



# Managing Information Risk

A guide for Accounting  
Officers, Board members  
and Senior Information  
Risk Owners

# Contents

Foreword	1
Overview	2
How to use this guide	4
Checklist for Accounting Officers and Boards	5
Key areas of information risk to consider	7
Governance and culture	8-15
Information management and information integrity	16-25
The human dimension	26-31
Information availability and use	32-39
Useful references	40

Prepared by The National Archives, with the support of Cabinet Office, CESG (The National Technical Authority for Information Assurance), CSIA (The Central Sponsor for Information Assurance), The Information Commissioner's Office and the Ministry of Justice.

For an electronic version of this guidance please visit [nationalarchives.gov.uk/services/publications](https://nationalarchives.gov.uk/services/publications)

Front cover image: © istockphoto.com/blackred

# Foreword

In recent years, all sectors of the economy have focused on risk management as the key to allowing organisations to successfully deliver their outcomes while protecting the interests of their stakeholders. As defined by the HM Treasury Orange Book, risk is uncertainty of outcome, and good risk management allows an organisation to:

- have increased confidence in achieving its desired outcomes
- effectively constrain threats to acceptable levels and
- take informed decisions about exploiting opportunities.

Good risk management allows stakeholders to have increased confidence in the organisation's corporate governance and ability to deliver.

'Information risk', however, is often not as visible as it should be, and therefore not always as well managed. The pace of technological change in the information age means new risks can appear quickly, and may not be as visible to Boards as other risks. Senior staff may wrongly assume information risks (unlike financial risks or physical threats) are secondary, and of less strategic importance. The guardianship and management of information in all its aspects (integrity, availability and confidentiality) is crucial to public service delivery.

Information is the currency of today's society, and it's hard to think of many public or private sector services that do not depend upon it. Citizens expect to access government services wherever they are and to do so seamlessly across departmental boundaries – which relies on our ability to share information securely. Information needs to be held – health, social care and many other public services cannot function without accurate and relevant information. Managing information is important for everyone working in the public sector, and we need to manage the associated risks. Following the Cabinet Office's Review of Data

Handling procedures in Government, Audit Committees will have to maintain oversight of information risk, and Accounting Officers will have to report explicitly on information risk as part of the Statement on Internal Control.

This guide seeks to support the non-information specialist, and particularly to help Accounting Officers, Chairs of Audit Committees and Board members understand information risk. It does not repeat existing risk management guidance, but assumes an understanding and knowledge of these tools and techniques. It does not seek to replicate existing specialist guidance on Information Assurance, which is complementary to this guide, and, in many cases, provides far more detail on some of the critical issues. Similarly, this guide does not explicitly cover restricted or confidential material, particularly relating to threats of external attack.

Instead, the aim of this guide is to give a non-specialist some insight into the nature of risks in managing information in the public sector, with questions to ask, and potential sources of assurance, that can support the Accounting Officer in managing risk in this critical area.



Sir Gus O'Donnell  
Cabinet Secretary  
and Head of the Home Civil Service

# Overview

It is essential that Boards consider all of the key risks associated with managing their business. Risk management guidance is already extensive, as outlined in the HM Treasury Orange Book and through subsequent guidance on setting and managing risk, which this guide does not seek to duplicate.

The aim of this guide is to highlight specific issues related to the management of 'information risk'. Understanding the nature of the risks to your business from failure to manage or use information is critical. The risks of managing information may not be understood as well as other risks by Boards and Accounting Officers. Yet, in many cases, they pose just as large a risk to the organisation as many of the more traditional risks.

However, Boards and Accounting Officers are not being asked to treat 'information risk' separately. Instead, you are asked to manage information risk within your standard business risk framework, and assess information risks alongside all other risks.

This guide aims to raise awareness of the nature of potential information risks to enable you to do this.

## What are 'information risks'?

Information is essential to today's society, and to most organisations and departments within government. Information can take many forms – from data sets of confidential personal information through to records of sensitive meetings, personnel records, policy recommendations, correspondence, case files and historical records. Information can be in many formats,

from databases through to emails, paper and video. Information is not the same as IT – IT systems are the platforms on which information is often exchanged and managed. Therefore, information risks are not necessarily the same as IT security risks (although managing IT security is usually a critical component of any strategy to manage information risks).

Risk management not only means mitigating risk, but also taking considered risks where the rewards are expected to be greater than any short-term losses. The risks of managing information illustrate this. The case studies in this guide highlight, for example, that in some cases the risks of not sharing information can be more serious than the risks of appropriately sharing it. Similarly, there are potentially significant social and economic benefits to re-using and making the best use of information in the public domain. Information risks have the same characteristics as other risks, and need to be managed with the same degree of strategic consideration.

A risk assessment is essential to prioritise the right actions for each part of government. Some information (e.g. published legislation, official publications, web publications) rarely carries security risks associated with disclosure – the risks around this information are more likely to be about tampering with the official record, or failure to get sufficient dissemination of key information. This is in contrast with sensitive personal data where risks are more likely to be around disclosure or integrity, although the tragic outcome in Victoria Climbié's case demonstrated that there are also risks to not sharing personal data appropriately, and of not keeping sufficiently accurate records.

### **Risk management within a whole government framework**

There are, as in any environment, some mandatory rules to abide by when managing information risks. In the context of the Cabinet Office's Review of Data Handling procedures in Government, Departments have agreed a set of core mandatory standards to apply across government. And, again, as in any environment, there is legislation and regulation in force. The Freedom of Information Act (2000), the Public Records Act (1958 as amended) and Data Protection Act (1998) are just a few examples of legislation that must be complied with. However, this just provides a framework. Your risks are generated as a result of the nature of your business and must be managed as such.

There are regulators in this arena, with the Information Commissioner regulating the management of Data Protection and Freedom of Information and the Office of Public Sector Information (part of The National Archives) regulating the re-use of public sector information.

Exposure to risks will vary according to your business, therefore following the rules as a stand-alone strategy will not manage business risk. The risk management approach needs to be complementary to adherence to the rules, which, in most cases, specify a minimum operating level only.

### **Embedding good management of information in your business**

The controls and approaches used to manage risk often include a significant cultural dimension. Major risks usually require staff awareness and appropriate behaviours in order to be controlled – managing the risk of fraud, or of damaging external relationships or reputation are always critically dependent upon management of staff and culture. Managing information risk is no different.

What this guide and the case studies provided seek to illustrate is that both processes and culture matter. Business processes can significantly reduce risk if, for example, system design takes into account information content and how the information will be used. At the same time managing information risk is dependent upon embedding behaviour and culture within your organisation.

# How to use this guide

This guide is written for Accounting Officers, their Boards, their Senior Information Risk Owners (SIROs) and the information management and information security practitioners supporting them. It contains high-level summaries, and also more detailed guidance to support those developing risk matrices for your organisation.

The risks detailed here are not meant to be exhaustive, but purely illustrative. We anticipate most of the major risks faced in information management by public sector organisations will be covered here in some shape or form. However, information risks are linked to business risk, and the risks that a data set or set of records pose in one business will be different from that in another. We therefore suggest that you use these examples as exactly that – examples – upon which to develop your own approach.

The case studies included demonstrate where risks have materialised, or 'where it's gone wrong'. These case studies are intended to be tangible, useful ways of illustrating the nature of risks to Boards and staff.

From 2008/9, all Accounting Officers will cover information risk explicitly in their Statement on Internal Control. Ensuring that you have addressed the issues raised in this guide is likely to be helpful in providing you and the Audit Committee with the confidence that you have addressed the major risks.

## Keeping this guidance relevant

Inevitably, new cases and issues will emerge which require changes to this guidance, or provide better advice or illustrations of key issues. This guidance will, therefore, be updated at regular intervals. Additionally, separate guidance will be issued covering risk management measures relating to the threat of external attack to electronic systems and information assets.

If you have comments on this guide, or details which you think will improve this guidance, please send comments to: [GKIMNetwork@nationalarchives.gov.uk](mailto:GKIMNetwork@nationalarchives.gov.uk)

# Checklist for Accounting Officers and Boards

## ***Have we assessed the importance of information to our business?***

- We know what information we hold and handle
- We know the relative security, sensitivity and importance of each set of information
- We understand which information systems support the management of key information
- We know how critical this information is for the management of our business

## ***Have we assessed our information risks?***

- We have developed a risk assessment of our information
- This risk assessment looks at all of our key risks and how critical they are to our business
- This assessment follows the approach we have taken overall to risk management, and embeds information risk management within our overall business risk model

## ***Do we have a plan for managing these risks?***

- We have identified what we need to do to mitigate risks to an acceptable level, which covers all key dimensions (i.e. the need to share as well as protect, and the need for resilience)
- We have a clear plan in place, with owners of the key actions
- The plan covers all key players in the delivery chain, including arm's-length bodies and partners
- The key players understand their role in managing these risks
- There is a regular process of assessing how well we are doing at implementing this plan

## ***Do all staff understand their roles and responsibilities in managing these risks?***

- All our staff understand their role in managing information, and the risks it poses
- All staff are clear on what's mandatory, and where they can make decisions
- All staff are clear about to whom they report concerns and 'near misses', so we can learn from incidents and mistakes
- We have built this into our culture through training, performance management and governance structures
- All staff understand the consequences of not following the rules

## ***Does my organisation have the right skills and technical capabilities to manage these risks?***

- My Board sufficiently understands our use of and reliance upon information and information risk to ask the right questions
- I have a capable Senior Information Risk Owner on the Board
- I have a capable team and infrastructure to manage my organisation's information, who are aware of all of the risk issues
- My IT, financial and other teams and infrastructure are attuned to the need to manage information risk

## ***Is management of information embedded in my business processes?***

- We consider information as one of many business processes, and business risks
- The Board considers information risk alongside, and as a contributory part of, other key risks, and gives it priority accordingly
- Information management is seen as a core skill, and is built into training, assessment and capability building processes



© istockphoto.com/urbancow

# Summary:

## Key areas of information risk to consider

Risk category	Example of risk
<b>Governance and culture</b>	<p>Lack of comprehensive oversight and control (so anything can go wrong)</p> <p>When something goes wrong, handling it badly and not learning (so it can happen again)</p> <p>Third parties let you down (letting down your customers and your reputation suffers)</p> <p>New business processes don't take information risk into account (with serious consequences)</p>
<b>Information management and information integrity</b>	<p>Critical information is wrongly destroyed, not kept or can't be found when needed (leading to reputational damage or large costs)</p> <p>Lack of basic records management disciplines (can have wide-ranging consequences)</p> <p>Inaccurate information (which causes the wrong decision to be made, or the wrong action to be taken)</p> <p>Vital electronic information becomes unreadable due to technical obsolescence (with legal, reputational or financial consequences)</p> <p>Critical information is lost (with legal, reputational or financial consequences)</p>
<b>The human dimension</b>	<p>Despite having procedures and rules, staff, acting in error, do the wrong thing (and things go badly wrong)</p> <p>Despite having procedures and rules, 'insiders', acting deliberately, do the wrong thing (and things go badly wrong)</p> <p>External parties get your information illegally (and expose it/act maliciously/defraud you or your customers)</p>
<b>Information availability and use</b>	<p>Inappropriate disclosure of sensitive personal information (causing reputational damage or worse)</p> <p>Failure to disclose critical information for case management/protection (at worst leading to loss of life)</p> <p>Failure to utilise the value of the information asset (leading to a waste of public money)</p> <p>Failure to allow information to get to the right people at the right times (leading your service to fail your customers)</p>

## Risk to manage

### Lack of comprehensive oversight and control (so anything can go wrong)

Questions to ask	Potential sources of assurance
<ul style="list-style-type: none"> <li>• Does the Board understand the information risks facing the organisation as a result of its business activities?</li> <li>• Has risk tolerance been set for information risk?</li> <li>• Is the Board aware of the potential impact on business integrity should the confidentiality, integrity or availability of information be compromised?</li> <li>• Does the Board see information risk as a business issue (in business language)?</li> <li>• Have you mapped what information you hold (paper, electronic, historical, current, case files, policy records etc)? Do you know where it is all kept? And how?</li> <li>• Have you assessed the risks associated with each key asset (risks of inappropriate disclosure/ failure to disclose/tampering/loss/deletion etc)?</li> <li>• Does this approach fit with your risk management for other business risks?</li> <li>• Have you reviewed the Data Protection and privacy issues surrounding particular sets of data (personnel files, CCTV footage, etc)?</li> <li>• Is it clear who owns and controls each asset?</li> <li>• Are your information systems (containing your key assets) accredited?</li> <li>• Are you as clear on the processes for managing paper as you are on electronic content? Are you confident that these processes (transfer, storage, access) are sufficiently secure and robust?</li> </ul>	<ul style="list-style-type: none"> <li>• Key information assets across the organisation identified (content and systems)</li> <li>• A Board-level senior information risk owner identified (supported by a team to manage the organisation's information, and information risks)</li> <li>• An information asset owner named for each information asset ('asset owners' must consider content, not just systems)</li> <li>• Risks of managing the different assets (in terms of their sensitivity, Data Protection/privacy issues, confidentiality, integrity, availability and other risks flagged in this guide)</li> <li>• A robust and regularly updated risk register for the organisation's information risks</li> <li>• Regular monitoring of the risk register and compliance with the mitigation plans</li> <li>• Compliance with legislation and key standards <sup>1</sup></li> <li>• Strong links between the information management team and IT teams</li> <li>• Information management factored into business and system design processes</li> <li>• Strong, regular engagement of the Audit Committee</li> <li>• Processes for regularly updating all of the above</li> </ul> <p><small><sup>1</sup> Standards include HMG Information Security Standard No. 2 (risk management and accreditation of information systems) and ISO 27001. Legislation includes the Public Records Act (1958 as amended), Freedom Of Information Act (FOIA) (2000), Data Protection Act (1998), Re-use of Public Sector Information Regulations (2005).</small></p>

## What can happen...

### Case study

A press release from the Financial Services Authority (FSA) in December 2007, stated that Norwich Union Life was fined £1.26 million for 'not having effective systems and controls in place to protect customers' confidential information and manage its financial crime risks. These failings resulted in a number of actual and attempted frauds against its customers.'

'During its investigation, the FSA found that Norwich Union Life had failed to properly assess the risks posed to its business by financial crime, including fraudsters seeking to obtain customers' confidential information.' It also concluded that 'the weaknesses in Norwich Union Life's systems and controls

allowed fraudsters to use publicly available information including names and dates of birth to impersonate customers and obtain sensitive customer details from its call centres.'

Norwich Union Life has since taken a number of remedial actions including carrying out a review of its information security processes, and has reinstated all fraudulently surrendered policies in full.

*Also see all of the following case studies – without good governance and culture to recognise the importance of information management, any of these risks could materialise.*



## Risk to manage

### When something goes wrong, handling it badly and not learning (so it can happen again)

Questions to ask	Potential sources of assurance
<ul style="list-style-type: none"><li>• Do you have escalation/whistleblowing/constructive owning-up procedures for finding out you have a problem quickly? Do you and your staff know how to escalate and report breaches?</li><li>• Do you have a plan to contain and address potential breaches?</li><li>• Do you have a press and communications strategy for managing information incidents? Is this integrated into your overall major incident-handling plan? Is it clear in this who needs to do what, and when?</li><li>• Do you have a plan for managing the risks to those whose information has been compromised (if that is what happened)?</li><li>• Do you have a business recovery plan?</li><li>• Do you learn from your mistakes?</li><li>• Do you share your learning with others?</li></ul>	<ul style="list-style-type: none"><li>• A clear escalation and constructive owning-up policy</li><li>• Clear press and communications strategy as part of a major incident plan</li><li>• A 'lessons learned' process for learning from mistakes – and ideally which learns from 'near misses' as well, focusing on improvement rather than blame</li></ul>

# What can happen...

## Case study

In October 2007, the Healthcare Commission published the results of its investigation into outbreaks of *Clostridium difficile* at Maidstone and Tunbridge Wells NHS Trust.

The investigation highlighted that in 2004 and 2005 audits had established the Trust had poor documentation – and the poor quality of clinical records was a recurrent theme in legal claims. In relation to the *C. difficile* outbreak, the investigation found that before April 2006, figures on *C. difficile* were not reported in a way that would easily enable the Trust to detect outbreaks. The information was out of date, did not include basic information and did not trigger action.

As a consequence, it failed to identify an outbreak in 2005 that involved 150 patients.

The Trust did not make a second outbreak in 2006 public for two months and then produced figures that almost certainly underestimated the number of deaths. The Trust could not find about 10 per cent of case notes for its work in reviewing the notes of patients who died with *C. difficile* infection.

The Healthcare Commission carried out a follow up visit in December 2007, and found that Maidstone and Tunbridge Wells NHS Trust now has a new leadership team in place, is improving infection control and providing better care for patients with *C. difficile*.



## Risk to manage

# Third parties let you down (letting down your customers and your reputation suffers)

Questions to ask	Potential sources of assurance
<ul style="list-style-type: none"> <li>• Are any third party relationships with your organisation understood in terms of their information risks?</li> <li>• Are your suppliers clear what standards they need to meet? Have you spelt out the standards? Are the consequences of failure clear and contractually robust?</li> <li>• Do you have a robust process for assessing suppliers' performance against these standards?</li> <li>• Are you sufficiently confident that the supplier has mapped, and is managing, their information risks?</li> <li>• Are key staff aware of what suppliers can/can't do and can/can't request from you in terms of data?</li> <li>• Are you clear on ownership, accountability and decision-making processes if you share data with another part of government or outside of government departments?</li> </ul>	<ul style="list-style-type: none"> <li>• Mapping of key suppliers, and their associated information asset linkages, and their risks</li> <li>• Clear standards for suppliers to meet</li> <li>• Contractual obligations on suppliers which make clear the standards to be met, and the remedies in case of breach (e.g. financial penalties and rights to terminate)</li> <li>• A process for managing suppliers' performance/assurance against these standards, including looking at their activity 'on the ground'</li> <li>• Training for key staff (e.g. procurement, IT, HR etc) appropriate to their needs</li> <li>• Independent audits of key suppliers (as appropriate) which are disclosed to both parties</li> <li>• A handling strategy (see page 10, 'when something goes wrong, handling it badly and not learning') given that the accountability will remain with your organisation</li> <li>• System accreditation to recognised standards</li> </ul>



## Risk to manage

### New business processes don't take information risk into account (with serious consequences)

Questions to ask	Potential sources of assurance
<ul style="list-style-type: none"><li>• When you commission the design and operation of a new IT system, or change a business process, do you systematically assess the implications for how to manage the information content, and take information risk into account?</li><li>• Do you understand, and are you factoring in, what needs to be recorded, kept, kept secure, deleted or preserved at a sufficiently early stage in service or system design?</li><li>• Do the key teams involved in business change (business and general managers, IT teams, project managers) understand enough about information management and information risk to consider these issues sufficiently early?</li></ul>	<ul style="list-style-type: none"><li>• The procurement process, project management processes and business change processes have concrete steps involved to assess the implications for information risk management and take appropriate action</li><li>• Privacy Impact Assessments</li><li>• Penetration testing</li></ul>

# What can happen...

## Case study

As part of EU Common Agricultural Policy reforms, a single payment scheme (administered in England by The Rural Payments Agency) was introduced.

National Audit Office (NAO) investigations (HC 1631 2006 and HC 10 2007), found in the first year of the scheme the Agency had considerable difficulties in capturing and processing the data required to process the payments which were due.

The Agency implemented key aspects of the IT system without adequate assurance that every component was fully compatible with the rest of the system and supporting

business processes. The Agency had also deferred the development of software to draw out key information on the progress of each claim. As a result, the Agency did not have adequate management information to monitor progress and forecast future work effectively. This meant that problems with the scheme were not picked up early enough, by both the Agency and Department for Environment, Food and Rural Affairs (DEFRA), for corrective action to be taken.

The NAO also identified a number of errors in payments to farmers, many of which arose from errors in inputting data into the new computer system.



## Risk to manage

**Critical information is wrongly destroyed, not kept or can't be found when needed (leading to reputational damage or large costs)**

Questions to ask	Potential sources of assurance
<ul style="list-style-type: none"><li>• Are staff clear on what information needs to be retained, and for how long (case files, policy advice, personnel notes, personal information, legal documents etc)?</li><li>• Are staff clear where corporate information needs to be stored?</li><li>• Do you have stated corporate information availability requirements, and are you supporting them sufficiently?</li><li>• Are you following the requirements of the relevant legislation and guidance to support this? <sup>2</sup></li><li>• Do systems support the corporate storage of information (e.g. good Electronic Document and Records Management (EDRM) systems)?</li><li>• Is adherence to these policies regularly checked?</li></ul> <p><small><sup>2</sup> Relevant legislation includes the Public Records Act (1958 as amended), Freedom of Information Act (2000) and Data Protection Act (1998). The National Archives, Information Commissioner's Office and Ministry of Justice produce guidance on the implementation and use of these Acts.</small></p>	<ul style="list-style-type: none"><li>• Clear guidance and rules on what needs to be kept, and for how long</li><li>• Clear guidance on where key information needs to be kept – and on what can, and can't be kept on hard-drives</li><li>• A well-used EDRM system</li><li>• Regular compliance audits</li></ul>

# What can happen...

## Case study

An NAO report (HC 957, 2003) into compensation claims for personal injury or loss resulting from negligence paid by The Ministry of Defence (MoD), found that the MoD paid out £97m in 2001/2. The report was an examination of the effectiveness of the Department's arrangements for preventing incidents that lead to claims, and for handling claims that do arise in a timely and efficient manner.

It found the Department had sometimes encountered extra costs or delays by not applying good practice. It sometimes had problems in locating and providing documents required as evidence. Investigation reports and risk assessments can be key documents in the successful defence of a claim. However, the NAO found problems with the completeness and quality of the Department's data on incidents. The Department's own health and safety audits

suggested only about 40 per cent of all incidents were recorded on the health and safety database.

The NAO was also told that not all incident investigation records are properly retained, because of limitations of storage space (for example on board a ship or submarine when it is at sea on a lengthy tour).

Since the NAO report was published, MoD has introduced an Incident Recording and Information System (IRIS). IRIS now provides an important tool for users across the Ministry of Defence to identify common themes in accidents and incidents and to inform management decisions aimed at improving safety performance. IRIS also brings together data about claims and accidents and enables a better understanding of the true cost of accidents.



## Risk to manage

### Lack of basic records management disciplines (can have wide-ranging consequences)

Questions to ask	Potential sources of assurance
<ul style="list-style-type: none"><li>• Do staff know what records need to be kept? (See previous page)</li><li>• Are case files/key policy files kept up to date?</li><li>• Is there ongoing management of records?</li><li>• Are there processes for ensuring the integrity of the content is maintained/checks on tampering with key files?</li></ul>	<ul style="list-style-type: none"><li>• Clear records management policies and records management infrastructure in place, with Departmental Records Officer at a sufficiently senior level within the organisation</li><li>• Records management disciplines embedded in staff training</li><li>• Easy to use systems</li><li>• 'Exit routes' removed (e.g. ability to ignore rules and keep local files)</li><li>• Controls in place on access to/ability to change key files</li><li>• Good behaviour incentivised and valued</li><li>• Compliance with policies regularly monitored</li><li>• Clear responsibility for records management with a sufficiently capable team within the organisation</li><li>• Compliance with legislation such as the Public Records Act, Data Protection Act and relevant sections of the FOIA (and associated codes of practice/guidance)</li></ul>

# What can happen...

## Case study

In the US, regulators have taken action against a number of major companies as a result of failure to comply with record-keeping requirements. Many of these have been a direct result of electronic records being incorrectly deleted or unavailable due to poor record-keeping practices.

In 2004, Banc of America Securities LLC (BAS) paid \$10 million to settle charges that it failed to preserve or produce emails and other documents during an investigation by the US Securities and Exchange Commission (SEC).

In 2002, SEC, the New York Stock Exchange and NASD took joint action against five broker-dealers for violations of record-keeping requirements. Deutsche Bank Securities Inc.; Goldman, Sachs & Co.; Morgan Stanley & Co. Incorporated; Salomon Smith Barney Inc.; and U.S. Bancorp Piper Jaffray Inc. were fined \$8.25 million – \$1.65 million each – for failing to preserve emails.

In 2006, Morgan Stanley & Co. Incorporated paid \$15 million to settle charges of repeatedly failing to produce emails, and over-writing back-up tapes, requested in analyst investigations by SEC between 2000 – 2005.



© istockphoto.com/Katv

## Risk to manage

**Inaccurate information (causes the wrong decision to be made, or the wrong action to be taken)**

Questions to ask	Potential sources of assurance
<ul style="list-style-type: none"><li>• Do you have processes in place to check business critical data input?</li><li>• Are you aware of where the major points of vulnerability are? Do you have processes in place to address them?</li><li>• Do you know which data is quality controlled, and which is not (particularly important where relying on data input directly by customers/third parties)?</li><li>• Are staffing checks and controls in place to ensure that malicious data entry risks are minimised?</li></ul>	<ul style="list-style-type: none"><li>• An assessment of the major areas where poor/incorrect data input is of high risk to the organisation, and processes to manage that risk</li><li>• Spot checks/cross-reference to help ensure accuracy of sensitive personal data</li></ul>

# What can happen...

## Case study

UK Transplant provides a 24-hour service for the matching and allocation of donor organs. It maintains the National Transplant Database that holds details of all donors and patients waiting for a transplant.

Data is provided by NHS Trusts to UK Transplant in both paper and electronic formats. UK Transplant's own information-processing systems are thorough. For example, all paper records submitted are entered on the database on a double data entry process involving two individuals, which is designed to avoid inputting errors. All data are subject to hundreds of automatic validation rules to ensure accuracy. As a simple example, there are rules to highlight

discrepancies in clinical data or dates. If a patient's date of birth has been recorded on a form as after the date of being referred by a consultant, a validation rule will highlight this.

However, the system relies upon correct information being originally supplied by NHS Trusts. Errors are extremely rare, but recent media reports highlighted how a transplanted kidney had to be removed from a patient several hours after the initial operation, after a hospital worker incorrectly recorded the patient's blood type. This inaccurate information was then sent to UK Transplant and led to it sending out an incompatible kidney. The transplanted kidney was not compatible with the patient's true blood type.



## Risk to manage

### Vital electronic information becomes unreadable due to technical obsolescence (with legal, reputational or financial consequences)

Questions to ask	Potential sources of assurance
<ul style="list-style-type: none"><li>• Do you know what data sets or records (this is purely an electronic records problem) need to survive beyond 5 – 7 years post-creation?</li><li>• Do you have a strategy for these records?</li></ul> <p>(There is a pan-government project to address this issue – if you are not engaged in this project, you do need a separate strategy)</p>	<ul style="list-style-type: none"><li>• Clear identification of information you hold which needs to stay readable beyond 5 – 7 years</li><li>• Included in your IT strategy are explicit plans to manage hardware and software obsolescence</li><li>• Involvement in the pan-government Digital Continuity Project</li></ul>

# What can happen...

## Case study

In 2007, the Japanese Government faced a crisis sparked by poor record-keeping in the Social Insurance Agency. One factor contributing to the problem was the introduction in 1997 of a new system to integrate multiple pension numbers into one single number for each person. However, the records were not properly maintained and handled, and by 2007, 50 million pension records couldn't be linked to the individuals who had been making payments.

The Parliamentary session due to end in July 2007 had to be extended to rush through laws to reform the Department involved, a bill to abolish the statute of limitations on pensions and a further bill to reform the civil service.

The Government is currently attempting to match the 50 million unattributed pension records against the payment records of 100 million people – the entire population of those paying into the pension system or receiving payments. It has also guaranteed that everyone who made pension contributions will receive the pension due to them.

In January 2008, the new Prime Minister announced, 'The careless management of public documents, such as pension records, is absolutely unacceptable. We will conduct a fundamental review... for managing administrative records and will consider their legislation, and furthermore, we will improve the system for preserving public records, including expanding the national archives system.'



## Risk to manage

### Critical information is lost (with legal, reputational or financial consequences)

Questions to ask	Potential sources of assurance
<ul style="list-style-type: none"><li>• Does your Business Continuity strategy include identification of the key information you need to keep your business running? Do you have appropriate risk mitigation strategies/back-ups etc?</li><li>• Have you run crisis simulation exercises, which involve loss of some key data sources?</li><li>• Do you know which sources of external information/partners' information are critical to your own resilience?</li></ul>	<ul style="list-style-type: none"><li>• Tested business continuity plans, and simulation exercises which address critical data which you don't hold but need from others, as well as data you hold yourself</li><li>• Back-ups of key information and systems held in a secure, separate location</li></ul>

# What can happen...

## Case study

Hurricane Katrina hit the Gulf Coast of the US in August 2005, leaving more than 1,500 dead, hundreds of thousands homeless and destroying 90,000 square miles of land – an area the size of the UK.

The Federal government runs a wide array of programmes to provide assistance to special-needs populations, including disaster victims. The Federal Response: Lessons Learned Report highlighted that the Disaster Recovery Centres (DRCs) did not provide a single-point access to apply for aid. Staff did not have access to information on all programmes available and many DRCs were not able to

process disaster assistance registrations or assist victims in obtaining other benefits they were already receiving, such as Social Security payments.

Staff at the DRCs directed victims to register by telephone or via the Internet – but most households in Hurricane Katrina-affected areas were without power or telephone service. This problem was exacerbated by the fact that many people affected had also either lost or forgotten basic documents, such as insurance information, birth certificates, and marriage licences, which would later prove essential to rebuilding their lives.



## Risk to manage

Despite having procedures and rules, staff, acting in error, do the wrong thing (and things go badly wrong)

Questions to ask	Potential sources of assurance
<ul style="list-style-type: none"> <li>• Is there a culture of valuing information as an asset in your organisation?</li> <li>• Do senior managers lead by example and talk about the importance of information management?</li> <li>• Is the risk to information seen as a business risk, and treated with the same importance as other business risks?</li> <li>• Are the procedures in plain English and understood by all staff?</li> <li>• Are staff aware of what they can, and can't, say to callers (on the telephone)?</li> <li>• Are there safeguards (e.g. IT security, physical checks, personnel security, escalation procedures) to minimise the risk of errors, or someone just not obeying the rules, or even reckless damage?</li> <li>• Do you manage access to key data sufficiently (e.g. security clearance for people dealing with sensitive data, tracking systems for seeing who has accessed what, removing access rights as soon as they are not needed)?</li> <li>• Do you have systems which monitor what is happening locally?</li> <li>• Is the message consistently reinforced through induction events and training?</li> <li>• Is good information management valued in staff appraisals? Is poor information management addressed?</li> <li>• Are staff at all levels given personal accountability and held accountable for their actions when dealing with key information?</li> </ul>	<ul style="list-style-type: none"> <li>• Inclusion in values statements/corporate objectives</li> <li>• Link to performance evaluation formalised for relevant grades/staff/managers</li> <li>• Clear accountability for information management in the organisation</li> <li>• Inclusion in induction/training programmes – made relevant to specific staff groups (e.g. for call centre staff, focus might be around what information can and can't be given to callers)</li> <li>• Automatic (IT, security, HR checks etc) processes to mitigate some of the risks, including records of who has access to which system</li> <li>• Audit checks on inappropriate use of key systems, personnel security etc</li> <li>• A culture of valuing information as an asset, evidenced through staff surveys</li> </ul>

## What can happen...

### Case study

In October 2007 two discs were lost, which contained the unencrypted personal information of millions of citizens. Action taken by Her Majesty's Revenue and Customs (HMRC) immediately after this incident included ensuring that staff knew the rules, and understood the importance of adhering to them.

There was also the imposition of a complete ban on the transfer of bulk data onto removable media without adequate security protection such as encryption.

Kieran Poynter, commissioned to review the

situation, commented in his interim report in December 2007, 'On starting this review, my immediate impression of HMRC was one of complexity, both in terms of its many constituent parts and its matrix management structure. In particular I found it difficult to relate roles and responsibilities amongst senior management to accountability.' He added, 'the longer term solution will rely on a combination of factors which I will address as the review progresses. As envisaged in my terms of reference, these include the management accountability framework, tone from the top, culture and training as well as technical measures.'



## Risk to manage

Despite having procedures and rules, 'insiders', acting deliberately, do the wrong thing (and things go badly wrong)

Questions to ask	Potential sources of assurance
<ul style="list-style-type: none"><li>• Does your supplier and contractor recruitment meet the required government standards?</li><li>• Are there sufficiently robust systems in place to look for fraud patterns?</li><li>• Do managers look for potentially suspicious activities – e.g. working weekends or unusual work patterns?</li><li>• Do managers check on patterns of access?</li><li>• Are access and functionality rights properly managed?</li><li>• Are contractors, and people working independently or remotely, properly monitored?</li><li>• Is vetting/security clearance sufficiently rigorous for each job? And are contractors and temporary staff brought into this process early enough?</li></ul>	<ul style="list-style-type: none"><li>• Appropriate systems to identify potential fraudulent activity</li><li>• Training for managers to recognise danger signs</li><li>• Education and awareness programmes for all staff</li><li>• 'Whistleblowing' procedures in place and well understood</li><li>• Full management of access rights on systems</li><li>• Systems to monitor usage of internal systems by people working externally</li><li>• Suppliers and contractors meeting the new government Baseline Personnel Security Standard</li></ul>

## What can happen...

### Case study

In 2007 the media reported the sacking of a hospital staff member in Northern Ireland following claims of leaked confidential patient information. Press reports alleged that the leaked information may have been linked to the intimidation of witnesses in a court case and was investigated by the police.

Contractors working within one Department set up false accounts on the Finance system and embezzled over £100,000. Once the fraud was detected, improved systems of accountability were implemented, and those involved in the fraud arrested and successfully

prosecuted. The Department's records were critical evidence for the prosecution.

Exploiting assets and information is a fraud risk identified by HM Treasury. This type of fraud is potentially a high-risk area, as demonstrated in 2005 – 2006, where in one case, a government employee was providing details of departmental records to an external accomplice to perpetrate the fraud. The losses to the department involved totalled £1,250,000.



## Risk to manage

### External parties get your information illegally (and expose it, act maliciously or defraud you or your customers)

Questions to ask	Potential sources of assurance
<ul style="list-style-type: none"><li>• Are you meeting the right IT security standards?</li><li>• Have you got the right paper security standards in place?</li><li>• Have you assessed all of the risk points in the chain (e.g. back-up tapes, call centre infiltration, risk of theft of data in transit as well as IT security, risk of fraudsters recovering data from hard-drives or landfill sites which should have been destroyed)?</li><li>• Do you have evidence of fraud or crime that could be useful for learning for others?</li></ul>	<ul style="list-style-type: none"><li>• Meeting IT security standards</li><li>• Risks mapped, prioritised and action plans in place</li><li>• Responsibility for monitoring and delivering solutions is clear, and sufficiently resourced</li><li>• SIRO provided with sufficient information to be able to give Board assurance</li><li>• Security incidents reported to HMG's incident management schemes and, if necessary, to Cabinet Office and Information Commissioner</li><li>• Penetration testing of large systems by external experts</li><li>• Secure disposal/shredding</li></ul>

## What can happen...

### Case study

The Fraud report 2006 – 2007 (HM Treasury) included the following details of a fraud attempt by external parties. An unsuccessful attempt was made to defraud one department by diverting two compensation claims totalling £52,750 to false bank accounts, established by the perpetrators. The nature of the fraud suggested that the perpetrators had some knowledge of the organisation's procedures and it appeared that mail had been intercepted and some substitution of documents had taken place. Internal audit carried out an investigation and the police pursued enquiries into the alleged

perpetrators (who were known to them). It is unlikely that the police investigation will result in any action against the suspected perpetrators and in the meantime internal procedures have been strengthened.

The news agency Reuters reported in August 2007 that around 146,000 people using a US government jobs website had their personal information stolen by hackers. The hackers' goal was to use the information to launch 'phishing attacks' on the job seekers who had their personal data stolen.



## Risk to manage

# Inappropriate disclosure of sensitive personal information (causing reputational damage or worse)

Questions to ask	Potential sources of assurance
<ul style="list-style-type: none"> <li>• Are the minimum mandatory standards set, and being met, for each key asset type including:               <ul style="list-style-type: none"> <li>– who can access it?</li> <li>– what each user can do?</li> <li>– what is the clearance process for exceptional use?</li> </ul> </li> <li>• Are vulnerabilities identified (e.g. physical security, customer calls, temporary staff, IT security)? Are they sufficiently mitigated?</li> <li>• Are relevant individuals clear about their responsibilities for managing and protecting these assets? Have you provided appropriate training? Have you tested understanding?</li> <li>• Are the relevant safeguards (IT security, escalation procedures) in place to minimise risk?</li> <li>• Do you have a clear Data Protection regime in place, with a Data Protection Officer ensuring appropriately wide awareness of the issues?</li> <li>• Are protective security markings appropriately used and managed?</li> </ul>	<ul style="list-style-type: none"> <li>• Rules in place (in plain English) for asset owners and users of high-risk systems</li> <li>• The right rules in place (in plain English) for appropriate use of protective security markings</li> <li>• A clearly identifiable Data Protection regime, with a clear owner, appropriate training, and embedded in business processes</li> <li>• Corporate Security policy in place, covering the key risks that affect information assets</li> <li>• Appropriate IT security standards met</li> <li>• Mandatory training in place for asset owners and system users</li> <li>• Regular checks/audits to assess levels of understanding and compliance across all aspects</li> <li>• Compliance with ICO rules/compliance with enforcement regime</li> <li>• Clear ownership as a business issue, not just an IT issue</li> <li>• A link to performance evaluation formalised for relevant grades/staff/managers</li> </ul>

# What can happen...

## Case study

The Information Commissioner's Office (ICO) found the Department of Health in breach of the Data Protection Act following an investigation into a security breach on the Medical Training Application Service (MTAS) website.

Sensitive, personal details of junior doctors applying for jobs, were made public on the application website in 2007. This information included details regarding religious beliefs and sexual orientation. The ICO required the Department of Health to sign an undertaking to comply with the principles of the Data Protection Act and to encrypt any personal

data on its website which could cause distress to individuals if disclosed. The undertaking also required regular penetration and vulnerability testing to be carried out on developing applications and systems to minimise unauthorised access as well as Data Protection training for appropriate staff on an ongoing basis.



## Risk to manage

### Failure to disclose critical information for case management/protection (at worst leading to loss of life)

Questions to ask	Potential sources of assurance
<ul style="list-style-type: none"><li>• Are you clear where there are boundaries between your organisation and others, where sharing data is potentially important/critical?</li><li>• Do your staff really understand Data Protection legislation? And Freedom of Information legislation?</li><li>• Are the rules of what should be shared, and when, clear to all frontline staff?</li><li>• Are (easy to use) escalation procedures in place to allow staff to raise and resolve doubts quickly?</li></ul>	<ul style="list-style-type: none"><li>• Key points of cross-Agency/Department working (vis-à-vis data sharing) mapped</li><li>• Clear understanding of what data you own, and your responsibilities for shared data clarified with the other key parties</li><li>• Clear, well-publicised escalation/query resolution procedures for frontline staff</li><li>• Training programmes for frontline staff in place</li></ul>

# What can happen...

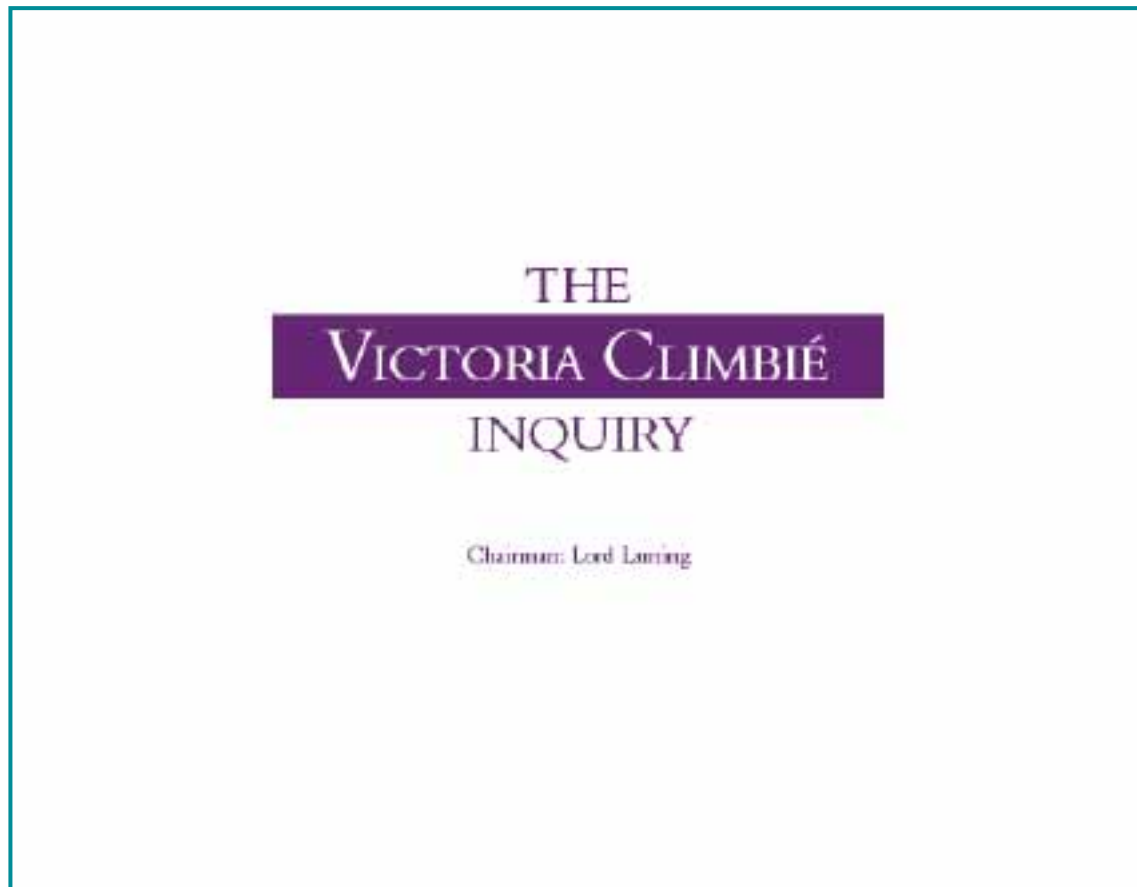
## Case study

Lord Laming's independent inquiry in 2003 into the murder of 9-year-old Victoria Climbié, concluded that 'Victoria was known to no fewer than four social services departments, three housing departments and two specialist child protection teams of the Metropolitan Police. Furthermore, she was admitted to two different hospitals because of concerns that she was being deliberately harmed and was referred to a specialist Children and Families Centre managed by the NSPCC. All of this between 26th April 1999 and 25th February 2000.'

'What transpired during this period can only

be described as a catalogue of administrative, managerial and professional failure by the services charged with her safety. In Brent, Victoria's case was given no less than 5 "unique" reference numbers. Retrieving files was, I was told, "like the National Lottery, and with similar odds". After her death, Haringey could not even secure Victoria's file, with the result that vitally important sections of it went missing.'

'Improvements to the way information is exchanged within and between agencies are imperative if children are to be adequately safeguarded.'



## Risk to manage

### Failure to utilise the value of the information asset (leading to a waste of public money)

Questions to ask	Potential sources of assurance
<ul style="list-style-type: none"> <li>• Are there information assets you hold which are publicly shareable and which would add value if shared more widely?</li> <li>• Have you received requests for access to information that have not been resolved to mutual satisfaction?</li> <li>• Are your research/analysis results appropriately stored and searchable to allow for (appropriate) use by other teams?</li> <li>• Are you using your disclosable information to help with your wider citizen consultation and engagement agenda?</li> <li>• Are you using the publication scheme (under FOIA) to proactively and routinely release appropriate information?</li> </ul>	<ul style="list-style-type: none"> <li>• Compliance with the Re-use Regulations, and a member of the Information Fair Trader scheme</li> <li>• Log of requests for access to information made, and conclusions</li> <li>• A named person championing the information re-use agenda for your department/organisation.</li> <li>• Systems and cultures which encourage the (appropriate) sharing of research results and knowledge (evidenced by staff surveys)</li> <li>• Well-used and well-populated e-information repositories</li> <li>• A strategy for using information for wider citizen engagement</li> <li>• Appropriate use of FOIA Publication Scheme</li> <li>• Appropriate use of the government's Information Asset Register (a register of unpublished information resources)</li> </ul>

# What can happen...

## Case study

Public sector information (PSI) can add a great deal to the economy. Businesses can use PSI and add value, such as in-car navigation systems for example (which use public sector mapping information), which in turn appeal to and are of value to consumers.

The Commercial Use of Public Information (CUPI) by the Office of Fair Trading (November 2006) report estimated that the economy could be forfeiting around £500 million a year as a result of the failure to open public sector information for wider re-use.

Similarly, *The Power of Information: An Independent review* by Ed Mayo and Tom Steinberg (June 2007), highlighted major opportunities for government to engage with citizens better through the re-use of existing public sector information online. As the review identified, government produces a vast amount of highly valuable information, and the internet increases its potential social and economic value.



## Risk to manage

**Failure to allow information to get to the right people at the right times (leading your service to fail your customers)**

Questions to ask	Potential sources of assurance
<ul style="list-style-type: none"><li>• Are you aware of the impact on business effectiveness and reputation should key information sources be unavailable at certain times?</li><li>• Do you know when the peaks of demand for your information are likely to be? Have these been tested against the availability of your key systems?</li><li>• Are there plans to allow appropriate access at peak demand times?</li><li>• Are you critically dependent upon just a few people to manage your key systems?</li></ul>	<ul style="list-style-type: none"><li>• Resilience plans to cope for peaks of demand for information, including staffing issues, IT factors and an assessment of risk and criticality of different sources</li></ul>

# What can happen...

## Case study

Media reports highlight examples where failure to accurately predict peaks in demand have led to negative publicity.

In October 2007, the BBC reported that Transport for London's website crashed under demand for discounted student Oyster cards at the beginning of the university term, leaving disgruntled students paying full price for tickets.

In January 2008, HMRC extended the deadline for submission of self-assessment tax returns after the website failed to fully

cope with demand on the deadline day, prompting extensive media coverage.

On the evening of 13 September 2007, the BBC broke the story that Northern Rock was seeking emergency financial help from the Bank of England. This led to a huge surge of online customers attempting to withdraw money overnight, causing the website to freeze. The failure of the website contributed to the run on the bank, and led to queues of savers standing outside Northern Rock's 72 branches the following day.



© istockphoto.com/Kolan

# Useful References

1. Audit Committee Handbook: HM Treasury, March 2007  
Key questions for an audit committee to ask on the strategic process for risk, control and governance and risk management processes (Annex F)  
<http://www.hm-treasury.gov.uk/media/8/3/auditcommitteehandbook140307.pdf>
2. Cabinet Office Data Handling Procedures in Government Review, 2008  
[www.cabinetoffice.gov.uk](http://www.cabinetoffice.gov.uk)
3. Communicating risk (a toolkit). Government Information and Communications Service (GICS). UK Resilience.  
<http://www.ukresilience.info/upload/assets/www.ukresilience.info/communicatingrisk.pdf>
4. DTI Foresight Intelligent Infrastructure Systems Project. Science Review Summary: Public Perception of Risk. Richard Eiser, December 2004  
[http://www.foresight.gov.uk/Previous\\_Projects/Intelligent\\_Infrastructure\\_Systems/Reports\\_and\\_Publications/Intelligent\\_Infrastructure\\_Futures/PublicPerceptionofRisk/Intelligent%20Infra%203rd.pdf](http://www.foresight.gov.uk/Previous_Projects/Intelligent_Infrastructure_Systems/Reports_and_Publications/Intelligent_Infrastructure_Futures/PublicPerceptionofRisk/Intelligent%20Infra%203rd.pdf)  
Data Handling procedures in government Review
5. HMG Information Security Standard No. 1, Issue 3.2 (January 2008)
6. HMG Information Security Standard No. 2, Issue 3.0 (January 2008)  
<http://www.cesg.gsi.gov.uk/bookstore/title.html>  
(GSI access only)
7. Managing Risks to improve public services. Report by the Comptroller and Auditor General HC 1078-1 October 2004  
[http://www.nao.org.uk/publications/nao\\_reports/03-04/03041078.pdf](http://www.nao.org.uk/publications/nao_reports/03-04/03041078.pdf)

8. Management of Risk – Guidance for practitioners (2004) Office of Government Commerce (OGC)  
<http://www.m-o-r.org/nmsruntime/saveasdialog.asp?IID=255&sID=104>
  
9. The Orange Book – Management of Risk – Principles and Concepts. HM Treasury, October 2004  
<http://www.hm-treasury.gov.uk/media/3/5/FE66035B-BCDC-D4B3-11057A7707D2521F.pdf>
  
10. Supporting innovation: Managing risk in government departments. Report by the Comptroller and Auditor General HC 864 17 August 2000  
[http://www.nao.org.uk/publications/nao\\_reports/9900864.pdf](http://www.nao.org.uk/publications/nao_reports/9900864.pdf)
  
11. Thinking about risk. HM Treasury, December 2006 (3 papers):
  - Setting and communicating your risk appetite
  - Managing your risk appetite: A practitioner's guide
  - Managing your risk appetite: Good practice examples[http://www.hm-treasury.gov.uk/documents/public\\_spending\\_reporting/governance\\_risk/psr\\_governance\\_risk\\_thinking\\_about\\_risk.cfm](http://www.hm-treasury.gov.uk/documents/public_spending_reporting/governance_risk/psr_governance_risk_thinking_about_risk.cfm)
  
12. Risk and Engineering. Royal Academy of Engineering (2002) (3 reports):
  - The Societal Aspects of Risk
  - Common Methodologies for Risk Assessment and Management
  - Risks posed by Humans in the control Loop[http://www.raeng.org.uk/news/publications/list/reports/The\\_Societal\\_Aspects\\_of\\_Risk.pdf](http://www.raeng.org.uk/news/publications/list/reports/The_Societal_Aspects_of_Risk.pdf)

