CABINET OFFICE

Office of the *e-Envoy*

Leading the drive to get the UK online

delivering UK online

Business Services

e-Government Strategy Policy Framework and Guidelines

Version 2.0
September 2002

Contents

1. Introduction

1.1 Ownership and maintenance

The e-Government business services framework policy and guidelines document 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. It has been prepared by the Office of the e-Envoy, part of the Cabinet Office, on behalf of the e-Champions.

This document builds on the e-Government security policy[2] that sets out the e-Government security requirements. It specifically addresses those security requirements related to the provision of business services to support access to e-Government services.

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

1.2 Terminology

In the context of this document, the term '**business services'** refers to the applications and infrastructure within the government domains that provide or support the delivery of e-Government services[3].

This loose definition covers a very wide range of applications, including:

a) Passive web services that allow information retrieval from a departmental web site;

b) Interactive services that enable information exchange with an individual government department, for example applying for a grant or licence;

c) Passive web services that allow information retrieval from multiple departmental assets, for example information on business travel overseas from FCO and DTI;

d) Interactive web services that enable information exchange with multiple government departments, for example notification and receipt of confirmation of a change of address;

e) Private correspondence with Government officials where some level of trust (traceability and accountability) is required of the information exchanged and in the electronic media of communication; and

---

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

3 This is the delivery of e-Government services to citizens and to businesses.

f) Complex multi-function services that enable both passive and interactive interaction with multiple departmental assets. For example citizens might access 'joined–up' services via a single web portal that logs their query, and identifies and notifies the relevant government departments via e-mail.

This paper discusses obligations on both clients and government users for the secure design, configuration and operation of e-Government business services:

a) **client** is used here to denote a person, organisation, representative of the person or organisation, or a process seeking to carry out a transaction with government.

b) **government user** in this context denotes a person or process that interacts with an e-Government service from a back-office system or access system (in any capacity). This includes third parties involved in the provision of e-Government services.

The meaning ascribed to these and other specific terms in the document is provided in the glossary in the overarching security framework.

A list of abbreviations is provided at annex A.

1.3 Who should read this document?

This document is aimed at those 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.

1.4 Background

The e-Government registration and authentication[4], confidentiality[5] and trust services[6] framework documents are concerned with proper access of clients and government users to e-Government services, confidentiality of private information involved in transactions and the ability to make binding commitments electronically.

---

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, confidentiality*. Available at http://www.e-envoy.gov.uk

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

In contrast the network defence[7] and business services framework documents are concerned with the protection of the e-Government service provision domain as a whole against electronic attack (both malicious and non-malicious) and non-malicious failure. Measures to be taken against physical attack and natural disasters (*eg* fire and flood) are outside the scope of the framework.

The essential difference between the business services and network defence frameworks is that the business services framework deals with protection of the systems and services against failure not prompted by attack (for example against compromise of service through faulty software) and the network defence framework is concerned with protection against malicious and inadvertent attack.

This document deals specifically with the protection of the e-Government service provision domain (*ie* the business services and the systems that host them) against non-malicious failure. In particular, this paper outlines measures to ensure that e-Government business service applications and the systems that host them are designed, configured and operated in a secure manner. This includes:

a) ensuring that connections provide access to e-Government services and data assets as and when required, and that business service applications are designed to be robust and reliable. These measures contribute to the security framework service control objectives OS10 - **Service availability** and OS11 – **Information availability**.

b) ensuring that the system is capable of determining those actions performed by users (both clients and government users) that have compromised or may compromise the security of the system. This contributes to the security framework service control objective OS13 – **Effective audit and accounting**[8].

1.5 Objective

This document is intended to set out a number of trust levels for business services in e-Government transactions.

Current guidance on the use of the security framework documents in the context of e-Government services is set out in the companion security architecture document.

1.6 Scope

This document is concerned with the correct design, configuration and operation of e-Government business services in order to ensure maximal secure service and information availability.

This framework applies to all business services, and the systems that host them, in the e-Government service provision domain. This includes both access systems and back office systems that are involved in the provision of e-Government services.

It is not the intention that the security requirements set out in the security framework documents should be applied retrospectively to existing systems. It is however envisaged that such systems, relevant to the delivery of e-Government services, should be addressed when modified.

---

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

8 Effective audit and accounting is included in this document as it is of general application for the delivery of business services (*eg* for performance monitoring).

1.7 Organisations affected by this document

This framework applies to all electronic transactions carried out by or on behalf of government. It is intended to ensure that all government bodies, and organisations providing services on their behalf, utilise business services in a consistent manner when providing services electronically.

Central government departments and agencies must comply with this framework in respect of electronic transactions. They shall, when introducing an electronic transaction:

a) follow the guidance in this framework in order to allocate the transaction to a business service level;

b) follow the guidance in this framework to deliver appropriate business service processes and functionality for the assigned level; and

c) ensure that they have considered all the risks set out in section 4 of this paper, and instituted adequate countermeasures.

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.

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 this and other 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 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 addresses the following objectives:

a) OS5 – Non repudiation;

b) OS6 – Evidence of receipt;

c) OS7 – Trusted commitment service;

d) OS9 – Integrity.

The confidentiality framework document addresses the following objective:

a) OS8 – Privacy and confidentiality.

The business services framework document (this document) addresses the following objectives:

a) OS10 – Service availability;

b) OS11 – Information availability;

c) OS13 – Effective audit and accounting.

The network defence framework document addresses the following objective:

a) OS12 – Service protection.

The assurance framework[9] document addresses the means by which trust in the implementation of security elements can be assured.

1.9 Availability of advice

In the first instance, advice on the application of the business services framework may be obtained from the Office of the e-Envoy[10].

CESG[11] 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 *E-government strategy framework policy and guidelines, assurance,* V1.1, 17 May 2002

10 http://www.e-envoy.gov.uk.

11 Telephone 01242 237323 or via http://www.cesg.gov.uk.

2. Summary of government's approach to business services

2.1 Introduction

This section sets out the approach to the provision of all or part of e-Government services by third parties, including obligations on third parties for business services.

An overarching operations concept for a client engaging in e-Government transactions in the context of the Government Gateway, and with the current limitations on the use of PKI, is given in the Security Architecture.

2.2 Third party participation in provision of e-Government services

2.2.1 Third party service delivery

The Modernising Government white paper makes clear the government's intention to work in partnership with local authorities, the voluntary sector, and with third-party delivery channels such as the Post Office and private sector companies. Where third-party service providers are conducting transactions on the government's behalf, they will be required to provide business services to the same standards as government itself would. Government will in turn accept transaction data from those delivery channels, who will certify that they have carried out the transaction to the agreed standard.

2.2.2 Use of commercial technologies

Government will make use of normal commercial technologies and techniques for business services, subject to compatibility with these guidelines.

The use of system components that have been formally certified under the ITSEC and/or Common Criteria schemes is encouraged. However, there will be no general requirement for systems to undergo ITSEC or Common Criteria evaluations. The process for assurance of e-Government services is described in the e-Government assurance framework.

It is considered acceptable to require a client to install a standard commercial security product in order to access e-Government services, for example a web browser with an up-to-date version of the Secure Sockets Layer (SSL) protocol. However, the requirement of client-installed custom software to access e-Government services should be avoided.

Government will make best efforts to ensure that services are accessible from a wide range of platforms (*eg* Personal Computers (PCs), kiosks *etc*), but cannot guarantee to include all. In those circumstances electronic services may be unavailable.

2.3 General approach to business services

For the purposes of e-Government transactions, this document defines levels of business services that are appropriate for differing classes of transaction. In general, informal or lower value transactions will attract the lower levels of business services. Higher value or legally significant transactions will attract more stringent business services.

A business service level should be assigned to a transaction independently of levels assigned in respect of registration, authentication, trust services, confidentiality and network defence. For example, there is no requirement that the business service level assigned to an e-Government transaction is the same as that for authentication.

When allocating a business service level to a transaction, service providers will need to consider the effect of non-malicious service failure on the public perception of security and reliability in e-Government services.

It is recognised that a Public Key Infrastructure (PKI), certificate enabled applications, or access tokens (such as smart cards) may not be available in the first instance. In this case, other mechanisms may be implemented initially, with an intention to adopt PKI mechanisms in due course.

3. Business service levels in government transactions

3.1 Introduction

This section defines the four business service levels, which represent degrees of impact of non-malicious failure of e-Government services. The levels are layered according to the severity of consequences that might arise.

It also gives examples of transactions and service provision guidelines under this scheme. Examples of transactions that might merit particular business service levels are not intended to be definitive.

In allocating transactions to business service levels, the relying party must consider all the direct and indirect consequences laid out in the definitions of the levels. In addition, departments will need to consider the terms 'minor', 'significant' and 'substantial' in the context of the parties likely to be affected. A significant financial loss to an individual might, for example, be a minor matter to a large company.

In addition, the implications of service failure may vary depending on other factors such as the time of year. For example, outage of an application allowing electronic submission of tax returns is likely to be much more of a problem in the week before the tax return filing deadline than at other times in the year.

Departments must determine the level implied for each consequence and allocate the highest of these to the transaction. For example, if non-malicious failure might result in risk to the client's personal safety then the transaction must be allocated to business service level 3, even if potential financial loss or other consequences are minimal.

Service providers must also consider the level assigned in terms of risks to the service as a whole, cost of implementation, practicality and overall business benefit. Departments may, in exceptional circumstances, be granted a waiver on adherence to this framework, subject to review during the assurance process.

Service provision guidelines are given in association with each level. These are related to service control objectives OS10 ('Service availability'), OS11 ('Information availability') and OS13 ('Effective audit and accounting'). The aspects of availability that relate to attack are dealt with in the network defence framework[12].

Audit and accounting has a key role to play in the provision of, and promoting confidence in, e-Government services. Audit logs may be required to provide evidence to support transactions varying

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

in nature from informal to legally binding. As a consequence, service providers must ensure that the confidentiality, integrity and availability of audit logs are protected to a level consistent with the strength of evidence that they may be required to provide. The potential compromise of evidence through poorly restricted access to and ease of alteration of such logs must not be underestimated. Business sponsors must ensure that evidence of transactions is retained as necessary and the retention is also in accordance with the Data Protection Act.

Service provision guidelines include business continuity planning and measures for restoring services after failure. These measures are also applicable to the after effects of electronic attack. Accordingly, the measures and processes adopted should be considered in conjunction with the guidance given in the network defence framework.

In this section we detail the *additional* measures that should be taken for each business service level, assuming that:

a) all legal obligations including privacy (*eg* under the Data Protection Act) and monitoring legislation, are fully implemented, for instance warning individuals sending information into an HMG domain that their communications may be monitored, recorded and retained, are being adhered to; and

b) the service is already being operated in a professional and businesslike manner.

Service providers must confirm that the above assumptions are correct.

This document covers only IT and communications systems and services. Service providers will also need to consider measures covering, for example, business continuity aspects of premises and personnel.

3.2 Level 0 - protection of transactions which might result in minimal damage

3.2.1 Definition

Level 0 business services are appropriate for e-Government transactions in which **minimal damage** might arise from non-malicious failure. In particular, failure of the transaction at level 0 might result in at most:

minimal inconvenience to any party; or

no risk to any party's personal safety; or

no release of personally or commercially sensitive data to third parties; or

minimal financial loss[13] to any party; or

no damage to any party's standing or reputation; or

no distress being caused to any party; or

no assistance in the commission of or hindrance to the detection of serious crime.

3.2.2 Examples

Examples of transactions that might merit level 0 business services include:

[13] In this context, 'financial loss' includes the results of any claim for damages.

a) a client reads or downloads publicly available information from a government website. Unavailability of the information due to non-malicious failure would cause at most minimal inconvenience to the client, who could attempt to access the information at a later date.

b) a client e-mails a government department with a request for general information and expects the material to be returned via e-mail. Failure of the transaction by malfunction of the business service application would not cause risk to safety, release of sensitive data or other serious consequences. The client would experience at most minimal inconvenience and could re-submit the request at a later date.

3.2.3 Service provision

3.2.3.1 OS10: Service availability

Normal good system practice should be adopted in respect of designing, implementing and managing the system. It is likely that at level 0 no explicit availability measures are required.

3.2.3.2 OS11: Information availability

At level 0 no special measures need be taken to ensure data backup or continuity of service following an interruption to service. In particular, no special measures need to be taken to recover partially completed transactions, other than for those that affect the integrity of existing information.

3.2.3.3 OS13: Effective audit and accounting

At level 0 no specific audit and accounting functionality is required.

3.3 Level 1 - protection of transactions which might result in minor damage

3.3.1 Definition

Level 1 business services are appropriate for e-Government transactions in which **minor damage** might arise from non-malicious failure. In particular, failure of the transaction at level 1 might result in at most:

minor inconvenience to any party; or

no risk to any party's personal safety; or

no release of personally or commercially sensitive data to third parties; or

minor financial loss to any party; or

minor damage to any party's standing or reputation; or

minor distress being caused to any party; or

no assistance in the commission of or hindrance to the detection of serious crime.

3.3.2 Examples

Examples of transactions that might merit level 1 business services include:

a) a client arranges a meeting with a government official by email. The impact of non-malicious failure (such as service unavailability) might be inconvenience and lost time, possibly minor financial loss, but no lasting impact on either party.

b) a client purchases a low cost government publication over the Internet. The impact of non-malicious failure might be inconvenience and possibly refunding or recovering incorrect payments.

3.3.3 Service provision

3.3.3.1 OS10: Service availability

Protection against non-malicious failure at this level should be provided by:

a) Availability: Availability for the business service to be provided should be set to be compatible with the assessment of the business need at level 1. It is likely that at level 1 no specific availability measures need be taken.

b) Sizing: Careful consideration should be given to sizing of the communications and information systems so as not to compromise availability. The sizing should be based on realistic estimates of demand for the e-Government service.

c) Alternative communications plans: Alternative communications paths that can be switched in within the timescale appropriate to the business need at level 1 should be available. It is likely that immediate failover is not necessary at level 1.

d) Power supply: Battery backup should be provided to allow ‘soft’ failure with power recovery achievable within the timescale appropriate to the business need at level 1.

e) Configuration management plan: A configuration management plan and processes covering the communications and information systems providing the service should be designed and implemented. Configuration changes should be approved by the system manager before implementation. Software should only be introduced with the approval of the system manager.

f) Failure impact analysis: Accreditors should ensure that a failure impact analysis has been carried out and recorded for all information and communication system components. This should be reviewed in the event of significant configuration changes.

g) Business continuity plan: A business continuity plan should be in place and subject to regular review. The plan should address:

   management roles and responsibilities for business continuity;

   recovery procedures and audit trail;

   security specific recovery actions.

3.3.3.2 OS11: Information availability

At this level no special measures need be taken to ensure data backup or continuity of service following an interruption to service. In particular, no special measures need to be taken to recover partially completed transactions, except for those that affect the integrity of existing information.

Protection against non-malicious failure at this level should be provided by:

a) Backups: At this level information back up should enable restoration of all relevant information to within one week of the current date. Commercial best practice should be followed with a full backup being taken, weekly when the system is offline with backup media being stored offsite. The restoration process should be documented in the business continuity plan and tested regularly.

b) Technical integrity features: Commercial best practice should be followed. This includes, for example, the use of parity checks or cyclic redundancy checksums for system software, configuration data and storage facilities.

c) Password recovery: A process should be available to provide access for a client to his/her account in the event of loss of a password.

3.3.3.3 OS13: Effective audit and accounting

Audit and accounting at this level covers:

a) Accounting: Basic client related information should be recorded (*eg* client identifier, time of service access, transaction used, success or failure of transaction).

b) Audit: The capability to carry out basic display and analysis of the accounting records should be provided.

3.4 Level 2 - protection of transactions which might result in significant damage

3.4.1 Definition

Level 2 business services are appropriate for e-Government transactions in which **significant damage** might arise from non-malicious failure. In particular, failure of the transaction at level 2 might result in at most:

significant inconvenience to any party; or

no risk to any party's personal safety; or

the release of personally or commercially sensitive data to third parties; or

significant financial loss to any party; or

significant damage to any party's standing or reputation; or

significant distress being caused to any party; or

assistance in the commission of or hindrance to the detection of serious crime.

3.4.2 Examples

Examples of transactions that might merit level 2 business services include:

a) a client completes an income tax return online. Non-malicious failure of business services or the systems that host them might result in sensitive information being released to an unauthorised third party. Other types of service failure, such as unavailability, might cause significant inconvenience to the client.

b) financial transactions, in which the inadvertent disclosure of a debit card number, for example, would be likely to cause significant distress and inconvenience to a client.

3.4.3 Service provision

3.4.3.1 OS10: Service availability

Protection against non-malicious failure at this level should be provided by:

a) Availability: Availability for the business service to be provided should be set to be compatible with the assessment of the business need at level 2. It is likely at level 2 that current good commercial architecture design is appropriate (*eg* use of multi-tier, high redundancy architectures (eg redundant processor configurations, mirrored disks, RAID arrays *etc*) and geographical distribution). Service Level Agreements (SLAs) for externally provided services should be set to meet the availability requirements (including transaction availability). Particular consideration needs to be given to the availability requirements for accounting logs.

b) Sizing: Careful consideration should be given to sizing of the communications and information systems so as not to compromise availability. The sizing should be based on realistic estimates of demand for the e-Government service.

c) Power supplies: battery backup should be provided to allow 'soft' failure, and power recovery should be achievable within the timescale appropriate to the business need at level 2. Consideration should be given to the use of an Uninterruptible Power Supply (UPS).

d) Alternative communications paths: Alternative communications paths that can be switched in within the timescale appropriate to the business need at level 2 should be available. At this level consideration should be given to the use of alternative communications paths with immediate failover.

e) Configuration management: a configuration management plan and processes covering the communications and information systems providing the service should be designed and implemented. Operational and security configuration should be checked for compliance with documentation, supplemented by a penetration test or CHECK[14] process. Configuration changes should be approved by the system manager before implementation and should be subject to secure audit (technical or procedural). Software should only be introduced with the approval of the system manager and a full inventory of all hardware and software and a network diagram showing all approved connections should be maintained.

f) Failure impact analysis: Accreditors should ensure that failure impact analysis has been carried out and recorded for all information and communications components. This should be reviewed in the event of significant configuration changes. No upgrades should be permitted without prior offline testing and assessment.

g) Correct equipment operation: A commercial best practice self-test process should be in place.

h) Business continuity plan: A business continuity plan should be in place and subject to regular review. The business continuity plan should be subject to regular rehearsal. The plan should address:

    management roles and responsibilities for business continuity;

    recovery procedures and audit trail;

    security specific recovery actions.

[14] www.cesg.gov.uk/partnership/pwi/check/index.htm

3.4.3.2 OS11: Information availability

At this level it is appropriate to identify partially complete transactions that might have failed in the event of non-malicious failure and to inform the parties involved accordingly. However, no special measures need be taken to recover partially completed transactions except for those that affect the integrity of existing information.

Protection against non-malicious failure at this level should be provided by:

a) Backups: At this level information back up should enable restoration of all relevant information to within one day of the current data. Commercial best practice should be followed with a full backup being taken weekly with daily incremental backups when the system is offline. The backup should be compared against the original before the backup media is stored offsite. The restoration process should be documented in the business continuity plan and tested regularly.

b) Technical integrity features: Baseline level cryptographic checksums or secure software isolation for system software, configuration data and storage facilities should be provided. A secure self-test process should be undertaken regularly using these facilities.

c) Password and key recovery: A process should be available to provide access for a client to his/her account in the event of loss of a password or access token.

3.4.3.3 OS13: Effective audit and accounting

Audit and accounting at this level cover:

a) Accounting: Basic client related information should be recorded (*eg* client identifier, time of service access, transaction used, success or failure of transaction).

b) Audit: The capability to carry out basic display and analysis of the accounting records should be provided.

3.5 Level 3 - protection of transactions which might result in substantial damage

3.5.1 Definition

Level 3 business services are appropriate for e-Government transactions in which **substantial damage** might arise from non-malicious failure. In particular, failure of the transaction at level 3 might result in at most:

substantial inconvenience to any party; or

risk to any party's personal safety; or

the release of personally or commercially sensitive data to third parties; or

substantial financial loss to any party; or

substantial damage to any party's standing or reputation; or

substantial distress being caused to any party; or

assistance in the commission of or hindrance to the detection of serious crime.

3.5.2 Examples

Examples of transactions that might merit level 3 business services include:

a) electronic movement of a client's medical records or results of health screening. Non-malicious failure such as information unavailability might cause substantial distress and/or risk to the health of the client.

b) an organisation filing a Value Added Tax (VAT) return electronically. Non-malicious failure might result in the release of commercially sensitive data to third parties and possibly substantial inconvenience and financial loss.

3.5.3 Service provision

3.5.3.1 OS10: Service availability

Protection against non-malicious failure at this level should be provided by:

a) Availability: The availability of the overall business service and individual transactions should be set to be compatible with the assessment of the business need at level 3. At level 3 current good commercial practice architecture design should be used (*eg* use of multi-tier, high redundancy architectures (*eg* redundant processor configurations, mirrored disks, RAID arrays *etc*) and geographical distribution). SLAs for externally provided services should be set to meet the availability requirements (including transaction availability). Particular consideration needs to be given to the availability requirements for accounting logs.

b) Sizing: Careful consideration should be given to sizing of the communications and information systems so as not to compromise availability. The sizing should be based on realistic estimates of demand for the e-Government service.

c) Power supplies: battery backup should be provided to allow 'soft' failure, and power recovery should be achievable within the timescale appropriate to the business need at level 3. It is anticipated that at this level a UPS will be required.

d) Alternative communications paths: Alternative communications paths that can be switched in within the timescale appropriate to the business need at level 3 should be available. It is anticipated that at this level alternative communications paths with immediate failover will be required.

e) Configuration management: a configuration management plan and processes covering the communications and information systems providing the service should be designed and implemented. Operational and security configuration should be checked for compliance with documentation, supplemented by a penetration test or CHECK[15] process. Configuration changes should be approved by the system manager before implementation and should be subject to secure audit (technical or procedural). Software should only be introduced with the approval of the system manager and a full inventory of all hardware and software and a network diagram showing all approved connections should be maintained.

f) Failure impact analysis: Accreditors should ensure that failure impact analysis has been carried out and recorded for all information system and communication components. This should be reviewed in the event of significant configuration changes. No upgrades should be permitted without prior offline testing and assessment.

---

[15] www.cesg.gov.uk/partnership/pwi/check/index.htm

g) Correct equipment operation: A commercial best practice self-test process should be in place.

h) Business continuity plan: A business continuity plan should be in place and subject to regular review. The business continuity plan should be subject to regular rehearsal. The plan should address:

management roles and responsibilities for business continuity;

recovery procedures and audit trail, covering the system, communications and transactions;

security specific recovery actions.

3.5.3.2 OS11: Information availability

At this level it is appropriate to identify and recover partially complete transactions that might have failed in the event of non-malicious failure and to inform the parties involved accordingly.

Protection against non-malicious failure at this level should be provided by:

a) Backups: At this level information back up should enable restoration of all relevant information to within one day of the current data. Commercial best practice should be followed with a full backup being taken weekly with daily incremental backups when the system is offline. The backup should be compared against the original before the backup media is stored offsite. The restoration process should be documented in the business continuity plan and tested regularly.

b) Technical integrity features: Baseline level cryptographic checksums or secure software isolation for system software, configuration data and storage facilities should be provided. A secure self-test process should be undertaken regularly using these facilities.

c) Key recovery: A process should be available to provide access for a client to his/her account in the event of loss of an access token.

3.5.3.3 OS13: Effective audit and accounting

Audit and accounting at this level cover:

a) Accounting: Relevant client related information should be recorded for each transaction (*eg* client identifier, time of service access, transaction used, success or failure of transaction, current transaction status).

b) Audit: The capability to carry out display and detailed analysis of the accounting records should be provided .

4. Risks and countermeasures

4.1 Introduction

This section considers general risks of non-malicious failure pertaining to the business service applications and systems that host e-Government services and sets out possible countermeasures against each of the stated risks.

It does not consider risks and countermeasures relating to malicious or non-malicious electronic attack on the e-Government service provision domain; these are considered in the network defence framework.

Risk	Possible countermeasures
R1) Technical failure. Technical failure of computer systems, applications, networks or connection equipment may lead to security failures.	Possible countermeasures to prevent breaches of security as a result of technical failure include: C1a) use of a good commercial practice architecture design (*eg* use of redundant processor configurations, mirrored disks, RAID arrays *etc*) to meet availability requirements (including transaction availability); C1b) setting SLAs for externally provided services to meet availability requirements (including transaction availability); C1c) provision of backup power supplies, UPS and alternative communications paths; C1d) technical integrity features such as checksums and secure self-test processes to verify correct equipment operation; C1e) failure impact analysis to ensure configuration provides for security resilience in the event of information system or communications component failure; C1f) use of backups at an appropriate frequency to recover lost or damaged information; C1g) provision of a password recovery or key recovery service; C1h) development and implementation of a configuration management plan, so that the original configuration can always be securely restored; C1i) development and rehearsal of a business continuity plan; C1j) comprehensive testing of business service applications and the systems that host them; C1k) recording and analysis of accounting logs, so as to derive information about interruption of service and transaction failures both to prevent future failures and to aid recovery.

A Abbreviations

PC	Personal Computer
PKI	Public Key Infrastructure
SLA	Service Level Agreement
UPS	Uninterruptible Power Supply
VAT	Value Added Tax

Online copies of this document will be made available at: www.govtalk.gov.uk

Office of the e-Envoy, Stockley House, 130 Wilton Road, London, SW1V 1LQ