

# Busy Reader Guide for Information Assurance for OGC Gateway™ Reviewers





## Purpose

This guide was developed in association with OGC and provides sample questions, which can be used by Reviewers at each OGC Gateway stage to probe the Information Assurance (IA) aspects of programmes or projects. It is aimed at Reviewers who are not IA experts. It gives examples of the evidence (indented below each question) that should be produced to support the system accreditation process mandated by the HMG Security Policy Framework (SPF). The completeness and quality of the recommended evidence that is provided should allow the Reviewer to judge how well IA is being addressed and delivered, and whether further probing is needed in order to reach a sensible level of assurance. **It is not intended to replace, or substitute for, IA accreditation.**

## Introduction to IA

IA is the confidence that information systems will protect the information they handle and will function as and when they need to, as required by legitimate users. The 2008 Data Handling Review mandated that the OGC Gateway Review process would include information risk as well as privacy. The HMG Information Assurance Standards (IS) form part of the SPF. The most relevant for the Gateway Review process are IS1 (Technical Risk Assessment) and IS2 (Risk Management and Accreditation of Information Systems). Accreditation is the documented assessment of an information system against its IA requirements, and the process is designed to align with the OGC Gateway Review Process.

## Questions and Evidence expected at each stage

### Gateway Stage 0:

Will the programme deliver changes that will handle, store or process personal, sensitive or protectively marked information?

- The type and business impact level of the information involved are understood.
- The applicable Departmental and HMG IA Policies and Standards, legislation and regulatory requirements have been identified and are being considered.

Is there a clear understanding of the IA dependencies?

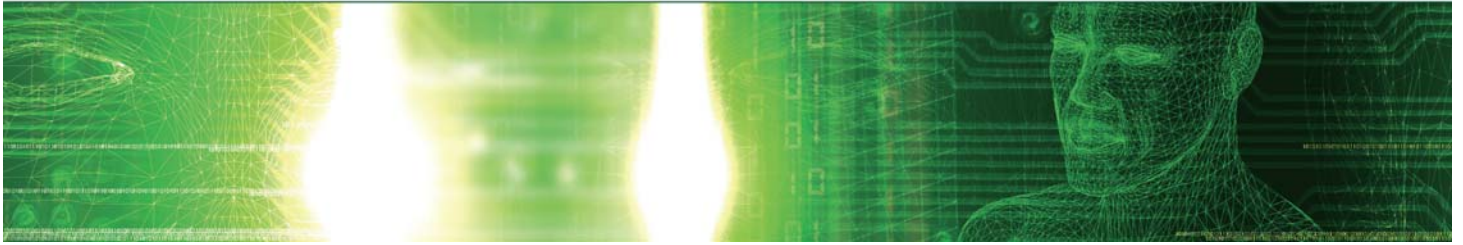
- The dependencies or impact on other departments, delivery partners, third parties or services have been considered.
- Processes for the ongoing coordination and management of IA across the programme have been established and resourced.

Has an initial IS1 technical risk assessment been produced? (only applicable at initial Gateway 0)

- A 'snapshot' IS1 technical risk assessment and a business impact statement that presents the outcome to the business stakeholder(s).

### Gateway Stage 1:

Has an accreditation plan been produced and the need for a Privacy Impact Assessment (PIA) been considered?



- An initial accreditation plan that also considers the PIA process<sup>1</sup>(if applicable) and assurance activities.

Have individuals who are responsible for IA been identified or appointed?

- Mandatory IA roles, including identified Information Asset Owners, are in place.
- Security working groups or a security accreditation panel established.

### **Gateway Stage 2:**

Has a full technical risk assessment been produced?

- A full IS1 technical risk assessment, risk register and initial risk treatment plan.

Has the IA requirement been documented and approved?

- An IA requirement endorsed by the Accreditor that forms part of the ITT.

### **Gateway Stage 3:**

Does the selected bid/solution raise any issues for the IA requirement?

- Any non-compliance with the IA requirement has been addressed and appropriate remedial action agreed.
- The risk register has IA-related risks reflected appropriately.

### **Gateway Stage 4:**

Have the IA processes been tested and approved?

- An endorsed plan for testing and validating the system security functionality has been applied, the outcomes considered and any remedial action taken.

Has the system been accredited?

- An approved Risk Management and Accreditation Document Set (RMADS).
- An accreditation certificate (which may be conditional).

### **Gateway Stage 5:**

Are systems in place to maintain and monitor the IA requirements?

- Periodic compliance checks against the RMADS and audit records.
- Significant changes to the risk components (threat, vulnerability and impact) have been addressed.

Are plans in place for periodic re-accreditation as required by IS2?

- Corporate IA policy reflects the re-accreditation requirements contained in IS2.

Threat and risk assessments must be revisited periodically throughout the lifetime of projects and programmes. When no longer required, systems must be securely decommissioned.

---

<sup>1</sup> For more details, see [www.ico.gov.uk/for\\_organisations/topic\\_specific\\_guides/pia\\_handbook.aspx](http://www.ico.gov.uk/for_organisations/topic_specific_guides/pia_handbook.aspx)

CESG's Busy Reader Guides are issued by the UK's National Technical Authority for Information Assurance with the aim of informing intended recipients of the general security issues they should consider in their approach to information and communications technologies. They are not a replacement for tailored technical or legal advice on specific systems or issues. GCHQ/CESG and its advisers accept no liability whatsoever for any expense, liability, loss, claim or proceedings arising from reliance placed upon this Guidance

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

OGC Gateway is a trade mark of the Office of Government Commerce

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.