

# INFORMATION & COMMUNICATIONS TECHNOLOGY

## Standard

The organisation has a consistent, comprehensive and systematic approach to the management of electronic information and systems.

## Overview

The provision of health and social care is driven to a large extent by the quality of the data that is available at the point of care and quality of the information used to make decisions that impact upon people and society.

Care outcomes are directly related to the quality, reliability, access, security, confidentiality, safety, cost-effectiveness and effective use of information and information technology.

Good quality data and information together with well-implemented and managed technologies can greatly improve all aspects of organisational performance. Poor quality data and information and badly managed technologies can make existing problems far worse.

So improving the quality of data and the management and use of information is essential to meeting core objectives of the HSC. This is supported by implementation of the HPSS ICT Programme, involving co-operation in regional initiatives, the use of agreed standards, and development and implementation of local ICT Programmes that complement and support the HPSS Programme.

Electronic care records and electronic care communications are key themes of the HPSS ICT Strategy. The development of electronic records will offer benefits for care services and for administration, but will also create significant challenges. The ICT Programme is introducing more extensive use of ICT to enable service modernisation and is taking forward the transition from paper to electronic services. All HSC organisations have a role to play in this transition. Local policies and strategies should take account of the opportunities presented by the initiatives within the HPSS ICT Programme as well as addressing specific commitments.

ICT and Records Management strategies need to include measures to effectively ensure the confidentiality, integrity and availability of electronic records. Record keeping must be fully compliant with the Data Protection Act 1998 as well as with specific legislation and regulation regarding care records. Important aspects in this regard include the management of consent to recording; clear rules and controls regarding disclosure; data subjects' rights of access to records (with controlled exceptions); right of correction of factual errors; and robust data custodian procedures. Business continuity planning should take account of electronic care records and related needs and dependencies of information partners.

If the various agencies involved in care are to provide a seamless service there needs to be a focus on sharing and transfer of personal care information. This needs to be undertaken within a framework of agreed

information-sharing protocols and inter-operability standards, together with effective and comprehensive information security management arrangements.

In order to realise the expected benefits from ICT, HSC organisations need to have a consistent and systematic approach towards collecting meaningful data, and managing both the resultant information and the technologies that produce it.

This standard is based substantially on the equivalent NHS standard. New Information Governance arrangements to be introduced in the NHS will draw together a coherent package of best practice guidance dealing with confidentiality, data protection, data quality, records management and information security management which will result in updates to the NHS IM&T Controls Assurance standard.

The illustrative examples of verification listed in this standard may be used to verify compliance with a particular criterion. Organisations may wish to use many other examples, just as valid as those provided in the standard, and these will vary depending on the nature of a particular organisation.

### Assessment Guidance

HSC organisations vary significantly in size and in the nature of the services they deliver. It follows that not all controls assurance standards will apply to each organisation. This is implicit in the current Departmental guidance, eg. *The Reference Table on Applicability and Expected Levels of Compliance* which should be referred to before commencing the self-assessment exercise.

Even where a standard is generally applicable to the work of an organisation it is quite possible that not all of the criteria will be materially applicable. Before self-assessing against a standard, therefore, an organisation should consider the relevance of each criterion to its own business and conduct its assessment accordingly. Thus, where a criterion is clearly relevant to an organisation, the score should be based on the **totality of the action taken to address the requirement**. Where there is little or no relevance, the criterion should be considered “not applicable” and ignored for scoring purposes as explained in the guidance on *Reporting Compliance* issued by the Department.

This approach will ensure that the assessment has no unfairly detrimental effect on the organisation’s overall score but reflects a proper evaluation of the key areas of risks identified and the actual levels of controls put in place to manage those risks.

Likewise, the *Examples of Verification* set out in the standard are just that – examples, for guidance only. Once again, it is the nature of each organisation’s business that determines the type of evidence needed to prove that appropriate controls are in place. In effect, this may mean that only some of the examples listed are relevant to a particular HSC organisation or, indeed, that there are other more relevant examples which can be adduced as

evidence of compliance. It is also the case that some evidence can be deployed to demonstrate compliance with more than one criterion or standard.

## KEY REFERENCES

References specific to the HSC are given. There are also references in this section and elsewhere that relate to the English NHS. These are advisory, listed for information and further reference.

The HPSS ICT Standards and Procedures manual, the “Blue Book”, currently includes:

- Project approval
- Notification of internal project approval procedures
- Procurement of Information Systems

The following sections have been superseded by the Department of Finance and Personnel guidance formally issued to the HPSS in July 2004.

- *Project Management*
- *Business Case Guidance*
- *Project Monitoring*
- *Requirements for Post-implementation review*
- *Project Management Evaluation*
- *Project Benefit Evaluation*

Relevant DFP guidance can be found on their Successful Projects in Government website:

<http://spring.dfpni.gov.uk/>

### **Information Strategies**

HPSS ICT Strategy

<http://hpssweb.n-i.nhs.uk/RegInfo/ICTProgramme/index.htm>

### **Security and Confidentiality**

HPSS ICT Security Policy

<http://hpssweb.n-i.nhs.uk/dis/security>

The Protection and use of Patient and Client information: DHSSPS, 1999  
(Under review)

OGC Successful Delivery Toolkit – Risk Management

[http://www.ogc.gov.uk/resource\\_toolkit.asp](http://www.ogc.gov.uk/resource_toolkit.asp)

British Standards Institution (2005) *Information Technology – Security Techniques – Information Security Management Systems - Requirements*, BS ISO/IEC27001: 2005. BSI London

<http://www.iso.org>

Department of Health (2007) *Information Security Management: NHS Code of Practice*. Department of Health, London

[http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH\\_074142](http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_074142)

Connecting For Health (2008) *Information Governance Toolkit*. Department of Health, London

<https://www.igt.connectingforhealth.nhs.uk/>

### **ICT Procurement**

HPSS ICT Standards and Procedures Manual – Procurement of Information Systems

HPSS CE letters on ICT Procurement from 2001 and 2003

Department of Health (2004) *Investment in IM&T in the NHS*. Department of Health, London

[http://www.dh.gov.uk/ProcurementAndProposals/PublicPrivatePartnership/PrivateFinanceInitiative/InvestmentInIMTInNHS/InvestmentInIMTNHSArticle/fs/en?CONTENT\\_ID=4070052&chk=p8UFde](http://www.dh.gov.uk/ProcurementAndProposals/PublicPrivatePartnership/PrivateFinanceInitiative/InvestmentInIMTInNHS/InvestmentInIMTNHSArticle/fs/en?CONTENT_ID=4070052&chk=p8UFde)

### **Controls Assurance**

Governance in the HPSS

<http://www.dhsspsni.gov.uk/hss/governance/governance-guidance.htm>

Northern Ireland HSS (PPM) 3/2002 – Corporate Governance: *Statement on Internal Control*

Northern Ireland HSS (PPM) 4/2005 – AS/NZS 4360:2004 – Risk Management

Northern Ireland HSS (PPM) 8/2002 – Risk Management in the Health and Personal Social Services

HSS (PPM) 10/02 Governance in the HPSS – Clinical and Social Care Governance: Guidelines for Implementation

Northern Ireland HSS (PPM) 13/2002 – Governance in the HPSS: Risk Management

Northern Ireland HSS (PPM) 5/2003 – Governance in the HPSS: Risk Management and Controls Assurance

HSS (PPM) 8/04 Governance in the HPSS: Controls Assurance Standards – Update

Northern Ireland DAO (DFP) 5/2001 – Corporate Governance: Statement on Internal Control

Northern Ireland DAO (DFP) 25/2003 – Statement of Internal Control

Association of Australia. Strathfield NSW.

Home Office (2000) *How resilient is your business to disaster? A comprehensive guide for any organisation to survive and recover from disaster*. Home Office

<http://www.ukresilience.info/contingencies/business/resilient1.htm>

### **ICT Skills and Training**

OGC Successful Delivery Toolkit – Skills Programme

<http://www.ogc.gov.uk/sdtoolkit/reference/skills/index.html>

NHS Executive (1998) *IM&T Good practice guidance for NHS Board members*. NHS Executive, London

<http://www.sciteb.com/wcitcol/guide/WCITGuidance.pdf>

### **Clinical and Social Care Governance**

HSS (PPM) 10/2002 *Clinical and Social Care Governance: Guidelines for Implementation*

<http://www.dhsspsni.gov.uk/hss/governance/governance-guidance.htm>

## **INDEX OF ICT CRITERIA**

### **Criterion 1 (Accountability arrangements)**

The Chief Executive of the organisation has overall responsibility for all aspects of ICT and there are clear lines of accountability throughout the organisation leading to the Board.

### **Criterion 2 (Director responsibility)**

The Board takes responsibility for the organisation's ICT, including ICT projects, and the use, sharing and management of information.

### **Criterion 3 (ICT Steering Group)**

An ICT Steering Group, or equivalent, oversees decisions and is accountable to the Board for all matters in relation to ICT.

### **Criterion 4 (ICT Manager)**

There is an ICT Manager, or equivalent, with appropriate skills and qualifications

### **Criterion 5 (ICT Policy)**

There is a comprehensive ICT Policy that is agreed by the Board and links into the organisation's overall strategic plan.

### **Criterion 6 (ICT Programme)**

There is a local programme for the exploitation of ICT, designed to achieve the organisation's business objectives, which is reviewed regularly.

### **Criterion 7 (ICT Procurement)**

An agreed ICT procurement process is adhered to throughout the organisation.

### **Criterion 8 (Project Management)**

The PRINCE2 project management methodology is used and adhered to throughout the organisation together with a consistent set of management and control processes.

### **Criterion 9 (Care information)**

All care information, either electronic or paper-based, is validated as authentic.

### **Criterion 10 (Security measures)**

All data and information is protected through the application of robust security measures, to ensure its confidentiality, integrity and availability.

### **Criterion 11 (Business continuity plan)**

The organisation has up to date and tested continuity plans for all critical infrastructure components and core services.

**Criterion 12 (Risk management)**

The risk management process contained within the Risk Management standard is applied to all aspects of ICT.

**Criterion 13 (Legislation and guidance)**

The organisation has access to up-to-date legislation and guidance relating to information management and technology.

**Criterion 14 (Staffing)**

The ICT function is adequately staffed with appropriately skilled ICT specialists.

**Criterion 15 & 16 (Training)**

All ICT stakeholders are appropriately trained to perform their duties with the information technology that is provided to them.

All ICT stakeholders are trained to manage the information that they produce and use within their role.

**Criterion 17 (Key indicators)**

Key indicators capable of showing improvements in the management of ICT and/or providing early warning of risk are used at all levels of the organisation, including the board, and the efficacy and usefulness of the indicators is reviewed regularly.

**Criterion 18 (Monitoring and review)**

The system in place for managing ICT, including risk management arrangements, is monitored and reviewed by the board and senior management in order to make improvements to the system.

**Criterion 19 (Audit)**

The Board seeks independent assurance that an appropriate and effective system of managing ICT is in place and that the necessary level of controls and monitoring are being implemented.

## CRITERION 1

**The Chief Executive of the organisation has overall responsibility for all aspects of ICT and there are clear lines of accountability throughout the organisation leading to the board.**

### Source

- Governance in the HPSS  
<http://www.dhsspsni.gov.uk/hss/governance/governance-guidance.htm>
- HPSS ICT Standards and Procedures Manual, Project Control and Monitoring
- DFP – Successful Projects in Government website:  
<http://spring.dfpni.gov.uk/>
- Successful Delivery Toolkit (OGC)  
<http://www.ogc.gov.uk/sdtoolkit/index.html>
- NHS Executive (1999) *Clinical Governance in the New NHS*. HSC 1999/065. 1999
- NHS Executive (1998) *IM&T Good practice guidance for NHS Board members*. NHS Executive, London
- Standards Australia (2004) *Risk Management AS / NZS 4360:2004*. Standards Association of Australia. Strathfield NSW.
- Northern Ireland HSS (PPM) 3/2002 – Corporate Governance: *Statement on Internal Control*
- Northern Ireland HSS (PPM) 4/2005 – AS/NZS 4360:2004 – Risk Management
- Northern Ireland HSS (PPM) 8/2002 – Risk Management in the Health and Personal Social Services
- Northern Ireland HSS (PPM) 10/2002 – Governance in the HPSS: *Clinical and Social Care Governance – Guidelines on Implementation*
- Northern Ireland HSS (PPM) 13/2002 – Governance in the HPSS: Risk Management
- Northern Ireland HSS (PPM) 5/2003 – Governance in the HPSS: Risk Management and Controls Assurance
- HSS (PPM) 6/2004 Reporting and Follow-up on Serious Adverse Incidents: Interim Guidance
- Northern Ireland DAO (DFP) 5/2001 – Corporate Governance: Statement on Internal Control
- Northern Ireland DAO (DFP) 25/2003 – Statement of Internal Control

**Guidance**

The Chief Executive, through a named Director, is responsible for ensuring that the organisation uses a common and systematic process for identifying, evaluating, specifying, procuring, using and safely maintaining ICT, in accordance with the organisation's overall strategic plan and HPSS ICT policy and strategy.

The Chief Executive, through a named Director, is responsible for ensuring that all data and information are appropriately secure, confidential, private, complete, accurate and authentic and comply with the Data Protection Act 1998 and other legislation.

The Chief Executive should ensure that the use of information and information systems is regarded internally as an underpinning and enabling element of mainstream care, care planning and service delivery.

**Examples of Verification**

- Documented evidence of the Director's responsibilities such as Board minutes/job description;
- Accountability arrangements chart;
- ICT steering group and risk management group minutes.

**Links with other standards**

All standards (generic criterion)

## CRITERION 2

**The board takes responsibility for the organisation's ICT, including ICT projects, and the use, sharing and management of information.**

### Source

- HPSS ICT Standards and Procedures Manual, Project Control and Monitoring
- DFP – Successful Projects in Government website:  
<http://spring.dfpni.gov.uk/>
- Successful Delivery Toolkit (OGC)  
<http://www.ogc.gov.uk/sdtoolkit/index.html>
- NHS Executive (1998) IM&T Good practice guidance for NHS Board members. NHS Executive, London

### Guidance

To ensure that the organisation fulfils its strategic objectives, the Board must understand, own and communicate the role of ICT within the mission and vision of the organisation. Its decisions must support that understanding.

The Board's responsibility for ICT includes:

- Development and maintenance of the organisation's ICT policy and local ICT programme, ensuring consistency with regional policy objectives;
- Ensuring that all data and information (patient, client, practitioner, organisational), are appropriately secure, confidential, private, accurate, timely and complete;
- Ensuring that all staff are appropriately trained to competently use information technology and to responsibly handle and control data and information;
- Approval of programmes and major projects involving ICT, and the mechanisms for their funding, monitoring, and control;
- Ensuring that service developments properly exploit and take account of ICT implications;
- Ensuring that ICT programmes and projects are directed by fully competent and accountable staff working within appropriate terms of reference and under the direction of the Board or an appropriate Director;
- Ensuring that the focus of ICT is on benefits to the organisation and that programmes and projects work towards the realisation of benefits and achievement of organisational outcomes from investments in ICT.

## **Examples of Verification**

- Documented evidence of Board responsibilities in relation to ICT; for example, job description of Board member with responsibility for ICT;
- Programme Board and Project Board minutes.

## **Links to other standards**

Governance

Risk Management

### CRITERION 3

**An ICT Steering Group, or equivalent, oversees decisions and is accountable to the board for all matters in relation to ICT.**

#### Source

- HPSS ICT Standards and Procedures Manual, Project Control and Monitoring
- DFP – Successful Projects in Government website:  
<http://spring.dfpni.gov.uk/>
- NHS Executive (1998) *IM&T Good practice guidance for NHS Board members*. NHS Executive, London

#### Guidance

Although the Board and Chief Executive are ultimately responsible for ICT, an appropriate ICT steering group should direct the detail and management of technology and information.

Forming an ICT group may be difficult because the professionals who deal with technology are often different from those concerned with information itself. Ideally, these issues should eventually be combined in local arrangements for Information Governance.

This criterion does not prescribe either one or two ICT groups; neither does it dictate their composition. It requires a body or bodies at a senior management level to co-ordinate decisions around ICT and information.

#### Examples of Verification

- Documentary evidence of existence of ICT Steering Group;
- Copies of minutes of meetings;
- Board approved terms of reference for the ICT Steering group.

#### Links to other standards

All standards

## CRITERION 4

### **There is an ICT Manager, or equivalent, with appropriate skills and qualifications**

#### **Source**

- NHS Executive (1998) *IM&T Good practice guidance for NHS Board members*. NHS Executive, London

#### **Guidance**

There is no statutory or mandatory requirement for there to be a full-time, dedicated ICT Manager. However, the Good Practice Guidance for NHS Board Members states:

"Traditionally, the responsibility for (ICT) management has often been merged with other functions, eg finance. NHS Boards should seriously question this arrangement, as the rate of change in technology and the demand for quality and timely information increases."

And that:

"... the individual with lead responsibility for ICT has adequate authority, seniority and influence at Board level within the organisation."

Some organisations may feel that two or more people, who together combine to perform the duties that would otherwise be given to a dedicated manager, can fulfil this function. Where the duties are divided between two or more people, the arrangement needs to be justified and integrated into a mutually comprehensive and co-ordinated set of responsibilities.

#### **Examples of Verification**

- ICT Manager(s) job description;
- Qualifications of post holder(s).

#### **Links to other standards**

None

## CRITERION 5

**There is a comprehensive ICT Policy that is agreed by the board and links into the organisation's overall strategic plan.**

### Source

- HPSS ICT Standards and Procedures Manual, Project Control and Monitoring
- HPSS ICT Strategy  
<http://hpssweb.n-i.nhs.uk/RegInfo/ICTProgramme/index.htm>
- Department of Health (2007) *Information Security Management: NHS Code of Practice*. Department of Health, London
- NHS Executive (1998) *IM&T Good practice guidance for NHS Board members*. NHS Executive, London

### Guidance

There has been a basic set of principles set out in relation to an ICT policy which should include, but is not limited to, the following elements:

- Individual person-based care records are used by care professionals;
- Information about individuals and populations is considered;
- Security and confidentiality of personal care data and information are respected;
- Technology is flexible, designed for change and is supported through staff awareness, training and development;
- Technology is linked and networked to defined care objectives;
- Technology supports high-quality, cost-effective care;
- Management information used to make decisions should be reliable and reflect operational activity;
- Personal data and information should be reliable, authentic and not duplicated;
- Individuals are responsible for keeping data and information current, accurate and confidential;
- Data and information are standardised to be conducive to networking and benchmarking with the HSC and others;
- Staff training and development should help the organisation maximise the potential of its ICT;
- Staffing levels should be appropriate to achieve the benefits of ICT.

## Examples of Verification

- ICT Policy document;
- Board minutes;
- Training needs analyses;
- Training records;
- Audits of record use;
- Data quality audit.

## Links with other standards

While there are no direct links to other controls assurance standards, authors of ICT strategies need to be aware of all relevant policies and procedures within the organisation which may be affected by it, or have an effect on it.

## CRITERION 6

**There is a local programme for the exploitation of ICT, designed to achieve the organisation's business objectives, which is reviewed regularly.**

### Source

- HPSS ICT Standards and Procedures Manual, Project Control and Monitoring
- HPSS ICT Strategy  
<http://hpssweb.n-i.nhs.uk/RegInfo/ICTProgramme/index.htm>
- Department of Health (2007) *Information Security Management: NHS Code of Practice*. Department of Health, London
- NHS Executive (1998) *IM&T Good practice guidance for NHS Board members*. NHS Executive, London

### Guidance

The ICT policy should state the organisation's approach towards ICT, which should be reflected through an ICT Programme for its achievement.

As is the case for the policy, it is not appropriate to prescribe the detail of the local ICT Programme. Questions that should be answered in any organisation's ICT programme include:

- How will the ICT policy be supported (resources and operationally)?
- How will technology and the information it processes be used, shared, and managed?
- How will existing ICT systems and infrastructure be impacted?
- How will ownership of the ICT Programme be ensured throughout the organisation?
- How will benefits be identified and managed through to their measurable realisation?
- What mechanisms will be used to review the Programme?
- How is the ICT Programme linked to other organisational strategies?
- What is the organisation's realistic ability to introduce and manage change through the ICT Programme?

## Examples of Verification

- Board approved ICT Programme document;
- Benefits realisation plan;
- Regular review of achievement of the HPSS ICT Programme objectives;
- Training needs analyses;
- Training records.

## Links with other standards

While there are no direct links to other controls assurance standards, authors of ICT strategies need to be aware of all relevant policies and procedures within the organisation which may be affected by it, or have an effect on it.

## CRITERION 7

**An agreed ICT procurement process is adhered to throughout the organisation.**

### Source

- Northern Ireland Public Sector Procurement Policy
- HPSS ICT Standards and Procedures Manual, Procurement of Information Systems
- HPSS Procurement Circular
- HPSS CE Letter on ICT, March 2003
- OGC Successful Delivery Toolkit – Procurement  
<http://www.ogc.gov.uk/sdtoolkit/workbooks/procurement/index.html>
- NHS Executive (1998) *IM&T Good practice guidance for NHS Board members*. NHS Executive, London

### Guidance

The process through which ICT products and services are procured is critical to the cost-effective and strategic management of ICT as a whole.

ICT procurement in the HSC is undertaken in accordance with procedures set out in the HPSS ICT Standards and Procedures Manual and in collaboration with a recognised Centre of Procurement Expertise (CoPE).

There is a well-established policy of collaboration in procurement with other HSC organisations, with procurements being co-ordinated and prioritised in line with the strategic ICT Programme.

Procurements often use framework contracts established specifically for the HSC or for the NHS or the public sector generally. The pattern of ICT procurement will include some or all of the following stages:

- Early contact with a CoPE;
- Planning, including procurement strategy, market research, project planning, setting up project structures, and developing the outline and full business case;
- Preparing the documentation, including the Summary of Need, the Official Journal of European Union (OJEU) advertisement, and the contract framework;
- Purchasing the system or services, including issuing documents to suppliers and the circulation of supplier responses and the award of contract;

- Performing the contract, including contract implementation and management, as well as post-implementation review;
- Ongoing management of supplier service contracts.

Procurements at the level requiring OJEU advertisement, and others as set out in the guidance, will require involvement of the Directorate of Information Systems and will be subjected to the OGC Gateway process.

### **Examples of Verification**

- Project Terms of Reference with CoPE;
- Documented Specification for ICT procurement.
- Gateway Review reports.

### **Links with other standards**

Management of Purchasing and Supply

## CRITERION 8

**The PRINCE2 project management methodology is used and adhered to throughout the organisation together with a consistent set of management and control processes.**

### Source

- HPSS ICT Standards and Procedures manual;
- DFP – Successful Projects in Government website:  
<http://spring.dfpni.gov.uk/>
- Successful Delivery Toolkit (OGC)  
<http://www.ogc.gov.uk/sdtoolkit/index.html>
- Department of Health (1999) *Managing Successful Projects with PRINCE2*. Department of Health, London
- NHS Executive (1998) *IM&T Good practice guidance for NHS Board members*. NHS Executive, London

### Guidance

In order to ensure the organisation's ability to deliver projects on time, to budget and specification, the PRINCE2 (Projects IN Controlled Environments) project/programme management methodology should be used.

The benefits of PRINCE2 are described as:

- Controlled development stages;
- Regular reviews of progress against the plan and business case;
- Flexible decision points;
- Management control of plan, progress and any deviations or exceptions;
- The timely involvement of both management and stakeholders;
- Clear identification of anticipated benefits and planning for their delivery;
- Specified communication channels.

The following are the main stages of development for ICT projects that the Board should ensure are reflected in project plans and controls:

- Requirements Analysis;
- Benefits Analysis;
- Functional Specification;
- System Architecture and Design;
- Creation or selection of Software;

- Testing;
- Assuring fulfilment of project objectives;
- Assuring quality;
- Acceptance and Implementation;
- Operation and Maintenance.

### **Examples of Verification**

- Documentary evidence of ICT project plans;
- Evidence of training of staff in project management skills;
- Assigned project responsibilities;
- Evidence of project documentation, quality assurance, acceptance report and sign-off.

### **Links with other standards**

Risk Management

## CRITERION 9

**All care information, either electronic or paper-based, is validated as authentic.**

### Source

- HPSS ICT Security Policy  
<http://hpssweb.n-i.nhs.uk/dis/secure/index.htm>
- Department of Health (2007) *Information Security Management: NHS Code of Practice*. Department of Health, London
- HSS (PPM) 6/2004 Reporting and Follow-up on Serious Adverse Incidents: Interim Guidance

### Guidance

Before the security and confidentiality of any information can be evaluated, the information must be validated as authentic. An acute risk to the individual and to the organisation would exist if fraudulent or inaccurate information were to appear in a care record. Organisations need mechanisms in place to ensure that all care information is validated as authentic.

Authentic data input is the direct responsibility of the person inputting the data, supported by their line manager. All systems will include input validation processes to check in full or in part the acceptability of the data. Depending on the system, later validation may be necessary to maintain referential integrity. Systems should report all data errors with helpful reasons to facilitate correction.

Errors should be corrected at the source of input as soon as they are detected. This is increasingly important as systems are linked and errors can be rapidly transmitted between systems.

Any loss or corruption of data should be reported immediately to the relevant system manager. The reporting process should involve invoking incident recording and management mechanisms.

### Examples of Verification

- Validation procedure, for example data accreditation programme;
- Gap analysis reports;
- Improvement plans;
- Incident reports.

**Links with other standards**

Risk Management

Records Management

## CRITERION 10

**All data and information is protected through the application of robust security measures, to ensure its confidentiality, integrity and availability.**

### Source

- HPSS ICT Security Policy  
<http://hpssweb.n-i.nhs.uk/dis/security>
- British Standards Institution (2005) *Information Technology – Security Techniques – Information Security Management Systems - Requirements*, BS ISO/IEC27001: 2005. BSI London
- Department of Health (2007) *Information Security Management: NHS Code of Practice*. Department of Health, London
- Connecting For Health (2008) *Information Governance Toolkit*. Department of Health, London

### Guidance

In the context of ICT, risk management means the protection against the threats and vulnerabilities of all personal or business data and information; particularly where that could cause potential harm to service users, disruption to business, or incur legal liabilities for the organisation, if it were inappropriately accessed, altered or used.

The security and confidentiality of care information involves four key management practices:

- ICT systems used in the HSC are subject to appropriate security counter-measures and benefit from appropriate management arrangements;
- The confidentiality, integrity, and availability of the data and information held on information systems is monitored;
- All staff are aware of their roles and responsibilities for information security;
- There is adequate provision for communicating the importance of information security.

The extent to which an organisation does not follow the above management practices represents a risk to service users, staff and the organisation.

More specifically, the presence of the following security measures would represent an organisation's relative level of commitment to information security and confidentiality:

- A trained and skilled information security officer;
- An organisational information management and technology security policy;
- ICT system level security policies;

- Email usage policy;
- Internet usage policy
- An ICT assets inventory;
- Organisational and system level risk assessments;
- Counter-measures register;
- Environmental and equipment security;
- Access control and management systems;
- Security incident reporting and management processes;
- Up to date virus and malicious software control measures;
- Business continuity plans;
- Housekeeping procedures;
- Security monitoring and review.

Any corruption or loss of data or information should be reported to the relevant system manager at once. This should initiate the invoking of incident recording mechanisms immediately, and possibly also major incident control.

### **Examples of Verification**

- ICT security policies/protocols;
- BS ISO/IEC 27001:2005 Gap analysis reports;
- BS ISO/IEC 27001:2005 Improvement plans;
- Security risk registers;
- Organisational and systems level business continuity plans;
- Security incident management records;
- Systems maintenance and update records;
- Systems access management records;
- External assessments.

### **Links with other standards**

Risk Management

## CRITERION 11

**The organisation has up to date and tested continuity plans for all critical infrastructure components and core services.**

### Source

- British Standards Institution (2006) *Business Continuity Management – Code of Practice* BS25999-1:2006. BSI, London.
- British Standards Institution (2007) *Business Continuity Management – Specification* BS25999-2:2007. BSI, London.
- Department of Health (2007) *Information Security Management: NHS Code of Practice*. Department of Health, London.
- Cabinet Office (2007) *Business Continuity Management Toolkit*. Cabinet Office, London.

### Guidance

Business continuity planning is a core component of business corporate risk management and emergency planning. Its purpose is to counteract serious interruptions to an organisation's business activities.

The development and maintenance of effective business continuity plans should be based upon periodic analysis of risks and impacts that may affect the organisation, its business processes and partnerships.

Business continuity plans should contain both contingency fall-back and recovery components, defining the organisation's arrangements for achieving acceptable interim levels of service and for the restoration of full services at a determined point.

Key responsibilities for implementing and managing business continuity plans should be agreed and assigned to appropriate senior managers. All potentially affected employees should be aware of their own roles and responsibilities and what actions they are expected to take in the event of interruptions to their business activities. Where necessary, the organisation should provide adequate awareness or skills training.

Each organisation needs to ensure that there are sufficient plans developed to meet differing contingencies and service obligations, including ICT. Plans should address minimum and sustainable service levels, options for fallback, systems recovery and co-ordination arrangements. Rates of change in risk profiles are likely to increase the vulnerability of each organisation and therefore plans should be tested, reviewed and updated at regular intervals, at least on an annual basis.

Any change to business continuity plans should take place under formal change control procedures.

## Examples of Verification

- Business plans containing relevant ICT contingency and recovery plans;
- Documented evidence of testing schedules, tests and their outcomes;
- Improvement plans;
- Documented evidence of review processes and any changes to business continuity plans.

## Links with other standards

Risk Management

Emergency Planning

Records Management

## CRITERION 12

**The risk management process contained within the risk management standard is applied to all aspects of ICT.**

### Source

- Circular HSS (PPM) 13/2002 Risk Management
- HPSS ICT Security Policy  
<http://hpssweb.n-i.nhs.uk/dis/secure/index.htm>
- Investment in IM&T in the NHS – Standard IM&T Risk Register  
[http://www.dh.gov.uk/ProcurementAndProposals/PublicPrivatePartnership/PrivateFinanceInitiative/InvestmentInIMTInNHS/InvestmentInIMTNHSArticle/fs/en?CONTENT\\_ID=4070052&chk=p8UFde](http://www.dh.gov.uk/ProcurementAndProposals/PublicPrivatePartnership/PrivateFinanceInitiative/InvestmentInIMTInNHS/InvestmentInIMTNHSArticle/fs/en?CONTENT_ID=4070052&chk=p8UFde)
- Connecting For Health (2008) *Information Governance Toolkit*.  
Department of Health, London
- Standards Australia (2004) *Risk Management AS/NZS 4360:2004*.  
Standards Association of Australia. Strathfield NSW.

### Guidance

There are many sources of risk in the area of ICT, and each risk can have significant implications. In addition to assessing risks associated with specific ICT criteria, organisations should identify all sources of risk that could threaten the integrity or security of ICT systems and review them on a continuous basis. This information can come from current and historical analysis of incidents, complaints and claims, directly or indirectly related to ICT.

Important information can also come from proactive risk assessments done to identify risks before they become incidents, complaints and claims. For example, ICT risk assessments could, on a directorate-specific basis, look at whether or not:

- There are secure access controls for data and information held on systems;
- There is awareness about, and up-to-date checking on all systems for, computer viruses and malicious software
- All records are complete and accurate;
- Information is received and dealt with in a timely manner;
- Care referrals and requests are authenticated;
- Access to care data is authorised and appropriate;

- The procurement of information technology is in accordance with the organisation's policy, the HPSS Standards and Procedures manual and DHSSPS directives;
- Networked or linked information systems are compatible;
- Information systems and technologies are working to specification;
- Information systems and technologies are subject to extraneous environmental factors;
- There are cost and time overruns;
- Staff practices maintain security and confidentiality;
- Information technology equipment is protected from physical damage;
- Other risks as identified.

Other important risks could be identified simply by talking with stakeholders about technology and information. They may provide a realistic context for risks that may not be apparent in either a periodic risk assessment or the baseline assessment against the ICT standards.

For example, a focus group with departmental staff might reveal that one reason why confidentiality and/or privacy is sometimes compromised is that the physical design of the department is not conducive to privacy, taking into account the volume and speed of activity.

All three sources of ICT risk information – achievement with the standards, ongoing risk assessment, and feedback from ICT stakeholders – feed into the organisation-wide Risk Register.

The following risk management elements should be in place:

- All risks should be identified and documented as part of a Risk Register and systematically assessed and prioritised;
- Risk treatment plans should be developed and implemented (in order of priority and alongside other risk treatments which are necessary to deal with the wider risks faced by the organisation, where appropriate) in order to minimise risk;
- Risk and the effectiveness of implemented risk treatments should be monitored and reviewed on a continuous basis;
- Senior management and the board should be informed of any significant risks and associated risk treatment plans;
- All relevant staff, including those on fixed term contracts, and other relevant stakeholders, should receive information on systems in place to minimise risks associated with using the assets described in this standard;
- Staff awareness and in-service training should be provided;
- All contingencies should be covered in plans for Business Continuity and Disaster Recovery.

Good records need to be maintained at all times.

## Examples of Verification

- Board or risk management group minutes;
- Risk assessments and registers;
- Risk reduction plans;
- Business continuity plans;
- Disaster recovery plans;
- Staff training/ information log;
- Stakeholder consultation.

## Links with other standards

Risk Management

Records Management

## CRITERION 13

**The organisation has access to up-to-date legislation and guidance relating to information management and technology.**

### Source

- <http://hpssweb.n-i.nhs.uk/>
- DFP – Successful Projects in Government website:  
<http://spring.dfpni.gov.uk/>
- Successful Delivery Toolkit (OGC)  
<http://www.ogc.gov.uk/sdtoolkit/index.html>

### Guidance

Access to legislation and guidance is essential for the organisation to carry out the statutory duties imposed upon it by law and mandatory duties required by the Department of Health, Social Services and Public Safety.

As a minimum, those involved in ICT should have access to the key references listed on the front page of this standard.

Up-to-date Department of Health guidance can be accessed on the Internet on the Department of Health's database:

<http://www.dh.gov.uk/PolicyAndGuidance/InformationTechnology/fs/en>

and the Information Policy Unit's website:

<http://www.dh.gov.uk/PolicyAndGuidance/InformationTechnology/InformationPolicyUnit/fs/en>

Her Majesty's Stationery Office website contains up to date information on all Northern Ireland legislation:

[www.hmso.gov.uk](http://www.hmso.gov.uk)

The Department's governance website contains guidance and information on risk management/controls assurance:

[www.dhsspsni.gov.uk/governance](http://www.dhsspsni.gov.uk/governance)

Wherever possible, the Health Care Standards Unit website, <http://www.hcsu.org.uk/>, also contains relevant advice and guidance.

### Examples of Verification

- Library
- CD-ROMs

- Internet access
- Hardcopy documents

### **Links with other standards**

All standards (generic criterion)

## CRITERION 14

**The ICT function is adequately staffed with appropriately skilled ICT specialists.**

### Source

- NHS Executive (1998) *IM&T Good practice guidance for NHS Board members*. NHS Executive, London
- NHS Executive (2001) *NHS Information Authority Professional Qualifications for NHS Informatics Specialists*. NHS Executive, London.

### Guidance

There is more demand for ICT professionals across all industries than perhaps any other skilled profession. The Good Practice Guidance for NHS Board Members states:

"Appropriate ICT personnel should be recruited on the basis of their wider experience, as integral members of a change team. Boards need to be aware that there is real benefit in employing strategic 'change agents' who are specialists in ICT, and have valuable exposure to matters such as procurement, business re-engineering, contract negotiations, managing change, strategy formulation and finance." (P.22).

The Guidance also states that the principal responsibilities of ICT professionals are:

- Delivery and maintenance of existing services (probably under Service Level Agreements with user departments) including management of support contracts;
- Provision of professional advice on ICT policy, strategy, plans and future opportunities;
- Management of specific projects to successful completion and measurement of benefits.

It is incumbent upon each HSC organisation to ensure that its ICT function has an adequate resource of appropriately skilled ICT specialists and that individual ICT projects and programmes of work are adequately resourced.

### Examples of Verification

- ICT staff job descriptions

- Evidence of ICT staff qualifications
- Staff references
- Projects delivered on time and to specification

### **Links with other standards**

Human Resources

## CRITERION 15

**All ICT stakeholders are appropriately trained to perform their duties with the information technology that is provided to them.**

### Source

- NHS Executive (1998) *IM&T Good practice guidance for NHS Board members*. NHS Executive, London
- NHS Executive (2001) *NHS Information Authority Basic IT Skills – Guidance for Local Health Communities*. NHS Executive, London.
- NHS Executive (2001) *NHS Information Authority Health Informatics Competency Profiles for the NHS*. NHS Executive, London.

### Guidance

Recent work has shown that information technology, the data it holds and information it produces, are not always used so as to provide the most effective care or for maximum efficacy in business transactions. Human factors are considered to be the single biggest reason for this.

In order to successfully implement the HPSS ICT Programme at a local level, it is necessary for all care professionals to improve their skills and knowledge in informatics in support of improved services and better-targeted health and social care.

The Good Practice Guidance for NHS Board Members states very explicitly that Board members must ensure that:

"Relevant staff have appropriate skills and qualifications commensurate with their responsibilities and degree of accountability." (P.22).

In NHS the Elite (E-learning in IT Essentials) training programme is the standard base qualification. Although this is not the case for the HSC, Elite training and testing is available to the HSC at the same favourable rate as the NHS and the HSC also continues to provide ECDL (European Computer Driving Licence) training where appropriate.

Informatics training and testing is also available for HSC staff.

With respect to using technology to its desired potential, the following staff should receive training, based on their learning needs, to help them achieve a high degree of competency with the technology they use:

- Primary users, including medical and professional staff
- Managers at all levels
- ICT specialists who maintain and service technology
- Trainers in technology

## **Examples of Verification**

- Training Policy document
- Evidence of staff training programmes
- Training attendance records
- Training needs analyses
- ECDL, or equivalent qualifications
- NHS Elite qualifications
- Infomatics qualifications

## **Links with other standards**

Human Resources

## CRITERION 16

**All ICT stakeholders are trained to manage the information that they produce and use within their role.**

### Source

- NHS Executive (1998) *IM&T Good practice guidance for NHS Board members*. NHS Executive, London

### Guidance

As health and social care is information-driven, the threat associated with poor information or "information overload" is a direct risk to the quality of care and service.

The critical importance of training staff at all levels to produce and use information in a way that provides clarity and context and helps facilitate decisions cannot be underestimated. In this regard, it is critical for staff to understand the organisation's rules about the confidentiality, security, privacy, timeliness and accuracy of data and information used directly to support care or for management purposes.

An increasingly important aspect of information training is for staff to know how to express information in a format that is accurate, clear and conducive to eliciting action.

Training for staff on how to use and present the information in their work should involve discussion about:

- What is considered confidential
- Who is allowed to see what
- What are the organisation's standards for timeliness
- What is required to ensure accuracy
- How do I know it is complete
- How should information best be presented
- What media are appropriate for sharing information (phone, email, etc.)

### Examples of Verification

- Evidence of staff training
- Records of attendance
- Training agendas identifying the above issues

**Links with other standards**

Human Resources

Records Management

## CRITERION 17

**Key indicators capable of showing improvements in the management of ICT and/or providing early warning of risk are used at all levels of the organisation, including the board, and the efficacy and usefulness of the indicators is reviewed regularly.**

### Source

- Successful Delivery Toolkit (OGC)  
<http://www.ogc.gov.uk/sdtoolkit/index.html>
- NHS Executive. Governance in the New NHS: Controls Assurance Statements 2000/2001 and Establishment of the Controls Assurance Support Unit. HSC 2001/005. 2001
- Northern Ireland HSS (PPM) 3/2002 – Corporate Governance: Statement on Internal Control
- Northern Ireland HSS (PPM) 8/2002 – Risk Management in the Health and Personal Social Services
- Northern Ireland HSS (PPM) 5/2003 – Governance in the HPSS: Risk Management and Controls Assurance

### Guidance

The organisation should develop indicators that demonstrate the risks associated with ICT. One indicator is degree of compliance with this standard. Ideally the indicators should be designed to demonstrate improvement in the management of risks associated with ICT over time.

The number of indicators devised should be sufficient to comprehensively monitor the key aspects of ICT. It is not necessarily the case that the board will use all the indicators. The board should select those that are useful for ensuring that the internal controls are working satisfactorily and ICT services are meeting their objectives.

### Examples of Verification

- Key indicators
- Evidence of usage at all levels

### Links with other standards

All standards (generic criterion)

## CRITERION 18

**The system in place for managing ICT, including risk management arrangements, is monitored and reviewed by the board and senior management in order to make improvements to the system.**

### Source

- HPSS ICT Standards and Procedures Manual, Project Control and Monitoring
- DFP – Successful Projects in Government website:  
<http://spring.dfpni.gov.uk/>
- NHS Executive. *Governance in the New NHS: Controls Assurance Statements 2000/2001 and Establishment of the Controls Assurance Support Unit*. HSC 2001/005. 2001
- Northern Ireland HSS (PPM) 3/2002 – Corporate Governance: Statement on Internal Control
- Northern Ireland HSS (PPM) 8/2002 – Risk Management in the Health and Personal Social Services
- Northern Ireland HSS (PPM) 5/2003 – Governance in the HPSS: Risk Management and Controls Assurance

### Guidance

It is the responsibility of the Chief Executive and the board to monitor and review all aspects of the organisation's application of ICT, including:

- Accountability arrangements
- Processes, including risk management arrangements
- Capability
- Outcomes
- Internal audit findings

### Examples of Verification

- Board minutes

**Links with other standards**

All standards (generic criterion)

## CRITERION 19

**The board seeks independent assurance that an appropriate and effective system of managing ICT is in place and that the necessary level of controls and monitoring are being implemented.**

### Source

- HPSS ICT Standards and Procedures Manual, Project Control and Monitoring
- DFP – Successful Projects in Government website:  
<http://spring.dfpni.gov.uk/>
- Northern Ireland HSS (PPM) 3/2002 – Corporate Governance: Statement on Internal Control
- Northern Ireland HSS (PPM) 8/2002 – Risk Management in the Health and Personal Social Services
- Northern Ireland HSS (PPM) 5/2003 – Governance in the HPSS: Risk Management and Controls Assurance
- NHS Executive (1995) *NHS Internal Audit Manual 1995*. NHS Executive, London.

### Guidance

Management should consider the range of independent internal and external assurance available, and avoid duplication and omission.

The adequacy of the independent assurance will depend upon the scope and depth of the work performed, bearing in mind its timeliness and the competence of the staff performing it. The level of reliance that can be placed upon such assurances should consider, among other things, the professional standing of the assurer, their level of independence, and whether they could reasonably expect to provide an objective opinion.

It is important that any review that takes place results in a report, recommendations for action where necessary, and the retention of sufficient evidence to enable other potential reviewers to rely upon the work already undertaken. The reports should be made to the appropriate sub-committee of the board.

Management arrangements will include an internal audit function, as well as other quality control and assurance functions such as clinical audit. The internal audit function is required to give an opinion to the board on the adequacy and effectiveness of the overall system of internal control. In doing so, they will seek to work with, and rely on the work of, other review bodies as far as is practical. The HSC is given external assurance by external audit.

**Examples of Verification**

- Schedule of planned reviews
- Copy of reports
- Committee minutes
- Action plans
- Notes of follow up of actions
- Evidence file
- Details of staff involved in the review.

**Links with other standards**

All standards (generic criterion)