MANAGEMENT BOARDS

INFORMATION & DATA SECURITY

Note by the SIROs

Purpose

1. This note sets out recommendations for the governance of information and data security issues in the two Houses.

Action for the Boards

2. The Boards are asked to agree the proposed governance arrangements.

Background

3. As SIROs for the two Houses, we have been co-operating on setting up arrangements to help us to discharge our duties effectively. We have both been involved in contact with other SIROs, and have recently undertaken a range of training specifically aimed at SIROs.

4. In Government, the role of the SIRO is described as to:

   i. Ensure your organisation has an information risk management culture which recognises that the business use of your information should drive decision making about its management

   ii. Ensure there is a multi-disciplinary approach to information risk management in your organisation

   iii. Ensure the risk to digital continuity is being managed efficiently and effectively

   iv. Ensure your organisation's Information Asset Register (IAR) is used to manage digital continuity

   v. Ensure your Information Asset Owners (IAOs) are managing the risks to the digital continuity of their Information Assets

   vi. Drive and monitor progress by measuring against the digital continuity maturity indicators in the IAMM7

5. The role does not exist in a vacuum, but is intended to be part of an infrastructure which provides for proper executive responsibility for managing information security risks, and appropriate assurance.

6. The general wisdom is that information and data security are becoming significantly more important, and that public sector organisations need to

address these risks more vigorously. Some aspects of the risks are becoming more prevalent: in particular the risk of cyber-attacks on IT systems and data is said by CESG to be increasing rapidly, and different methodologies for addressing those risks are increasingly required. Predictably, many of the known major data security failures have come about partly through human factors (lack of awareness, disaffection or other insider threats).

Governance proposals

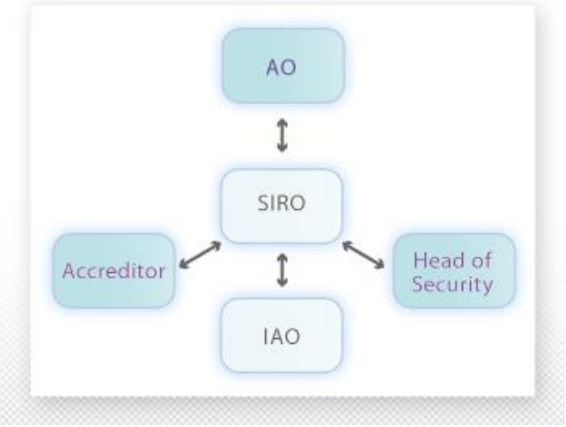
7. In the light of the work we have done so far, and the advice and training we have received, we propose that there should be greater clarity in our governance of information and data security and risks, and some strengthening of our effort ("ensurance" in the description above is about executive responsibility for making these things happen, as opposed to "assurance" which is about reporting on whether or not it has happened).

8. The recent appointment of the Parliamentary security Director has clarified one aspect of governance significantly, in placing with him strategic oversight of data security as well as physical security. In the light of this, our proposals to complete the arrangements for information security are:

- The SIROs should have authority to require action on all aspects of information and data security. We propose to discharge this duty through a Data Security Group (DSG), which we have already set up. Terms of reference are attached.
- Information asset owners (IAOs) should be identified in both Houses for all *major* information assets. IAOs will have specific responsibility for providing assurance and making sure that action is taken to manage the digital continuity of key information assets;
- An accreditor or acccreditors[1] should be appointed to make an impartial assessment of the risks to which an information system may be exposed in the course of meeting a business requirement. The Accreditor would be responsible for advising the SIROs on information risk and formally accrediting systems. The Accreditor would not look at all information systems, but concentrate on major systems and smaller systems involving particularly sensitive information. We have in mind that this role would be carried out on our behalf by a third party – possibly a specialist contractor – as and when required. There would be some cost (we are exploring options), but it is not a full-time activity.

9. These roles are set out diagrammatically below in a standard central Government model. The main difference for us is that we have two SIROs and two Accounting Officers. And in practice in all large organisations there are multiple IAOs.

[1] Accreditors are well established as part of the Whitehall approach to data security, and are an important technical resource for SIROs. Work is continuing on how best to adapt the accreditor role in a Parliamentary context.



Other actions required

10. More generally we believe that some further actions will need to be taken, and we propose to work through DSG to develop these, to ensure that our response to the cyber threat in particular is sufficiently robust. Examples include making data classification stick; dealing more effectively with data losses and lessons learned; ensuring a systematic approach to data security audit; evaluating the risks of the Cloud; and promoting behavioural changes in the handling and management of information.

Conclusion

11. Overall, our aim is to raise the profile of information risk and influence behaviours on handling of information as the profile of risks changes in the coming years, particularly with mobile computing and the Cloud. We seek the Board's support in agreeing the arrangements for managing these growing risks.

A J Walker
DG of HR & Change

Rhodri Walters
Reading Clerk

January 2012

ANNEX

Data Security Group (DSG)

Objective

- To support the Senior Information Risk Owners (SIROs) of both Houses in the discharge of their duties in the area of data security.

Terms of Reference

- To provide a forum to discuss and, where appropriate, agree actions in regard to:
  - current in house data security issues and risks
  - external issues and risks, such as cyber threats and Government recommendations
  - advising the SIROs on the data security implications of new IT-enabled projects, such as Cloud solutions
  - an integrated approach to data security for both Houses and PICT

- To ensure that both Houses and PICT have effective policies and management arrangements covering all aspects of data security in line with the overarching policies including, but not limited to:
  - Data Protection Policy
  - Parliamentary ICT Security Policy

- To monitor cyber threats and other external factors that may affect data security and liaise as appropriate with:
  - Parliamentary Security Board (PSB)
  - Information Rights and Information Security (HoC)
  - Information Compliance (HoL)
  - PICT
  - The Information Management Group

- To receive and consider reports into breaches of data security and undertake or recommend remedial action as appropriate.

- To liaise with Internal Audit in the area of data security risk, engage with the audit planning process and review management audit actions.

- To consider issues, comments and suggestions raised by Departmental Information Risk Owners (HoC) and Information Security Co-ordinators (HoL) brought to the attention of the group in the area of data security.

Meetings

The Group will meet approximately bi-monthly.

Membership

Andrew Walker, Director General of DHRC and SIRO for the House of Commons (Chair)
Rhodri Walters, Head of Corporate Services and SIRO for the House of Lords (Chair)
Peter Mason, Parliamentary Security Director
[Bob Castle], Head Of Information Rights and Information Security (IRIS) (HOC)
Victoria Payne, IRIS Information Manager (HOC)
Frances Grey, FOI Officer and Assistant Clerk of the Records (HOL)
Alex Daybank, Information Compliance Manager (HOL)
Mark Harbord, ICT Security and Risk Manager (PICT)
Alistair Duncan, IRIS Support Officer (HoC) (Secretary)

Invited to attend when appropriate

Paul Dillon-Robinson, Director of Internal Audit (HoC)
Paul Thompson, Head of Internal Audit (HoL)
Fergus Reid (PICT)
Departmental Information Risk Owners (DIROs) (HoC)
Information Security Co-ordinators (HoL)