



The Hannigan Report: “Data Handling Procedures in Government”.

How Sapphire can help organisations work with the Hannigan recommendations.

The Hannigan Report

The loss of two discs by HM Revenue and Customs (HMRC) started an intensive process as all Departments re-examined their practices. This work was commissioned by the Prime Minister following high profile data losses in 2007.

This work was conducted in parallel with a set of independent reviews: the Poynter Review into the HMRC loss; the Burton Review into the loss of a Ministry of Defence laptop; and the Walport / Thomas review of data sharing, commissioned before the losses.

The Hannigan Report describes how Government has put in place new measures to protect information which is applicable across all central Government.

The report set out minimum rules, in that individual departments and agencies will continue to assess their own risk and often put in place a higher level of protection. The Government’s guiding principle is that the protections outlined in this report, or their equivalent, should be in place and effective, no matter how information is held and processed for UK Government purposes.

Any contractors or 3rd parties will also be required to adhere to the standards outlined in the Hannigan Report. Work is underway to develop equivalent material for the wider public sector. The standards for information security within the report are detailed below along with how Sapphire can help central and local Government departments and the wider public sector comply with these.

Information Security and Management Recommendations from the Report

Section 1: Scene-setting

The report states that good practice in managing information may be drawn from the public and private sectors. Technical and process measures need to be taken to minimise the scope for error or malicious action. Organisations need to achieve a culture that underpins the safe use of information, both when planning business and operating it. Clear accountability is vital, particularly at senior levels, to ensure that risks to information are considered from the start. Because no information handling system provides total protection, performance needs to be monitored and lessons learned on an ongoing basis.

How Sapphire Can Help

Who is Sapphire?

Sapphire has worked solely within Information Assurance since 1996. Extensive IS `Security services have been provided to over 1,500 clients across the UK in both the public and private sectors. Clients include major blue chip organisations, many local Government associations, some of the higher levels of central Government and their agencies, police forces and utilities.

Sapphire has an enviable reputation in providing tailored advice, guidance and training to a wide variety of clients. The consultancy team at Sapphire offers clients assurance that their corporate information is reliable and their systems are trusted. They cover all the professional guidance standards including **IIA** (Institute of Internal Auditors), **ISACA** (Information Systems Audit and Control Association), CIPFA (Chartered Institute of Public Finance and Accountancy) and **ICAEW** (Institute of Chartered Accountants in England and Wales). This type of assurance is crucial for any organisation adhering to or realising the importance of Corporate Governance.

ISO 27001:2005 Consultancy

Sapphire provides technical consultancy, information security products and systems. Sapphires consultants specialise in **ISO 27001**, an International Information Security Standard and ISO 27002 which gives comprehensive guidance on best practice methods for managing risks to information within an organisation. Sapphires consultants have extensive experience working with both public and private sectors assisting with improving their information security measures. Sapphire can assist organisations in the development of robust information security management systems that will:

- Objectively identify and manage risks to information;
- Progress towards organisational security maturity;
- Satisfy Corporate Governance, customers, statutory and insurance requirements.

Challenges and Good practice

The Hannigan report discusses the challenges Government faces regarding information risk management and the fact that they are not unique to the UK or to the public sector. The report summarises good practice. The material is drawn from Government departments, interviews with business and input from external experts.

The rest of this document explores best practices detailed within the Hanningan report which Government departments should seek to implement and how Sapphire can aid organisations to implement the recommendations.

Staff Vetting and Review of User Access Rights

The report gives a best practice example to be considered:

Company A adopts a risk-based approach to its staff, with regular **vetting procedures for employees** in accordance with their level of exposure and access to sensitive personal data. Staff are by default provided with minimum user access rights. Line managers are accountable for **system access rights** within their team and are required to evaluate the appropriate level of access rights for each role in their team, put forward a business case for additional access, and review and report on those access rights on a regular basis.

How Sapphire can help

ISO 27002 Best Practices for Information Security

Sapphires **ISO** consultants can help organisations implement best practices surrounding this area, specifically by helping to implement policy based around **Human Resources Security** (ISO 27002) which details how staff should be **vetted** “All candidates for employment, contractors and third party users should be adequately screened, especially for sensitive jobs” and “Verification checks should take into account all relevant privacy, protection of personal data and/or employment based legislation, and should, where permitted, include the following”:

- a) Availability of satisfactory character references, e.g. one business and one personal;
- b) A check (for completeness and accuracy) of the applicant’s curriculum vitae;
- c) Confirmation of claimed academic and professional qualifications;
- d) Independent identity check (passport or similar document);
- e) More detailed checks, such as credit checks or checks of criminal records.

With regard to system access rights Sapphires consultants ensure organisations implement a **review of user access rights** control and help develop policy to ensure they consider the following guidelines:

- a) Users’ **access rights** should be reviewed at regular intervals, e.g. a period of 6 months, and after any changes, such as promotion, demotion, or termination of employment;
- b) User access rights should be reviewed and re-allocated when moving from one employment to another within the same organisation;
- c) Authorisations for special privileged access rights should be reviewed at more

frequent intervals, e.g. at a period of 3 months;

d) Privilege allocations should be checked at regular intervals to ensure that unauthorised privileges have not been obtained;

e) Changes to privileged accounts should be logged for periodic review.

Development of a Culture of Security within an Organisation

The report states that strong organisations seek to foster a **culture of individual accountability** throughout the organisation, with targeted, relevant, role-based training to ensure that employees have a clear understanding of how to use and share information securely. At the same time as recognising the importance of cultural change, many commentators highlighted the difficulty of achieving it and the time taken to do so.

How Sapphire Can Help

Information Governance Training and Awareness

As well as ISO 27002 training Sapphire can provide general information security awareness training, drawing on experience of a wide ranging security practice across technical and systems disciplines. Specific training includes policy and procedure workshops, internal audit training, information security awareness seminars, computer forensics training and a range of technical workshop sessions.

Sapphire also provides specific information security awareness training for specified groups e.g. Senior Management (incl. HR and Legal) which ensure **individual accountability**; and staff training to selected 'IS co-ordinators' (skills transfer) to develop an effective IS culture based upon 'shared responsibility', drawing on experience of wide ranging security practices across technical and systems disciplines.

The process Sapphire takes when assisting an organisation to implement an information security management system ensures that a **culture of security and individual accountability** is established over a period of time (usually 8-12 months) which helps to ease the difficulty of a culture change.

Accountability for risk

Senior level ownership of information risk is a key factor in success. **Senior leadership** demonstrates the importance of the issue and is critical in obtaining resource. A simple governance structure, **with clear lines of ownership**, is essential. **Well defined roles** and responsibilities are needed to follow up identified information security threats and managing incidents. Internal audit can play an important role in examining and assuring actions taken by others.

How Sapphire Can Help

Establishing Accountability

From initial scope to completion of a project **clearly defined roles** for information security specifically how information and information assets are to be protected within the organisation are established by Sapphires consultants in partnership with the **project owners**.

Sapphires consultants ensure that information ownership risk management is clearly established with **top level management** commitment to information security established on day one of a Sapphire project. This then enables the allocation of information security responsibilities in accordance with a high level information security policy and controls, policy and procedures can then be assigned to individuals who are made responsible for ensuring that they are relevant and properly maintained.

Section 2: Better Data Handling

This section sets out how the Government is improving data handling, to achieve:

- Core measures to protect information, including personal data, in place across Government, to enhance consistency of protection and transparency of that protection to others;
- A culture that properly values protects and uses data, both in the planning and delivery of public services;
- Stronger accountability mechanisms for Departments. The individual Department or agency is best placed to understand and address risks to their information, including personal data; and
- Stronger scrutiny of performance, to build confidence and ensure that lessons are learned and shared

Core Measures to Protect Information

Specific elements of the package relating to the transfer of data include:

- Specifying personal data benefiting from higher levels of protection;
- Where possible, not transferring such information, but accessing it on its home system or **remotely via a secure channel**;

How Sapphire Can Help

Secure Remote Access - IAG

Sapphire partners with **Microsoft** and offers a secure remote access solution namely Microsoft **IAG** (Intelligent application gateway). The Microsoft Intelligent Application Gateway is an **SSL VPN** remote access solution, featuring end-point detection and application fire walling.

It provides **granular secure remote access**, authorisation and content inspection for web based applications and native applications alike. IAG enforces user access rights depending upon the different levels of authorisation applied by the administrator to each individual. IAG minimises data leakage as by being able to access data and systems securely from outside the normal working environment means that employees are less likely to copy information to removable media thereby reducing the number of opportunities for data loss or accidental leakage.

Secure Remote Access - Swivel

Sapphire partners with **Swivel Secure** a leading provider of strong authentication solutions. Swivel's two-factor authentication server software **PINsafe** replaces **RSA SecurID** and enables workforces to securely authenticate and access corporate network-resources via a VPN from wherever they are in the world. This is accomplished using PINsafe's unique browser interface and a one-time code (OTC) extraction process.

- Where transfer must occur, doing this through **secure electronic transfer**, so that discs are phased out where possible; and

- Where data have to be put onto removable media such as discs or laptops, minimising the information transferred, and using **encryption**.

Secure Electronic Transfer - RMS

RMS is a Microsoft windows rights management system. RMS is information protection technology. RMS helps organisations safeguard confidential information from unauthorised use.

RMS combines Windows Server 2003 features, developer tools and proven security technologies including encryption, certificates based on Extensible Rights Mark-up Language (XrML) and authentication, to help create reliable information protection solutions. RMS helps safeguard confidential information from unauthorised use both online and offline, inside and outside of the firewall. Information workers can define how the recipient may use the information: open, modify, print, forward, or take other action with it.

Organisations can create centralised custom usage policy templates such as “Confidential – Read Only” that work with any RMS enabled application and can be applied directly to information such as financial reports, product specifications, customer data, and e-mail messages.

Helping to enforce an organisation’s security strategy and policies, **RMS protects information** through persistent usage policies, which remain with the information, no matter where it goes. If a recipient accidentally forwards rights protected information or loses a diskette with a rights protected file, the protection still applies.

Encryption – BeCrypt

Sapphire partners with **BeCrypt** a UK based company. BeCrypt provides a range of market leading **encryption** and **data protection** products and services that can be tailored to meet the individual requirements of each local authority. BeCrypt is involved with the Project Nomad, the national project for mobile computing and e-Government in local authorities that is sponsored by the Office of the Deputy Prime Minister.

DISK Protect is one of BeCrypts flagship products. DISK Protect provides full disk encryption which transparently encrypts a computer's hard disk(s), automatically encrypting and decrypting data on the fly so that applications can be used as normal. It can be configured to call for a strong password or a token and a PIN. Authenticating the user at boot-time means that the operating system may be encrypted to prevent unauthorised data access using low-level tools. It is compatible with most of the widely used tokens and smart cards.

DISK Protect encrypts mass storage devices, such as USB memory sticks and floppy disks to protect data in transit. The latest version of DISK Protect supports up to 26 password protected accounts or an unlimited number of token and PIN protected user accounts per machine and each user may have DISK Protect accounts on several machines.

Culture

The Information Commissioner has made a powerful case for Government to adopt Privacy Impact Assessments. These are structured assessments of a project's potential impact on privacy, carried out at an early stage. They enable organisations to anticipate and address the likely impacts of new initiatives, foresee problems and negotiate solutions.

Risks can be managed through the gathering and sharing of information with stakeholders. Systems can be designed to avoid unnecessary privacy intrusion and features can be built in from the outset that reduces any impact on privacy. The Privacy Impact Assessment adopts a risk management process approach, periodic reports from which (Privacy Impact Assessment Reports) may be published or distributed to stakeholders.

How Sapphire Can Help

Impact Assessments and CLAS consultancy

Sapphire has **CLAS** consultants (**CESG** Listed Advisor Scheme) who are qualified to manage protectively marked information with UK Government contractors and related sectors (including List X). CLAS creates a pool of high quality consultants approved by CESG to provide information assurance advice to all public sector organisations.

Sapphires CLAS consultants aid these organisations in taking account of the aggregation of information (CESG good practice guide 9). Aggregation is the term used to describe the collecting together of large quantities of information with one or more levels of impact, the consequence of which is to raise the Impact Level of the compromise of the aggregated information to a higher level than its individual elements.

Conceptually there are two ways in which low-level information can aggregate to a higher level. These are: **accumulation**, where increasingly large amounts of information stored together **as a project unfolds** increases the overall Impact Level of compromise of Confidentiality, Integrity and/or Availability and; **association** where the association of different types of information occurs **during a project**, which in themselves have no or a low level impact when compromised, when combined together have a higher Impact Level of compromise, usually but not exclusively to Confidentiality. There may also be a combined affect of both accumulation and association.

Sapphires consultants help organisations consider Impacts and threats as Part of an *IS1 Analysis* and on the back of this they then help draw up mitigation plans drawing up these plans consider using a mix of personnel, physical, procedural and technical measures.

Stronger accountability

Many Departments will, as now, work towards or achieve external ISO accreditation for some or all other information systems. Departments will:

- define their information risk policy, which says how information risk will be **managed** within the Department and their delivery partners and how effectiveness will be assessed;
- identifying **information assets**,
- Defined relevant businesses (Information **Asset Owners** - IAOs) give them clear responsibility
- assessing risks to the confidentiality, integrity and availability of information

How Sapphire Can Help

Sapphire ISO 27001 Risk Assessment Methodology

An information risk policy would take the form of clearly defined risk assessment procedure and associated risk treatment plan. The **risk treatment** plan ensures the organisation has reviewed industry requirements regarding information security and adopted best working practice for **managing** the risk.

It then considers what level of risk it's willing to accept (see risk figures and key in example diagram below "treatment required" column) and options for the treatment of risk which include:

- Transfer of Risk,
- Avoidance of Risk,
- Risk Acceptance in accordance with the Security Policy and Application of Controls.

The risk assessment methodology that is conducted follows the process bullet below and takes the form of diagram A:

- Identifies all important **information assets**
- Assign **values** to the information asset class
- Defines the asset **owner**
- Identify **threats** to the information asset
- Identify associated **vulnerabilities**
- Identify the **likelihood** of the threat exploiting the vulnerability
- What **Impact** would this have on the organisation
- Establish an **unmanaged** risk exposure figure
- Identify the need for a **control/process/procedure/mitigation**
- Produce an overall **managed** risk exposure figure once a control has been selected

Diagram A

How Vulnerable to threat?	Likelihood of threat exploiting Vulnerability	Impact on organisation if this happened	Unmanaged Risk Exposure	Treatment Required (+7) Y/N?	Treatment Selected from ISO27001	Treatment Description (ISO27001)
4	4	4	12	Y	Training/ Info back up	A.10.5.1
2	1	7	10	Y	N/A	N/A

Key

1	Very Low
2.	Low
3.	Medium
4.	High
5.	Very High

Section 3: Implementation

The Government's guiding principle is that the protections outlined in the Hannigan report, or their equivalent, should be in place and effective, no matter how information is held and processed for central Government purposes.

Many of the specific controls to enhance protection for personal data are already in place in Departments themselves.

All Departments have:

- formalised the role SIRO (Senior Information Risk Owner);
- identified what personal data are held and used within the Department itself that falls into the new definition of "protected personal data";
- established procedures and policies to ensure such data are handled as if they are protectively marked;
- an encryption programme for such data, where it is on removable media, except where that is not possible, for example because of the need to access back-ups;
- where such data are stored electronically, minimised the use of removable media and the amount of data transferred to them and minimised the user rights to copy files onto such media;
- introduced new arrangements where needed for secure disposal from the Department of paper and electronic records; and
- **Reviewed procedures** for reporting information risk incidents.

Other steps, including the deployment of **penetration testing** will take place during 2008/09. The first full annual assessments of progress will take place following the end of 2008/09 and be reflected in the first annual Cabinet Office Report on overall progress.

How Sapphire Can Help

Information Risk Management Audit

Sapphire has **IRCA** (International Register of Certificated Auditors) registered ISO 27001 lead assessors, who can conduct a full sanity check and information security audit in order to ensure that the controls that have already been established are appropriate and there is an established culture of continual improvement of security within the organisation.

The audit would ensure that the operation of key issues of information governance would be checked to ensure that they are functioning to guarantee that the new culture of information security is in place and that all staff are conscious of a more 'security-focussed way of working'.

The elements of the information security risk management would be subjected to a cycle of compliance audits to objectively ensure that information handling and processing activities are in accordance with the relevant controls and opportunities for improvement would be reported to the organisation.

Penetration Testing

Sapphire has professionally qualified **CHECK penetration testers** (Team leaders and Team members) who are authorised to conduct tests for central and local Government departments at secret level.

The service can include dial up systems, wireless networking and individual bespoke applications.

The testing team can identify any weaknesses present in an organisation's network, demonstrate and quantify those weaknesses and then deliver a report on the countermeasures required to eliminate those weaknesses.

Commissioning a test provides a level of comfort that security technologies are in place and functioning correctly. An assessment by Sapphire can also provide peace of mind that an organisation's software, servers, workstations and infrastructure are all behaving in a manner to protect its critical business data and reputation from external or internal attack.

Strategic Support Agreement (SSA)

Sapphire realises that the number of organisations that allow for a contingency amount in their Information Security budget is small. Sapphire addressed the needs of their clients and realised the importance of having a contingency plan. Should it be a major security incident or perhaps the implementation of a new product or solution, having a strategic agreement already in place will give you peace of mind, as well as ensuring you are prepared for any eventuality.

With an **SSA**, you can rest assured that Sapphire will become the middleman to make certain your solutions work together and you get the best kind of protection. What in effect is being presented to the client in the form of a SSA is a single source for all their information security requirements, with added bonus of our organisation's full certification to ISO27001, the global standard for information security.

The provision of Strategic Support enables our clients to ensure that their security knowledge, systems, technical security and processes are maintained at the highest level. The support agreement can include:

1. Computer Forensics and Data Recovery
2. ISO 27001 Security Audit Consultancy
3. Penetration Testing
4. Regular Security Reviews and Health-checks
5. Education and Training
6. Technical Services
7. Access to the Sapphire Helpdesk

Need Further Guidance?

Please contact Sapphire on **01642 702100** and ask to speak to one of our business consultants.