk assessments, and the higher security requirements noted in test plans. Each instance of use should be authorised, and the same level of access controls as applied for the operational system should be in place. When the tests have been finalised and the data are no longer needed, they should be erased immediately and securely from the test system(s).

Auditing guidance

The auditor needs to confirm, by means of appropriate evidence, that data used for testing is properly controlled. Tests should be reproducible and the data used should be distinct and available for any re-testing. Use of live data for testing should be discouraged and, if used, it should be modified to remove any personal or otherwise sensitive information. This is not always completely possible – or not possible to completely assure – so check how this is handled and how any results of the testing, both data files, logs, debug files, caches and recorded results, are protected. There may also be legal requirements relating to the use of personal data for testing (e.g. a requirement to anonymise the data, or get explicit permission from the people to whom it pertains) that should be fully explored and satisfied.

The use of live data for testing should be properly authorised on each occasion – check that this is done. Check also that there is a method to completely remove any data put into live databases during testing, and verify the access control in place. Access to test application systems should be as tightly controlled as access to operational systems. All actions carried out during the tests should have been logged – check that these logs exist, and use them as evidence of how test data is handled and protected.

2.11 Supplier relationships (ISO/IEC 27001, A.15)

2.11.1 Information security in supplier relationships (ISO/IEC 27001, A.15.1)

"Objective: To ensure protection of the organization's assets that is accessible by suppliers."

2.11.1.1 Information security policy for supplier relationships (ISO/IEC 27001, 15.1.1)

"Information security requirements for mitigating the risks associated with supplier's access to the organisation's assets shall be agreed with the supplier and documented."

Implementation guidance

There are several ways in which suppliers can cause risks to the organisation's information and information processing facilities. This might be via physical access as well as via logical access, for example using online connections or remote working with the organisation's assets. It can also be by incidental exposure to sensitive material, such as papers on desks while someone is watering plants in an office.

If the organisation intends to allow suppliers to have access to sensitive data or to secure environments, it needs to have an overarching policy covering what suppliers must and must not do. It should also have a master list of suppliers. The risks that apply to each working relationship with suppliers need to be identified and assessed.

To manage the implementation of this policy, the organisation should create a standard process and procedure for managing supplier security, tailored to the security level of the information to which the supplier will be exposed. This procedure should take into account that the supplier may itself have other parties to which it has delegated certain activities (see 2.11.1.3).

Auditing guidance

The auditor should confirm that there are a set of principles and a top level policy and procedure for handling supplier security. ISO/IEC 27002, 15.1.1 contains a list of the types of information that can be in the policy. The auditor should also check that risk assessments are carried out to assess the risks related to suppliers.

Ask for a master list of suppliers. This should indicate the security level of the information to which each supplier is authorised to be exposed, and should also reference the specific agreements made with that supplier (see 2.11.1.2).

2.11.1.2 Addressing security within supplier agreements (ISO/IEC 27001, 15.1.2)

"All relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organisation's information."

Implementation guidance

The same level of security as that which applies to the organisation's staff should be applied to supplier staff, including user IDs, passwords, data access controls, physical security, etc. This should be ensured when supplier personnel access assets on the organisation's site, as well as when a supplier processes information or uses information processing facilities on its site. What needs to be taken into account when developing the agreement that regulates supplier access is that the organisation is not in charge of the supplier's management, personnel controls, IT, and security policies and practices. The other organisation may also have a quite different set of ethics and business culture. These differences should be identified and assessed, perhaps before deciding to do business with the other party.

The key control that needs to be in place before anything else happens is a contract or agreement. This should spell out in appropriate detail the controls to be exercised. It should also provide extensive details on the facilities that each party will make available to the other, and the security controls to be put in place, as well as which entity is responsible for which security controls. Suppliers should not be given access to the organisation's information and/or information processing facilities until the appropriate controls have been implemented.

The implementation guidance of ISO/IEC 27002, 15.1.2 provides a list of suggested items to put in place as required by the results of the risk assessment. The contract or agreement clauses may also specify conformance with ISO/IEC 27001, or even certification, again depending on the requirements. Ensure that the signatories on both sides are properly identified and authorised.

The security documentation should include copies of all relevant contracts or agreements, and possibly several additional documents describing specific elements of the relationship. It might be helpful to include security controls, policies and procedures in a security plan that can be given to the third party. Any deviation from these requirements should be justified and documented.

Auditing guidance

The auditor can check the results of the risk assessments that the organisation has carried out for its suppliers. Risks can come from remote access to mainframe or server software, the Internet connection, badly isolated intranets or physical access to secure areas.

The auditor can also check that all security requirements and risks for supplier arrangements are identified and addressed in a formal contract or service level agreement between the two organisations. The implementation guidance of ISO/IEC 27002, 15.1.2 provides a list of issues that should be considered for inclusion in such agreements. The auditor can check that the organisation has adequate procedures in place to ensure that all security issues are addressed before giving supplier access to any of the organisation's assets.

It is also necessary to ensure that suppliers are actually aware of all the security arrangements they have to put in place, and understand and agree to these arrangements. An approach could be to ask the supplier for their ISMS certification. The auditor could also ask the organisation how the agreements cover the situation where a supplier does not perform in accordance with the expectations of the organisation. The auditor can check that all relevant liabilities and potential disruptions have been identified and are addressed appropriately. Provisions need to be in place for modifying agreements, when necessary, as well as for their termination.

2.11.1.3 Information and communication technology supply chain (ISO/IEC 27001, A.15.1.3)

"Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain."

Implementation guidance

Having a relationship with a supplier (e.g. a product vendor or cloud hosting provider) usually means that, through them, the organisation is exposed to risks posed by other suppliers to that first-party supplier. For example, the vendor of a piece of technology may outsource maintenance to another company that operates as a franchise. When specialist advice is required, the franchise staff may then bring in staff from the manufacturer. The manufacturer will have accounting and HR software, as well as possibly be using cloud services for storage of customer data – the so-called ‘supply chain’ is really a multiply connected network. Each of these entities may be able to make mistakes or carry out deliberate actions that affect the organisation’s security.

This network of suppliers should be managed via agreements with the supplier(s) with which the organisation has a direct contractual relationship. ISO/IEC 27001, A.15.1.3 contains a list of considerations to be taken into account when designing a supplier agreement to manage this ‘inherited’ risk. The organisation should also actively investigate its ICT supply network to a level of detail commensurate with the risk, and identify any increased areas of concern.

One key area is the question of how these suppliers change, and how they are chosen. Each entity in the network may do this differently, producing possible gaps in security.

Auditing guidance

The auditor can ask to review supplier agreements, and compare them against the list in ISO/IEC 27001, A.15.1.3. Are all relevant topics taken into account? Has a risk assessment been carried out on all supply chains? Have appropriate controls been identified and implemented? How is their effectiveness assessed? The auditor can look for unexpected suppliers, such as those related to disposal of sensitive waste, server room maintenance or laboratory cleaning.

2.11.2 Supplier service delivery management (ISO/IEC 27001, A.15.2)

"Objective: To maintain an agreed level of information security and service delivery in line with supplier agreements."

2.11.2.1 Monitoring and review of supplier services (ISO/IEC 27001, A.15.2.1)

"Organizations shall regularly monitor, review and audit supplier service delivery."

Implementation guidance

Once the operations of the service provider have begun, it is up to the organisation to ensure that the services delivered continue to conform to the requirements specified in the contract. One of the most important means to ensure that security controls, service definitions and service delivery levels are being provided as specified by the supplier (see 2.11.1.2), is to monitor and review these controls and services. This can include checking fairly obvious issues, such as the availability levels of the provided service, or it can be something more involved, such as the technical security controls in the supplier's environment. The organisation should put procedures in place to monitor service delivery and to review service reports produced by the supplier.

ISO/IEC 27002, 15.2.1 provides a list of activities that the supplier service management process should include.

Another issue to be monitored and reviewed is what the supplier does to manage information security incidents. It should be stated in the contract or agreement that the supplier provides the organisation with notifications about information security incidents, and the organisation should have assigned responsibilities, sufficient resources and procedures in place to review these reports, and initiate its own incident management process if required. Incident management reports should also be reviewed to verify that the supplier handles these events sufficiently well. The same is true for any other problems, faults, events, etc., that might happen and could have an impact on the organisation's information or the services provided to the organisation.

If the agreement or contract allows audits to take place, then this is another way the organisation can verify that the supplier acts in accordance with the contract or agreement. The organisation should have the following in place to ensure that the relevant information is obtained:

- ensuring that all relevant reports, records, audit logs, etc., should be provided by the supplier;
- having procedures should be in place, responsibilities assigned and sufficiently qualified personnel and other resources available to review the reports, records and logs should be available; and
- the ability to be able to react to any findings, nonconformities or security problems the supplier has not adequately dealt with.

Auditing guidance

The auditor can look for evidence that the organisation is receiving all relevant reports, records and logs of services provided, and that it has procedures in place to review these. To check this, the auditor can ask for records or reports, and for any records that are produced as a result of the reviewing activity of the organisation. These documents should also show that relevant activities, for example as listed in ISO/IEC 27002, 15.2.1, are taking place.

In addition, the auditor can look at records of actions the organisation has carried out to check the security controls, service definitions and service delivery levels, to ensure the procedures are applied correctly. The organisation should also have procedures in place to react to any nonconformity of the supplier with the requirements specified in the contract or agreement.

The auditor can also confirm that the organisation has assigned responsibilities for monitoring and reviewing activities, and that the people carrying out reviews have sufficient skills and time to carry them out.

If the agreement or contract allows the organisation to carry out audits of the supplier, it should be established, for example by looking at audit reports, that the organisation does audit the supplier, and that any findings are actively communicated to the supplier, followed up and resolved satisfactorily.

2.11.2.2 Managing changes to supplier services (ISO/IEC 27001, 15.2.2)

“Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks.”

Implementation guidance

It is usual that changes occur in the provision of services by suppliers. A list of possible types of changes is given in ISO/IEC 27001, 15.2.2. The organisation should have procedures in place to respond to, and to actively manage, these changes. This includes reassessing the risks involved in the new/changed arrangements (see 2.11.2.1), negotiating variations to changes and possibly modifying supplier contracts or entering into new agreements or contracts. It is important that this takes place following a well-defined procedure, and with appropriate authorisation.

Particular care should be taken in the case of changes that affect risk levels. If something has changed within the supplier, or in the technology used to provide the services, this should initiate a review of the security controls in place, resulting in changes to existing controls as required to maintain information security risk at an acceptable level.

Auditing guidance

The organisation should have procedures in place to manage any changes to services provided by suppliers. The auditor should check that these procedures include reassessing the risks, taking account of the possibly changed business requirements and the systems involved. The auditor should also check that the process requires management approval before any changes are made, and that all relevant stakeholders, for example roles with responsibility for legal matters, are given the opportunity to review changes to the contract or agreement.

2.12 Information security incident management (ISO/IEC 27001, A.16)

2.12.1 Management of information security incidents and improvements (ISO/IEC 27001, A.16.1)

“Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.”

2.12.1.1 Responsibilities and procedures (ISO/IEC 27001, A.16.1.1)

“Management responsibilities and procedures shall be established to ensure a quick, effective, and orderly response to information security incidents.”

Implementation guidance

Information security incidents can result in breaches of confidentiality, failure of integrity of equipment and data, and loss of availability. They are usually preventable and provide a valuable opportunity to improve procedures and processes to prevent them occurring again. Examples include fire or flood, electrical failure, hardware breakdown, failed software, virus infection, unauthorised access (actual or attempted) to controlled premises or to computer systems, corrupted or lost data, misdirected emails and failure of any security control.

The organisation should have procedures in place to ensure an orderly and effective reaction to reported information security events and weaknesses. The procedures should ensure that all reported events are reviewed and investigated where appropriate, that recovery procedures are triggered and that roles of suitable seniority are involved in reviews. ISO/IEC 27002, 16.1.1 provides a list of measures that should be applied to properly manage information security incidents.

Auditing guidance

The auditor should check that information security incident management procedures are in place, and that they are compatible with likely reporting scenarios, e.g. as described in ISO/IEC 27002, 16.1.2. They should also check that all reported information security events and weaknesses are reacted to appropriately. ISO/IEC 27002, 16.1.1 describes the procedures that should be in place to handle and recover from system failures, errors, security breaches, etc., including contingency arrangements and auditing activities.

2.12.1.2 Reporting information security events (ISO/IEC 27001, A.16.1.2)

“Information security events shall be reported through appropriate management channels as quickly as possible.”

Implementation guidance

If information security relevant events occur without being reported and responded to, they might cause more damage than necessary and present a lost opportunity to prevent recurrence. Failure to report events also gives a false sense of security and can bias risk assessments. Without a reporting procedure, even a major event might not find its way to those responsible for investigation and recovery until serious losses have been experienced. Minor events might also be reacted to and recovered from without a weakness in control being recognised and corrected.

The definition of an information security event is often difficult in practice, and clear guidance and training is required to ensure that all staff can recognise one when they see it. In plain terms, an information security event is anything that could result in loss or damage to information or assets associated with information, or an action that would be in breach of the organisation's security procedures. The organisation should consider listing categories of reportable events, for example, "virus detected on a PC or media, suspicion of misuse of a system (possible hacking), theft, password exposure, unexpected results from system monitoring, non-compliance with procedures or controls, uncontrolled system changes, loss of services, human errors", etc. ISO/IEC 27002, 16.1.2 provides a list of categories of information security events.

Any member of staff could be the first to notice a security event. Early reporting of the event to experienced technical staff can reduce its impact, for example in the case of system misuse. Build a culture of 'no blame' incident reporting. If staff are blamed for their mistakes they will be tempted to cover up the problems. A number of events might already be reportable under the procedures of other departments. Failures of computer and telecommunications equipment, for instance, will be reported to engineers for repair. However, they should also be reported and recorded as information security events (loss of information and service availability). Ensure that there are procedures covering the reporting and investigation of events, and that resolving actions are tracked and reported upon.

Reporting procedures should include standardised forms, and guidance on initial actions to take (or avoid taking). Contact points should be documented and staff made aware of them.

Timescales for reporting are also very important, as customers or legal requirements may state a minimum time for the organisation to notify them after it becomes aware of an incident. The organisation should ensure that sufficiently robust criteria are used to validate an initial report, to avoid false alarms (see 2.12.1.4).

An important consideration is what to report externally, when and to whom. The organisation should define the circumstances that would lead to notification of third parties or the public, based both upon the scope and impact of an incident, and upon the legal and contractual frameworks that are applicable in each of its geographies and to each of its customers.

Auditing guidance

The auditor should confirm that the organisation has appropriate procedures and management channels for reporting information security events. Auditors should check that the procedures deal with all possible events and provide an identified point of contact and sufficient response. If an organisation claims to have had no events to report, and thus the process cannot be demonstrated, it is probably the case that events and problems took place but no one noticed. The absence of reports does not represent a good sign of a well-functioning information security event reporting procedure.

Everyone in the organisation should be aware of their responsibility to report information security events, and they should know who the points of contact are, and what information the reporting form should contain. The auditor should check that the reporting forms are easy to find and fill in, and that they record information useful to the incident management process. The importance of timely reporting should be emphasised in training materials and in the documentation that general staff will have on hand to help them report an incident.

The auditor should check that the definition of what is and isn't an information security event is clearly described, and that staff understand this. It may be useful to ask example questions such as, "Would you consider finding an unattended security safe open a security incident?" and "If somebody reported receiving somebody else's salary slip, would that be considered a security incident?". Obviously, such questions need to be applicable in the environment concerned, but answers from staff can be quite revealing and indicate the general approach to such matters.

Where reports are present, check the reaction to this event. Has it been settled? Have the root causes been investigated? And has the person providing the original report been informed of the outcome (if this is not confidential)? Are procedures in place to address failure to report information security events?

2.12.1.3 Reporting security weaknesses (ISO/IEC 27001, A.16.1.3)

"Employees and contractors using the organization's information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services."

Implementation guidance

Any organisation will always be vulnerable to the exploitation of unrecognised security weaknesses. No system can be 100% secure. Because of their knowledge of how the security controls, systems and software work, many IT staff are in a very good position to recognise security weaknesses. They should be encouraged to report their suspicions, to allow proper investigation and corrective measures if necessary. This is, of course, equally true for any other users – if they observe any suspected security weakness in the information systems they are working with, they should be encouraged to report any such weaknesses immediately.

Procedures should require all users to note and report any observed or suspected security weaknesses in, or threats to, security controls, systems or services. Users should report these matters either to their line management, directly to their service provider or to any other defined point of contact, as quickly as possible. The report should then be recorded and investigated. Users should be aware that they should not try to exploit the identified weaknesses in any way.

Auditing guidance

The auditor should confirm that similar reporting procedures to those for information security events should be in place for suspected or real security weaknesses. The reporting process should be easy to use, supported by a good reporting form making the reporting and provision of relevant information easy, and there should be clearly identified points of contact.

It is important that all employees, contractors and third-party users are aware of the importance of reporting security weaknesses, and that this includes any weaknesses, not just those related to technical equipment – an open window might also be a security weakness. The procedures for reporting should also include requirements for employees to not attempt to exploit security weaknesses, for example to gain unauthorised access – even if the original intent is just to prove the weakness, this might cause serious damage.

2.12.1.4 Assessment of and decision on information security events (ISO/IEC 27001, A.16.1.4)

"Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents."

Implementation guidance

Each event that is reported should be reviewed by the person to whom it was reported (the point of contact) to ascertain its level of impact. This should be used to determine whether the event should be classified as an information security incident, and the decision and supporting justification recorded in the incident reporting system.

This is the initial triage phase of information security incident management, which ensures that the efforts of incident response teams are focused upon the correct events, and that serious incidents are handled promptly. In order to ensure that classification is consistent, the organisation should have an approved classification scale, with appropriate supporting guidance. The scale should be periodically reviewed for clarity, relevance and usefulness, and updated as required. The individuals responsible for triage should have a clear understanding of the organisation's requirements for timely triage, based on its legal and contractual requirements to notify customers/other entities of a breach.

The point of contact may not be the final arbiter of classification. If the organisation has a team that handles information security incidents, they should confirm the initial classification.

Auditing guidance

The auditor should ask for records of incidents and timeline documentation, and check that there is a point where a clear determination is made of whether an event should be classified as an incident. They should ask how this was determined. Guidance documentation should be readily available to all points of contact, and a list of points of contact available to all staff. Points of contact should be aware of how to classify an incident. There should also be a process for notifying points of contact should the guidance change. There should be targets for triage to ensure that people are managing the activity in a timely manner, and these should be consistent with the organisation's stated timescales for notification.

2.12.1.5 Response to information security incidents (ISO/IEC 27001, A.16.1.5)

"Information security incidents shall be responded to in accordance with the documented procedures."

Implementation guidance

Information security incidents should be responded to in accordance with management requirements, and as documented (see 2.12.1.1). ISO/IEC 27002, 16.1.5 provides a list of actions that should be carried out to properly manage information security incidents. The organisation should nominate a point (or points) of contact, to ensure that a clear reporting line is used.

One particularly important consideration with regard to incident response is that it must be decided very early on whether evidence will need to be collected (see 2.12.1.7). This will shape the whole incident response process.

Auditing guidance

The auditor should confirm that relevant activities, such as are described in ISO/IEC 27002, 16.1.5, are properly documented in procedures, that all responsibilities have been identified, that appropriate management control is exercised, and that all information security incidents and their follow-up activities are properly recorded.

2.12.1.6 Learning from information security incidents (ISO/IEC 27001, A.16.1.6)

“Knowledge gained from analysing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.”

Implementation guidance

In addition to detecting and taking action to resolve information security incidents, it is important that the organisation (and the relevant roles within the organisation) learns from these incidents to avoid future problems, or if they do occur again, to ensure they can be dealt with more effectively. This is also part of the “Performance evaluation” and “Improvement” aspects of the ISMS (see ISO/IEC 27001 Clauses 9 and 10), as the evaluation of incidents that have taken place helps to identify where controls do not work as intended, and where improvements are necessary. Learning from information security incidents will provide useful information about actions that need to be taken to enhance security, and suitably anonymised case studies should also be used judiciously in training and awareness programmes.

Auditing guidance

The auditor should review examples of how the organisation has responded to information security incidents, and software and system weaknesses, in the past. They should review how the organisation quantifies and measures incidents, and whether the incident management procedures are appropriate for the incidents that have occurred or are likely to occur in the future.

The auditor should check any claims that an insufficient number of incidents have occurred, or that insufficient information or evidence is available to be learnt from. The auditor should check whether this is a sign that the reporting procedures for information security events and weaknesses are not used, or the process is ineffective. The auditor should carry out a further review in these cases.

The auditor should confirm that a process to react to information security incidents and weaknesses is in place. Such a process should include the implementation of additional controls or procedures to avoid reoccurrences, to limit the damage, collect evidence or to allow a quicker and more efficient reaction in the future. Anonymised incidents should be used in training and awareness programmes to give real-life examples.

2.12.1.7 Collection of evidence (ISO/IEC 27001, A.16.1.7)

“The organization shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.”

Implementation guidance

It is important that an organisation ensures the collection of admissible and complete evidence for any information security incident that is taking place, since very often it is not obvious whether an incident might finally result in a court case or not. The organisation should have guidelines and procedures for the collection of evidence that ensure appropriate admissibility, quality and completeness of the evidence.

Once evidence is collected, it should be managed and stored securely, to guarantee that no one can modify or destroy it without authorisation. It should also be ensured that the evidence is available in a timely manner and in a form that is required by a court. Control 16.1.7 of ISO/IEC 27002 describes the factors that can be taken into account when writing procedures for the collection of evidence.

If the organisation is carrying out any investigative or forensic work, this should only be done using forensically sound copies of any evidence that might be required later, to ensure it can be proved that the actual evidence has not been altered or tampered with.

Auditing guidance

Collection of evidence is important to be able to provide adequate support in legal procedures and actions that might take place as a result of information security incidents, such as a breach of civil or criminal law. The auditor should confirm that the organisation has procedures in place to collect evidence. Auditors should check that these procedures include appropriate considerations, for example those in ISO/IEC 27002, 16.1.7, and that they ensure that:

- the information collected conforms to applicable standards or codes of practice for the production of such evidence to be deemed admissible as evidence; and
- the quality and completeness of such evidence, i.e. the weight of evidence, is appropriate.

Auditors should check where collected evidence is stored, and whether it is possible for unauthorised persons to access, modify or destroy such evidence. In addition, auditors should consider the conditions when the evidence collection process needs to be activated. Collection of evidence should start at an early stage to ensure that no evidence is destroyed or contaminated.

2.13 Information security aspects of business continuity management (ISO/IEC 27001, A.17)

2.13.1 Information security continuity (ISO/IEC 27001, A.17.1)

2.13.1.1 Planning information security continuity (ISO/IEC 27001, A.17.1.1)

“The organization shall determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.”

Implementation guidance

In the case of any serious unexpected event, especially one that affects business continuity, it is important that information security does not ‘fall by the wayside’. If a level of security is necessary when things are going well, then it is also necessary when things are going wrong – unless the organisation wishes to escalate a business continuity event into a combined business continuity event and information security incident.

It is therefore essential that information security is considered and included in the overall business continuity management process. The process that the organisation uses to manage and recover from crises (whether it is called the disaster recovery process, the business continuity process or something else) should have integrated into it the principle that information security remains important in a crisis, and should make this possible. The organisation should identify and document its information security requirements for business continuity. These should be based upon clearly realised and authorised objectives for information security in atypical circumstances.

If the organisation is dependent on the availability and reliability of services provided by a supplier, it should also check the plans that the supplier has put in place to deal with interruptions of its services. The organisation should ensure that the levels of information security provided in suppliers' business continuity arrangements are sufficient for its requirements. It might also be worthwhile testing these situations to know what to expect in an emergency situation.

Auditing guidance

The auditor should confirm that the organisation has a clear statement of its objectives for information security continuity. To support this, the auditor should check that the organisation has documentation that pertains to the management of serious adverse events (by whatever name). There should be a policy statement regarding preservation of information security during the management of, and recovery from, these events. There should be evidence of a risk assessment, leading to a list of requirements for information security during an adverse event.

2.13.1.2 Implementing information security continuity (ISO/IEC 27001, A.17.1.2)

“The organization shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.”

Implementation guidance

Business continuity/disaster recovery plans should be designed to achieve the security requirements that have been identified in the risk assessment (see 2.13.1.1). Control 17.1.2 of ISO/IEC 27002 describes the key elements that should be included in the information security continuity management process.

Both information security specialists and business continuity/disaster recovery specialists should be involved in integrating information security continuity into the plans.

Auditing guidance

The plan for handling adverse events should include information security considerations throughout the process, including within the business impact analysis stage. Auditors should confirm that the scope and details of this plan fulfil the organisation’s information security requirements, and that it has been signed off by management. A helpful list of criteria is given in ISO/IEC 27002, 17.1.2.

Auditors should check that the timescales associated with the plan are sufficient for the business requirements, and that they are realistic.

Staff responsible for managing crises should have access to (and understand) instructions on how information security should be managed. Staff with information security responsibilities should have access to (and understand) instructions on their responsibilities during a crisis.

In addition, the auditor should check that:

- all responsibilities are agreed and assigned;
- all procedures defined in the plans are documented and implemented according to the implementation schedule; and
- all staff are aware of and understand what they are supposed to do in case of emergencies and business interruptions.

Testing of continuity plans is essential, and auditors should determine the testing schedule, which may be defined in the planning framework or in the plan(s) itself. It is unlikely that plans with any degree of complexity will work perfectly first time. Individuals need to follow the procedures to handle the situation effectively, and this approach will only work if it has been practised.

2.13.1.3 Verify, review and evaluate information security continuity (ISO/IEC 27001, A.17.1.3)

“The organisation shall verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.”

Implementation guidance

Whenever anything in the organisation changes, for whatever reason (whether as part of a planned change, a change in external threats or as a result of disaster recovery activities), it is important that the appropriate level of information security is maintained and does not get omitted or left for later. Most importantly, when plans, processes and standards change, information security must also be considered in that particular type of change process. 2.10.2.2 also covers related considerations (change control).

The objectives for information security continuity should be referred to during the change process for any other process or plan, to ensure that the correct level of information security continuity is maintained. The updated process should be checked against the objectives to ensure that they are still met.

Auditing guidance

The auditor should confirm that there is a well-defined plan for review of all proposed changes to policies, processes and standards relating to information security continuity. ISO/IEC 27002, 17.1.3 contains a useful list of activities for the organisation to take; ask for records for relevant activities. The auditor should look for the results of functionality tests. Were any problems encountered, and have these been analysed and corrected?

The auditor should be suspicious of plans that have not been regularly updated. Are there records to demonstrate that these have been reviewed and that changes were not required? The auditor should check that responsibilities for the maintenance and updating of the plans have been defined, and that any changes to the plans can only be made with appropriate authorisation.

2.13.2 Redundancies (ISO/IEC 27001, A.17.2)

“Objective: To ensure availability of information processing facilities.”

2.13.2.1 Availability of information processing facilities (ISO/IEC 27001, A.17.2.1)

“Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.”

Implementation guidance

Availability is a core aspect of information security, along with other attributes such as confidentiality and integrity. In order to ensure availability, it is important to identify firstly what the organisation actually requires in terms of recovery times following failure, whether it can tolerate any loss of availability and what current systems provide. Where these are not in agreement, additional measures (such as redundant equipment) should be implemented to increase availability to match need. Risk assessments of the IT and physical architecture of the facility should be carried out, to identify and manage any increased risks (for example from copying data between mirrored systems in geographically separate locations via public networks).

Auditing guidance

The auditor should request documents detailing availability requirements, risk assessments, information regarding redundant systems, testing records, records of recovery times following unplanned loss of availability and any compensating controls that may have been introduced to address additional risks incurred by the introduction of redundant equipment. The auditor should confirm that the organisation has appropriate redundancy arrangements that are sufficient to meet availability requirements.

2.14 Compliance (ISO/IEC 27001, A.18)

2.14.1 Compliance with legal and contractual requirements (ISO/IEC 27001, A.18.1)

“Objective: To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.”

2.14.1.1 Identification of applicable legislation and contractual requirements (ISO/IEC 27001, A.18.1.1)

“All relevant legislative statutory, regulatory, contractual requirements and the organization’s approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and the organisation.”

Implementation guidance

All statutory, regulatory and contractual requirements should be identified and documented by the organisation to ensure their fulfilment. The organisation should identify the approach that it will take to coordinate and meet these requirements. Especially when thinking of conducting business in other countries, the identification of applicable legislation should be supported by an expert, e.g. a lawyer. Special attention is also required when conducting online business or trading, to ensure compliance with all relevant legislation in the countries involved. As the statutory, regulatory and contractual requirements will change over time, it is important that the organisation has appropriate change control procedures in place that incorporate these considerations.

Auditing guidance

The auditor should inspect the actions that have been taken to identify, document and comply with all applicable statutory, regulatory and contractual requirements. The auditors should check that no applicable legislation, regulations or contracts have been forgotten or missed by mistake. This may require specialist expertise.

The auditor should confirm that the organisation has controls in place to comply with the requirements that it has identified. Responsibilities for these controls should be identified and documented, and those responsible should be aware of their responsibilities. For example, someone should be responsible for keeping the identified statutory, regulatory and contractual requirements up to date, as these will change over time. Changes to requirements should be traceable to changes to implemented controls.

2.14.1.2 Intellectual property rights (ISO/IEC 27001, A.18.1.2)

"Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products."

Implementation guidance

Organisations are vulnerable to failure to comply with restrictions on usage of copyright material. There is a serious risk of legal action being taken against the organisation and individual staff where, for example, software is being used on more than the number of systems it is licensed for.

The organisation should put rules in place for the handling of material, and these rules should take into account all types of restrictions, for example, software or document copyright, design rights, trademarks, patents and source code licences. Staff should be made aware of the rules. For software, it is especially important to make staff aware of these rules, and inventory checks should be carried out at least annually to provide assurance that all software in use (that is, software loaded on the system) is properly licensed. Documentary records should be maintained of the inventory of software on each system (see also 2.4.1.1).

It is also important to note that rules relating to copyright, etc., vary significantly in different countries, so the organisation should take this into account when operating internationally.

Control 18.1.2 of ISO/IEC 27002 provides guidelines on the protection of copyright material. The organisation and all staff should be aware that copyright infringement can lead to legal action that may involve criminal proceedings.

Auditing guidance

Auditors should confirm that the organisation has procedures in place to protect the intellectual property rights of copyrighted information and software. These procedures should describe rules for handling material that is marked as copyright, design rights or trademarks, and employees should be aware of how to handle such material. These rules should address the handling of all copyright material, irrespective of the form it takes. The auditor should confirm that users are aware that any unauthorised use or copying of intellectual property rights material or software might lead to legal action.

There should be strict controls on the use of software and other copyrighted material (for example subscription-based online content) in the organisation. Auditors should investigate what licences have been purchased and how compliance is maintained. Many commercial packages provide licence agreements on the packaging, which comes in various forms – there is no common format for information such as number of users, restrictions to use, etc. – further information must be gathered to check that each software package is being used in compliance with the related licensing agreement.

One way to address these issues is to draw up a table of resources protected by copyright, and then identify the key aspects of each licence, together with a record of actual use. The auditor should look at the use of development tools and libraries. Have these been used correctly? With bespoke software developed for the organisation, look at the development or support contract. Is access to source code provided? Can in-house changes be applied? Are there restrictions on the use or location of the software? Ensure that the responsible personnel in the organisation are fully aware of their obligations regarding software copyright. The auditor should also check a random sample of computers (both workstation and server) for unlicensed material.

2.14.1.3 Protection of records (ISO/IEC 27001, A.18.1.3)

"Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislatory, regulatory, contractual and business requirements."

Implementation guidance

Organisations will have a number of essential documents and records, such as accounting records, database records, transaction logs, audit logs and operational procedures that need to be retained and should be protected from loss, breach of confidentiality or modification. These items should be listed in the asset inventory (see also 2.4.1.1), and appropriate controls selected and implemented to ensure the protection of these records until the end of their retention period. The continued presence of the items should be confirmed by a documented inventory check at least annually.

For example, under various regulations organisations are required to maintain business records of certain types for periods of up to ten years, and an organisation is open to prosecution where this has not been carried out.

When keeping records for such a long time, due consideration should be given to deterioration of the media on which these records are stored, and it should be ensured that tools (e.g. microfiche readers, software and cryptographic keys) are still available, and it is still possible to actually access records up to the end of their retention period. Control 18.1.3 of ISO/IEC 27002 provides further guidance on the protection of organisational records.

Auditing guidance

Records required for legal or regulatory purposes are usually a subset of all the records an organisation will need to keep for business purposes or other reasons. The auditor should confirm that all records required for legal or regulatory purposes (e.g. financial records, customs records, legal records and environmental records) are identified, and that all requirements are complied with.

The exact requirements will vary from country to country, and the organisation needs to be aware of, and comply with, all applicable requirements. The auditor should check that this has been done and verified by the appropriate personnel. The storage arrangements (including security) and the requirements for review and disposal should all be defined in procedures.

There should be an inventory of records, and auditors should check this for accuracy. Some documentation might now be held electronically, either because that was the original format or because they have been scanned. The auditor should check that the organisation has reviewed the legal admissibility of this storage medium and is complying with any additional requirements for preservation of the integrity or availability of these records. The auditor should also check that the organisation has considered the risk of media deterioration and the resulting loss of accessibility of data if electronic storage media are chosen, and that it has measures in place to ensure the availability of the necessary cryptographic keys, if encryption was chosen to protect the records (see also 2.6.1).

2.14.1.4 Privacy and protection of personally identifiable information (ISO/IEC 27001, A.18.1.4)

"Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable."

Implementation guidance

In many countries, legislation or regulation is in place to protect the privacy of personal information. Failure to comply with such legislation can leave the organisation open to prosecution and a fine, or at least to serious loss of image and reputation if it became public. Several laws also specify a number of requirements for the collection, processing, accessibility and protection of personal information in any form. Failure here can also lead to prosecution. Finally, prompt breach notification is a significant requirement in some legislation.

If the organisation stores, processes or transmits any personal data, and if there is applicable legislation or regulations, it should develop and implement a policy that ensures that no requirements are disregarded. An inventory of personal data should be kept, and a role should be given the responsibility for providing guidance to staff and suppliers. Responsibility for handling personally identifiable information should be assigned in a manner that complies with legal and contractual requirements. Procedures are necessary to ensure that changes in the use of personal data are reflected as necessary in the asset inventory. A documented review should be carried out at least annually, and compliance with all requirements stated in the relevant laws or regulations should be ensured.

Auditing guidance

Careful control of personally identifiable information is necessary to comply with the applicable legislation and regulations that might apply. Many countries, for example in Europe, have well-developed data protection legislation. The legislation might also require the organisation to register its use of personally identifiable data. The auditor should confirm that the organisation has identified all relevant legislative or regulative requirements, and has put policies, procedures and controls in place to comply with them. The auditor should also look at the type of data held. Is it necessary? Has it been validated? Is it transmitted or otherwise conveyed outside of the organisation? Who has access to this data, and is it necessary for their job function?

The auditor should check that the organisation monitors changes to requirements in this area – new, tighter restrictions can be introduced with specified periods for compliance. Is there sufficient awareness within the organisation? Are there plans to introduce compliance within the timeframe? Auditors should ensure that they themselves are fully up to date with this area of legislation.

2.14.1.5 Regulation of cryptographic controls (ISO/IEC 27001, A.18.1.5)

"Cryptographic controls shall be used in compliance with all relevant agreements, legislation, and regulations."

Implementation guidance

The legal and regulatory requirements and rules for the use of cryptographic controls, and the effort and resources necessary to comply with them, should be assessed. The results of these assessments should be taken into account in the decision about the use of cryptographic controls. This assessment should not only include the laws and regulations applicable for encryption controls, but also the legal environment for the use of digital signatures and other electronic communications. Because of the differences and ongoing changes in the legal situation of various countries, special care should be taken to ensure, and maintain, compliance with legislation in all those countries that are involved in business or travel. ISO/IEC 27002, 18.1.5 lists items that should be taken into account when creating policies and procedures.

Auditing guidance

The organisation should present to the auditors the actions they have taken to identify applicable legislation and regulations for cryptographic controls, and the legal advice they have taken where necessary to ensure compliance. The controls that are taken to fulfil these requirements should be documented, implemented and maintained. The auditor should check that the implementation of the policy for the use of cryptographic controls as described in 2.6.1.1 is commensurate with the legal requirements identified. The auditor should also find out how the organisation is tracking changes to legislation and regulations in the jurisdictions within which it operates.

2.14.2 Information security reviews (ISO/IEC 27001, A.18.2)

“Objective: To ensure that information security is implemented and operated in accordance with the organizational policies and procedures.”

2.14.2.1 Independent review of information security (ISO/IEC 27001, A.18.2.1)

“The organization’s approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) shall be reviewed independently at planned intervals or when significant changes occur.”

Implementation guidance

As with all business activities, the organisation’s approach to information security and its implementation should be reviewed from time to time to ensure that everything is still suitable and effective. Additional reviews should be carried out when major changes are planned, or major unplanned changes have occurred. These additional reviews should be initiated by a clear trigger that is linked to the organisation’s change and incident management processes.

The results of these reviews should be reported to management. Each review should be carried out by an independent body (either within the organisation or outside), to provide assurance to senior management that the organisation’s ISMS practices are adequate and effective.

‘Independent’ does not exclude an internal review, provided that the reviewer has appropriate independence from the management and staff being reviewed. An internal audit department would be appropriate. However, a small organisation might find it necessary to use an external party for the review. A certification audit undertaken by a suitably accredited organisation would also satisfy the requirements of this control.

All results of independent reviews should be recorded, as well as any corrective action that is taken if the independent review identifies areas for improvement.

Auditing guidance

It is important for the auditor to check that independent reviews of the organisation's approach to information security and its implementation are taking place, and that they are carried out by an independent party. Without this, objectivity cannot be achieved. A third-party audit satisfies this requirement. In cases where third-party audits are not being performed, the requirement for independence can be satisfied by review via internal auditors, management or other bodies external to the security practitioners/implementer teams.

Check the audit schedule, but also the process for identifying the need for a supplementary audit when a major change is planned. What are the criteria in use? Ask for examples showing where this has occurred.

The auditor should check the records of the independent reviews, and should verify that identified corrective actions have been implemented and have had the desired effect. The results of other reviews, such as those described in 2.1.1.2, should be taken into account.

2.14.2.2 Compliance with security policies and standards (ISO/IEC 27001, A.18.2.2)

“Managers shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.”

Implementation guidance

If the organisation is expending effort and resources in implementing controls, mechanisms should ensure that these controls are working effectively, as, for example, required by ISO/IEC 27001. Managers should review compliance in their area of responsibility with security policies, controls and standards. This can take place through a formal review, and/or through spot checks that can occur at any time during normal work. A combination of both techniques is possibly most successful.

Managers should react to identified non-compliances as described in control 18.2.2 of ISO/IEC 27002. A documented record of each review should be maintained, noting non-compliances, agreed action and follow-up. The managers should also report the results of their reviews into the internal review process (see also 2.14.2.1).

Auditing guidance

To determine the degree to which security policies and procedures are being complied with, the auditor should confirm that management has procedures in place to regularly review this compliance appropriate to their area of responsibility. These reviews should be fully documented, followed up to ensure resolution of non-compliant items and reported on to the internal review (see also 2.14.2.1), and as required to senior management.

Managers should also have procedures in place to respond to non-compliance. These procedures should ensure that the root cause(s) for the non-compliance are identified, that any necessary actions are taken to avoid recurrence of the non-compliance and that the appropriate corrective actions are identified and successfully implemented.

2.14.2.3 Technical compliance review (ISO/IEC 27001, A.18.2.3)

“Information systems shall be regularly reviewed for compliance with the organization’s information security policies and standards.”

Implementation guidance

The complexity of information systems, for example, servers, networks and firewalls, means that despite best intentions they might still be in an insecure state. Organisations may remain vulnerable to attacks and misuse, despite management believing that they have implemented the necessary controls. A full technical review should be carried out at suitable intervals, determined by risk assessment, to detect any technical nonconformities.

Operational information systems require skilled analysis, aided sometimes by tools that automate certain types of tests. Indeed, the use of such programs allows some tests to be carried out more frequently, as well as more swiftly, and with a lower chance of manual input errors.

These checks should only be carried out by, or under the close supervision of, competent, authorised persons. The integrity and availability of systems under test could be jeopardised should an insufficiently skilled person attempt this work. In addition, certain types of compliance tests, such as penetration testing, can result in criminal charges (related to computer misuse) if accidentally directed at the wrong systems. Also note that some testing tools may be identified as attack tools, since their purpose may be to try to compromise a system, and their use by unauthorised users should be treated as an information security incident. Access controls should generally prevent unauthorised persons from carrying out technical compliance reviews (see 2.5.1.1). The installation of tools used for testing should be strictly controlled (also see 2.5.4.4 and 2.8.6.2).

Reviews should be planned and documented. Results, nonconformities, actions and follow-up activities should be recorded and traceable to each other, so that, for example, a non-conformity can be traced to the action that was initiated to correct it, and there is also a record of the actual impact of that action. ISO/IEC 27001, Clause 10.1 requires non-conformities to be identified and rectified. It also requires the organisation to look out for the chances of similar issues in other areas.

Auditing guidance

The auditor should confirm that the organisation has scheduled checks in place to ensure that its information systems conform to security implementation standards. There should be a plan for technical conformity checking, showing what needs to be covered, and the frequency and methods employed. It is important that this type of conformity checking is performed by suitably competent and authorised personnel.

Records of checks should be traceable to findings and remedial actions, and finally to testing to ensure that the remedial actions had the desired effect. Ask if the organisation looks for patterns in issues and how it identifies and follows them up. A technical issue found on one system could exist on many more.

If a tool is used, the auditor should check what aspects of the information systems are actually being reviewed – it could purely be monitoring or conducting an audit of facilities. Has it been validated in any way? Check the individuals completing or reviewing the reviews, as compliance can only be effectively assessed by technically competent personnel. Personnel carrying out reviews should also have been authorised to do so.

FURTHER READING

IT Governance Publishing (ITGP) is the world's leading publisher for governance and compliance. Our industry-leading pocket guides, books, training resources and toolkits are written by real-world practitioners and thought leaders. They are used globally by audiences of all levels, from students to C-suite executives.

Our high-quality publications cover all IT governance, risk and compliance frameworks and are available in a range of formats. This ensures our customers can access the information they need in the way they need it.

Other resources you may find useful include:

Security Risk Management for ISO 27001/ISO 27002, third edition by Alan Calder and Steve G Watkins,
www.itgovernancepublishing.co.uk/product/information-security-risk-management-for-iso-27001-iso-27002-third-edition
•*Information Security A Practical Guide – Bridging the gap between IT and management* by Tom Mooney,
www.itgovernancepublishing.co.uk/product/information-security-a-practical-guide
•*ISO 27001 2013 ISMS Documentation*
www.itgovernancepublishing.co.uk/product/iso27001-2013-isms-standalone-documentation-toolkit

For more information on ITGP and branded publishing services, and to view our full list of publications, visit

To receive regular updates from ITGP, including information on new publications in your area(s) of interest, sign up for our newsletter at

Branded publishing

Through our branded publishing service, you can customise ITGP publications with your company's branding.

Find out more at

Related services

ITGP is part of GRC International Group, which offers a comprehensive range of complementary products and services to help organisations meet their objectives.

For a full range of resources on information security visit

Training services

The IT Governance training programme is built on our extensive practical experience designing and implementing management systems based on ISO standards, best practice and regulations.

Our courses help attendees develop practical skills and comply with contractual and regulatory requirements. They also support career development via recognised qualifications.

Learn more about our training courses in information security and view the full course catalogue at

Professional services and consultancy

We are a leading global consultancy of IT governance, risk management and compliance solutions. We advise businesses around the world on their most critical issues and present cost-saving and risk-reducing solutions based on international best practice and frameworks.

We offer a wide range of delivery methods to suit all budgets, timescales and preferred project approaches.

Find out how our consultancy services can help your organisation at

Industry news

Want to stay up to date with the latest developments and resources in the IT governance and compliance market? Subscribe to our Weekly Round-up newsletter and we will send you mobile-friendly emails with fresh news and features about your preferred areas of interest, as well as unmissable offers and free resources to help you successfully start your projects.