Network Defence

e-Government Strategy Framework Policy and Guidelines

Version 2.0
September 2002

Contents

1. Introduction

1.1   Ownership and Maintenance

The e-Government network defence 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 network defence services to support access to e-Government services.

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

1.2   Terminology

Network defence services are the technical means by which the threats associated with connecting business domains or IT resources electronically may be countered.

In the context of this paper, this refers primarily to ensuring that the e-Government service provision domain is adequately protected against outside malicious electronic attack (and inadvertent attack that might have the same effects) intended to:

a)   undermine continued provision of a service; and/or

b)   affect adversely the integrity of services or information provided; and/or

c)   use the information resources of e-Government in the commission of serious crime; and/or

d)   otherwise cause damage to government, systems or clients.

This corresponds to the security framework control objective OS12 – **Service protection**.

This paper discusses obligations on both clients and government users for network defence:

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.

---

[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

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 also 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[3], confidentiality[4] and trust services[5] 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 respectively.

In contrast, the network defence and business services[6] 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.

---

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

4   The latest version of *e-Government strategy framework policy and guidelines, confidentiality*. 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.

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

1.5   Objective

This document is intended to set out a number of trust levels for network defence 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 security measures required to ensure that the plant, stored data and other assets of e-Government services are properly protected against malicious and inadvertent electronic attack where domains are connected together.

This framework applies to all connections of government IT systems to other business domains within or without government for the provision of e-Government services.

1.7   Organisations affected by this document

This framework applies to all electronic transactions carried out by or on behalf of government where there is a need for network defence. It is intended to ensure that government bodies, and organisations providing services on their behalf, carry out network defence 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 network defence level;

b)   follow the guidance in this framework to deliver appropriate network defence 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 addresses the following objectives:

a) OS10 – Service availability;

b) OS11 – Information availability;

c) OS13 – Effective audit and accounting.

The network defence framework document (this document) addresses the following objective:

a) OS12 – Service protection.

The assurance framework[7] 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 network defence framework may be obtained from the Office of the e-Envoy[8].

CESG[9] 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.

---

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

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

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

2. Summary of government's approach to network defence 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 network defence 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 network defence 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 network defence 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 systems 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 network defence

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

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

Empirically, it may be the case that, for example, transactions that require high levels of confidentiality might require similarly high levels of network defence to safeguard information. However, there is no set rule for the relation between network defence and the other aspects of security. It is for the service provider to ensure that the levels assigned form a consistent set with all the necessary functionality.

When allocating a network defence level to a transaction, service providers will need to consider the effect of malicious electronic attack or inadvertent compromise of services / information on the public perception of security in e-Government services. For example, a transaction such as reading or downloading publicly available information is unlikely to require high levels of registration, authentication, confidentiality or trust services. However, a malicious electronic attack resulting in a defaced web site or altered content of publicly available government information could have an adverse effect on the public perception of e-Government services as a whole.

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.

Further guidance on network defence mechanisms may be found in the Manual of Protective Security (MPS).

3. Network defence levels in government transactions

3.1 Introduction

This section defines the four network defence levels, which represent degrees of impact of malicious or inadvertent electronic attack on 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 network defence levels are not intended to be definitive.

In allocating transactions to network defence 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 electronic attack might result in risk to the client's personal safety, then the transaction must be allocated to network defence 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 objective OS12 - Service protection.

Any network defence strategy needs to consider protection, detection and reaction. Some measures that might be taken as a reaction to a malicious or inadvertent electronic attack (such as the restoration of a service enabled by regular back ups) are also applicable to handling the after effects

of a non-malicious failure. Accordingly, the measures and processes adopted should be considered in conjunction with the guidance given in the business services framework[10].

Service providers must clearly identify the boundaries of the service provision domain to be protected. These must be specified in the documentation produced as part of the design and accreditation of an e-Government service (see the overarching security framework for a detailed discussion of this process). In addition if the domain to be protected covers more than one physical site, then the network connections between sites must also be protected.

System technical security measures must be subject to regular review, and regular testing where appropriate. The frequency of review and testing must be specified in the document produced as part of the design and accreditation of a service.

This document is concerned with the protection of the service provision domain, hence measures given relate to government users rather than clients. Clients may of course use similar measures to protect their information; however, government can bear no responsibility for this.

Effective network defence might require in some cases that only certain types of information be accepted by government systems. In these cases, the restrictions on acceptable types of information, attachments *etc* must be clearly communicated to clients.

e-Government back office or access systems may have mechanisms (eg Intrusion Detection Systems (IDS)) that monitor and detect untoward events. Any detections of untoward events should be disseminated to the business sponsor and / or e-Government service provider.

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

3.2.1   Definition
Level 0 network defence services are appropriate for e-Government transactions in which **minimal damage** might arise from electronic attack. In particular, a successful electronic attack (malicious or inadvertent) on the service provision domain 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[11] 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 network defence include:

---

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

[11]   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 web site. Malicious electronic attack, such as defacing of the web site might cause minimal inconvenience to the client and no embarrassment to the government in this case[12].

b) A client e-mails a government department with a request for general information and expects the material to be returned via e-mail. Electronic attack resulting in, for example, loss of integrity of the information might result in minimal inconvenience or loss of time to the client, but no serious consequences such as risk to safety.

3.2.3   Service provision

Prevention of electronic attack[13] on e-Government services should be provided at this level by adoption of normal good system practice for implementing and managing network connections; no explicit network defence services are required.

Detection of electronic attack on e-Government services is not required at this level.

Reaction to electronic attack on e-Government services should be provided at this level by:

a) Impact assessment: an assessment should be made of whether any damage, including loss of data integrity, has occurred and a recovery action plan drawn up.

b) Recovery: the system should be restarted; as far as possible any damaged data should be reloaded and external connections restarted.

c) Lessons learnt: system security staff should examine all incidents of electronic attacks and determine whether any additional electronic or procedural countermeasures should be put in place.

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

3.3.1   Definition

Level 1 network defence services are appropriate for e-Government transactions in which **minor damage** might arise from electronic attack. In particular, a successful electronic attack (malicious or inadvertent) on the service provision domain 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.

---

[12]   Of course, should it be adjudged that defacement of a website would cause damage to reputation, a higher network defence level would be assigned.

[13]   Electronic attack is used as a generic term to describe both malicious attack and other inadvertent incidents that might have similar effects.

3.3.2 Examples
Examples of transactions that might merit level 1 network defence include:

a) A client arranges a meeting with a government official by email. The impact of loss of integrity or other consequences of electronic attack is 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 malicious electronic attack to attribute the purchase to the wrong client, or to alter the number of copies ordered, for example, would be inconvenience and possibly refunding or recovering incorrect payments.

c) A client reads or downloads publicly available information from a government web site. Malicious electronic attack, such as defacing of the web site might cause minor embarrassment to the government.

3.3.3 Service provision
3.3.3.1 OS12: Service protection
Prevention of electronic attack on e-Government services should be provided at this level by:

a) User application configuration: all government user applications capable of processing imported material shall be configured to do so safely. For instance, word processing and spreadsheet applications should preferably prevent automatic macro execution without prior user permission or a detection strategy should be in place.

b) Import restrictions: the import of information objects from another domain should be limited to information object types reasonably required to meet business needs; all imported objects should be screened for recognisable structures such as virus signatures. An anti-virus strategy with timely updates should be implemented, subjecting imported information objects to content analysis. Web site access for government users should be limited to known and 'trusted' sites or those that do not have entries on a blacklist.

c) User empowerment: the export of information objects from one domain to another should be limited to information object types reasonably required to meet business needs.

d) Service minimisation: there should be an effective configuration management process and routine inspections to ensure that cross-domain services and interfaces are limited to those necessary to meet the connection's business objectives.

e) Firewall: a properly configured firewall is required. System responses in the event of a service being refused (or permitted) should be designed so as to prevent anyone from deducing information that might be used to attack the system (*eg* physical IP addresses).

f) Security awareness training: where possible, ordinary government users should be trained in security awareness matters. Government users shall be made aware of the risks inherent in external connections, the relevant procedures for managing them, and the penalties for infringement. Government users shall sign to confirm that they accept privileges and responsibilities assigned to them.

g) Security staff training: those responsible for management of the security of a connection shall undertake security awareness and technical training commensurate with the emerging HMG Infosec Certificate.

Detection of electronic attack on e-Government services should be provided at this level by:

a) System monitoring: standard system-provided activity monitors should be regularly examined to ascertain whether there is any suspicious activity or pattern of activities that might indicate an electronic attack is being conducted. At this level, consideration should be given to the use of host and/or network based intrusion detection systems.

b) Reviewing accounting logs: standard system-provided accounting logs should be reviewed by system security staff to ascertain whether there is any activity or pattern of activities that might indicate an electronic attack has occurred.

Reaction to electronic attack on e-Government services should be provided at this level by:

a) Incident response plan: an incident response plan, incorporating actions that may range from immediate restoration of service to partial restoration or suspension of service, should be documented and subjected to regular testing and review.

b) Controlled closedown: a controlled connection closedown process should be available, maintaining the provision of essential business services as far as possible.

c) Impact assessment: an assessment should be made of whether any damage, including loss of data integrity, has occurred and a recovery action plan drawn up.

d) Recovery: the system should be restarted; as far as possible any damaged data should be reloaded and external connections restarted.

e) Lessons learnt: system security staff should examine all incidents of electronic attacks and determine whether any additional electronic or procedural countermeasures should be put in place.

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

3.4.1   Definition
Level 2 network defence services are appropriate for e-Government transactions in which **significant damage** might arise from electronic attack. In particular, a successful electronic attack (malicious or inadvertent) on the service provision domain 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 network defence include:

a)   A client completes an income tax return online. Electronic attack might result in details of the income tax assessment being released to an unauthorised third party.

b)   A client undertakes a financial transaction. Electronic attack resulting in 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   OS12: Service protection

Prevention of electronic attack on e-Government services should be provided at this level by:

a)   User application configuration: all government user applications capable of processing imported material shall be configured to do so safely. For instance, word processing and spreadsheet applications should preferably prevent automatic macro execution without prior government user permission or a detection strategy should be in place.

b)   Import restrictions: these comprise:

   a business case and risk assessment should be provided for each information type to be imported; all imported objects should be screened for recognisable structures such as virus signatures. An anti-virus strategy with timely updates should be implemented, subjecting imported information objects to content analysis. All import requests shall be recorded to meet specified audit requirements enabling trend analysis to be performed.

   website access should be granted explicitly subject to a business case, and limited to known and 'trusted' sites. PKI-based object certification should be considered where appropriate, signed by a trusted CA. Active web content should be removed on import or executed in a controlled safe space. E-mail attachments should be limited to permitted types.

c)   User empowerment: a business case and risk assessment should be provided for each information type to be exported.

d)   Export restrictions: government users must be made aware of all items selected for export, as hidden information might be included (such as deleted text in a word processor file).

e)   Service minimisation: there should be an effective configuration management process and routine inspections, monitoring and audit to ensure that cross-domain services and interfaces are limited to those necessary to meet the connection's business objectives.

f)   Firewall: a properly configured firewall is required. System responses in the event of a service being refused (or permitted) should be designed so as to prevent anyone from deducing information that might be used to attack the system (*eg* physical IP addresses).

g)   Security awareness training: ordinary government users should be trained in security awareness matters. Government users shall be made aware of the risks inherent in external connections, the relevant procedures for managing them, and the penalties for infringement.

h)   Security staff training: those responsible for management of the security of a connection shall undertake security awareness and technical training commensurate with the emerging HMG Infosec Certificate.

i) Currency: there must be procedures to receive and respond to notifications of security incidents and software updates for all security-relevant systems and software.

Detection of electronic attack on e-Government services should be provided at this level by:

a) Intrusion detection: host and/or network based intrusion detection systems should be used, in addition to the monitoring of standard system-provided activity monitors, to ascertain whether there is any suspicious activity or pattern of activities that might indicate an electronic attack is being conducted.

b) Reviewing accounting logs: standard system-provided accounting logs should be reviewed by system security staff to ascertain whether there is any activity or pattern of activities that might indicate an electronic attack has occurred. At this level, consideration should be given to the use of automated audit tools.

Reaction to electronic attack on e-Government services should be provided at this level by:

a) Incident response plan: an incident response plan, incorporating actions that may range from immediate restoration of service to partial restoration or suspension of service, should be documented and subjected to regular testing and review.

b) Controlled closedown: a controlled connection closedown process should be available, maintaining the provision of essential business services as far as possible.

c) Impact assessment: for each electronic attack identified, an assessment should be made of whether any damage, including loss of data integrity, has occurred and, if necessary, a specific recovery action plan drawn up in line with the guidance in the incident response plan.

d) Recovery: the system should be restored; as far as possible any damaged data should be reloaded and external connections restarted.

e) Lessons learnt: system security staff should examine all incidents of electronic attacks and determine whether any additional electronic or procedural countermeasures, including changes to the incident response plan, should be put in place.

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

3.5.1   Definition

Level 3 network defence services are appropriate for e-Government transactions in which **substantial damage** might arise from electronic attack. In particular, a successful electronic attack (malicious or inadvertent) on the service provision domain 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 network defence include:

a) A hospital stores electronically a client's medical records or results of health screening. Electronic attack resulting in disclosure of a client's medical information to an unauthorised third party, or loss of integrity, might cause substantial distress and/or risk to the health of the client.

b) An organisation files a Value Added Tax (VAT) return electronically. Electronic attack 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 OS12: Service protection

Prevention of electronic attack on e-Government services should be provided at this level by:

a) User application configuration: all user applications capable of processing imported material shall be configured to do so safely. For instance, word processing and spreadsheet applications should preferably prevent automatic macro execution without prior government user permission or a detection strategy should be in place.

b) Import restrictions: these comprise:

a business case and risk assessment should be provided for each information type to be imported; all imported objects should be screened for recognisable structures such as virus signatures. An anti-virus strategy with timely updates incorporating anti-virus products (the use of two products should be considered) should be implemented, subjecting imported information objects to content analysis. All import requests shall be recorded to meet specified audit requirements enabling trend analysis to be performed.

website access should be granted explicitly subject to a business case, and limited to known and 'trusted' sites. PKI-based object certification should be considered where appropriate, signed by a trusted CA. Active web content should be removed on import or executed in a controlled safe space. E-mail attachments should be limited to permitted types.

c) User empowerment: a business case and risk assessment should be provided for each information type to be exported.

d) Export restrictions: government users must be made aware of all items selected for export, as hidden information might be included (such as deleted or original text in a word processor file).

e) Service minimisation: there should be an effective configuration management process and routine inspections, monitoring and audit to ensure that cross-domain services and interfaces are limited to those necessary to meet the connection's business objectives.

f) Firewall: a properly configured firewall is required. System responses in the event of a service being refused (or permitted) should be designed so as to prevent anyone from deducing information that might be used to attack the system (*eg* physical IP addresses).

g) Security awareness training: ordinary government users should be trained in security awareness matters. Government users shall be made aware of the risks inherent in external connections, the relevant procedures for managing them, and the penalties for infringement.

h) Security staff training: those responsible for management of the security of a connection shall undertake security awareness and technical training commensurate with the emerging HMG Infosec Certificate.

i) Currency: there must be procedures to receive and respond to notifications of security incidents and software updates for all security-relevant systems and software.

Detection of electronic attack on e-Government services should be provided at this level by:

a) Intrusion detection: host and/or network based intrusion detection systems should be used, in addition to the monitoring of standard system-provided activity monitors, to ascertain whether there is any suspicious activity or pattern of activities that might indicate an electronic attack is being conducted.

b) Reviewing accounting logs: automated audit tools should be used by system security staff to examine standard system-provided accounting logs to ascertain whether there is any activity or pattern of activities that might indicate an electronic attack has occurred.

Reaction to electronic attack on e-Government services should be provided at this level by:

a) Incident response plan: an incident response plan, incorporating actions that may range from immediate restoration of service to partial restoration or suspension of service, should be documented and subjected to regular testing and review. There should be a properly trained Computer Incident Response Team (CIRT).

b) Incident recovery procedures: there should be detailed incident recovery operating procedures to be followed in the event of an attack, based on the incident response plan.

c) Controlled closedown: a controlled connection closedown process should be available, maintaining the provision of essential business services as far as possible.

d) Impact assessment: for each electronic attack identified, an assessment should be made of whether any malicious damage, including loss of data integrity, has occurred and, if necessary, a specific recovery action plan drawn up in line with the guidance in the incident recovery procedures.

e) Recovery: the system should be restored; as far as possible any damaged data should be reloaded and external connections restarted.

f) Lessons learnt: system security staff should examine all incidents of electronic attacks and determine whether any additional electronic or procedural countermeasures, including changes to the incident response plan and/or incident recovery procedures, should be put in place.

4. Risks and Countermeasures

This section considers some general risks pertaining to connections between e-Government systems and other domains, and sets out possible countermeasures against each of the stated risks. It does not consider risks inherent in the systems within domains, nor risks relating to specific technologies.

Risk	Possible countermeasures
R1) Introduction of malicious software. A user or users of the domain to which the e-Government service provision domain is connected may seek to exploit the intended or unintended services provided by the connection to introduce malicious software (*eg* viruses, Trojan horse).	Possible countermeasures to prevent the introduction of malicious software include: C1a) screening of all imported information objects for recognisable structures; and C1b) restriction of website access to known and trusted sites, and removal of active web content; and C1c) safe configuration of applications processing imported information; and C1d) PKI-based certification of imported information objects.
R2) Denial of service attack. A user or users of the domain to which the e-Government service provision domain is connected may seek to exploit the intended or unintended services provided by the connection to conduct a denial of service attack.	Possible countermeasures to prevent a successful denial of service attack include: C2a) monitoring of traffic for attack profiles, and the diversion or termination of suspect network traffic; and C2b) a controlled connection closedown process allowing essential business processes to be maintained in the absence of the connection.
R3) Export of unsuitable material. A user of the e-Government service provision domain may (be it intentionally, unintentionally or lured to do so by a user in the other domain) export material for which the receiving domain cannot prevent access by unauthorised recipients.	Possible countermeasures to prevent the export of such material include: C3a) limiting of exports to information object types necessary to meet business needs; and C3b) limiting cross-domain services and interfaces to those necessary to meet business needs; and C3c) user awareness of the risks of external connection, the procedures for managing them, and the penalties for infringement.

A   Abbreviations

CA   Certification Authority

CIRT   Computer Incident Response Team

CRL   Certificate Revocation List

MPS   Manual of Protective Security

PC   Personal Computer

PIN   Personal Identification Number

RA   Registration Authority

VAT   Value Added Tax