Office of the *e-Envoy*
Leading the drive to get the UK online

*delivering*
UK online

# Assurance

e-Government Strategy Framework Policy and Guidelines

Version 2.0
September 2002

# Contents

# 1. Introduction

## 1.1 Ownership and maintenance

This Assurance Framework is one of a series developed as part of the Government's commitment, in the Modernising Government White Paper[1], to developing a corporate IT strategy for government (e-Government). It has been prepared by the Office of the e-Envoy, part of the Cabinet Office, on behalf of the e-Champions.

This version of the document has been prepared following a public consultation exercise.

## 1.2 Terminology

The meaning ascribed to specific terms within this document is provided in the glossary at annex A of the overarching security framework document[2]. A list of abbreviations specific to this document is provided at annex A.

## 1.3 Who should read this document?

This document is aimed at those establishing, procuring and providing e-Government services. This includes Central Government Departments, non-departmental public sector bodies, Local Authorities and other local government bodies charged with the provision of e-Government services. It also encompasses regulatory bodies responsible for the proper audit and control of public assets and information.

In addition it includes the suppliers and service providers who wish to offer services themselves, provide and operate such systems on behalf of government or provide equipment in support of e-Government services.

It is also relevant to security authorities that may use this document to assess the suitability of offered solutions and accredit them for operational use.

---

[1] *Modernising Government white paper*.

[2] The latest version of *e-Government strategy framework policy and guidelines, security*. Available at http://www.e-envoy.gov.uk

## 1.4  Background

It is the aim of the Modernising Government programme to move towards the electronic delivery of government services. To this end Government has produced an e-Government strategy, including the overarching e-Government security framework. The latter includes the approach for determining the security requirements and assuring the presence and proper operation of security countermeasures meeting the security requirements.

## 1.5  Objective

The Assurance Framework specifically addresses how business sponsors, service providers and developers ensure that e-Government services are designed, configured and operated in a secure manner. In particular, it builds on the approach set out in the Security Framework document and details a methodology for assessing whether the threats and vulnerabilities to e-Government security systems have been met by appropriately assured countermeasures for each security objective.

## 1.6  Scope

The Assurance Framework applies to technical (hardware and software applications) and non-technical (physical, personal and procedural) measures used to provide electronic transactions or services carried out by or on behalf of government bodies. It is intended to ensure that all government bodies, and organisations providing service on their behalf, deliver the highest possible quality of service to the citizen and business by using well-designed and well-operated hardware and software applications.

## 1.7  Organisations affected by this document

Central government departments and agencies **must comply** with this framework when installing and operating electronic business services. They shall:

a)   ensure that a security concept is developed as part of service concept development;

b)   ensure a security policy exists (preferably compliant with BS7799);

c)   ensure that a threat and vulnerability analysis to their systems has been conducted;

d)   ensure a risk assessment to their systems has been conducted;

e)   ensure that the system has been designed, implemented[3] and tested to minimise the risks with appropriately assured countermeasures, both technical and non-technical;

f)   ensure that systems are operated in a secure manner, including:

---

[3]        Implementation includes both the development and configuration of services.

ensuring that processes are in place to receive and act upon current security alerts, warnings and briefings (*eg* use of UNIRAS by a government department);

ensuring that any patches and updates are tested and implemented in a timely fashion;

ensuring that threat and vulnerability assessments and hence risk assessment are reviewed on a periodic basis;

ensuring that compliance with this framework is reviewed on a periodic basis.

It is **strongly recommended** that other public sector bodies adopt the recommendations of this framework in respect of transactions that they conduct with businesses and the public or which are conducted on their behalf.

Where the provision of e-Government services is to be provided commercially, by a third party, the procuring body should consider mandating compliance with this framework as part of the contract.

## 1.8   Relationship to other framework documents

The over-arching e-Government security policy framework document defines the following service control objectives. The means of achieving these objectives are considered in detail in the security framework and the lower level framework documents.

The documents form a complete set and it is strongly suggested that they should be read together. The overarching security policy framework document also provides guidance on how the documents should be used for the process of service security requirements specification and accreditation.

The e-Government registration and authentication framework document[4] addresses the following objectives:

a)   OS1 – Effective user identification and authentication;

b)   OS2 – Effective user registration;

c)   OS3 – Effective access control;

d)   OS4 – Effective user access management.

The trust services framework document[5] addresses the following objectives:

a)   OS5 – Non repudiation;

---

[4]   The latest version of *e-Government strategy framework policy and guidelines, registration and authentication*. Available at http://www.e-envoy.gov.uk

[5]   The latest version of *e-Government strategy framework policy and guidelines, trust services*. Available at http://www.e-envoy.gov.uk

b)  OS6 – Evidence of receipt;

c)  OS7 – Trusted commitment service;

d)  OS9 – Integrity.

The confidentiality framework document[6] addresses the following objective:

a)  OS8 – Privacy and confidentiality.

The business services framework document[7] addresses the following objectives:

a)  OS10 – Service availability;

b)  OS11 – Information availability;

c)  OS13 – Effective audit and accounting.

The network defence framework document[8] addresses the following objective:

a)  OS12 – Service protection.

The assurance framework document (this document) addresses the means by which trust in the implementation of security elements can be assured.

For protectively marked information or where there is an enhanced integrity and availability requirement the assurance requirements are determined by using HMG Infosec Standard No.1 (IS1). HMG Infosec Standard No.3 (IS3) defines the functionality needed to provide assured connections between business domains. IS1 is not currently applicable to material that is not protectively marked, (i.e. most data within the e-Government domain), however, it can be used for integrity and availability. IS3 can be used to recommend functionality requirements for the integrity and availability of business domain connections. In the e-Government domain for each level of service needed (OS1 – OS13) for authentication, trust, confidentiality and network defence there will be an associated set of functionality and assurance requirements.

## 1.9   Availability of advice

In the first instance, advice on the application of the assurance framework may be obtained from the Office of the e-Envoy[9].

---

[6]      The latest version of *e-Government strategy framework policy and guidelines, confidentiality*.  Available at http://www.e-envoy.gov.uk

[7]      The latest version of *e-Government strategy framework policy and guidelines, business services*.  Available at http://www.e-envoy.gov.uk

[8]      The latest version of *e-Government strategy framework policy and guidelines, network defence*.  Available at http://www.e-envoy.gov.uk

CESG[10] is the national technical authority on information security and may be consulted for further advice and assistance on technologies, measures and products to meet these requirements.

---

[9]       http://www.e-envoy.gov.uk.

[10]      Telephone 01242 237323 or *via* http://www.cesg.gov.uk.

# 2. Approach to assurance

## 2.1   General approach to assuring e-Government services

As the electronic delivery of government services will take place within a fluid and a rapidly changing environment, any mechanism an e-Government service provider uses to assure the security of their systems must be flexible and able to deliver quickly and efficiently whilst maintaining the business functionality.

The e-Government assurance process is built upon the principle of demonstrating compliance with the e-Government Security Policy Framework and BS7799. The focus of this framework is therefore to ensure that the implementation and operation of e-Government security services are managed and monitored. This breaks down into the following key components: the stages are those used in the security framework document[11].

*Service concept development*
a)   produce a security concept as part of service concept development, describing the e-Government service, the top-level threats and the likely nature of the countermeasures;

*Service requirements specification and review of compliance*
b)   analyse the threats and vulnerabilities to the system and produce a risk assessment;

c)   produce a security policy (preferably compliant with BS7799);

*Service design, implementation and test*
d)   address the risks by appropriately assured countermeasures; the security countermeasures should be documented in the security design document;

e)   lock-down architecture to cover only required services, in line with good commercial practice; this should be documented in the security design document;

f)   check system configuration is compliant with security policy;

g)   assess residual risk – repeat steps d), e)and f), until the residual risk is acceptable;

h)   implement strong audit and accounting measures;

---

[11]      The latest version of *e-Government strategy framework policy and guidelines, security.*   Available at http://www.e-envoy.gov.uk

i)   establish security operating procedures;

*Service acceptance, including security accreditation*
j)   ensure that the security countermeasures are tested and reviewed and meet the security policy and the security design when operated in accordance with the security operating procedures;

*Service delivery*
k)   operate the system in accordance with the security operating procedures, including regularly monitoring system logs;

l)   review the assurance status of the countermeasures and security operating procedures on a periodic basis;

*Service close down*
m)  ensure that information assets are removed and transferred to a successor service, if appropriate, destroyed or stored securely in accordance with the service specific security policy.

This process is designed to augment, not replace, any existing BS7799 process that may already be in place. When such a process exists then the BS7799 process should take precedence.

Part of establishing assurance is documenting all aspects of the security policy, design and operation. This aids the security review process, leading to accreditation. The key components listed above assume the following suggested documentation set:

a)   security concept;

b)   security policy;

c)   security design;

d)   security operating procedures.

## 2.2   Management requirements

It is expected that departments and agencies delivering e-Government services will appoint a business sponsor responsible for ensuring the delivery of an e-business service.

All departments and agencies must have an accreditor who is responsible for providing advice to the business sponsor ensuring e-Government services are compliant with the e-Government Security Policy Framework, BS7799 and other relevant government standards (eg the Manual of Protective Security (MPS) and the e-Government Interoperability Framework (eGIF), where appropriate). The accreditor audits all the security aspects of the e-Government service provider's implementation of appropriately assured technical and non-technical countermeasures, including reviewing all security-relevant documentation (eg security concept, security policy, security designs and security operating procedures etc).

The business sponsor, based on the advice from the accreditor, and taking into account the trade-offs between residual risk, the benefits of the e-Government service and security relevant test results, is responsible for accrediting the operation of the service.

For pan-Government systems the Departmental accreditors work with the UKonline Programme accreditor. The UKonline business sponsor and accreditor have right of veto over pan-Government systems.

The business sponsor is responsible for periodically reviewing the assurance and the effectiveness of the security countermeasures in conjunction with the accreditor.

## 2.3   Use of external assessors

Departments are encouraged to make use of external security consultants to provide analysis and review of threats and measures taken to counter them. This should provide departments with a clear and unbiased view as to the adequacy of the steps that they have taken.

To this end CESG, the National Infosec Technical Authority, trains and licenses each year a number of non-Government Infosec Consultants for providing such services under the CESG Listed Advisor Scheme (CLAS)[12]. CESG also trains and licences IT Health Check teams, under the CHECK scheme.

## 2.4   Use of evaluated products

The e-Government Assurance methodology does not mandate the use of formally evaluated products; however, departments may recognise the added value that these types of products may bring to the overall security solution. To this end a section on the different evaluation schemes has been provided at Annex B.

---

[12]        A full list of CLAS and CHECK Companies can be found at http://www.cesg.gov.uk.

# 3. Assurance methodology

## 3.1　Method rigour

The requirement that all risks should be countered or deemed acceptable indicates the need for security functionality. Assurance is that level of trust placed in the functionality. There are numerous methods for identifying functionality requirements, including the e-Government security framework and, within central government, IS1 and IS3. The following methodology suggests ways for identifying functionality and the assurance required to minimise risk.

The methodology described here is suitable for all systems. The accreditor is responsible for advising the business sponsor on the rigour of the methodology and assessing the implementation. The following 2 models of rigour are offered as examples:

a) **Self-certification** – the system delivery manager produces the security policy including a risk assessment and provides appropriate countermeasures (steps 1 and 2), and the accreditor accepts these at face value. This may not be sufficiently rigorous for some code of connection agreements.

b) **Accreditation** – the system delivery manager produces security policy including the risk assessment and provides appropriate countermeasures (steps 1 and 2) and the accreditor only accepts them after an independent review and verification (steps 3 and 4). This is sufficient for all e-Government systems and services. Steps 3 and 4 together are referred to as "evaluation".

The business sponsor and the accreditor agree the methodology to be applied to a specific e-Government service.

The accreditor should advise the business sponsor on a period after which the assurance of the system should be re-validated (step 5).

## 3.2　Method steps

*Step 1 – Determine system risks*
A risk analysis is performed. This risk analysis must consider the likelihood and impact of threats and vulnerabilities, the value of assets to be protected and the cost of recovery against assurance of countermeasures. The Security Policy Framework documents provide some initial insight on threats and vulnerabilities. HMG Infosec Standard No.3 provides a comprehensive set of functionality requirements for connecting all e-Government domains.

There are numerous tools to help produce a risk assessment; the government preferred methodology is CRAMM 4. Whatever method is used it should be compliant with BS7799.

A security policy, preferably compliant with BS7799, is produced, including the risk analysis. The security policy must be approved by the accreditor.

*Step 2 – Determine security requirements and countermeasures*
The e-Government Security Policy Framework breaks down the security of a system into thirteen control objectives. Each security control objective needs to be considered for the entire system and by meeting such a measure minimising the risk. This process will need to be performed for each of the identified assets.

The countermeasures required to reduce risks to an acceptable level may be technical or non-technical (physical, personnel and procedural). The technical countermeasures will need appropriate assurance. System configuration must be compliant with security policy.

At the end of this process each risk will have been addressed, or reduced / managed to a level such that the residual risk is explicitly understood and accepted by the business sponsor, based on advice from the accreditor.

Steps 1 and 2 must be completed and agreed with the accreditor before implementation commences.

*Step 3 – Review implementation*
After implementation, an independent quality assessment of the security policy processes laid out in steps 1 and 2 should be performed before the system becomes operational. Areas where the implementation does not match the security policy need to be identified and addressed, either by increasing the assurance of countermeasures or using stronger non-technical measures.

*Step 4 – Verify Implementation*
An independent verification of the compliance of the security countermeasures put in place and of the system configuration against the security policy should be performed before the system becomes operational. Areas where the implementation does not match the policy, or where countermeasures are insufficient, need to be identified and addressed; either by increasing the assurance of the countermeasures or using stronger non-technical measures.

*Step 5 – Review Assurance Status*
The period of review should be agreed based on advice from the accreditor as part of step 2 when identifying countermeasures, as a regular review of system security acts as a measure in itself.

When reviewing the assurance status of a system the review needs to consider the following questions:

a)  Are the threats and vulnerabilities still applicable to the system?

b)  Are the countermeasures still applicable to existing threats and vulnerabilities?

c)  Have any new threats and vulnerabilities arisen or have existing threats and vulnerabilities changed within the interim period of review?

d) Do the countermeasures successfully deny these new threats and vulnerabilities?

e) Do new countermeasures need to be implemented to deny these new/changed threats and vulnerabilities?

f) Does the functionality and assurance level of products and/or services meet the current business needs?

It is recommended that a review be carried out as a minimum at least every 12 months. However, any new threat or vulnerability identified between reviews should have appropriate assured countermeasures applied as soon as possible.

To ensure security is fully exploited as a business enabler, accreditors should also be aware of the opportunity that reviews offer to look again at business requirements formerly rejected because of security requirements. Changes to technology or threat may mean some of these can now be accommodated with acceptable risk.

## 3.3   Level of assurance

*Not protectively marked information*
For the e-Government domain the level of assurance depends on the level of control (of registration and authentication, trust, confidentiality, business services and network defence) needed to provide the service. Typically, the assessment of levels will lead to a set of levels for each area, referred to as a levels profile. For initial guidance and agreement with the accreditor, the level of assurance necessary for a particular control element is determined by the level determined for that element. The following paragraphs provide guidance for the assurance level required for each level:

For level 0 elements no assurance is required. For level 1 elements functionality should be based on good commercial products. Formal assurance is not required, but best practice suggests significant threats and vulnerabilities should be considered.

For level 2 elements some form of assurance is recommended with some functionality being provided by appropriate evaluated commercial products[13]. Typically, at level 2 there would be a quality review of the e-Government service implementation carried out by independent policy auditors[14] together with a verification of the implementation carried out by independent compliance auditors[15]. Formal evaluation and formal component evaluation would be an exception at level 2.

For level 3 the use of products and services that satisfy security profiles defined through tscheme should be used. This will normally include CAPS and/or CC (ITsec) approved products and services. Typically, at this level, there would be a quality review of the e-Government service implementation carried out by independent policy auditors together with a verification of the implementation carried out

---

[13]    CESG's Fast Track Scheme or similar is recommended and for cryptography using FIPS-140 standards or EESSI electronic signature standards.

[14]    One possibility is the use of CLAS consultants.

[15]    One possibility is the use of CHECK consultants.

by independent compliance auditors as for level 2. However, this is likely to be more stringent and with a broader scope at level 3.

*Protectively marked information and enhanced integrity and availability*
For protectively marked information and enhanced integrity and availability requirements the level of assurance and functionality is defined in IS1 and IS3. IS1 provides assurance levels in terms of Common Criteria (CC) evaluation profiles. In general, but depending on the significance of the security measure, for products or services with EAL2 or less then an accreditor would accept "commercial best practice"[16]. For EAL3 or above then formal evaluation would be required[17].

---

[16]  For EAL2, this would typically comprise a quality review of the e-Government service implementation carried out by independent policy auditors together with a verification of the implementation carried out by independent compliance auditors as for level 2. For EAL1 this would typically comprise a quality review and security testing carried out by the implementation team.

[17]  This will normally include CAPS and/or CC (ITsec) approved products and services, depending on the security functionality.

# A    Abbreviations

CAPS        CESG Assisted Products Scheme

CC          Common Criteria

CLAS        CESG Listed Advisor Scheme

CLEF        CESG Licensed Evaluation Facility

EESSI       European Electronic Signature Standardisation Initiative

eGIF        e-Government Interoperability Framework

FIPS        Federal Information Processing Standard

ICTSB       Information and Communications Technologies Standards Board

IS1         HMG Infosec Standard No.1

IS3         HMG Infosec Standard No.3

ITsec       IT Security Evaluation and Certification

ITSEC       IT Security Evaluation Criteria

MPS         Manual of Protective Security

TOE         Target of Evaluation

UNIRAS      Unified Reporting and Alert Scheme

# B    Evaluation methodologies

## B.1    Introduction

The following provides a summary from related literature on the different types of evaluation schemes that are available.

Formal evaluation would be undertaken by a CESG Licensed Evaluation Facility (CLEF).

## B.2    Common Criteria

The Common Criteria[18] (CC) are the outcome of efforts to develop criteria for the evaluation of IT security that are widely useful within the international community. It is an alignment and development of a number of existing European, US and Canadian criteria (ITSEC, TCSEC and CTCPEC respectively). It is a contribution to the development of an international standard[19], and opens the way to worldwide mutual recognition of evaluation results.

The Common Criteria present requirements for the IT security of a product or system under the distinct categories of functional requirements and assurance requirements. The CC functional requirements define the desired security behaviour, and the assurance requirements are the basis for gaining confidence that the claimed security measures are effective and implemented correctly.

While it is not precluded that e-Government systems undergo a CC evaluation, this may not be suited to a dynamic environment with fast changing systems and products. However, system implementers may wish to use previously evaluated products within their systems. These products will have been submitted by their developers to an independent security assessor for evaluation against a particular Target of Evaluation (TOE). The extent to which the TOE covers how the product is to be used in any particular system should always be borne in mind.

## B.3    Fast Track

The Fast Track Assessment Service[20] was developed to address the end-user requirement for significant improvements in the flexibility and efficiency of the current evaluation process. The formal Infosec evaluation process under the UK IT Security Evaluation and Certification Scheme (ITsec) was designed to incorporate a number of highly desirable features, including internationally recognised certificates of evaluation to objective standards, repeatability and independent oversight. However, it has been recognised that not all the features

---

[18]    Further details of the Common Criteria and those products already evaluated can be found at: http://www.cesg.gov.uk/assurance/iacs/itsec/index.htm

[19]    The common criteria have been adopted as an International Standard (ISO IS 15408).

[20]    Further details about the Fast Track Assessment process can be found at: http://www.cesg.gov.uk.

associated with formal evaluations are necessary to meet the assurance requirements of sponsors in all cases.

The Fast Track Assessment Service defines a less formal evaluation process that aims to achieve very significant cost and time savings compared to the most formal evaluations, and be sufficiently widely applicable to be a genuinely useful addition to the range of assurance options available.

In cases where it is felt that some assurance about a particular product is required but there is no formally evaluated equivalent available, then the Fast Track process should be considered.

## B.4    CAPS

The CESG Assisted Products Scheme (CAPS)[21] supports the commercial development of cryptographic products for Government requirements. It is aimed at supporting those applications where commercial-grade cryptography is required in a government environment. Assessments of those products submitted to the scheme are carried out by CESG in house, and result in a fit-for-government use certificate being awarded if successful.

e-Government system business sponsors and service providers may wish to consider the use of a CAPS assessed product where the storage or transmission of data may require level 2 or above confidentiality measures.

## B.5    FIPS-140

The US Federal Information Processing Standard 140-2[22] (FIPS PUB 140-2) provides a framework for the evaluation of cryptographic modules for use in processing US unclassified material.

The standard was developed by US government and industry and identified requirements for four security levels of cryptographic modules to provide for a wide spectrum of data sensitivity, and a diversity of application environments.

While the security requirements in the standard are intended to maintain the security of a cryptographic module, conformance to the standard does not guarantee that a particular module is secure. Similarly, the use of a cryptographic module that conforms to this standard in an overall system does not guarantee the security of the overall system.

If it is not practicable or appropriate for a CAPS evaluated product to be used, then a FIPS-140 product, that provides the relevant level of security, may be considered. NIST, the owners of the standard, license a number of laboratories to provide conformance testing to the standard.

---

[21]    Further details about the CESG Assisted Products Scheme can be found at: http://www.cesg.gov.uk.

[22]    Further details about FIPS PUB 140-2 can be found at http://www.nist.gov.

## B.6    ICTSB/EESSI

The Information and Communications Technologies Standards Board (ICTSB), with support of the European Commission, set up the European Electronic Signature Standardisation Initiative (EESSI). This is composed of public authorities, industry and experts. EESSI seeks to identify standards to be implemented in association with the use of electronic signatures[23].

---

[23]    Further details can be found at http://www.ict.etsi.org.