

# Busy Reader Guide for Improving Information Assurance at the Enterprise Level



# Busy Reader Guide for Improving IA at the Enterprise Level



## Introduction

This guide complements the CESH Good Practice Guide on Improving IA at the Enterprise Level. It aims to explain to Senior Information Risk Owners (SIROs) and others with responsibilities for managing information risk across an entire government department, agency or other public body (ie at the enterprise level):

- the importance of driving IA improvement through an enterprise level change programme rather than through a system level accreditation process
- the key steps for improving IA at the enterprise level

## Detail

- Information systems typically have complex interconnections. Securing the enterprise system by system is seldom feasible.
- There are economies of scale when controls are designed, deployed and operated on an enterprise scale instead of at the system level
- Enterprises are only as secure as their weakest links. Identifying the best places to invest requires an enterprise view.

## What can go wrong when IA is only addressed through the system level accreditation process?

- Information risks are not mitigated consistently making some desirable business activities too risky to be undertaken
- Improvement in one system is negated by weaknesses elsewhere
- Poor cultural attitudes to security are not challenged leaving IA policies unenforced

- Insufficient support for improving IA is obtained from senior stakeholders
- Lack of an Enterprise Security Architecture prevents the optimum balance between security and other business objectives being achieved

## Key Steps for Improving IA at the Enterprise Level

- Identify the strategic business benefits that improved IA can enable
- Gain board level commitment for IA improvement
- Use the HMG IA Maturity Model to identify opportunities for improvement
- Establish an IA improvement programme sponsoring group
- Address cultural attitudes to IA
- Use a business change framework
- Specify the enterprise set of IA controls and resource them
- Develop an audit regime that improves understanding of residual risk and enables more flexible business practices
- Plan to identify, consult and influence stakeholders
- Recognise contributions to improved IA; establish disciplinary procedures for serious offences

# Busy Reader Guide for Improving IA at the Enterprise Level



## Points to Check

Do we know what strategic business benefits improved IA can enable?

- Reduced information risk
- Reduced total cost of ownership of information systems
- More effective business practices

Who was consulted to identify potential benefits enabled by improved IA?

- Senior execs: SIRO, CTO, CIO
- Business & operations managers
- IA staff: IAOs, DSO, ITSO, ComSO, accreditors, vetting officers<sup>1</sup>
- Incident Manager(s)
- Information System managers, project managers, users
- IA maturity assessor
- Internal Audit Unit

Is the organisation committed to improving IA at the enterprise level?

- The SIRO has personally made the case for IA improvement to the board of directors
- An IA improvement programme sponsoring group has been established
- There is a clear vision of what success looks like
- A project portfolio has been designed and resourced to deliver the wanted benefits
- Benefit delivery milestones have been identified

Does the IA improvement programme include appropriate business change activities?

- A training and awareness programme has been designed for all staff and for those with IA responsibilities
- Key stakeholders have been identified and their support gained
- A communications plan has been developed
- IA policies will be updated

Will IA controls be improved?

- New controls to be deployed
- Existing controls strengthened or their coverage extended
- Monitoring of control effectiveness to be improved

Is the level of Information Management sufficient to support improved IA?

- We understand what information we have
- We understand the potential business impact of breaches of confidentiality, integrity or availability
- Our data is labelled according to its sensitivity

Will the improvements to IA be sustainable?

- Resources have been assigned to new or extended IA controls
- Control effectiveness will be monitored
- Good performance to support IA will be recognised
- HR processes will respond to non-compliance

---

<sup>1</sup> These roles are mandated in the Security Policy Framework. Abbreviations refer to Information Asset Owners, Departmental Security Officer, IT Security Officer & Communications Security Officer

The copyright of this document is reserved and vested in the Crown.

IA  
CESG  
B2h  
Hubble Road  
Cheltenham  
Gloucestershire  
GL51 0EX

Tel: +44 (0)1242 709141  
Fax: +44 (0)1242 709193  
Email: [enquiries@cesg.gsi.gov.uk](mailto:enquiries@cesg.gsi.gov.uk)

© Crown Copyright 2010. Communications on CESG telecommunications systems may be monitored or recorded to secure the effective operation of the system and for other lawful purposes.