



Cabinet Office

Specification for training for DHR Mandatory Roles: AO, SIRO and IAO.

Audience This paper will be of particular interest to:

Action

- SIROs (on behalf of AO), IAOs and Learning & Development units

- Implement

Timing Immediate

Background

1. The data Handling Review states that Government will roll out at least a minimum level of information management training to all Information Asset Owners, on appointment and annually, and strategic information management training to Accounting Officers, Senior Information Risk Owners, and members of audit committees to support a managerial culture that understands the importance of information and deals actively with risks to it

Guidance

2. The guidance outlines the generic module structure, the core training specification the proposed delivery mechanism, methods of assessment and time frames for delivery.

Contacts Enquiries about content should be directed to:

datareviewteam@cabinet-office.x.gsi.gov.uk

© Crown Copyright May 2008

Specification for training for DHR Mandatory Roles: AO, SIRO, IAO

1. The Minimum Mandatory Measures identified three roles critical roles in the management of, and accountability for, information risk: the Accounting Officer (AO), the Senior Information Risk Owner (SIRO) and Information Asset Owner (IAO).
2. This paper outlines the training required for these roles.

Single training specification for all three roles

3. Although the three roles are separate and have distinct responsibilities, all need to understand each others' roles: a common approach to training is proposed, with a single short course covering information risk and addressing all three roles.

Audience

4. All those appointed to one or more of the three mandatory roles of AO, SIRO and IAO.
5. Other board members may also find the material useful in providing an appreciation of information risk. In particular the Chair(s) of Audit committee(s) should be invited to participate.
6. Members of staff who will be directly assisting the delegates discharge their responsibilities should attend an equivalent session.

Delivery mechanism

7. Cabinet Office will shortly convene a working group to establish how this training is best delivered within departments and is available centrally. It is anticipated that delivery will involve the NSG and CESG.

Timing

8. Initial delivery to be during autumn 2008, with the training available at regular intervals thereafter for refresh and those new to the roles.

Assessment

9. Whilst no formal assessment of the learning gained is required delegates will wish to demonstrate their competency to staff and colleagues. Delegates' performance will feature, indirectly, in subsequent peer reviews.

AO/SIRO/IAO Training Specification

10. Following training, the delegate will:
 - Understand the key concepts of information risk, its management and its relationship with other forms of risk;
 - Be in a position to lead the cultural change journey necessary to ensure that staff value, protect and use information for the public benefit. (It may be appropriate to include this activity in any cultural or organisational development

initiatives already planned or underway);

- Understand the relevant legislative, regulatory and Minimum Mandatory Measures applicable across government including the accountability and reporting requirements;
- be aware of the current threat environment.

Course content

11. The following should be included in the course (although some of these categories may be treated together rather than as discrete items of content):

- Definition of information risk and information assurance: “the confidence that the information risks are being appropriately addressed”;
- Relationship to the business risk framework of the organisation;
- Roles and responsibilities: AO, SIRO, IAO, and those that support them; audit committee, accreditor, all staff: “what is expected of me and what I can expect of others”;
- Legislative and reporting requirements.

Detailed material

12. For those departments wishing to develop their training in-house, specific material be available from the CSIA-led working group referred to above. This material will include guidance available in the National Archives publication “Managing Information Risk”, 2008 and from CESG.