**The ISMS Manual**

Lancashire County Council's ISMS documentation is contained within or referenced from the ISMS Manual and it consists of policy level ISMS documents and their annexes as follows.

**Part 1**

Section 1 Information Security Management System Overview
Section 2 Scope of the ISMS
Section 3 Information Security Policy
Section 4 Information Management System Policy
Section 5 Operation of the Information Security Management System
Section 6 Risk Management Report
Section 7 Statement of Applicability
Section 8 Approvals
Section 9 Change History

Appendix 1 Corporate Risk Management Strategy
Appendix 1a Update: Review of Lancashire County Council Risk Management
Appendix 2 Corporate Information Risk Assessment
Appendix 3 Security relevant legislation and regulation
Appendix 4 Reporting & effectiveness measures

**Part 2**

Section 1 Risk Treatment Plan
Section 2 Statement of Applicability Control objectives
Section 2a Table mapping ISO27001 controls to Information Security Forum framework
Section 3 Roles and Responsibilities for information security
Section 4 Training and awareness plan
Section 5 Resourcing plan

**Part 3**
Guidelines and procedures

**Part 4**
ISMS records

**SECTION 1**

**INTRODUCTION**

This manual provides the framework for the policies and procedures which Lancashire County Council has adopted to implement an information security management system which complies with ISO/IEC 27001:2005 (“the ISMS”)].

This manual explains the County Council’s approach to information security and contains both the management policy statement on information security in the Organisation and, because it identifies which of the controls identified in Annex A of ISO27001:2005 apply within the County Council, it is also Lancashire County Council’s Statement of Applicability.

Issue of this manual is authorised by:

Signature of [the Chief Executive]

On:

**OVERVIEW**

**The Information Security Management System (ISMS)**

The County Council has decided to implement a framework across the whole Authority, for managing information security risks in a consistent and demonstrable way.

A range of factors led to the decision and among the more significant are:

- Corporate Governance and the need to be able to demonstrate management control
- Partnership working
- Risk reduction
- Legal compliance with, principally , the Data Protection Act
- Enable shared services

An approach which uses a corporate framework is appropriate in the current circumstances, as the County as a whole, as opposed to individual Directorates, is viewed as the relevant entity when considering most of the factors listed above. There are also sound practical reasons, relating to consistency and economy, for following this approach.

The County has aspired to comply with the British Standard BS7799 Code of Practice for Information Security Management. The nomenclature of this standard has changed and now the standard to which compliance is sought is known as BS ISO/IEC 27001:2005 (or 27001 for short). This defines the specification for and Information Security Management System.

The ISMS is designed to ensure the selection and operation of adequate and proportionate security controls that protect information assets and give confidence to interested parties. The 27001 standard specifies how the process of achieving an ISMS should be established, maintained and documented.

There are two standards of compliance with ISO27001; certification and best practice. Certification involves an external auditor and is expensive & difficult. Best practice compliance omits the audit stage but to be claimable to an external party, demonstarble compliance with Clauses 4-8 of the standard are mandatory. Exclusion of controls found to be necessary to deal with acknowledged risks must be explicitly accepted by an accountable person.

The ISMS specified by the 27001 standard may be briefly outlined as follows.

The Standard follows a Plan-Do-Check- Act approach common in International Standards. In this context it means

- Understanding security requirements and setting policy and objectives
- Implementing & operating controls to manage risks in the context of the business
- Monitoring & reviewing the performance and effectiveness of these controls
- Continual improvement based on objective measurement/

In this standard the Clauses 4-8 cover these areas, hence their mandatory nature.

The process of working through the clauses produces outputs as follows:
Clause 4

- A defined scope for the ISMS
- An ISMS policy which includes and Information Security Policy
- A defined risk management approach to information security which aligns with the overall approach of the organisation to risk assessment.
- Selection of controls objectives and controls for the treatment of risks using as a starting point controls presented in the standard as good practice
- Management approval of residual risks
- Management approval to operate the ISMS

- A Statement of Applicability which details the control objectives and controls chosen by the organisation. This may exclude suggested control and may include additional controls. It is a summary of decisions about risk treatment
- A risk treatment plan (Action plan)
- Monitoring and reviewing the ISMS
- Maintaining and improving the ISMS
- Maintaining documentation

Clause 5

- Demonstration of management commitment
- Provision of resources
- Training, awareness and competence

Clause 6

- Internal audits of ISMS

Clause 7

- Management Review of ISMS

Clause 8

- Corrective action to improve ISMS

**Implementation of controls - overview**

The diagram overleaf illustrates the overall process for implementing security across the County.

Policy will be set by the CIM&SG and this will consist of a security policy and the adoption of the process described in the ISO27001 for risk management. The process is continually reviewed.

Risks will be addressed by the adoption of a standard framework of control objectives representing good practice which will be applied to critical information assets (applications, networks etc), as defined, by the owners of those assets. Assets may be significant to a service or they may be grouped at service level. Risks will be managed at the asset level through a standard process involving standard guidance on how to meet control objectives.

The Corporate information Security Manager will own the asset level risk assessment process, provide advice and support and receive reports about security incidents which may occur.

## 2. Scope of the ISMS

This ISMS applies to all information assets used or supported by Lancashire County Council in the course of its business. In the main this refers to the information and record keeping systems of the five Directorates and the three Direct Service Organisations but the specific areas covered by the ISMS are as follows.

**Areas covered by this ISMS:**

- Corporate network and all assets connected to it including Pensions Scheme
- All hardware software and information records held by employees or agents of Lancashire County Council for Lancashire County Council business purposes
- People's Network
- The LGFL network
- Shared sites where facilities are supported by Lancashire County Council.
- Facilities owned by Lancashire County Council and connected to its networks but operated from the premises of other organisations.
- Privately owned equipment used in the course of employment with the County Council
- The Contact Centre
- Telephony network

**Areas not covered by the ISMS**

- LCDL
- Organisations for which Lancashire County Council is merely the accountable body
- Schools

The County Council is a local authority with particular functions defined by statute. Principal among those functions is the delivery of services such as Education, Social Services and Highways. Services are now delivered through multi-agency working mainly through the Local Area Agreement. As a Public Authority it is not a profit making body although some services are traded.

Specific legislation such as the Data Protection Act places particular compliance requirements on the County Council which may affect the operation of the ISMS. Under the Civil Contingencies Act 2004 County Councils are Category 1 Responders and as such must assess the risk of an emergency occurring and maintain plans for the purposes of responding to such an emergency as it would affect the operation of the County Council.

The County Council has a legally defined geographical area of jurisdiction and has responsibility for delivery of services within that area. Almost all activities are confined to that area but occasionally some activities are carried on outside the County boundary

The assets covered by the ISMS include

- Information holdings in whatever form. This includes paper filing systems, paper records, video, audio and static images.
- Software assets including application and other software
- Physical assets including equipment and media
- Services
- People, their qualifications, skills and experience
- Intangibles such as image and reputation

The technology infrastructure employed by the County Council consists of a corporate network which links a centralised data centre with decentralised desktop and mobile facilities. There is a strong trend towards remote working involving the increased use of laptops and PDA's to be used in the field, at touchdown centres, at home or "hot desks".

Under multi-agency arrangements non-employees are often required to access the corporate network and sites shared with other organisations are becoming more common.

## SECTION 3 INFORMATION SECURITY POLICY

The ICT&EGSG and CMB have approved and authorised an information security policy for the County Council which is reproduced below as part of this manual. A current version of this document is available to all staff and contractors on the corporate intranet and to external parties. The development and maintenance of the information security policy is carried out under the PDCA process described in section 4 of the Information Security Manual.

### INFORMATION SECURITY POLICY

Lancashire County Council is committed to preserving the confidentiality, integrity and availability of all its physical and electronic information systems and records in order to provide assurance that the organisation manages information risk

- so that the needs of service users and citizens and the requirements of corporate governance and are met;
- to establish confidence that partnership arrangements involving sharing and exchange of information are legal and secure
- to establish that designed and implemented security features are effective and correct
- to provide confidence that services & products offered by third party suppliers of information security assurance are adequate and fit for purpose;

Information and information security requirements will continue to be aligned with LCC goals and the Information Security Management System (ISMS) is intended to be an enabling mechanism for information sharing, for electronic operations, remote and distributed working, for e-commerce and for reducing information-related risks to acceptable levels.

Control objectives for information security are contained in the Manual and are supported as appropriate by specific, documented policies and procedures. In particular, it is the Policy of Lancashire County Council to ensure that

- Information will be protected against unauthorised access
- Confidentiality of information will be assured[1]
- Integrity of information will be maintained[2]
- Regulatory and legislative requirements relevant to information systems will be met[3]
- Business Continuity Plans will be produced, maintained and tested[4]
- Information Security Training will be available to all staff
- All breaches of Information Security, actual or suspected, will be investigated and reported to the Corporate Information Security Manager

All employees and elected Members of the County Council and other non-employees granted access as users of LCC information systems are expected to comply with this policy and with the ISMS that implements this policy as appropriate to their work roles. All staff, and certain external parties, will receive appropriate training.

---

[1] The protection of sensitive or valuable information from unauthorised disclosure or intelligible interruption or theft

[2] Safeguarding the accuracy and completeness and authenticity of information by protecting against unauthorised modification of information and systems

[3] This includes, among others, the requirements of the Data Protection Act and external requirements such as NHS Codes of Connection

[4] This will ensure that information and vital services are available in a useable form to users when and where they need them

It is a key principle of this policy that all information assets (as defined by the ISMS) should have a nominated “owner”. For the purposes of the ISMS assets are defined as

- critical business applications and filing systems and the information held thereon,
- installations
- networks
- systems under development.

This information security policy was approved by the CMB on [date] and is issued on a version controlled basis under the signature of the [CEO]

Signature: Date:

## SECTION 4 Information Management System Policy

The ISMS is the Information Security Management System, of which this policy, the information security manual ("the Manual") and other supporting and related documentation is a part, and which has been designed in accordance with the specification contained in ISO/IEC 27001:2005

Lancashire County Council is committed to achieving best practice compliance with ISO/IEC 27001:2005. The ISMS is subject to continuous, systematic review and improvement and will be reviewed to respond to any relevant events or annually, whichever the shorter.

### Status and Scope of the ISMS

Lancashire County Council's current strategic business plan and risk management framework provide the context for systematically identifying, assessing, evaluating and controlling information-related risks through the establishment and maintenance of a corporate Information Security Management System.

The ISMS Manual sets out how information-related risks are controlled. The Corporate Information Security Manager is responsible for the management and maintenance of the manual and supporting documentation. Additional risk assessments may, where necessary, be carried out to determine appropriate controls for specific risks.

To ensure that the County Council benefits from its adoption of this framework, it is essential that the requirements of the manual are implemented.

Compliance with the ISMS policies and guidance is mandatory on all staff (with the exception of schools) and associated individuals within the scope of the ISMS irrespective of their Directorate, Direct Service Organisation or role in the County Council. Any member of staff who fails to comply may be subject to disciplinary action under the County Council's Disciplinary Policy.

It is the responsibility of Chief Officers and DSO Managers (or their specifically nominated representatives) to ensure that staff are made aware, as appropriate to their work role, of the existence and content of the ISMS and that all staff with responsibilities for handling information are fully acquainted with them

### Internal sponsorship of the ISMS

Lancashire County Council has established the CIM&SG, chaired by a member from the ICT&EGSG and including the Corporate Information Security Manager and other Directorate representatives to support the ISMS framework and to periodically review the security policy. All changes to the information security manual are therefore subject to approval by the County Council's CIM&SG.

### Definitions

Where terms which are used in ISO27001:2005 are used here, the definitions provided in clause 3 of that standard are applied. Where terms are defined in ISO17799:2005 but not in ISO27001:2005, the ISO17799:2005 definitions are applied here.

In particular, the **Information Security Management System** ("ISMS") is defined as the part of the County Council's overall management system which, based on a business risk approach, enables management to establish, implement, operate, monitor, review, maintain and improve information security within the Authority.

A current version of this document is available to all members of staff on the corporate intranet. It does not contain confidential information and can be released to relevant external parties.

This information security policy was approved by the CMB on [date] and is issued on a version controlled basis under the signature of the [CEO]

Signature: Date:

## SECTION 5 OPERATION OF THE INFORMATION SECURITY MANAGEMENT SYSTEM

### Roles and responsibilities in relation to the ISMS

Responsibilities in relation to ISMS, which cannot be delegated, have been defined as follows:

a) The County Management Board has ultimate authority over the Information Security policy and ISMS but this is delegated to the ICT & E-government Steering Group and approves and authorises all changes to the Information Security Policy, the Statement of Applicability, the Information Security Manual and any separate policy statements (Level 1 documents).

b) The Chairman of the CIM&SG (see section 6.1.3.2 below) has lead responsibility for information security and works with the CIM&SG to approve, authorise and issue all Level 2 and Level 3 documents.

c) The Corporate Information Security Manager owns and maintains ISMS documentation, subject to the paragraphs above.

d) Owners of information assets are responsible for identifying business risks associated with information handling and information systems, for the day-to-day protection of their information asset(s) and for the day-to-day operation of related security processes, in accordance with policy and guidance contained in this manual. The responsibility for carrying out these processes or associated task(s) can be delegated to anyone within the Owner's area of responsibility, provided that:

    i) The individual has the necessary skill, competence and resources to carry out the processes or task(s) and
    ii) The Owner retains accountability for ensuring that the process or task is carried out correctly.

e) Owners of information assets are likely to be senior Directorate managers who will not be involved in day to day processes. The Standard requires that individuals are made responsible for local security co-ordination and support and Directorates should establish an appropriate network of such individuals.

f) Personal responsibilities of employees and other users of Lancashire County Council information and information systems are not specified in any single authoritative document. Documents such as the Acceptable Use Policy (AUP), job descriptions, published procedures, professional codes of conduct etc contain specific advice. Personal responsibilities outlined in such documents, including those relating to access to systems cannot be delegated.

g) The authority to change or develop information processing facilities lies with management. There is no single procedure within the County for authorising new information processing facilities but all such proposals should pass through appropriate financial, procurement, legal and technical checks and there are plicies governong those areas.

**Documentation**

The documentation contained within the manual belongs to one of three levels:

a. Level 1 which contains Policies (which provide requirements approved by senior management on specific control areas)
b. Level 2 which contains a mixture of more detailed directions which may be a mix of guidelines which are frameworks describing how policies should be applied and standards or procedures which contain specific mandatory advice. A single document may contain a mix of mandatory and discretionary guidance.
c. Level 3 contains ISMS management information maintained for the purposes of the PDCA processes consisting of records of the County Council's control of its information security processes, including details of audits, information security incidents and management reviews gathered during the CHECK phase, described in 4.X below, [ISO27001 4.3.1h].

This supporting documentation is either included in, or referenced from, this manual.

**Control of documents**

The County Council's ISMS documentation is protected and controlled. Documents should be approved at the levels described in paras a) & b) above. The procedure for approval [ISO27001 4.3.2] and for the management of records connected with the ISMS which defines the controls for identification, storage, protection, retrieval, retention time and disposal of records is described below [ISO27001 4.3.3] Documents are available to those who need and are authorised to access them in line with these retention requirements.

Documents required by the ISMS shall be protected and controlled as follows:

a) The group responsible for approving a document will ensure that the adequacy of documents is confirmed before issue;

b) Documents will include a review date which will be the sooner of 12 months or a major change relevant to the document;

c) Documents will contain metadata which will ensure that changes and the current revision status of documents are identified; docuemnts of external origin will be identified

d) The CISM will ensure that all ensure that relevant versions of applicable documents are available via the Lancashire County Council intranet in pdf format; sensitive documents (potentially exempt under Freedom of information) may not be posted on the intranet at the discretion of the CISM.

e) All documents relevant to the ISMS will be regarded as part of the Information Security Manual and will be assigned an Information Security Manual reference and stored electronically in a repository and made accesible via the Lancashire County Council intranet.

f) Stored and ultimately disposed of in accordance with the procedures applicable to their classification;

h) Documents will contain details of the intended audience and it the responsibility of the CISM to ensure adequate circulation of documents at the appropriate time.

i) So that the unintended use of obsolete documents is avoided all documents will contain an expiry date which will appear on both on-line and printed versions.

**Control of records**

Records shall be established and maintained to provide evidence of conformity to requirements and the effective operation of the ISMS. They shall be protected and controlled. The ISMS shall take account of any relevant legal or regulatory requirements and contractual obligations. Records shall remain legible, readily identifiable and retrievable. The controls needed for the identification, storage, protection, retrieval, retention time and disposition of records shall be documented and implemented. Specific requirements will be detailed in Level 2 guidance. Records should be retained for current year plus previous year as a default.

**Management Arrangements for the Information Security Management System**

ICT&EGSG has decided that its current requirements could be met by achieving "best practice" standards of compliance with the ISO/IEC 27001:2005 standard. Because the Authority will be claiming compliance then requirements of Clauses 4, 5, 6, 7 and 8 of the Standard must be met. This section the Manual documents how these requirements will be met within Lancashire County Council.

**CLAUSE 4 PLAN-DO-CHECK-ACT**

**The PLAN phase – establish the ISMS**

The **scope** of the ISMS is defined in section 2 of this manual.

The County Council has approved an **information security policy**, which is set out in Section 3, to apply throughout the County Council as defined in the scope. [ISO27001 4.2.1(a)]. The policy includes:

a) a framework for setting objectives for the ISMS for action with regard to information security; [ISO27001 4.2.1 b1)] ("to provide assurance that the organisation manages information risk so that the needs of service users and citizens and the requirements of corporate governance and are met; to establish confidence that partnership arrangements involving sharing and exchange of information are legal and secure to establish that designed and implemented security features are effective and correct to provide confidence that services & products offered by third party suppliers of information security assurance are adequate and fit for purpose; Information and information security requirements will continue to be aligned with LCC goals and the Information Security Management System (ISMS) is intended to be an enabling mechanism for information sharing, for electronic operations, remote and distributed working, for e-commerce and for reducing information-related risks to acceptable levels.)

b) the requirement for "legal, regulatory and contractual compliance"; [ISO27001 4.2.1 b2)]

c) the strategic organisational and risk management context for the establishment and maintenance of the ISMS ("the Organisation's current strategic business plan and risk management framework provide the context for identifying, assessing, evaluating and controlling information-related risks"); [ISO27001 4.2.1b3)] and

d) reference to a systematic approach to risk assessment, the risk management framework in which the criteria for risk evaluation are described and the structure of the risk assessment is defined [ISO27001 4.2.1 b4)]

e) The policy, and this manual, have been approved by ICT&EGSG [ISO27001 4.2.1 b5)]

The County Council has identified a suitable, systematic approach to and framework for risk assessment that produces comparable and reproducible results and that is appropriate for its business, legal, regulatory and contractual requirements, and this is described in Section 6 of Part 1 of this manual. [ISO27001 4.2.1c)]. This risk assessment framework identifies risks and evaluates options for risk treatement. [ISO27001 4.2.1d)], [ISO27001 4.2.1e)], [ISO27001 4.2.1f)]

Control objectives and controls are selected from Annex A of ISO27001:2005 to meet the criteria and requirements of the risk management framework, to take into account the risk acceptance criteria (Section 6, below) and to meet current legal, regulatory and contractual requirements. They are contained in the Statement of Applicability [ISO27001 4.2.1g].

The Statement of Applicability is contained in Part 2 of this manual and in approving this manual management accept the residual risks (see Section 6 para 6.11) [ISO27001 4.2.1h)]

ICTEG&SG authorises implementation of the ISMS and any changes to this manual and approves the residual risks [ISO27001 4.2.1i)]

**4.2 The DO phase – implement and operate the ISMS**

4.2 a) The Organisation's risk treatment plan contained in Part 2 reflects the decisions made in the PLAN phase, and identifies the management action, responsibilities and priorities for managing the identified information security risks. [ISO27001 4.2.2a)].

4.2 b) Appropriate funding and resources are, as described in the risk treatment plan, allocated to its implementation. [ISO27001 4.2.2b)]

4.2 c) The selected controls are implemented (and their implementation is co-ordinated across the County Council to meet the identified control objectives. [ISO27001 4.2.2c)]

4.2 d) The County Council has defined how it measures the effectiveness of its controls and has specified how to use these measurements to improve control effectiveness to produce comparable and reproducible results, and this is set out in Appendix 4 tp Part 1 o fthis Manual. [ISO27001 4.2.2d]

4.2 e) Training and awareness programmes are implemented as required in the risk treatment plan. [ISO27001 4.2.2e)]

4.2 f) The operational policies, guidelines, standards and procedures produced as a result of this policy are implemented. [ISO27001 4.2.2f)]

4.2 g) The County Council has committed specific resources to the effective management of the ISMS, including the nomination of a member of ICTM&SG with responsibility for information security and the establishment of a Corporate Information Security Manager and Assistant. [ISO27001 4.2.2g)]

4.2 h) The County Council has implemented monitoring procedures and controls as required by ISO27001 Annexe A control objectives 10.10 (detecting unauthorised info processing) and 13.1 (incident reporting) below. [ISO27001 4.2.2h)]

**4.3 The CHECK phase – monitor and review the ISMS**

4.3 a) The controls referred to in para 4.2.h are operated to detect processing errors, security events, to identify failed and successful security breaches and incidents, to enable management to assess whether security activities are performed in line with the criteria set for them, and to allow them to take action to resolve any breach of security in a way that reflects the County Council's priorities. See ACT phase also [ISO27001 4.2.3a)]

4.3 b) The County Council and its management regularly review the effectiveness of the ISMS, in line with the policy and procedures set out in the Lancashire County Council Information Security Manual, seek to continuously improve the effectiveness of the ISMS through analysing audit results, and monitoring events and activity, all in the context of the business goals and risk treatment plan, and at least once a year. [ISO27001 4.2.3b) and e)]

4.3 c) The County Council measures the effectiveness of controls, as set out in Appendix 4 Reporting & effectiveness Measures, to verify that security requirements have been met. [ISO27001 4.2.3c)]

4.3 d) At planned intervals as well as whenever there are significant changes relevant to the ISMS , those aspects of its risk assessment and risk treatment plan, including levels of residual risk and acceptable risk (taking into account changes in the effectiveness of controls), that are affected by the changes will be reviewed. Specific risks in relation to new technologies, systems or any innovations that affect County Council information or information assets will be also be reviewed. [ISO27001 4.2.3d)]

4.3 e) Management ensures that the County Council carries out regular internal ISMS and other audits, and the results of these audits inform the reviews above. [ISO27001 5.1.g & 4.2.3e)]

4.3 f) Actions or events that could impact the effectiveness of the ISMS are recorded in line with ISO 27001 Annexe A sections 10.10 and 13 [ISO27001 4.2.3f & g)] and are reviewed at management review.

4.3 g) The risk treatment plan (Part 2) is updated to take into account the findings of monitoring and reviewing activities.

4.4 The **ACT** phase – maintain and improve the ISMS

4.4 a) Where improvement opportunities for the ISMS are identified during the CHECK phase, they are implemented if they meet the criteria of the risk treatment plan. [ISO27001 4.2.4a)]

4.4 b) The County Council has documented procedures for corrective and preventative action throughout the Information Security Manual and these include evaluating the need for action to prevent the occurrence of non-conformities. [ISO27001 4.2.4b]

4.4.c) The results of reviews are communicated to everyone involved and action delegated to the appropriate people. [ISO27001 4.2.4c)]

4.4 d) The implemented improvements are subject to monitoring and audit to ensure that their intended objectives have been achieved. [ISO27001 4.2.4 d)]

**4.2. Clause 5 Management Commitment to the ISMS**

Clause 5 of ISO27001 requires evidence of management commitment to the ISMS, recorded decisions on how the ISMS should operate, including resourcing of the ISMS and training of staff as follows:

*“ 5.1 Management commitment*

*Management shall provide evidence of its commitment to the establishment, implementation, operation, monitoring, review, maintenance and improvement of the ISMS by:*
*a) establishing an ISMS policy;*
*b) ensuring that ISMS objectives and plans are established;*
*c) establishing roles and responsibilities for information security*
*d) communicating to the organisation the importance of meeting information security objectives and conforming to the information security policy, its responsibilities under the law and the need for continual improvement;*
*e) providing sufficient resources to establish, implement, operate, monitor, review, maintain and improve the*
*f) deciding the criteria for accepting risks and the acceptable levels of risk;*
*g) ensuring that internal ISMS audits are conducted (see 6); and*
*h) conducting management reviews of the ISMS (see 7)*

*5.2 Resource management*

*5.2.1 Provision of resources*

*The organisation shall determine and provide the resources needed to:*
*a) establish, implement, operate, monitor, review, maintain and improve an ISMS;*
*b) ensure that information security procedures support the business requirements**;***
*c) identify and address legal and regulatory requirements and contractual security obligations;*
*d) maintain adequate security by correct application of all implemented controls;*
*e) carry out reviews when necessary, and to react appropriately to the results of these reviews; and where required, improve the effectiveness of the ISMS*
.
*5.2.2 Training, awareness and competence*

*The organisation shall ensure that all personnel who are assigned responsibilities defined in the ISMS are competent to perform the required tasks by:*
*a) determining the necessary competencies for personnel performing work effecting the ISMS;*
*b) providing training or taking other actions (e.g. employing competent personnel) to satisfy these needs;*
*c) evaluating the effectiveness of the actions taken; and*
*d) maintaining records of education, training, skills, experience and qualifications (see 4.3.3).*

*The organisation shall also ensure that all relevant personnel are aware of the relevance and importance of their information security activities and how they contribute to the achievement of the ISMS objectives.*

**Clauses 6, 7 & 8 Review and Improvement of the ISMS**

Clause 6 requires that the organisation should conduct independent internal ISMS audits at planned intervals to determine the compliance of the ISMS to the standard, to ensure it is effectively implemented and maintained and performs as expected.

Internal Audit have agreed to undertake internal ISMS audits at planned intervals on the terms set out in Clause 6 of the standard. The management responsible for the area being audited (the ISMS) shall ensure that actions are taken without undue delay to eliminate detected nonconformities and their causes. Follow-up activities shall include the verification of the actions taken and the reporting of verification results {see clause 8).

Clause 7 requires that Management shall review the organisation's ISMS at planned intervals of at least once a year to ensure its continuing suitability, adequacy and effectiveness. This review shall include assessing opportunities for improvement and the need for changes to the ISMS, including the information security policy and information security objectives. The results of the reviews shall be clearly documented and records shall be maintained. The standard specifies the types of evidence which should be considered as part of reviews and this may range from audit reports to feedback from interested parties.

Clause 8 requires that conclusions and recommendations resulting from the review process should be implemented via the ISMS processes.

## 6. RISK MANAGEMENT REPORT

6.1 This section outlines the risk assessment approach to be used by the ISMS at Lancashire County Council. This may briefly be summarised as

- Corporate information security risk and other corporate requirements for information security are addressed by the adoption of a standard framework of control objectives designed to meet most security risks
- Detailed implementation of the control objectives by business managers will require a risk assessment within the specific service context in which they operate.

6.2 Section 4.2 of ISO27001 requires that the risk assessment approach of the organisation is defined and an approach suited to the ISMS is identified. It further requires that the organisation should identify and assess risks in the business plan, to identify and evaluate options for the treatment of those risks, and to select control objectives and controls that will reduce those risks to acceptable levels within the context of the business plan, operational requirements, constraints and objectives and within relevant legislation and regulation. [ISO17799 4.1 and 4.2]

6.3 The County Council's approach to risk, which has been approved by management, is contained in the Corporate Risk Management Strategy which it applies to its overall strategic planning process. The Strategy has been amended by the report of the County Risk Manager entitled "Review of LCC Risk Management", taken to the Performance Working Group on 5th January 2007 and accepted by CMB.

6.4 The County Council's risk management framework as set out in the Corporate Risk Management Strategy (including updates) may be summarised as follows:

a) Service Management Teams define risks and own the risk management process in their own areas
b) Business plans are examined to identify cross cutting issues but no cross cutting issues are identified in the strategy in the sense that it is otherwise a purely business unit based strategy
c) Risk is expressed as a strategic or operational impact e.g. failure to deliver service
d) Risk is assessed by rating the impact of a risk on a scale of 1 to 7 and the probability of a single occurrence in the future 10 years. The two values are multiplied and risks rated as Very High , High, Medium or Low. Medium risks have a level of concern of "uneasy" attached to them and require mitigation and low risks have a level of concern "content" attached to them and should be subject to review only.
e) This table describes the acceptable level of risk and the corporate risk acceptance criteria.
f) The Corporate Strategy does not deal with cross cutting issues and ownership of this type of risk remains with the Senior Management Teams.
g) The review acknowledges that the current strategy considers only corporate level risks and that a Directorate or operational level risk management approach needs to be developed and integrated with the corporate level.
h) The Review acknowledges that scoring systems for service and operational risks will also need to be reviewed and an escalation process for 'red' risks identified at this level introduced, so that these are considered at the right level of authority. [ISO27001 4.2.1 b3 and b4, ISO17799 4.1 and 4.2]

6.5 Both the current Corporate Risk Management Strategy and ISO27001 implicitly assume the single step, detailed risk by risk logic outlined in para 6.4. This is not appropriate in the context of the ISMS because information risk is mainly an operational matter and this means that the inherent variety contained in numerous, individual business plans togetehr with the variety of risk across the Authority must be

taken into account. Risks cannot practically be treated as generic across this range of scenarios and the alternative, to attempt to pin down actual variations on risks, would be time consuming and complex.

6.6 In dealing with risk in this area in a way which complies with the standard, there are two overriding aims namely, that the outcome of the risk assessment process required by the standard is to choose appropriate control objectives for application across the Authority and that the aim of the Corporate Risk Management Strategy is to manage risks on the corporate risk register, information related risks having previously been identified as an area of corporate risk.

6.7 To meet these objectives, the single step approach described above has been modified and replaced with a two step approach.

6.8 The first step is a high level risk analysis which allows risk treatment and risk acceptance decisions to be made at a corporate level and allows control objectives to be chosen, as required by ISO 27001. The second level of risk assessment takes place at the more detailed level of the “information asset”. An “information asset” is defined as a significant example falling into one of the following categories: critical business application, installation, network, development project. The process of risk assessment will be owned by the Corporate Information Security Manager but will be conducted with the asset owner.

6.9 This approach meets the requirement to identify a risk management approach suitable for the organisation and effectively deals with information risk at a corporate level by the adoption of a framework of control objectives which must be applied to all critical information assets. It does not specifically identify threats vulnerabilities and impacts but makes the same assumptions on these matters as are employed by the 27001 standard. It is reasonable to assume that if these control objectives are employed as a holistic framework, most information related risks will be mitigated to acceptable levels. This approach also provides for consistency in approaching security controls across the organisation. An assessment of risks threats and impacts which generally justifies this position has been undertaken and is attached at Appendix 2 to Part 1 of this Manual. Appendix 2 also analyses risk treatment options and concludes that the main options, risk reduction and avoidance, are only available at the operational level.

6.10 There are other arguments for adopting a recognised framework of control objectives for an organisation beyond those relating to risk management which is only one of the objectives of adopting the ISMS. Partnership working, enablement of linked services, legal compliance and demonstrability of security all require a standard “framework” approach because these objectives require that the organisation communicates what it is doing to other organisations and allows them to evaluate this.

6.11 The criteria for acceptance of risk and the acceptable level of risk is defined in the Review of Lancashire County Council Risk Management (January 2007) as “Low Risk”.

6.12 Specific risk analysis and consideration of real business impacts is left to the second level. Risk treatment is most appropriate at this level. At this level once risk have been assessed then a gap analysis is carried out against the framework and an action plan developed which will meet those objectives in the current circumstances of the service carrying out the assessment. Any need for additional control objectives or controls beyond those recommended will be considered at this point. This process will also highlight any need to escalate risk management beyond SMT level. The fact that control objectives (as opposed to purely prescripive controls) are implemented, means that actions are proportionate.

6.13 The implementation is reviewed for effectiveness and, where possible, improvements are identified and these, within the context of the overall ISMS, are implemented as part of the PDCA process applied within the ISMS.

6.14 The approach has been discussed and has been agreed as reasonable by the Corporate Risk Manager. The method proposed may be regarded as one which will produce comparable and reproducible results.

**Section 7**

**Statement of Applicability**

The control objectives and controls selected as a result of carrying out the corporate level risk assessment are documented in the Statement of Applicability, which appears in Part 2 of this manual.

The control objectives in Annex A of [ISO27001/ISO17799:2005] have been accepted in their entirety as a set of baseline control objectives which will address information related risks where exposures are medium to high.

For mainly presentational reasons it has been decided to set out the Statement of Applicability using the framework of principles and objectives contained in the Information Security Forum's Standard of Good Practice January 2005 edition. A table showing how the Information Security Forum meets the requirements of Annexe A is included at Section 2a. This is an amalgamation of the best practice contained in BS7799, ITIL and COBIT standards, all three internationally recognised. The Section on Human Resources Security in the ISO27001 Annexe A (Section 8) and some miscellaneous sections have been carried forward as the ISF is not sufficiently explicit about those aspects.

The Statement of Applicability is found in Part 2 Section 2 of this Manual

**APPROVALS**

**ICT&EGSG/CIM&SG has agreed the following in respect of Clause 4, 5, 6, 7 and 8 of ISO/IEC 27001:2005**

1. ICT&EGSG/CIM&SG discussed and agreed that it was appropriate to plan and implement an Information Security Management System (ISMS) that would conform to the requirements of ISO/IEC 27001:2005 because of strategic objectives relating to partnership requirements, operational efficiency, risk management and compliance requirements.

2. It was agreed that the Information Security Manual would be signed off by the Chief Executive and the adoption of the ISMS would be communicated via Core Brief and Team Briefings.

3. Responsibilities for the ISMS were agreed as follows:
    a. Lead responsibility for information security, in the management team, is explicitly assigned to the Chair of the CIM&SG.
    b. The Information Security Policy states that all staff must comply with the policy as appropriate. Clear responsibilities are to be allocated to management and to specific individuals for specific aspects of information security and these responsibilities are documented at Appendix 4 or Part 1 of this manual and throughout the manual.
    c. In particular the principle of documenting and defining assets and assigning “ownership” to each was accepted. The principle of local security co-ordination in key service areas is agreed as essential to the effectiveness of the framework.
    d. a Corporate Information Security Manager provides for specialist information security advice and reports to CIM&SG. CIM&SG is responsible for reviewing the effectiveness and value of this advice and ensuring that it is co-ordinated across the Authority.
    e. It was agreed that CIM&SG should act as the Information Security Forum required by the ISO 27001 standard.

4. The CIM&SG authorised implementation of the Information Security Management System (ISMS) in the way set out below.
    a. The ISMS and policy deriving from it will be documented in the Lancashire County Council Information Security Manual which will be made available on the Intranet. Other associated material will be made available on the Intranet when possible.
    b. The Security Manual and the proposed supporting policies, guidance, standards and procedures are agreed as provisional for the first year of operation and the overall approach, content and progress in implementation will be reviewed and , if felt appropriate, confirmed at that time. This is in addition to the annual management review required by the standard.
    c. The scope of the Information Security Management System as set out in Section 1 of this manual was agreed as appropriate.
    d. It was agreed that the Information Security Management System should cover relevant legal, regulatory and contractual compliance issues. Those issues are listed at Appendix 3 to Part 1 of this manual.
    e. It was agreed that the Information Security Policy set out at Section 7 of this manual should be adopted as the County Council’s Information Security Policy.

f. The proposed risk management framework as set out in Section 6 to Part 1 of this manual for assessing and controlling information risk was discussed and agreed.
   i. In particular, the CIM&SG has agreed that the controls identified in the Statement of Applicability (sections 5 to 15 of the Information Security Manual) are appropriate and are aimed at mitigating risks to "low" level as defined by the Corporate Risk Manager (see Appendic 1a to Part 1 of this Manual). The residual risks implied at this level, generally "minimal" or "non-existent"[5] are accepted.
   ii. It was agreed that all but "low" risks should be subject to risk reduction measures as defined by the risk treatment plan. Supporting documentation contained within this ISMS (Policies, guidelines, standards and procedures) will, where possible, indicate appropriate levels of control for differing levels of risk.
   iii. The risk treatment plan (See Part 2 of this Manual) was discussed and agreed
g. It was agreed that the Information Security Manual would be reviewed by the CIM&SG whenever there are significant changes in the threat environment or in the County Council and at least once per year, on or about the anniversary of this meeting.
h. CIMS&G will ensure that Audits of the operation of the ISMS take place and that reviews take into account all available evidence.

5. CIM&SG discussed the requirement outlined on Clause 5 of ISO/IEC 27001:2005 to ensure that all relevant staff receive appropriate training and that adequate general levels of awareness are maintained.
   - The CISM was requested to produce an outline of requirements in this area
   - Options were discussed and the following approach was agreed…

6. CIM&SG discussed the requirement outlined on Clause 5 of ISO/IEC 27001:2005 to ensure that sufficient resources are applied to the operation and maintenance of the ISMS. The following cost headings/principles/sources of funds were agreed…..
   - Local responsibilities of management
   - Local security co-ordination
   - CISM
   - Training costs/promotional material
   - Aspects of controls which may be expensive/require a project e.g. asset management

[5] corresponding to HMG Impact Table definition for Impact Level 0 and the e-government service provision level 0,

## 9 Change history

| | | |
|---|---|---|
| Issue 1 | [Issue date] | Initial issue |

**Document Meta Data**

| | |
|---|---|
| Document title and version number: | |
| Stored as: **isms document template.doc** | |
| Publisher | Corporate Information Assurance Manager |
| Author, job title | |
| Review/expiry date | |

## Version Control History

| Release no | Release Date | Release Notes |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

## Document Approvals

| Name | Role | Date |
|---|---|---|
| | | |
| | | |
| | | |

## Document Review (for each version)

| Name | Role | Date |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

## Distribution

| Name | Directorate |
|---|---|
| | |
| | |
| | |
| | |

Lancashire County Council

Risk treatment plan

Section 4.2.2.a) of ISO/IEC 27001 requires that a risk treatment plan is formulated. This plan should identify appropriate management action, resources, responsibilities and priorities for managing information security risks.

There are three main areas of action:
1. ISMS management and processes to be established
2. Security training for all staff who handle information
3. Implementation of control objectives included in the Statement of Applicability.

The overall action plan and further details on each heading is shown on the table below at Appendix 1. In the early years the emphasis will be on embedding the framework subject to overall strategic objectives of demonstrability, compliance, partenrship working and risk reduction being met.

The ISMS processes include a review stage and this brings together any metrics about progress on action plans developed during the second level risk analyses, any reports of security incidents, audit reports, information about changes to the organisation or the threat environment. Internal Audit will independently check the operation of the ISMS and scrutinise the strength of controls operated in the organisation.

Responsibilities for action are defined for the organisation in the ISMS policy statement on roles and responsibilities and specific policies supporting the ISMS. Specific action plans will flow from the second level risks analyses. The method for this is shown at Appendix 2

Resources are expected to come from within existing budgets held by the owners of information assets.

| | | | | |
|---|---|---|---|---|
| 1 | **ISMS Management & processes** | Approve Manual | 2007 | Snr Management |
| | | Approve supporting policy | 2007 | Snr Management |
| | | Implement security organisation | 2007 | Snr Management |
| | | Review | Annual | Snr Management |
| | | Make improvements | Annual | Snr Management |
| | | | | |
| 2 | **Security awareness and training** | Originate & promulgate material. Monitor take-up | 2007 & on-going | CISM |
| | | Cascade | 2007 & on-going | Asset owners and support staff e.g. HR, ICT etc |
| 3 | **Implementation of control objectives included in the Statement of Applicability** | Implement security organisation | 2007 | Snr Management |
| | | Risk assessment & gap analyses for: | | CISM with asset owners |
| | | Information processing installations & networks (technical infrastructure) | 2007 | CISM with asset owners |
| | | Operational workforces (for each Directorate or part thereof)(Human "infrastructure") | 2007 | CISM with asset owners |
| | | Development projects | ASAP and On-going | CISM with asset owners |
| | | Critical business applications in priority order | Commence 2007 & continue over 2 years | CISM with asset owners |
| | | Non-critical applications (without risk analysis) | ASAP and On-going | Asset owners |
| | | Review processes incl incident | ASAP and | CISM & snr management |

| | | | | |
|---|---|---|---|---|
| | | reporting | On-going | |
| | | | | |
| | | | | |

Appendix 2

**Detailed risk analysis at information asset level (second level analysis).**

There will be an risk evaluation process for each of the major assets in the categories of

- Directorate (or part thereof) operational workforce
- Critical business application,
- Installation or network and
- Development projects

The evaluation will be undertaken by the CISM in conjunction with the owner of the asset or another person(s) of their choice. It is important to nominate the correct person(s) for this as the final product will need signing off as an authoritative statement.

The aim of the process is to assess risk in the context of the business and its current circumstances so that the output will always remain relevant and proportionate to the business. It is envisaged that most of the input will come from the asset owner's side. The role of the CISM is to provide guidance and ensure a level of consistency across the organisation.

The evaluation process will produce a risk analysis report, a gap analysis and an action plan. The result of the gap analysis and the progress against the action plan will be monitored.

The steps in the evaluation are set out below. Some notes on the rationale behind each step are included.

**Stage 1 System description.**

The aim of this stage is to gather together any information about the system/service which might affect consideration of security. There is a detailed questionnaire which prompts for relevant information. This stage would allow managers to more easily form a comprehensive view as to security & compliance requirements which they should take into account. It has been found that, in strictly practical terms, this stage is essential background for subsequent stages and any time spent on this stage repays itself later..

**Stage 2 Risk assessment**

**(a) Statement of security requirements**.

This is a statement by management of the security requirements surrounding their operations (the "drivers") and their view of the maximum impact of failing to meet these requirements. The outcome is likely to be either

- to confirm that maximum ratings fall into the expected category of "medium" and that good practice as required by the manual should adequately mitigate risks and keep them at or below this level.

- to show that most aspects of the area under review can be rated as medium but that there are some aspects of the system which should be rated as "high" require special consideration to ensure that unacceptable probabilities will be mitigated.

The requirements are analysed under four headings:

- confidentiality of information
- integrity of systems and data
- availability of systems
- legal, contractual or regulatory compliance.

**Typical approach**

The high level corporate risk analysis points to the need to treat information security measures as a "housekeeping" necessity particularly because of technological developments such as the Internet , wireless and mobile technology. This indicates compliance with a standard of good practice for information security as a default.

Specific legislation, contractual or regulatory conditions may also create requirements which directly or indirectly require that adequate security controls are implemented.

An example of direct influence is the Data Protection Act which requires that this data is kept confidential & safe (seventh principle). Partnership working, information sharing arrangements & connections to partner networks require that we demonstrate good practice across the County Council.

Examples of regulations which indirectly create information security requirements could be

- official returns to Central Government
- professional codes of practice which refer to standards of record keeping

**(b) Listing "vulnerabilities"**

The aim of this stage is to list any factors, concerns or issues which would make the potential impacts outlined above more likely, more frequent or indeed magnify the potential impact. Although there will be a prompt sheet with standard vulnerabilities there would be no limit to what is listed here. Just listing these factors will not necessarily raise risk ratings or generate extra work beyond the basic good practice but it would perhaps underline the need for certain controls. It would however highlight any specific issues which might need to be emphasised or tracked separately from the general issues. It may help to rank potential risks within your service.

The only category of vulnerability which should be excluded at this stage is the absence of a control or gaps in good practice as they are picked up at the next stage.

**(c) Stage 4 Gap analysis**

The aim at this stage is to compare your current information security procedures with standard good practice as outlined on the Information Security Manual. The manual is

based on a set of control objectives for information security which are supported by guidelines. The guidelines are a mix of mandatory and discretionary advice. It would however be mandatory to follow the overall framework.

This is perhaps the most time consuming aspect of the risk assessment but provides an immediate return in clarifying quality of procedures and levels of support surrounding the system.

**(d) Action Plan**

The gap analysis is essentially designed round control objectives and the good practice necessary to achieve them. Results on any particular point will indicate that level of response needed to meet that point, as follows:

- no work to do
- some work to do
- everything to do

The actual work required should take account of the potential impact, specific requirements outlined in the information security manual and the vulnerabilities or any other concerns you have identified. Because the actions here should ensure that control objectives are met in your circumstances, the actions should be proportional to your perceived levels of risk at a very local level. Because the infosec manual is based on industry good practice it should, applied sensitively, cover most risks. Anything which cannot be addressed this way may need bespoke stronger controls and this may or may not be manageable at local/Directorate level. Because the framework requires continuous review, actions decided here may be adjusted in the light of experience.

**(e) Risk rating summary**

The aim of this stage is to produce a summary of the results of the previous four stages so that we get an impressionistic view of:

- potential impacts
- potential likelihoods
- extent of action required or extent to which controls already mitigate risks

This stage is necessary to bring the assessment into a single view but also so that any extreme aspect in potential impact, likelihood or ability to locally mitigate risks is highlighted - if it exists. Should any risk of this magnitude be documented here then the Corporate Risk Manager should be notified and then an assessment made in the context of the corporate risk register. If it is then decided that the risk is more than local then the Corporate Risk Manager would need to advise on the way forward.

## Part 2 Statement of Applicability & Risk treatment Plan

## Summary of principles and objectives

### SM Security Management (enterprise-wide)



### CB Critical Business Applications



### CI Computer Installations



### NW Networks



### SD Systems Development

**AREA SM1 HIGH-LEVEL DIRECTION**
This area covers top management's direction on, and commitment to, information security. It includes an information security policy and a set of staff agreements that should be applied to all individuals who have access to the information and systems of the enterprise.

**Section SM1.1 Management commitment**
Principle Top management's direction on information security should be established, and commitment demonstrated.

Objective To establish top management's direction on, and commitment to, information security.

**Section SM1.2 Security policy**
Principle A comprehensive, documented information security policy should be produced and communicated to all individuals with access to the enterprise's information and systems.

Objective To document top management's direction on and commitment to information security, and communicate it to all relevant individuals.

**Section SM1.3 Staff agreements**
Principle Staff agreements should be established that specify information security responsibilities, are incorporated into staff contracts and are taken into account when screening applicants for employment.

Objective To ensure that staff agreements are consistent with and support the enterprise's information security policy.

**Area SM2 SECURITY ORGANISATION**
Safeguarding information and systems requires information security activity to be organised effectively throughout the enterprise. Accordingly, this area covers the organisational arrangements for managing information security throughout the enterprise, raising security awareness amongst staff and ensuring they have the skills required to run systems correctly and securely.

**Section SM2.1 High-level control**
Principle Control over information security should be provided by a high-level working group, committee or equivalent body, supported by a top-level director.

Objective To provide a top-down management structure and a practical mechanism for co-ordinating information security activity throughout the enterprise.

**Section SM2.2 Information security function**
Principle A specialist information security function should be established, which has enterprise-wide responsibility for promoting information security.

Objective To ensure good practice in information security is applied effectively throughout the enterprise.

**Section SM2.3 Local security co-ordination**
Principle Arrangements should be made to co-ordinate information security activity in business units/departments.

Objective To ensure that security activities are carried out in a timely and accurate manner, enterprise-wide,
and that security issues are resolved effectively.

**Section SM2.4 Security awareness**
Principle Specific activities should be undertaken, such as a security awareness programme, to promote security awareness to all individuals who have access to the information and systems of the enterprise.

Objective To ensure all relevant individuals understand the key elements of information security and why it is needed, and understand their personal information security responsibilities.

**Section SM2.5 Security education**
Principle Staff should be educated/trained in how to run systems correctly and how to develop and apply security controls.

Objective To provide staff with the skills required to run systems correctly and fulfil their information security responsibilities.

**Area SM3 SECURITY REQUIREMENTS**
Ensuring that the safeguards applied to information and systems are proportionate to their importance to the business is a fundamental element of good practice. Accordingly, this area covers arrangements for classifying critical information and systems, assigning ownership and identifying risk.

**Section SM3.1 Security classification**
Principle A security classification scheme should be established that applies throughout the enterprise, based on the criticality and sensitivity of information and systems in use.

Objective To communicate how information and systems should be treated in order that attention can be focused on those that are most critical.

**Section SM3.2 Ownership**
Principle ‘Ownership’ of critical information and systems should be assigned to capable individuals, with responsibilities clearly defined and accepted.

Objective To achieve individual accountability for all information and systems throughout the enterprise and
give responsible individuals a vested interest in their protection.

**Section SM3.3 Risk analysis**
Principle Critical applications, computer installations, networks and systems under development should be subject to a formal risk analysis on a periodic basis.

Objective To enable individuals who are responsible for information and systems to identify key risks and determine the controls required to keep those risks within acceptable limits.

**Area SM4 SECURE ENVIRONMENT**
Achieving a consistent standard of good practice in information security across an enterprise is a complex undertaking. The difficulties can be eased by introducing a common framework of disciplines and by making standard arrangements at enterprise level, rather than on an individual basis, for example by appointing an individual to manage information privacy for the whole enterprise. Accordingly, this area covers the arrangements required to build a secure environment enterprise-wide.

**Section SM4.1 Security architecture**
Principle An 'information security architecture' should be established, which provides a framework for the application of standard security controls throughout the enterprise.

Objective To enable system developers and administrators to implement consistent, simple-to-use security functionality across multiple computer systems throughout the enterprise.

**Section SM4.2 Information privacy**
Principle Responsibility for managing information privacy should be established and security controls for handling personally identifiable information applied.

Objective To prevent information about individuals being used in an inappropriate manner, and ensure compliance with legal and regulatory requirements for information privacy.

**Section SM4.3 Asset management**
Principle Proven, reliable and approved hardware/software should be used that meet security requirements and are recorded in an inventory.

Objective To reduce the risk of information security being compromised by weaknesses in hardware/software and ensure compliance with legal/regulatory requirements.

**Section SM4.4 Physical protection**
Principle All buildings within the enterprise that house critical IT facilities (e.g. data centres, network facilities and key user areas) should be physically protected against accident or attack.
Objective To restrict physical access to authorised individuals and ensure that IT facilities processing critical or sensitive information are available when required.

**Section SM4.5 Business continuity**
Principle Documented standards/procedures should be established for developing business continuity plans and for maintaining business continuity arrangements throughout the enterprise.

Objective To enable the enterprise to withstand the prolonged unavailability of critical information and systems.

**Area SM5 MALICIOUS ATTACK**
Organisations are often subject to malicious attack from third parties, for example by viruses or hacking. Consequently, this area covers the security controls required to protect against viruses and other malicious code, provide intrusion detection capabilities, respond to a serious attack and manage forensic investigations.

**Section SM5.1 Virus protection**
Principle Virus protection arrangements should be established, and maintained enterprise-wide.

Objective To protect the enterprise against virus attack and ensure it can respond to virus infection within critical timescales.

**Section SM5.2 Malicious mobile code protection**
Principle Enterprise-wide arrangements should be established to protect against malicious mobile code, such
as that downloaded from the web.
Objective To protect the enterprise against disruption caused by the introduction of malicious mobile code.

**Section SM5.3 Intrusion detection**
Principle Intrusion detection mechanisms should be applied to critical systems and networks.
Objective To identify suspected or actual malicious attacks and enable the enterprise to respond before serious damage is done.

**Section SM5.4 Emergency response**
Principle An emergency response process should be established, supported by an emergency response team, which outlines actions to be taken in the event of a serious attack.
Objective To respond to serious attacks quickly and effectively, reducing any potential business impact.

**Section SM5.5 Forensic investigations**
Principle A process should be established for dealing with incidents that require forensic investigation.
Objective To identify perpetrators of malicious acts and preserve sufficient evidence to prosecute them if required.

**Section SM5.6 Patch Management**

Principle There should be a strategy for patch management that should be supported by a management framework and a documented patch management process.
Objective To address potential vulnerabilities quickly and effectively in order to reduce the likelihood of a serious business impact arising.

**Area SM6 SPECIAL TOPICS**
The rapid pace of change in business and technology has resulted in the emergence of special topics with particular security concerns that should be dealt with enterprise-wide. Accordingly, this area covers the special security controls that apply to the use of cryptography, public key infrastructure, e-mail, remote working, the provision of third party access, electronic commerce and outsourcing.

**Section SM6.1 Use of cryptography**
Principle Cryptographic solutions should be approved, documented and applied enterprise-wide.
Objective To ensure that cryptographic services are managed effectively, thereby protecting the confidentiality of sensitive information, preserving the integrity of critical information and confirming the identity of the originator of information.

**Section SM6.2 Public key infrastructure**
Principle Where a public key infrastructure (PKI) is used, it should be protected by 'hardening' the underlying operating system(s) and restricting access to Certification Authorities.
Objective To ensure that the public key infrastructure (PKI) operates as intended, is available when required and can be recovered in the event of an emergency.

**Section SM6.3 E-mail**
Principle E-mail systems should be protected by a combination of policy, awareness, procedural and technical
security controls.
Objective To ensure that e-mail services are available when required, the confidentiality and integrity of messages is protected in transit, and the risk of misuse is minimised.

**Section SM6.4 Remote working**
Principle Personal computers used by staff working in remote locations should be purchased from a list of approved suppliers, tested prior to use, supported by maintenance arrangements and protected by physical controls.
Objective To ensure that computers used by staff working in remote locations operate as intended, remain available and do not compromise the security of any facilities to which they can be connected.

**Section SM6.5 Third party access**
Principle Connections from third parties (i.e. external organisations, such as customers or suppliers) should be uniquely identified, subjected to a risk analysis, approved, and supported by contracts.
Objective To ensure that access to the enterprise's information and systems is restricted to authorised third parties.

**Section SM6.6 Electronic commerce**

Principle A process should be established to ensure that information security is incorporated into electronic commerce initiatives enterprise-wide.
Objective To keep the increased risks associated with the development and deployment of electronic commerce within acceptable limits.

**Section SM6.7 Outsourcing**
Principle A process should be established to govern the selection and management of outsource contractors, supported by documented agreements that specify the security requirements to be met.
Objective To ensure that security requirements are satisfied and maintained when the running of a particular environment is entrusted to an outsource contractor.

Area SM7 MANAGEMENT REVIEW
An accurate understanding of the information security condition of the enterprise is required in order to manage information security effectively. Accordingly, this area covers the arrangements needed to provide decision-makers with sound information on the security condition of information and systems throughout the enterprise.

**Section SM7.1 Security audit/review**
Principle The information security status of critical IT environments should be subject to thorough, independent and regular security audits/reviews.
Objective To provide individuals who are responsible for particular IT environments, and top management, with an independent assessment of the security condition of those environments.

**Section SM7.2 Security monitoring**
Principle The information security condition of the enterprise should be monitored periodically and reported to top management.
Objective To provide top management with an accurate, comprehensive and coherent assessment of the security condition of the enterprise.

A critical business application requires a more stringent set of security controls than other applications. By understanding the business impact of a loss of confidentiality, integrity or availability of information, it is possible to establish the level of criticality of an application. This provides a sound basis for identifying business risks and determining the level of protection required to keep risks within acceptable limits.

Aspect CB Critical Business Applications

**AREA CB1 SECURITY REQUIREMENTS**
Business applications vary enormously in their importance to the business; hence the level of protection required also varies. Accordingly, this area identifies the information security requirements of the application.

**Section CB1.1 Confidentiality requirements**
Principle The impact of business information stored in or processed by the application being disclosed to unauthorised individuals should be assessed.
Objective To document and agree the confidentiality requirements (the need for information to be kept secret or private within a predetermined group) of the application.

**Section CB1.2 Integrity requirements**
Principle The impact of business information stored in or processed by the application being accidentally corrupted or deliberately manipulated should be assessed.
Objective To document and agree the integrity requirements (the need for information to be valid, accurate and complete) of the application.

**Section CB1.3 Availability requirements**
Principle The impact of business information stored in or processed by the application being unavailable for any length of time should be assessed.
Objective To document and agree the availability requirements (the need for information to be accessible when required) of the application.

**AREA CB2 APPLICATION MANAGEMENT**

Keeping business risks within acceptable limits requires a coherent set of information security arrangements. Accordingly, this area covers the roles and responsibilities required (including 'business ownership'), integral application controls and additional controls for handling sensitive material or transferring sensitive information. In addition, this area covers general management controls including change management, incident management and business continuity.

**Section CB2.1 Roles and responsibilities**

Principle An 'owner' should be identified for the application, and responsibilities for key tasks assigned to individuals who are capable of performing them.

Objective To assign 'ownership' of the application, provide a sound management structure for staff running or using it and give responsible individuals a vested interest in its protection.

**Section CB2.2 Application controls**

Principle The full range of application controls should be considered, and required controls identified.

Objective To build in the required application controls to protect information stored in or processed by the application.

**Section CB2.3 Change management**

Principle Changes to the application should be tested, reviewed and applied using a change management
process.

Objective To ensure that changes are applied correctly and do not compromise the security of the application.

**Section CB2.4 Incident management**

Principle All incidents – of any type – should be recorded, reviewed and resolved using an incident management process.

Objective To identify and resolve incidents effectively, minimise their business impact and reduce the risk of similar incidents occurring.

**Section CB2.5 Business continuity**

Principle A business continuity plan should be developed, supported by contingency arrangements, and tested periodically.

Objective To enable the business processes associated with the application to continue in the event of a disaster.

**Section CB2.6 Sensitive information**

Principle Additional protection should be provided for applications that involve handling sensitive material or transferring sensitive information.

Objective To protect the integrity and confidentiality of sensitive information.

**AREA CB3 USER ENVIRONMENT**
Critical business applications can be used by internal or external business or technical users. These individuals may be sited locally or at a remote location, often with differing business and security requirements. Accordingly, this area covers the disciplines required to control access to the application, configure workstations and ensure users are aware of information security and understand their personal responsibilities.

**Section CB3.1 Access control**
Principle Access to the application and associated information should be restricted to authorised individuals and enforced accordingly.
Objective To ensure that only authorised individuals gain access to the application, and that individual accountability is assured.

**Section CB3.2 Application sign-on process**
Principle Users should be subjected to a rigorous sign-on process before they can gain access to the application.
Objective To ensure that only authorised users gain access to the application.

**Section CB3.3 Workstation configuration**
Principle Workstations connected to the application should be purchased from a list of approved suppliers, tested prior to use, supported by maintenance arrangements and protected by physical controls.
Objective To ensure workstations operate as intended, are available when required and do not compromise the security of the application.

**Section CB3.4 Security awareness**
Principle Users of the application should be made aware of the key elements of information security and why it is needed, and understand their personal information security responsibilities.
Objective To ensure users of the application apply security controls and prevent the security of information used in the application from being compromised.

**AREA CB4 SYSTEM MANAGEMENT**
To enable applications to function, they have to run on one or more computers and typically make use of one or more networks. Accordingly, this area covers service agreements, the resilience of the application, external connections and the back-up of essential information and software.

**Section CB4.1 Service agreements**
Principle Computer and network services required to support the application should only be obtained from service providers capable of providing required security controls, and be supported by documented contracts or service level agreements.
Objective To define the business requirements for providers of any computer or network services that support the application, including those for information security, and to ensure they are met.

**Section CB4.2 Resilience**
Principle The application should be run on robust, reliable hardware and software, supported by alternative or duplicate facilities.
Objective To ensure that the application is available when required.

**Section CB4.3 External connections**
Principle All external connections to the application should be individually identified, verified, recorded, and approved by the application ‘owner’.
Objective To ensure that only authorised individuals gain access to the application via external connections.

**Section CB4.4 Back-up**
Principle Back-ups of essential information and software used by the application should be taken on a regular basis, according to a defined cycle.
Objective To ensure that, in the event of an emergency, essential information or software required by the application can be restored within critical timescales.

**AREA CB5 LOCAL SECURITY MANAGEMENT**
The security controls applied to a business application should be proportional to business risk. Accordingly, this area covers the arrangements made to identify the relative importance of the application, the associated business risks and the level of protection required. It also addresses local security co-ordination and the need for the application to be subject to thorough, independent and regular security audits/reviews.

**Section CB5.1 Local security co-ordination**
Principle An individual should be appointed to co-ordinate the information security arrangements of the application.
Objective To ensure that security activities are carried out in a timely and accurate manner, and that security issues are resolved effectively.

**Section CB5.2 Security classification**
Principle The application should be classified according to the criticality and sensitivity of information stored in or processed by the application, using a security classification scheme that applies throughout the enterprise.
Objective To communicate the level of security controls required by the application.

**Section CB5.3 Risk analysis**
Principle The application should be subject to a formal risk analysis on a periodic basis, the results of which should be documented, reviewed, and agreed by the application ‘owner’.
Objective To identify key risks associated with the application and determine the security controls required in order to keep those risks within acceptable limits.

**Section CB5.4 Security audit/review**
Principle The information security status of the application should be subject to thorough, independent and regular security audits/reviews.
Objective To ensure that security controls have been implemented effectively, that risk is being managed and to provide the application ‘owner’, and top management, with an independent assessment of the security status of the application.

## AREA CB6 SPECIAL TOPICS

The rapid pace of change in business and technology has resulted in the emergence of special topics with particular security concerns. Where these topics apply to a critical business application, special security arrangements are required. Accordingly, this area covers the additional security controls required by applications that provide third party access, employ cryptographic key management, use a public key infrastructure (PKI) or are based on web-enabled technology.

### Section CB6.1 Third party agreements

Principle Connections from third parties (i.e. external organisations, such as customers, suppliers and members of the public) should be subject to a risk assessment, approved by the application 'owner' and agreed by both parties in a documented agreement, such as a contract.
Objective To ensure that only agreed and approved third parties gain access to the application.

### Section CB6.2 Cryptographic key management

Principle Cryptographic keys should be managed tightly, in accordance with documented standards/procedures, and protected against unauthorised access or destruction.
Objective To ensure that cryptographic keys are not compromised, for example through loss or disclosure.

### Section CB6.3 Public key infrastructure

Principle Any public key infrastructure (PKI) used by the application should be protected by 'hardening' the underlying operating system(s) and restricting access to Certification Authorities.
Objective To ensure that the public key infrastructure (PKI) operates as intended, is available when required and can be recovered in the event of an emergency.

### Section CB6.4 Web-enabled applications

Principle Specialised technical controls should be applied to web-enabled applications.
Objective To ensure that the increased risks associated with web-enabled applications are minimised.

**Aspect CI Computer Installations**
Computer installations typically support critical business applications and safeguarding them is, therefore, a key priority. Since the same information security principles apply to any computer installation – irrespective of where information is processed or on what scale or type of computer it takes place – a common standard of good practice for information security should be applied.

**AREA CI1 INSTALLATION MANAGEMENT**
Computer installations used for processing information need to be well managed. Accordingly, this area covers the roles and responsibilities of the staff involved in running computer installations, agreements made with business users, management of key assets (e.g. hardware and software) and monitoring of the systems associated with the installation.

**Section CI1.1 Roles and responsibilities**
Principle An 'owner' should be identified for the computer installation, and responsibilities for key tasks assigned to individuals who are capable of performing them.
Objective To achieve individual accountability for the computer installation, provide a sound management structure for staff running it and give responsible individuals a vested interest in its protection.

**Section CI1.2 Service agreements**
Principle Users' service requirements should be classified in a way that identifies their criticality to the business and documented in agreements, such as contracts or service level agreements.
Objective To define the business requirements, including information security requirements, for services provided by the computer installation.

**Section CI1.3 Asset management**
Principle Essential information about hardware and software (e.g. unique identifiers, version numbers and physical locations) should be recorded in inventories, and software licensing requirements met.
Objective To protect information stored in or processed by the installation and meet legal/regulatory requirements.

**Section CI1.4 System monitoring**
Principle Systems associated with the computer installation should be monitored continuously, and from a business user's perspective.
Objective To assess the performance of the computer installation, reduce the likelihood of system overload and detect potential or actual malicious intrusions.

**AREA CI2 LIVE ENVIRONMENT**
Service targets are more likely to be achieved if computer installations are designed well. Accordingly, this area covers the design of the installation, logging of key events and the configuration of host systems and workstations. It also covers the resilience of the installation and its protection from physical loss or damage.

**Section CI2.1 Installation design**
Principle Computer installations should be designed to cope with current and predicted information processing requirements and be protected using a range of in-built security controls.
Objective To produce a computer installation that has security functionality built-in and enables additional controls to be incorporated easily.

**Section CI2.2 Event logging**
Principle Logs of all key events within the computer installation should be maintained (preferably using automated tools), reviewed periodically and protected against unauthorised change.
Objective To ensure individual accountability and to enable incidents, such as access violations, to be investigated and resolved.

**Section CI2.3 Host system configuration**
Principle Host systems should be configured to function as required, and to prevent unauthorised or incorrect updates.
Objective To ensure host systems operate as intended and do not compromise the security of the computer installation.

**Section CI2.4 Workstation configuration**
Principle Workstations connected to systems within the computer installation should be purchased from a list of approved suppliers, tested prior to use, supported by maintenance arrangements and protected by physical controls.
Objective To ensure workstations operate as intended and do not compromise the security of the systems to which they are connected.

**Section CI2.5 Resilience**
Principle The computer installation should be run on robust, reliable hardware and software, supported by alternative or duplicate facilities.
Objective To ensure that the systems supported by the computer installation are available when required.

**Section CI2.6 Hazard protection**
Principle Computer equipment and facilities should be protected against fire, flood, environmental and other natural hazards.
Objective To prevent services being disrupted by damage to computer equipment or facilities.

**Section CI2.7 Power supplies**
Principle Critical computer equipment and facilities should be protected against power outages.

Objective To prevent services provided by the computer installation from being disrupted by loss of power.

**Section CI2.8 Physical access**
Principle Physical access to critical computer installation facilities should be restricted to authorised individuals.
Objective To prevent services being disrupted by loss of or damage to equipment or facilities.

**AREA CI3 SYSTEM OPERATION**
Achieving service targets requires computer installations to be run in accordance with sound disciplines. Accordingly this area covers basic controls over system operation (i.e. handling computer media, back-up and change management) and arrangements for identifying and resolving incidents (i.e. incident management and emergency fixes).

**Section CI3.2 Back-up**
Principle Back-ups of essential information and software used by the computer installation should be taken on a regular basis, according to a defined cycle.
Objective To ensure that, in the event of an emergency, essential information and software required by the installation can be restored within critical timescales.

**Section CI3.3 Change management**
Principle Changes to any part of the computer installation should be tested, reviewed and applied using a change management process.
Objective To ensure that changes are applied correctly and do not compromise the security of the installation.

**Section CI3.4 Incident management**
Principle All incidents – of any type – should be recorded, reviewed and resolved using an incident management process.
Objective To identify and resolve incidents effectively, minimise their business impact and reduce the risk of similar incidents occurring.

**Section CI3.5 Emergency fixes**
Principle Emergency fixes to computer equipment, business applications, systems software and business information should be tested, reviewed and applied in accordance with documented standards/procedures.
Objective To respond to emergencies quickly and effectively, reducing any potential business impact.

**Section CI3.1 Handling computer media**
Principle Information held on data storage media (including magnetic tapes, disks, printed results, and stationery) should be protected against corruption, loss or disclosure and additional security controls applied to media containing sensitive information.
Objective To protect computer media in accordance with their information security requirements.

**Area CI4 ACCESS CONTROL**
Effective access control mechanisms can reduce the risk of unauthorised access to information and systems. Accordingly, this area covers the access control disciplines applied to users and the steps taken to control access to information and systems within the computer installation.

**Section CI4.1 Access control arrangements**
Principle Access control arrangements should be established to restrict access by all types of user to approved system capabilities of the computer installation.
Objective To ensure that only authorised individuals gain access to information or systems within the computer installation, and that individual accountability is assured.

**Section CI4.2 User authorisation**
Principle All users of the computer installation should be authorised before they are granted access privileges.
Objective To restrict access to any information or systems within the computer installation to authorised users.

**Section CI4.3 Access privileges**
Principle All users of the computer installation should be assigned specific privileges to allow them to access particular information or systems.
Objective To provide authorised users with access privileges which are sufficient to enable them to perform their duties but do not permit them to exceed their authority.

**Section CI4.4 Sign-on process**
Principle Users should follow a rigorous system sign-on process before they can gain access to target systems.
Objective To ensure that only authorised users gain access to any information or systems within the computer installation.

**Section CI4.5 User authentication**
Principle All users should be authenticated by using UserIDs and passwords or by strong authentication mechanisms (e.g. smartcards or biometric devices, such as fingerprint recognition) before they can gain access to target systems.
Objective To ensure that only authorised users gain access to any information or systems within the computer installation.

**AREA CI5 LOCAL SECURITY MANAGEMENT**

A computer installation typically supports one or more critical business applications, holds information that needs to be protected, and is an important asset in its own right. Each of these perspectives needs to be considered in order to provide appropriate protection. Accordingly, this area covers the arrangements made to identify the relative importance of the computer installation, the associated business risks and the level of protection required. It also covers the arrangements made to ensure that information security is co-ordinated locally, staff are aware of information security and understand their personal responsibilities, and the need for the installation to be subject to thorough, independent and regular security audits/reviews.

**Section CI5.1 Local security co-ordination**

Principle An individual should be appointed to co-ordinate the information security arrangements of the computer installation.
Objective To ensure that security activities are carried out in a timely and accurate manner, and that security issues are resolved effectively.

**Section CI5.2 Security awareness**

Principle Staff running the installation should be made aware of the key elements of information security and why it is needed, and understand their personal information security responsibilities.
Objective To ensure that staff running the installation apply security controls and prevent the security of information used in the computer installation from being compromised.

**Section CI5.3 Security classification**

Principle The computer installation should be classified according to the criticality and sensitivity of information stored in or processed by the installation, using a security classification scheme that applies throughout the enterprise.
Objective To communicate the level of security controls required by the computer installation.

**Section CI5.4 Risk analysis**

Principle The computer installation should be subject to a formal risk analysis on a periodic basis, the results of which should be documented, reviewed, and agreed by the installation ‘owner’.
Objective To identify key risks associated with the computer installation and determine the security controls required in order to keep those risks within acceptable limits.

**Section CI5.5 Security audit/review**

Principle The information security status of the computer installation should be subject to thorough, independent and regular security audits/reviews.
Objective To ensure that security controls have been implemented effectively, that risk is being managed and to provide the installation ‘owner’, and top management, with an independent assessment of the security status of the installation.

**AREA CI6 SERVICE CONTINUITY**

If there is a serious interruption to information processing, for example if a disaster occurs, the computer installation may be unavailable for a prolonged period. Considerable forethought is required to enable information processing to continue in these circumstances and to keep the business impact to a minimum. Accordingly, this area covers the development of contingency plans and arrangements, and their validation.

**Section CI6.1 Contingency plan**

Principle A business continuity plan should be developed and documented.
Objective To provide individuals with a documented set of actions to perform in the event of a disaster,
enabling information processing to be resumed within critical timescales.

**Section CI6.2 Contingency arrangements**

Principle Alternative processing arrangements should be established, and made available when required.
Objective To enable information processing to resume within critical timescales, using alternative facilities.

**Section CI6.3 Validation and maintenance**

Principle Contingency plans and arrangements should be tested on a periodic basis.
Objective To ensure that information processing can resume within critical timescales, using alternative facilities.

**Aspect NW Networks**
Computer networks convey information and provide a channel of access to information systems. By their nature, they are highly vulnerable to disruption and abuse. Safeguarding business communications requires robust network design, well-defined network services, and sound disciplines to be observed in running networks and managing security. These factors apply equally to local and wide area networks, and to data and voice communications.

**AREA NW1 NETWORK MANAGEMENT**
Computer networks are complex. They have to link different systems together, are subject to constant change and often rely on services provided by external parties. Orchestrating the technical and organisational issues involved requires sound management. Accordingly, this area covers the organisational arrangements for running a network, its design, resilience and documentation, and the management of relationships with service providers.

**Section NW1.1 Roles and responsibilities**
Principle An 'owner' should be identified for the network, and responsibilities for key tasks assigned to individuals who are capable of performing them.
Objective To achieve individual accountability for the network, provide a sound management structure for staff running it and give responsible individuals a vested interest in its protection.

**Section NW1.2 Network design**
Principle The network should be designed to cope with current and predicted levels of traffic and be protected using a range of in-built security controls.
Objective To produce an operational network that has security functionality built-in and enables additional controls to be incorporated easily.

**Section NW1.3 Network resilience**
Principle The network should be run on robust, reliable hardware and software, supported by alternative or duplicate facilities.
Objective To ensure that the network is available when required.

**Section NW1.4 Network documentation**
Principle Networks should be supported by accurate, up-to-date documentation.
Objective To ensure that the network is configured accurately and securely.

**Section NW1.5 Service providers**
Principle Network services should only be obtained from service providers capable of providing relevant security controls, and be supported by documented contracts or service level agreements.
Objective To define the business requirements for network service providers, including those for security, and ensure they are met.

**AREA NW2 TRAFFIC MANAGEMENT**
Computer networks can handle many types of traffic from a wide variety of sources. To manage network traffic effectively, network devices have to be configured correctly and particular types of network traffic denied access. Accordingly, this area covers the disciplines required to ensure undesirable network traffic and unauthorised external or wireless users are prevented from gaining access to the network.

**Section NW2.1 Configuring network devices**
Principle Network devices should be configured to function as required, and to prevent unauthorised or incorrect updates.
Objective To ensure that the configuration of network devices is accurate and does not compromise the security of the network.

**Section NW2.2 Firewalls**
Principle Network traffic should be routed through a firewall, prior to being allowed access to the network.
Objective To ensure unauthorised network traffic is not allowed to gain access to specified parts of the network.

**Section NW2.3 External access**
Principle All external connections to the network should be individually identified, verified, recorded, and approved by the network ‘owner’.
Objective To ensure that only authorised external users gain access to the network.

**Section NW2.4 Wireless access**
Principle Wireless access should be authorised, authenticated, encrypted and permitted only from approved locations.
Objective To ensure that only authorised individuals gain wireless access to the network and that wireless transmissions cannot be monitored.

**AREA NW3 NETWORK OPERATIONS**
Maintaining continuity of service to users requires computer networks to be run in accordance with sound disciplines. Accordingly this area covers the arrangements needed to monitor network performance and to manage changes and incidents. In addition, the area covers the arrangements required to provide physical security, take back-ups and ensure service continuity.

**Section NW3.1 Network monitoring**
Principle Key network activities should be monitored.
Objective To assess the performance of the network, reduce the likelihood of network overload and detect potential or actual malicious intrusions.

**Section NW3.2 Change management**
Principle Changes to the network should be tested, reviewed and applied using a change management process.
Objective To ensure that changes are applied correctly and do not compromise the security of the network.

**Section NW3.3 Incident management**
Principle All network incidents – of any type – should be recorded, reviewed and resolved using an incident management process.
Objective To identify and resolve network incidents effectively, minimise their business impact and reduce the risk of similar incidents occurring.

**Section NW3.4 Physical security**
Principle Physical access to critical network facilities should be restricted to authorised individuals.
Objective To prevent services being disrupted by loss of or damage to communications equipment, power or facilities.

**Section NW3.5 Back-up**
Principle Back-ups of essential information and software used by the network should be taken on a regular basis, according to a defined cycle.
Objective To ensure that, in the event of an emergency, essential network information or software required by the network can be restored within critical timescales.

**Section NW3.6 Service continuity**
Principle A service continuity plan should be developed, supported by effective contingency arrangements,
and tested periodically.
Objective To enable critical network services to continue in the event of a disaster.

**Section NW3.7 Remote maintenance**
Principle Remote maintenance of the network should be restricted to authorised individuals, confined to
individual sessions, and subject to review.
Objective To prevent unauthorised access to the network through the misuse of remote maintenance

facilities.

**AREA NW4 LOCAL SECURITY MANAGEMENT**
Computer networks play an essential role in the functioning of many critical business applications. They convey information that needs to be protected, and are valuable assets in their own right. Accordingly, this area covers the arrangements made to identify the relative importance of the network, the associated business risks and the level of protection required. It also covers the arrangements made to ensure that information security is co-ordinated locally, network staff are aware of information security and understand their personal responsibilities, and the need for the network to be subject to thorough, independent and regular security audits/reviews.

**Section NW4.1 Local security co-ordination**
Principle An individual should be appointed to co-ordinate the information security arrangements of the network.
Objective To ensure that security activities are carried out in a timely and accurate manner, and that security issues are resolved effectively.

**Section NW4.2 Security awareness**
Principle Network staff should be made aware of the key elements of information security and why it is needed, and understand their personal information security responsibilities.
Objective To ensure network staff apply security controls and prevent the security of information transmitted across the network from being compromised.

**Section NW4.3 Security classification**
Principle The network should be classified according to the criticality and sensitivity of information transmitted across it, using a security classification scheme that applies throughout the enterprise.
Objective To communicate the level of security controls required by the network.

**Section NW4.4 Risk analysis**
Principle The network should be subject to a formal risk analysis on a periodic basis, the results of which should be documented, reviewed, and agreed by the network ‘owner’.
Objective To identify key risks associated with the network and determine the security controls required in order to keep those risks within acceptable limits.

**Section NW4.5 Security audit/review**
Principle The information security status of the network should be subject to thorough, independent and regular security audits/reviews.
Objective To ensure that security controls have been implemented effectively, that risk is being managed and to provide the network ‘owner’, and top management, with an independent assessment of the security status of the network.

## AREA NW5 VOICE NETWORKS

Business processes can be disrupted if voice networks, such as telephone systems, are unavailable or overloaded. Harm can also be caused if voice networks are subject to unauthorised use by outsiders, or sensitive conversations are overheard. Accordingly, this area covers the security arrangements applied to voice networks.

### Section NW5.1 Voice network documentation

Principle Voice networks should include documentation of essential components and be supported by documented standards/procedures.
Objective To provide employees with a clear statement of the security disciplines they are expected to follow in relation to voice networks.

### Section NW5.2 Resilience of voice networks

Principle Voice networks should be supported by a robust and reliable set of hardware and software, with alternative facilities available when required.
Objective To ensure that voice network facilities (e.g. telephone exchanges) are available when required.

### Section NW5.3 Special voice network controls

Principle Voice network facilities (e.g. telephone exchanges) should be monitored regularly and access to them restricted.
Objective To prevent and detect the misuse of voice network facilities.

**Aspect SD Systems Development**
Building security into systems during their development is more cost-effective and secure than grafting it on afterwards. It requires a coherent approach to systems development as a whole, and sound disciplines to be observed throughout the development cycle. Ensuring that information security is addressed at each stage of the cycle is of key importance.

**AREA SD1 DEVELOPMENT MANAGEMENT**
Producing robust systems, on which the enterprise can depend, requires a sound approach to systems development. Accordingly, this area covers the organisation of systems development staff, the methodology used in developing systems, quality assurance and the security of development environments.

**Section SD1.1 Roles and responsibilities**
Principle An individual with overall responsibility for the development activity, together with business 'owners', should be appointed to manage system development activities, and responsibilities for key tasks assigned to individuals who are capable of performing them.
Objective To achieve individual accountability for system development activities, provide a sound management structure for staff performing them and give responsible individuals a vested interest in their protection.

**Section SD1.2 Development methodology**
Principle Development activities should be carried out in accordance with a documented system development methodology.
Objective To ensure that systems under development meet business requirements, including those for information security.

**Section SD1.3 Quality assurance**
Principle Quality assurance of key security activities should be performed during the development lifecycle.
Objective To provide assurance that security requirements are defined adequately, agreed security controls are developed and security requirements are met.

**Section SD1.4 Development environments**
Principle System development activities should be performed in specialised development environments, isolated from the live environment, and protected against disruption and disclosure of information.
Objective To provide a secure environment for system development activities.

**AREA SD2 LOCAL SECURITY MANAGEMENT**

In common with live systems, systems under development need to be supported by a sound organisational structure and run by staff who are aware of information security and know how to apply security controls effectively. Accordingly, this area covers the arrangements made to ensure that information security is co-ordinated locally, systems development staff are aware of information security and understand their personal responsibilities, and the need for systems development activities to be subject to thorough, independent and regular security audits/reviews.

## Section SD2.1 Local security co-ordination

Principle An individual should be appointed to co-ordinate the information security arrangements of system development activities.
Objective To ensure that security activities associated with systems development are carried out in a timely and accurate manner, and that information security issues are resolved effectively.

## Section SD2.2 Security awareness

Principle Systems development staff should be made aware of the key elements of information security and why it is needed, and understand their personal information security responsibilities.
Objective To ensure systems development staff apply security controls and prevent the security of information used in development activities from being compromised.

## Section SD2.3 Security audit/review

Principle The information security status of systems development activity should be subject to thorough, independent and regular security audits/reviews.
Objective To ensure that security controls are designed effectively, that risk is managed, and to provide the business ‘owner’, and top management, with an independent assessment of the security status of system development activities.

## AREA SD3 BUSINESS REQUIREMENTS

A thorough understanding of business requirements (including those for the confidentiality, integrity and availability of information) is essential if systems are to fulfil their intended purpose. Accordingly, this area covers the arrangements made for specifying business requirements, determining security requirements and conducting risk assessments.

### Section SD3.1 Specification of requirements

Principle Business requirements (including those for information security) should be documented and agreed before detailed design commences.
Objective To ensure that information security requirements are treated as an integral part of business requirements, are fully considered and approved.

### Section SD3.2 Confidentiality requirements

Principle To document and agree confidentiality requirements (the need for information to be kept secret or private within a predetermined group) before detailed design commences.
Objective To ensure that confidentiality requirements are treated as an integral part of business requirements, are fully considered and approved.

### Section SD3.3 Integrity requirements

Principle To document and agree integrity requirements (the need for information to be valid, accurate and complete) before detailed design commences.
Objective To ensure that integrity requirements are treated as an integral part of business requirements, are fully considered and approved.

### Section SD3.4 Availability requirements

Principle To document and agree availability requirements (the need for information to be accessible and usable when required) before detailed design commences.
Objective To ensure that availability requirements are treated as an integral part of business requirements, are fully considered and approved.

### Section SD3.5 Risk assessment

Principle A formal risk assessment should be carried out for critical systems under development.
Objective To identify key risks associated with critical systems under development and determine the security controls required in order to keep those risks within acceptable limits.

**AREA SD4 DESIGN AND BUILD**
Building systems that function as intended requires the use of sound disciplines throughout the design and build stage of development. Accordingly, this area covers the arrangements needed to address information security during design, acquisition and system build, and the identification of required application, general and web-specific security controls.

**Section SD4.1 System design**
Principle Information security requirements for the system under development should be considered when designing the system.
Objective To produce an operational system based on sound design principles which has security functionality built-in and enables controls to be incorporated easily.

**Section SD4.2 Application controls**
Principle The full range of application controls should be considered when designing the system under development.
Objective To ensure that required application controls are built-in to the system under development.

**Section SD4.3 General security controls**
Principle The full range of general security controls should be considered when designing the system under development.
Objective To ensure that required general security controls are built-in to the system under development.

**Section SD4.4 Acquisition**
Principle Robust, reliable hardware and software should be acquired, following consideration of security requirements and identification of any security deficiencies.
Objective To ensure that hardware and software acquired from third parties provides the required functionality and does not compromise the security of systems under development.

**Section SD4.5 System build**
Principle System build activities (including coding and package customisation) should be carried out in accordance with industry good practice, performed by individuals provided with adequate skills/tools and inspected to identify unauthorised modifications or changes which may compromise security controls.
Objective To ensure that systems are built correctly and that no security weaknesses are introduced during the build process.

**Section SD4.6 Web-enabled development**
Principle Specialised technical controls should be applied to the development of web-enabled applications.

Objective To ensure that the increased risks associated with the development of web-enabled applications are minimised.

## AREA SD5 TESTING

Testing is a fundamental element of good practice in systems development. Planned well and performed correctly, it provides assurance that systems, including security controls, function as intended and reduces the likelihood of system malfunctions occurring. Accordingly, this area covers the arrangements needed to carry out testing thoroughly, without disrupting other activities.

### Section SD5.1 Testing process

Principle All elements of a system (i.e. application software packages, system software, hardware and services) should be tested before the system is promoted to the live environment.
Objective To ensure systems function correctly and meet security requirements.

#### Section SD5.2 Acceptance testing

Principle Systems under development should be subject to rigorous acceptance testing in an isolated area that simulates the live environment.
Objective To ensure that only systems that have been tested rigorously and satisfy user requirements (including those for information security), are promoted to the live environment.

**AREA SD6 IMPLEMENTATION**
Sound disciplines are required when new systems are promoted from the development into the live environment. Accordingly, this area covers system promotion criteria, the installation of new systems in the live environment and post-implementation reviews.

**Section SD6.1 System promotion criteria**
Principle Rigorous criteria should be met before new systems are promoted into the live environment.
Objective To ensure that only tested and approved versions of hardware and software are promoted into the live environment.

**Section SD6.2 Installation process**
Principle New systems should be installed in the live environment in accordance with a documented installation process.
Objective To ensure that new systems are installed in the live environment without disruption.

**Section SD6.3 Post-implementation review**
Principle Post-implementation reviews should be conducted for all new systems.
Objective To check that systems – and information security controls – function as intended.

| | Control objectives | Security Management | Directorate workforce | Critical application | Installation | Network | System Development |
|---|---|---|---|---|---|---|---|
| ✓ | **Clause 4 Establish the ISMS** | **ISO27001** | | | | | |
| ✓ | **Clause 5 Management Responsibility** | **ISO27001** | | | | | |
| ✓ | **Clause 6 Internal ISMS audits** | **ISO27001** | | | | | |
| ✓ | **Clause 7 Management Reviews** | **ISO27001** | | | | | |
| ✓ | **Clause 8 ISMS Improvement** | **ISO27001** | | | | | |
| ✓ | | | | | | | |
| ✓ | 5 Security Policy | | | | | | |
| ✓ | ***5.1 Infosec Policy*** | | | | | | |
| ✓ | ***5.1.1 Information security policy document*** | **SM1.2 Security Policy** | | | | | |
| ✓ | ***5.1.2 Review of the information security policy*** | **ISO27001**<br>**SM1.1 Management commitment**<br>**SM1.2 Security Policy** | | | | | |
| ✓ | 6 Organization of information security | | | | | | |
| ✓✓ | ***6.1 Internal organisation*** | | | | | | |
| ✓ | ***6.1.1 Management commitment to information security*** | **SM1.1Management commitment** | | | | | |
| ✓ | ***6. 1.2 Information security coordination*** | **SM2.1 High level control**<br>**SM2.2 Infosec function**<br>**SM2.3 Local sec co-ordination** | **CB5.1 Local security co-ordination** | **CB5.1 Local security co-ordination** | **CI5.1 Local security co-ordination** | **NW4.1 Local security co-ordination** | **SD2.1 Local security co-ordination** |
| ✓ | ***6.1. 3 Allocation of information security responsibilities*** | **SM2.3 Local security management**<br>**SM3.2 Ownership** | **SM2.3 Local security management**<br>**SM3.2 Ownership**<br>**CB2.1 Roles & responsibilities** | **CB2.1 Roles & responsibilities** | **CI1.1 Roles & responsibilities**<br>**CI1.2 Service agreements** | **NW 1.1 Roles &Responsibilities** | **SD1.1 Roles &Responsibilities** |
| ✓ | ***6.1.4 Authorization process for information processing facilities*** | **SM4.1 Security architecture**<br>**SM4.3 Asset Management**<br>**SD6.1 System Promotion criteria** | | | **CI1.3 Asset mangement** | | **SD6.1 System promotion criteria** |
| ✓ | ***6.1.5 Confidentiality agreements*** | **SM4.2** | | | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| ✓ | ***6.1.6 Contact with authorities*** | **SM2.2.5** | | | | | |
| ✓ | ***6.1.7 Contact with special interest groups*** | **SM2.2.5** | | | | | |
| ✓ | ***6.1.8 Independent review of information security*** | **SM7.1 Security audit/review** | **CB5.4 Security audit/review** | **CB5.4 Security audit/review** | **CI5.5 Security audit/review** | **NW4.5 Security audit/review** | **SD2.3 Security audit/review** |
| ✓ | ***6.2 External parties*** | | | | | | |
| ✓ | ***6.2.1 Identification of risks related to external parties*** | **SM6.5 Third party access** | **CB6.1 Third party agreements** | **CB6.1 Third party agreements** | **SM6.5 Third party access** | **SM6.5 Third party access** | **SM6.5 Third party access** |
| ✓ | ***6.2.2 Addressing security when dealing with customers*** | **SM6.5 Third party access** | **CB6.1 Third party agreements** | **CB6.1 Third party agreements** | **SM6.5 Third party access** | **SM6.5 Third party access** | **SM6.5 Third party access** |
| ✓ | ***6.2.3 Addressing security in third party agreements*** | **SM6.5 Third party access** | **CB6.1 Third party agreements** | **CB6.1 Third party agreements** | **SM6.5 Third party access** | **SM6.5 Third party access** | **SM6.5 Third party access** |
| | **Possible extra ISF Objective** | | | | | | |
| ✓ | **Security architecture** | **SM4.1 Security architecture**<br>**SM1.2 Security Policy** | | | | | |
| | | | | | | | |
| | **7 Asset management** | | | | | | |
| | ***7.1 Responsibility for assets*** | | | | | | |
| ✓ | ***7.1.1 Inventory of assets*** | **SM4.3 Asset management** | | | **CI1.3 Asset Management** | | |
| ✓ | ***7.1.2 Ownership of assets*** | **SM3.2 Ownership** | **CB2.1 Roles & responsibilities** | **CB2.1 Roles & responsibilities** | **CI1.1 Roles & responsibilities** | **NW1.1 Roles & responsibilities** | **SD1.1 Roles & responsibilities** |
| ✓ | ***7.1.3 Acceptable use of assets*** | **SM1.3 Staff agreements** | | | | | |
| | ***7.2 Information classification*** | | | | | | |
| ✓ | ***7.2.1 Information shall be classified in terms of its value, legal requirements, sensitivity and criticality to the organization.*** | **SM3.1 Security classification** | | **CB5.2 Security classification** | **CL5.3 Security classification** | **NW4.3 Security classification** | |
| ✓ | ***7.2.2 An appropriate set of procedures for information labelling and handling shall be developed and implemented in accordance with the classification scheme adopted by the organization.*** | **SM3.1 Security classification** | | **CB2.6 Sensitive information** | **CL5.3 Security classification** | **NW4.3 Security classification** | |
| | **8 Human resources security** | | | | | | |
| ✓ | ***8.1 Prior to employment*** | | | | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| ✓ | ***8.1.1 Roles and responsibilities*** | **SM2.3 Local security management SM3.2 Ownership SM1.3.1 Responsibilities in JD & TC of Emp** | **SM2.3 Local security management SM3.2 Ownership CB2.1 Roles & responsibilities** | **CB2.1 Roles & responsibilities** | **CI1.1 Roles & responsibilities CI1.2 Service agreements** | **NW 1.1 Roles &Responsibilities** | **SD1.1 Roles &Responsibilities** |
| ✓ | ***8.1.2 Screening*** | **SM1.3.5 Appropriate screening** | | | | | |
| ✓ | ***8.1.3 Terms and conditions of employment*** | **SM1.31, SM1.3.2 T&C** | | | | | |
| | ***8.2 During employment*** | | | | | | |
| ✓ | ***8.2.1 Management responsibilities*** | **SM2.3 Local security management SM3.2 Ownership SM1.3.1 Responsibilities in JD & TC of Emp** | **SM2.3 Local security management SM3.2 Ownership CB2.1 Roles & responsibilities** | **CB2.1 Roles & responsibilities** | **CI1.1 Roles & responsibilities CI1.2 Service agreements** | **NW 1.1 Roles &Responsibilities** | **SD1.1 Roles &Responsibilities** |
| ✓ | ***8.2.2 Information security awareness, education and training*** | **SM2.4 Security awareness SM2.5 Security education** | | **CB3.4 Security awareness** | **CI5.2 Security awareness** | **NW4.3 Security awareness** | **SD2.2 Security awareness** |
| ✓ | ***8.2.3 Disciplinary process*** | **SM1.2.7 Sec Pol** | | | | | |
| ✓ | ***8.3 Termination or change*** | | | | | | |
| ✓ | ***8.3.1 Termination responsibilities*** | **SM3.2 Ownership** | **CB2.1 Roles & responsibilities CB3.1 Access control** | **CB2.1 Roles & responsibilities CB3.1 Access control** | **CI1.2.3 Service agreements** | | |
| ✓ | ***8.3.2 Return of assets*** | **SM3.2 Ownership** | **CB2.1 Roles & responsibilities CB3.1 Access control** | **CB2.1 Roles & responsibilities CB3.1 Access control** | **CI1.2.3 Service agreements** | | |
| ✓ | ***8.3.3 Removal of access rights*** | **SM3.2 Ownership** | **CB2.1 Roles & responsibilities CB3.1 Access control** | **CB2.1 Roles & responsibilities CB3.1 Access control** | **CI1.2.3 Service agreements** | | |
| ✓ | **9 Physical and environmental security** | | | | | | |
| ✓ | ***9.1 Secure areas*** | **SM4.4. Physical protection** | | | | | |
| ✓ | ***9.1.1 Physical security perimeter*** | **SM4.4 Physical protection** | **SM4.4 Physical protection** | **SM4.4 Physical protection** | **CI2.1 Installation Design** | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | CI2.8 Physical Access | | |
| ✓ | *9.1.2 Physical entry controls* | SM4.4 Physical protection | SM4.4 Physical protection | SM4.4 Physical protection | CI2.1 Installation Design CI2.8 Physical Access | | |
| ✓ | *9.1.3 Securing offices, rooms and facilities* | SM4.4 Physical protection | SM4.4 Physical protection | SM4.4 Physical protection | CI2.1 Installation Design CI2.8 Physical Access | NW3.4 Physical security | |
| ✓ | *9.1.4 Protecting against external and environmental threats* | SM4.4 Physical protection | SM4.4 Physical protection | SM4.4 Physical protection | CI2.6 Hazard Protection | | |
| ✓ | *9.1.5 Working in secure areas* | | SM4.4 Physical protection | SM4.4 Physical protection | CI2.1 Installation Design | | |
| ✓ | *9.1.6 Public access, delivery and loading areas* | | SM4.4 Physical protection | SM4.4 Physical protection | CI2.1 Installation Design | | |
| ✓ | *9.2 Equipment security* | | | | | | |
| ✓ | *9.2.1 Equipment siting and protection* | | CB3.3 Workstation configuration | CB3.3 Workstation configuration | CI2.6 Hazard Protection | | |
| ✓ | *9.2.2 Supporting utilities* | | CB3.3 Workstation configuration | CB3.3 Workstation configuration | CI2.6 Hazard Protection CI2.7 Power supplies | | |
| ✓ | *9.2.3 Cabling security* | | CB3.3 Workstation configuration | CB3.3 Workstation configuration | CI2.6 Hazard Protection | | |
| ✓ | *9.2.4 Equipment maintenance* | | CB3.3 Workstation configuration | CB3.3 Workstation configuration | | | |
| ✓ | *9.2.5 Security of equipment off-premises* | | CB3.3 Workstation configuration | CB3.3 Workstation configuration | | | |
| ✓ | *9.2.6 Secure disposal or re-use of equipment* | | | | | | |
| ✓ | *9.2.7 Removal of property* | | | | | | |
| ✓ | Resilience | | | CB4.2 Resilience | CI2.5 Resilience | NW1.3 Network resilience NW5.2 Resilience of voice networks | |
| ✓ | Host system Configuration | | | | CI2.3 Host system configuration | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| ✓ | **Work Station Configuration** | | | | **CI2.4 Work station configuration** | | |
| ✓ | **10 Communications and operations management** | | | | | | |
| ✓ | ***10.1 Operational procedures & responsibilities*** | | | | | | |
| ✓ | ***10.1.1 Documented operating procedures*** | **SM4.1 Security architecture** | | | | | |
| ✓ | ***10.1.2 Change management*** | | **CB2.3 Change management** | **CB2.3 Change management** | **CI3.3 Change Management** | **NW3.2 Change management** | |
| ✓ | ***10.1.3 Segregation of duties*** | | **CB2.1.5 Roles CB4.1.3 Servcie agreements** | **CI1.1.3 R&R CI2.2.2 Restrictions on utilities CI4.1.2 Access control arrangements** | **NW1.1.3** | **SD4.3.2 Assessment of security controls** | |
| ✓ | ***10.1.4 Separation of development, test and operational facilities*** | | | | **CI2.1.3 Installation design** | **SD 1.4 Development environments** | |
| | ***10.2 Third party service delivery management*** | | | | | | |
| ✓ | ***10.2.1 Service delivery*** | **SM6.7 Outsourcing** | | **CB4.1 Service agreements (internal or external)** | **CI1.2 Service agreements** | **NW1.5 Service providers** | |
| ✓ | ***10.2.2 Monitoring and review of third party services*** | **SM6.7 Outsourcing** | | **CB4.1 Service agreements (internal or external** | **CI1.2 Service agreements** | **NW1.5 Service providers** | |
| ✓ | ***10.2.3 Managing changes to third party services*** | **SM6.7 Outsourcing** | | **CB4.1 Service agreements (internal or external** | **CI1.2 Service agreements** | **NW1.5 Service providers** | |
| | ***10.3 System planning & acceptance*** | | | | | | |
| ✓ | ***10.3.1 Capacity management*** | | **CB4.1 Service agreements** | **CB4.1 Service agreements** | **CI1.2.2 Service agreements C1.4.2 System monitoring** | **NW1.2 Network design NW1.5.2 Service providers NW3.1.2 Network monitoring** | |
| ✓ | ***10.3.2 System acceptance*** | | | | **CI2.3 Host** | | **SD6.1 System** |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | **system configuration** | | **promotion criteria SD6.2 Installation process SD6.3 Post-implementation review** |
| | ***10.4 Protection v malicious & mobile code*** | | | | | | |
| ✓ | ***10.4.1 Controls against malicious code*** | **SM5.1 Virus protection** | | | | | |
| ✓ | ***10.4.2 Controls against mobile code*** | **SM5.2 malicious mobile code protection** | | | | | |
| | ***10.5 Back up*** | | | | | | |
| ✓ | ***10.5.1 Information back-up*** | | | **CB4.4 Back-up** | **CI3.2 Back up** | **NW3.5 Back up** | |
| | ***10.6 Network security management*** | | | | | | |
| ✓ | ***10.6.1 Network controls*** | | | | | **NW1.Network Management NW4 Local security management** | |
| ✓ | ***10.6.2 Security of network services*** | | | | | **NW1.5 Service providers** | |
| ✓ | ***10.7 Media Handling*** | | | | | | |
| ✓ | ***10.7.1 Management of removable media*** | | | | **CI3.1 Handling computer media** | | |
| ✓ | **Handling of documents?** | | | | | | |
| ✓ | ***10.7.2 Disposal of media*** | | | | **CI3.1.6 Handling computer media** | | |
| ✓ | ***10.7.3 Information handling procedures*** | | **CB2.6 Sensitive information** | **CB2.6 Sensitive information** | | | |
| ✓ | ***10.7.4 Security of system documentation*** | | | | **CI3.1.5** | | |
| ✓ | ***10.8 Exchange of information*** | | | | | | |
| ✓ | ***10.8.1 Information exchange policies and procedures*** | | | | | | |
| ✓ | ***10.8.2 Exchange agreements*** | **SM3.2.2 Owners** | | | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | **responsibility to develop** | | | | | |
| ✓ | ***10.8.3 Physical media in transit*** | | | | **CI3.1.6 Handling computer media** | | |
| ✓ | ***10.8.4 Electronic messaging*** | **SM6.8 Instant messaging SM6.3 Email** | **CB6.4 Web-enabled applications** | **CB6.4 Web-enabled applications** | | | |
| ✓ | ***10.8.5 Business information system (e-info sharing)*** | | **CB6.4 Web-enabled applications** | **CB6.4 Web-enabled applications** | | | |
| ✓ | ***10.9 Electronic commerce services*** | | | | | | |
| ✓ | ***10.9.1 Electronic commerce*** | **SM6.6 Electronic commerce** | | **CB6.4 Web-enabled applications** | | | |
| ✓ | ***10.9.2 On-line transactions*** | **SM6.6 Electronic commerce** | | **CB6.4 Web-enabled applications** | | | |
| | ***10.10 Monitoring*** | | | | | | |
| ✓ | ***10.10.1 Audit logging*** | | **CB2.2.6 Application CB3.1.6 User environment** | **CB 2.2.6 Application controls CB3.1.6 User environment** | **CI1.4 System monitoring** | **NW1.2.2 Network design** | |
| ✓ | ***10.10.2 Monitoring system use*** | | | | **CI1.4 System monitoring CI2.2 Event logging** | **NW3.1 Network monitoring** | |
| ✓ | ***10.10.3 Protection of log information*** | | **CB3.17 Protection of logs** | **CB3.17 Protection of logs CI2.2.4 Format of logs** | **CI1.4 System monitoring** | | |
| ✓ | ***10.10.4 Administrator and operator logs*** | | **CB5.4.5** | **CI2.2. Event logging** | **CI1.4 System monitoring** | NW2.1.2, nw2.3.6 | |
| ✓ | ***10.10.5 Fault logging*** | | | **CI2.2. Event logging** | **CI1.4 System monitoring** | | |
| ✓ | ***10.10.6 Clock synchronization*** | | | **CI2.1.5 Clock standard** | | | |
| | **10.11 Malicious attack** | | | | | | |
| ✓ | ***Intrusion detection*** | **SM 5.3 Intrusion detection** | | | **CI1.4 System monitoring** | | |
| ✓ | ***Emergency response*** | **SM5.4 Emergency response** | | | **CI3.5 Emergency** | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | fixes | | |
| ✓ | *Forensic investigations* | SM5.5 Forensic investigation | | | | | |
| ✓ | *Patch management* | SM5.6 Patch management | | | CI2.3.6 CI3.6 Patch Management | NW1.3.5 Firewall patches | |
| ✓ | *Penetration testing* | SM7.1.3 | CB5.4.5 | CB5.4.5 | CI5.5.5 | NW4.5.5 | SD5.2.2 |
| ✓ | 11 Access control | | | | | | |
| ✓ | *11.1 Business requirement for access control* | | | | | | |
| ✓ | *11.1.1 Access policy* | SM4.1 Security architecture SM4.2 Information privacy | CB1.1 Confidentiality requirements | CB1.1 Confidentiality requirements | CI4.1 Access Control Arrangements | | |
| | *11.2 User access management* | | | | | | |
| ✓ | *11.2.1 User registration* | | CB3.1 Access control CB3.2 Application sign on process | CB3.1 Access control CB3.2 Application sign on process | CI4.2 User authorisation | | |
| ✓ | *11.2.2 Privilege management* | | CB3.1 Access control | | CI4.3 Access privileges | | |
| ✓ | *11.2.3 User password management* | | CB3.2 Application sign on process | | CI4.2 User authorisation | | |
| ✓ | *11.2.4 Review of user access rights* | | CB3.1 Access control | | CI4.2 User authorisation | | |
| ✓ | *11.3 User Responsibilities* | | | | | | |
| ✓ | *11.3.1 Password use* | SM2.4 Security awareness | CB3.4 Security awareness | CB3.4 Security awareness | | | |
| ✓ | *11.3.2 Unattended user equipment* | SM2.4 Security awareness | CB3.4 Security awareness | CB3.4 Security awareness | | | |
| ✓ | *11.3.3 Clear desk and clear screen policy* | SM2.4 Security awareness | CB3.4 Security awareness | CB3.4 Security awareness | | | |
| | *11.4 Network access control* | | | | | | |
| ✓ | *11.4.1 Policy on use of network services(user level access)* | | | | | NW2.1.2 Network devices CI4.1 Access control arrangements | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| ✓ | ***11.4.2 User authentication for external connections*** | | **CB4.3 External connections** | **CB4.3 External connections** | | **NW2.3 External access**<br>**NW2.4 Wireless access**<br>**NW3.7 Remote maintenance** | |
| ✓ | ***11.4.3 Equipment identification in networks*** | | | | | **NW1.4 Network documentation**<br>**NW5.1 Voice network documentation** | |
| ✓ | ***11.4.4 Remote diagnostic and configuration port protection*** | | | | | **MW2.1 Configuring network devices** | |
| ✓ | ***11.4.5 Segregation in networks*** | | | | | **NW1.2 Network design**<br>**NW2.1 Configuring network devices**<br>**NW2.2 Firewalls** | |
| ✓ | ***11.4.6 Network connection control*** | | | | | **NW2.2 Firewalls**<br>**Nw2.3 External access** | |
| ✓ | ***11.4.7 Network routing control*** | | | | | **NW2.1 configuring network devices** | |
| | ***11.5 Operating system access control*** | | | | | | |
| ✓ | ***11.5.1 Secure log-on procedures*** | | **CB3.2 Application sign-on process** | **CB3.2 Application sign-on process** | **CI4.4 Sign –on process**<br>**CI4.5 User authentication** | | |
| ✓ | ***11.5.2 User identification and authentication*** | | **CB3.2 Application sign-on process** | **CB3.2 Application sign-on process** | **CI4.4 Sign –on process CI4.5 User authentication** | | |
| ✓ | ***11.5.3 Password management system*** | | **CB3.2 Application sign-on process** | **CB3.2 Application sign-on process** | **CI4.4 Sign –on process CI4.5 User authentication** | | |
| ✓ | ***11.5.4 The use of utility programs that might be capable of overriding system and*** | | | | **CI2.3.3 Host system** | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | ***application controls shall be restricted and tightly controlled.*** | | | | **configuration** | | |
| ✓ | ***11.5.5 Session time-out*** | | **CB3.3.3 time-out** | **CB3.3.3 time-out** | **CI2.3.1 & CI2.3.4 Host system configuration** | | |
| ✓ | ***11.5.6 Limitation of connection time (optional technique)*** | | | | **CI2.3.1 & CI2.3.2 Host system configuration** | | |
| | ***11.6 Application & information access control*** | | | | | | |
| ✓ | ***11.6.1 Information access restriction*** | | | **CB3.1 Access control**<br>**CB3.2 Application sign-on process** | | | |
| ✓ | ***11.6.2 Sensitive system isolation*** | | | **CB2.6 Sensitive information**<br>**CB6.4 Web-enabled applications** | | | |
| | ***11.7 Mobile computing & teleworking*** | | | | | | |
| ✓ | ***11.7.1Mobile computing and communications*** | **SM6.4 Remote working** | | **CB3.3 workstation configuration** | | | |
| ✓ | ***11.7.2 Teleworking*** | **SM6.4 Remote working** | | **CB3.3 workstation configuration** | | | |
| ✓ | **12 Information systems acquisition, development and maintenance** | | | | | | |
| ✓ | ***12.1 Security requirements of information systems*** | | | | | | |
| ✓ | ***12.1.1 Security requirements analysis and specification*** | **SM1.2 Security Policy**<br>**SM4.1 Security architecture**<br>**SM4.2 Information privacy** | **CB1.1 Confidentiality requirements**<br>**CB1.2 Integrity requirements**<br>**CB 1.3 Availability requirements** | **CB1.1 Confidentiality requirements**<br>**CB1.2 Integrity requirements**<br>**CB 1.3 Availability requirements** | **CI1.2 Service agreements** | | **SD3.1 Specification of requirements**<br>**SD3.2 Confidentiality requirements**<br>**SD3.3 Integrity requirements**<br>**SD3.4 Availability requirements**<br>**SD3.5 Information risk** |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | | | **analysis SD1.2 Development methodology SD1.3 Quality assurance** |
| ✓ | ***12.2.1 Input data validation*** | | | **CB2.2 Application Controls** | | | **SD4.1 System design SD4.2 Application controls SD4.3 General security controls SD4.4 Acquisition** |
| ✓ | ***12.2.2 Control of internal processing*** | | | **CB2.2 Application Controls** | | | |
| ✓ | ***12.2.3 Message integrity*** | | | **CB2.2 Application Controls** | | | |
| ✓ | ***12.2.4 Output data validations*** | | | **CB2.2 Application Controls** | | | |
| ✓ | ***12.3 Cryptographic controls*** | | | | | | |
| ✓ | ***12.3.1 Policy on the use of cryptographic control*** | **SM6.1 Cryptography** | | | | | **SD4.3 General security controls** |
| ✓ | ***12.3.2 Key management*** | **SM6.2 PKI management** | | **CB6.2 Cryptographic key management CB6.3 Public key infrastructure** | | | **SD4.3 General security controls** |
| ✓ | ***12.4 Security of system files*** | | | | | | |
| ✓ | ***12.4.1 Control of operational software*** | | | | | | **SD1.4 Development environment** |
| ✓ | ***12.4.2 Protection of system test data*** | | | | | | **SD1.4 Development environment** |
| ✓ | ***12.4.3 Access to program source code shall be restricted.*** | | | | | | **SD1.4 Development environment** |
| ✓ | ***12.5 Security in development & support processes*** | | | | | | |
| ✓ | ***12.5.1 Change control procedures*** | | | | | | **SD6** |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | | | **Implemntation** |
| ✓ | ***12.5.2 Technical review of applications after operating system changes*** | | | | | | **SD6 Implemntation** |
| ✓ | ***12.5.3 Restrictions on changes to software packages*** | | | | | | **SD6 Implemntation** |
| ✓ | ***12.5.4 Information leakage*** | | | | | | SD3.2 Confidentiality requirements SD 1.4 Development environment |
| ✓ | ***12.5.5 Outsourced software development*** | **SM6.7 Outsourcing** | | | | | |
| | ***12.6 Technical vulnerability management*** | | | | | | |
| ✓ | ***12.6.1 Control of technical vulnerabilities(patch management)*** | **SM 2.2.4, SM 3.3.5, SM6.6.3 SM5.6 Patch management SM7.1.3 Security audit/review** | **CB 5.3, CB 5.4** | **CB 5.3, CB 5.4** | **CI1.4 System monitoring CI3.6 Patch management CI5.4, CI5.5** | **NW1.3.5 NW 3.1.3 NW4.4, NW4.5** | |
| | **13 Information security incident management** | | | | | | |
| | ***13.1 Reporting events & weaknesses*** | | | | | | |
| ✓ | ***13.1.1 Reporting information security events*** | **27001 SM2.2 Information Security function** | **CB2.4 Incident management** | **CB2.4 Incident management** | **CI3.4 Incident management** | **NW3.3 Incident management** | |
| ✓ | ***13.1.2 Reporting security weaknesses*** | **27001 SM2.2 Information Security function** | **CB2.4 Incident management** | **CB2.4 Incident management** | **CI3.4 Incident management** | **NW3.3 Incident management** | |
| | ***13.2 Management of incidents*** | | | | | | |
| ✓ | ***13.2.1 Responsibilities and procedures*** | | | **CB2.4 Incident management** | **CI3.4 Incident management CI3.5 Emergency fixes SM5.4 Emergency response** | **NW3.3 Incident management** | |
| ✓ | ***13.2.2 Learning from information security incidents*** | **27001 SM2.2 Information Security function** | | **CB2.4 Incident management** | **CI3.4 Incident management** | **NW3.3 Incident management** | |
| ✓ | ***13.2.3 Collection of evidence*** | **SM5.5 Forensic** | | **CB2.4 Incident** | **CI3.4 Incident** | **NW3.3 Incident** | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | investigation | | management | management | management | |
| | 14 Business continuity | | | | | | |
| | *14.1 Info sec aspects of BCM* | | | | | | |
| ✓ | *14.1.1 Including information security in the business continuity management process* | SM4.5 Business continuity | | CB2.5 Business continuity | | | |
| ✓ | *14.1.2 Business continuity and risk assessment* | SM4.5 Business continuity | | CB2.5 Business continuity | CI6.1 Contingency Plan | | |
| ✓ | *14.1.3 Developing and implementing continuity plans including information security* | SM4.5 Business continuity | | CB2.5 Business continuity | CI6.1 Contingency Plan<br>CI6.2 Contingency arrangements | NW3.6 Service continuity | |
| ✓ | *14.1.4 Business continuity planning framework (plan of plans)* | SM4.5 Business continuity | | CB2.5 Business continuity | CI6.1 Contingency Plan | | |
| ✓ | *14.1.5 Testing, maintaining and re-assessing business continuity plan* | SM4.5 Business continuity | | CB2.5 Business continuity | CL6.3 Validation & maintenance | | |
| | 15 Compliance | | | | | | |
| ✓ | *15.1 Compliance with Legal Req's* | | | | | | |
| ✓ | *15.1.1 Identification of applicable legislation* | 270001<br>SM1.2.3 Security Policy<br>SM1.3.2 Staff Agreements | CB1.1, CB1.2, CB1.3 CIA Requirements | CB1.1, CB1.2, CB1.3 CIA Requirements | | | |
| ✓ | *15.1.2 Intellectual property rights (IPR)* | 270001<br>SM1.2.3 Security Policy<br>SM1.3.2 Staff Agreements | | | | | |
| ✓ | *15.1.3 Protection of organizational records* | | | | | | |
| ✓ | *15.1.4 Data protection and privacy of personal information* | SM4.2Information privacy | | | | | |
| ✓ | *15.1.5 Prevention of misuse of information processing facilities* | SM1.3 Staff agreements<br>SM6.3 E-mail | | | | | |
| ✓ | *15.1.6 Regulation of cryptographic controls* | SM6.1 use of | | | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | **cryptography SM6.2 Public Key Infrastructure** | | | | | |
| | ***15.2 Compliance with sec policies & standards & technical compliance*** | | | | | | |
| ✓ | ***15.2.1 Compliance with security policies and standards*** | **SM7.1 Security audit/review SM7.2 Security monitoring** | **CB5.1 Local security-co-ordination CB5.3 Information risk analysis CB5.4 Security audit/review** | **CB5.1 Local security-co-ordination CB5.3 Information risk analysis CB5.4 Security audit/review** | **CI5.1 Local security-co-ordination CIB5.4 Information risk analysis CI5.5 Security audit/review** | **NW4.1 Local security-co-ordination NW4.4 Information risk analysis NW4.5 Security audit/review** | **SD2.1 Local security co-ordination SD2.3 Security audit/review** |
| ✓ | ***15.2.2 Technical compliance checking*** | **SM7.1 Security audit/review** | | | | | |
| ✓ | ***15.3 Info systems audit considerations*** | | | | | | |
| ✓ | ***15.3.1 Information systems audit controls*** | **SM7.1 Security audit/review** | **CB5.4 Security audit/review** | **CB5.4 Security audit/review** | **CI5.5 Security audit/review** | **NW4.5 Security audit/review** | |
| ✓ | ***15.3.2 Protection of information systems audit tools*** | **SM7.1 Security audit/review** | **CB5.4 Security audit/review** | **CB5.4 Security audit/review** | **CI5.5 Security audit/review** | **NW4.5 Security audit/review** | |

**Part 2 Section 3 Roles & Responsibilities**

**Information security processes required for compliance with ISO/IEC 27001:2005/ISO17799: 2005 - Allocation of responsibilities**

**Purpose of this document**

This document outlines roles and responsibilities in relation to the Information Security Management System implemented by Lancashire County Council. It has been produced to meet the requirements of the Information Security Policy which requires clear definition of roles and responsibilities.

**1.0 Information assets and information security roles**

1.1 The standard refers to accountabilities for and ownership of individual systems, assets or security processes. The Standard's definition of an "asset" is wide but flexible: staff and their skills, relationships with partners and intangibles such as organisational reputation may be regarded as an asset and if systems are sufficiently complex assets may be grouped as a service and the service assigned an owner.

1.2 The Standard requires general and specific responsibilities to be defined but allows delegation by asset/system owners. At the Information Security Policy level definition needs to be taken only as far as is necessary to ensure that assets have owners and to be able to determine who this is or should be.

1.3 Given that the standard is asking for definition of responsibilities in relation to information assets in general and does not categorise them in any way organisations which apply the standard must adopt a way of defining assets. Given the size and variety of the Authority's assets it make sense to simply identify specific categories of "assets to be secured" for the purposes of the framework. Risk analysis and design of controls may then take place by reference to these categories with variations applied in individual circumstances.

1.4 Assets are classified into the categories shown in the following table:

| Information asset | Focus | Overall objective in this area | Scope & coverage |
|---|---|---|---|
| Operational workforce | Employees who provide a discrete service and who use information systems. Groups yet to be identified. | How the security requirements of employees and their personal facilities are identified, communicated and enforced | Levels of awareness<br>Personal ICT security<br>Communication<br>HR issues<br>Relations with support staff |
| Critical business application/group of applications | A business application(s) that is critical to the success of the enterprise | The security requirements of the area of activity supported by the application and the arrangements made for identifying risks and keeping them within acceptable levels | The status of critical business applications of any:<br>• Type (including e.g. transaction processing, process control, funds transfer, customer service & desktop applications but also paper systems)<br>• Size (e.g. applications supporting from one or a few to '000's of users) |
| Computer installations | A computer installation that supports one or more business applications | How requirements for computer services are identified and how the computers are set up and run in order to meet | • The status of computer installations:<br>• Of all sizes (mainframes down to a |

| | | | |
|---|---|---|---|
| | | those requirements | PC)<br>• Running in any environment(e.g. data centre, workshop, desktop)<br>• any operating systems |
| Networks | A network that supports one or more business applications | How requirements for network services are identified and how the computers are set up and run in order to meet those requirements | Any type of network including:<br>• wide area or local area networks<br>• large or small scale<br>• those based on Internet technology such as intranets or extranets<br>• voice, data or integrated |
| Systems development | A systems development unit or a particular systems development project. | How business requirements(including information security requirements) are identified & how systems are designed and built to meet those requirements. | The status of developments of all types including:<br>• projects of all sizes<br>• those conducted by any developer including business user, specialists or outsourced<br>• those based on tailor made software or application packages |

1.5 Given that these assets will have been developed to support business units, security of information may be provided either at Directorate level or from within the business units and/or through the provision of services by other business areas (most notably support functions such as ICT Services, Property Group, HR, Legal Services etc). Under this approach the main requirement is to define areas comprehensively.

1.6 Given that this project covers the formal implementation of a management standard, roles need to be defined for security management which is not an information asset in its own right.

| **Additional security area** | **Focus** | **Overall objective in this area** | **Scope & coverage** |
|---|---|---|---|
| Security Management | Security Management at enterprise and departmental level | Senior management commitment to promoting good information security practices across the enterprise. Central co-ordination and policy maintenance. Demonstrability | County-wide. All Directorates and Business units |

1.7 The approach therefore is to define simplified roles within the organisation and then outline responsibilities for each of those roles. This has been done in a way which reflects the Standard (ISO7799) and management arrangements within Lancashire County Council.

**2.0 INFORMATION SECURITY ROLES**

2.0.1 The following broad, simplified roles are suggested.

- Leaders
- Management
- Users
- Support

**2.1 LEADERS**

2.1.1 Leaders are mainly Executive Directors and Directors, anyone else who may act as a policymaker within the County Council and conceivably including Members from time to time. This is the level which authorises a policy and the manner of its implementation. Policy approved at this level may be formulated in a more detailed way in some key areas.

2.1.2 This group includes the Corporate Steering Groups CICT&EGSG and CIM&SG, CITG and may include CMB.

2.1.3 The main interest of leaders is at policy level and therefore responsibilities are defined in relation to the high level areas of the standard.

2.1.4 Those high level issues are the approval of a security policy, the manner of its application and authorisation of the security organisation (allocation of responsibilities etc). To have an acceptable ISMS (in terms of the standard), Leadership needs to

- publicly endorse the security policy,
- ensure the ISMS procedures are followed,
- establish roles & responsibilities
- ensure adequate training and resources and
- to agree risk acceptance criteria.

**2.2 MANAGEMENT**

2.2.1 It is assumed that there is a **senior management** level below Director Level in all Directorates, which is responsible for activities in discrete areas. This level would supply system owners, to use the ISO27001 phraseology, and be accountable for information security in their own areas. Core systems cross Directorate boundaries and “owners” would need to be specifically nominated.

2.2.2 In implementing the direct management responsibilities for information security, managers will be assisted by support groups and by delegation to a level of **middle management** who would be responsible for implementation and enforcement of these policies in a practical way.

2.2.3 However, as system owners, managers remain accountable for the security of information and systems within their business areas. In terms of allocation of responsibilities, this means that even though others (either from within the County or externally sourced) may provide security services, senior managers ultimately own any residual risks which remain after those services have been supplied.

2.2.4 The precise picture of who is responsible for managing particular parts of an information system will necessarily vary between business areas. It is therefore vital for managers to understand the security requirements which apply to their own areas and to understand how and, by whom, they are to be delivered.

2.2.5 The major responsibilities of this role are as follows.

**a. Understanding the security requirements of the business area**

- Basic requirements of the security policy and any special local risks
- The means of delivery.

**b. Ensuring that support groups supply security services at the appropriate level**

- ICT Services - virus controls, access controls, secure communications etc
- Property Group – building security etc
- Other support functions – advice and guidance

**c. Ensuring staff receive appropriate training and direction**

- Training
- Awareness
- Communication with support groups

**d. Business continuity planning**

- A general problem which includes information systems
- Safeguarding organisational records: ensuring that sensitive and /or business critical information is protected from damage or loss.

**e. Ensuring legal and policy compliance**

- Compliance with software licence conditions
- Compliance with Data Protection legislation; defining local procedures
- Procedures for ensuring compliance with the security regime; defining local procedures and including operation of disciplinary procedures when necessary.

**f. Ensuring security considerations are taken into account in non-standard situations**

- In purchasing and developing information systems
- When other significant changes occur
- When third party access occurs, in third party contracts or outsourcing

g. **Ensuring that corporate security information requirements are met**

- Asset inventory information – new and changed information is reported
- Security incidents, malfunctions and weaknesses are reported
- Information about staff starting, leaving or changing duties and information re authorisations is reported.

**2.3 USERS**

2.3.1 Any member of staff using an ICT system in whatever capacity is a user and has certain general responsibilities. The exact nature of these responsibilities may vary according to an individual's job. The thing which they all have in common is that they are the responsibility of, and can only be carried out by, the individual.

2.3.2 The requirements are scattered through the standard but may be summarised under the following headings.

a. **Access control systems**.

- These may be either logical (passwords, screensavers, menus etc) or physical (secure areas, intruder alarms etc).
- It is the user's responsibility to comply with requirements in these areas as overall security depends on users employing good practice.

b. **Looking after assets**.

- Assets may consist of hardware, software, data or people but the Standard is not concerned with human health and safety per se. Safe custody and management of assets depends greatly on co-operation by users.
- Informing the relevant administrator of the asset inventory database of changes
- Compliance with good custodial procedures (taking equipment or data off site, security of floppy disks/CD's, printed information and paper files, siting of equipment etc).

**c. Legal compliance**

- The Data Protection Act places requirements on users of systems which process personal data.
- The Copyright Designs & Patents Act prohibitions re copying of software and
- The Computer Misuse Act prohibitions against users who access systems to which they are not authorised.
- Information technology is now becoming relevant to compliance with other legislation by, for example, creating new risks (downloading pornography, libel by email) etc or new situations not covered by current law(digital signatures).

d. **Incidents** .

- Feedback from users of systems on any security related incidents, malfunctions and weaknesses. Users must always report these events so that they can be dealt with and lessons learned.

e. **Miscellaneous**.

- Aspects of good user practice which do not fit into easy categories, some of which may be publicised as a specific topic (the Internet Acceptable Use Policy) and others may be specialised points of practice.
- Users should ascertain which advice is relevant and follow the advice. Local interpretations of the general rules may exist.
- Users should ensure they are up to date with issued advice.

f. **Personal Computers and Mobile Devices including removable storage.**

- User responsibilities as defined here exclude management and technical responsibilities. However, if a user has responsibility for a PC, laptop or portable or even a locally based server, some of the management or technical responsibilities may apply in respect of that machine or the systems or data held on it.

**2.4 SUPPORT FUNCTIONS**

**There are functions which provide services and advice within the County Council which are relevant to information security.**

**2.5 SUPPORT FUNCTION: CORPORATE INFORMATION SECURITY MANAGER**

2.5.1 The Corporate Information Security Manager has an on going role to advise and co-ordinate information security issues within the Authority. The Corporate Manager is required as this subject needs a focus within the organisation.

a. **Advice and guidance**

- agree and provide general guidance and ad hoc advice for managers, users, technical staff and other support groups on security issues.

**b. Co-ordination**

- develop & maintain policy
- monitor risks, threats and incidents and, through consultation and research, develop appropriate controls to mitigate or avoid the potential outcomes.

**c. General training and awareness measures**

- Develop appropriate training & awareness material and organise its delivery

**d. Compliance**

- Maintain ISMS
- Monitor operation of controls
- Authorise departures where necessary

**2.6 SUPPORT FUNCTION: ICT PROFESSIONALS**

2.6.1 There are central and (decreasingly) Directorate ICT staff who provide support for live and developing systems and technical infrastructure. The security role of ICT staff is to provide a secure environment in which information processing can take place. Because of the need for technical input there may be occasions when technical considerations determine aspects of guidelines, standards and procedures of the ISMS.

**a. Design, operation and management of a secure network to documented standards**

- Arrangements should be documented in consultation with the Information Security Manager and CIM&SG Group and when relevant, with business managers. In terms of a secure network infrastructure it must be said that security is largely a strategic or technical matter.
- The aim of a secure infrastructure is to create a secure environment in which to process information and to minimise security related procedures which users need to operate; technical staff will operate the infrastructure in such a way as to ensure confidentiality, integrity and availability of systems and data. In some ways the installations and networks are special examples of critical business applications and managers have the same responsibilities as those outlined for owners of critical business applications.
- There is also an area of technical security in areas such as system software configuration which users will not normally be concerned about, which IT professionals should implement. In this latter case consultation is unlikely to be required.
- Special measures may be needed with regard to personnel security as many IT professionals need unrestricted access privileges in order to be able to carry out their primary function.

**b. Operation of those parts of the infrastructure which are security controls in themselves**

- Typically these include services such as access controls systems, anti-virus software, patch management, firewall installation, security aspects of configurations of devices such as routers, back up of data, disaster recovery and monitoring of network events.

c. **Application development**

- Analysis of security requirements
- Integration of requirements into systems

**d. Advice and assistance**

- Technical specification
- Special investigations
- Specifying procedures which might be carried out by non-technical staff yet which have a technical content.

**2.7 SUPPORT FUNCTIONS: PROPERTY GROUP, PERSONNEL, LEGAL SECTION, INTERNAL AUDIT**

2.7.1 Examples of services to business areas which may have a relevance to information security.

a. Property Group provides building security in various ways and installs cabling and power supplies.
b. Human Resources operates recruitment, training and disciplinary procedures.
c. Legal Section advise on legal matters.
d. Internal Audit provides an independent check on compliance and conduct investigations including forensic collection of evidence.

**Part 2 Section 4 Training and awareness plan**

**ISMS requirements for information security training**

Clause 5.2.2 of BS 27001:2005 sets out the following requirements

*5.2.2 Training, awareness and competence*

*The organization shall ensure that all personnel who are assigned responsibilities defined in the ISMS are competent to perform the required tasks by:*
*a) determining the necessary competencies for personnel performing work effecting the ISMS; .*
*b) providing training or taking other actions (e.g. employing competent personnel) to satisfy these needs;*
*c) evaluating the effectiveness of the actions taken; and*
*d) maintaining records of education, training, skills, experience and qualifications (see 4.3.3).*

*The organization shall also ensure that all relevant personnel are aware of the relevance and importance of their information security activities and how they contribute to the achievement of the ISMS objectives.*

The Statement of Applicabillity (FD Part Section 2) includes the following objective in relation to training

*Section SM2.4 Security awareness*

*Principle: Specific activities should be undertaken, such as a security awareness programme, to promote security awareness to all individuals who have access to the information and systems of the enterprise.*

*Objective: To ensure all relevant individuals understand the key elements of information security and why it is needed, and understand their personal information security responsibilities.*

**Responsibilities for training**

Part 2 Section 3 Roles & Responsibilities Statement of the Lancashire County Council Information Security Manual sets out responsibilities in relation to the ISMS.

The key responsibilities are:

- Managers should ensure that their staff receive appropriate training
- The Corporate Information Security Manager should support the overall training process by originating training & awareness material and organising its delivery

**Training content**
Guidelines for "Section SM2.4 Security awareness" include the training, awareness and education. ements.

**Training has three aspects**
- Meaning of information security
- Importance of compliance with the policy and associated procedures
- Personal responsibilities for information security

**Examples of Awareness Material**
- Packs of summarised material
- Reminder material
- Theme based
- Personal interest material
- Links & contacts
- Intranet
- Examples of security incidents and security successes

**Education consists of techncial and professional training**
- CISM Staff
- ICT Staff
- Local Co-ordinators

**Possible Trainee groups with potential training approach to each**

**Top management**
Briefings on paper/probably not in person

**CIMSG & groups**
Meetings

**SMT's**
Briefings – 30-45 minutes 7 incl 3 DSO's but probably a few extra sessions. How can we get these? Message has to include IG and good housekeeping angles. Also compliance, partnership etc (about which they will know more than us). Inform ation about other roles/training

**Business Managers**
Dedicated (a) critical systems (b) service representation – every unit. How do we organise this? Bit of the above. E-training. Are they receptive at this level? Alternative is written material.

**Directorate IG Local Security Co-ordinators**
One to ones if they exist could be >1 per Directorate in big Directorates and one of the above groups in the DSO's. Infrastructure?

**Application Support**
Separate from Co-ordinators? Critical apps team by team

**All users**
General training e-training & intranet. Induction/e-module & intranet. AUP

**LICTS Infrastructure**
Written advice with refresher sessions

**LICTS Application Support**

Written advice with supplementary refresher sessions. Development areas of ISF

**LICTS Customer Service**

Written advice with supplemental refresher sessions. Development areas of ISF

**Records Management**

One session & written advice

**Property Group**

One or two sessions with on-going contact

**Human Resources**

One or two sessions with on-going contact

**Third Party Staff**

Hand-out/email. How many circumstances?

Delivery issues

Sessions/means/timing/options

Conclusions

E-training form