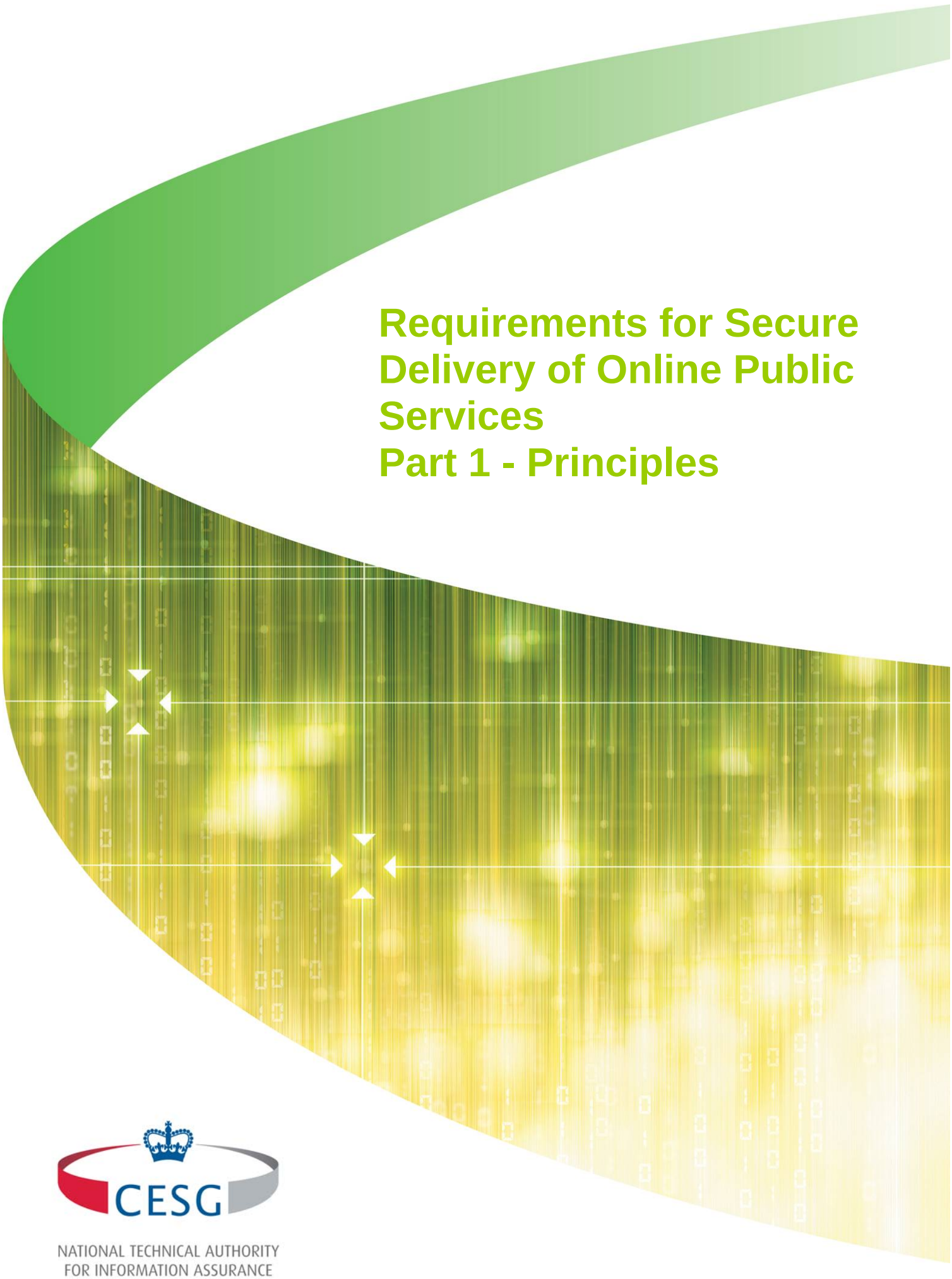
July 2010
Issue No: 1.0

Requirements for Secure Delivery of Online Public Services
Part 1 - Principles



CESG

NATIONAL TECHNICAL AUTHORITY
FOR INFORMATION ASSURANCE

Requirements for Secure Delivery of Online Public Services
Part 1 - Principles

Issue No: 1.0
July 2010

Requirements for Secure Delivery of Online Public Services
Part 1 - Principles

Intended Readership

The intended readership of this document is those responsible for provision of online public services from their inception through to delivery and operation. It is of particular relevance to those responsible for service and system security including procurement and provisioning, accreditation, and security management.

It is, by intent, UNCLASSIFIED, and is intended to be available to all with a wider interest in the provision of on-line citizen facing government services.

Executive Summary

This document, Requirements for Secure Delivery of Online Public Services (RSDOPS), is a response to the challenge of delivering online public services to the citizen and sets out a proposed approach to deriving, communicating, and discussing security requirements for public services delivered online.

It is being published initially as a discussion document to foster wider public review and debate on the approach proposed with the expectation that it will replace the E-Government Security Framework (e-GSF) last updated in 2002 (Ref [a]).

By taking a transactional rather than data centric viewpoint, it presents a way of describing and reasoning about information risk that is arguably closer to the business function and the distributed service model than current approaches that focus directly on data access and protection.

The document is in 2 parts, this Part 1 (Principles) contains:

- Introductory, background, and contextual material explaining the scope and purpose of the document and related standards and legislation.
- The conceptual model and technical approach.
- An analytical approach to be followed in the production of a security case.
- Security expectations of stakeholders for incorporation into a security case.
- A summary of Security Components for incorporation into a security case.

Part 2 (Components) is presented as a separate document.

Aims and Purpose

In response to the changed technical and political environment for provision of online public services, the following design aims were set for RSDOPS:

- **Take forward the National IA Strategy (NIAS)** – NIAS (Ref [b]) objective 1 requires the information owner to understand, accept, and manage the information risk of doing business. In response, the RSDOPS approach does not mechanistically derive or mandate measures, rather it requires Information Risk Owners to work through a process for developing an understanding of the information risk, and provides a language to articulate and communicate their response. The aim is for risk owners to fully comprehend their information risk exposure, and be able to share and justify their response to it.
- **Wider Audience** – RSDOPS is, by intent, UNCLASSIFIED and is made publicly available with the aim of demonstrating to all stakeholders (including the public) that public sector attention to information risk is fair, reasoned, and proportionate and is not a disincentive to uptake of online public services.
- **Stakeholder Neutral** – RSDOPS is explicitly stakeholder neutral and responds to the reasonable expectations of all involved parties. Specifically, it pays attention to the expectations of the public in respect of their interests and information.
- **Discourage Inappropriate Risk Transfer** – RSDOPS discourages the transfer of poorly appreciated risk. Risk transfer must be informed and understood by the recipient who must be qualified and willing to accept and respond to it. Risks must be actively managed, and not ignored or dispersed through inappropriate use of process.
- **Evident Roots in the 2002 SF** – The 2002 e-GSF (Ref [a]) has been widely used as a language to describe security challenges and responses. RSDOPS must fulfil that need and support a self evident mapping from the new language to the old. However, a direct traceability statement is inappropriate and unlikely to help encourage new behaviours.

This working draft (and feedback received) will replace the e-GSF

Contents

THIS PAGE IS INTENTIONALLY LEFT BLANK

Chapter 1 - Introduction and Scope

Key Principles

- RSDOPS consists of two parts - Principles and Requirements Components (this is Principles).
- Provides guidance on determining security requirements for Government ICT systems providing online services to the citizen.
- Developed for Central Government and of relevance and applicability to wider Public Sector.
- UNCLASSIFIED and available to all.
- Promotes informed risk management decision making.

Introduction

1. Requirements for Secure Delivery of Online Public Services (RSDOPS), is a response to the challenge of delivering online public services to the citizen and sets out an approach to deriving, discussing, and agreeing security requirements for systems delivering public services electronically. It revises, repositions, and will replace e-GSF.

2. RSDOPS is divided into two Parts. This part, Part 1 Principles, describes scope, context, and a process for deriving security requirements for public sector systems and services.

3. Part 2 presents detailed descriptions of the Security Components that are used to express the security requirements. Worked examples that illustrate the application of the method will be made available in due course.

Status

4. This is a draft of the RSDOPS that is being made available for wider review and comment. RSDOPS is being made available to all who have an interest on the understanding that it is still under review does not imply a commitment to release it as a formal standard. It should not be cited as part of a contractual agreement though its use is encouraged for informal discussions.

Scope

5. This document is applicable when determining security requirements for Information and Communication Technology (ICT) systems intended to deliver government services to individuals and businesses. It is applicable to systems delivering service by, or on behalf of, central government. The requirements and guidance set out in this document are also applicable to systems delivering ICT services for, or on behalf of, Local Authorities, Health Authorities, and other public bodies.

6. Its intended audience is those responsible for provision of online public services from inception through to delivery and operation. It is of particular relevance to those responsible for service and system security including procurement and provisioning, accreditation, and security management.

7. It is, by intent, UNCLASSIFIED, and is available to all with a wider interest in the secure provision of public sector services electronically.

Purpose

8. The intent and positioning of this document differs from the 2002 e-Government Security Framework. The changes accommodate developments in National IA Strategy (NIAS) (Ref [b]) and account for the increasing volume of detailed guidance and requirements material that has been produced both centrally and locally in response to specific programme needs. This document focuses on supporting business Information Risk Owners in developing an understanding of the factors that will inform their information risk management decisions. It presents a common language to describe risk mitigation needs and choices and share these with other concerned stakeholders in order to reach consensus on information risk management.

9. The complexity and scale of future online public services suggests that formulaic approaches to deriving security requirements and risk mitigation measures are less likely to lead to helpful conclusions. This document therefore concentrates on supporting Objective 1 of the NIAS, ‘Clear and effective information risk management by organisations’ through supporting the development of better understanding within and between businesses of their information risk management drivers, opportunities and choices.

Chapter 2 - Context

Key Principle

- Will Inform Debate leading to statement of National IA Policy for online services.
- Applicable within legislative constraints.
- Used within national and international standards frameworks.

Policy

10. RSDOPS informs debate on future national IA policy, it has been developed by CESG in its role as National Technical Authority for IA and published under the direction of the IA Policy Committee. Relevant current national policy statements include the HMG Security Policy Framework (SPF) (Ref [c]) as the authoritative statement of HMG Protective Security policy, and the 2002 E-Government Security Framework.

11. RSDOPS and follow on developments are intended to serve a wider audience than the SPF, which is principally a policy statement for central government. It cannot therefore be treated as a fully integrated component of the SPF. It differs in positioning, authority, relevance, presentation, and style from the core SPF. RSDOPS is fully in line with national policy principles but extends the audience for, and content of, policy and guidance.

Legislation

12. Online public services must be delivered within the terms of the policy and legislation that applies to the handling of government, commercial, and personal information. Individual departments, non-departmental public sector bodies, local authorities, and other affiliated bodies will also possess their own corporate information handling and security policies that provide a more specific interpretation of national policy and legislative frameworks. Organisational policies are not cited explicitly here, but are presumed to express requirements for good business practice. In addition, government aims to take a lead in the setting of, and conforming to, high standards of management in its control of publicly held information assets.

13. The principal items of legislation that are of relevance to most public sector services include, but are not limited to:

    a. Data Protection Act 1998;

    b. Freedom of Information Act 2000;

    c. Human Rights Act 1998;

    d. Computer Misuse Act 1990;

External Standards

14. This document is intended to supplement and complement existing processes, standards and assurance services. Relevant external standards include:

    a. ISO/IEC 27000 family of standards covering Information Security Management Systems (ISMS);

    b. BS 25999 and ISO 24762 on Business Continuity;

    c. ISO/IEC 18044 on Incident Management;

    d. BIP 0008 that provides a code of practice for legal admissibility and evidential weight of information stored electronically;

    e. SPF (see www.cabinet-office.gov.uk/spf.aspx);

    f. HMG IA Standards (see CESG IA Policy Portfolio[1]);

    g. CESG IA Good Practice Guides (see CESG IA Policy Portfolio);

    h. Privacy Impact Assessment Handbook, Information Commissioners Office, 2009.

15. The standards and guidance listed above set the principles and direction. IA standards are a dynamic and developing area and a complete listing at time of publication is neither feasible nor desirable. Reference should be made to current standards, recommendations, and guidance in formulating security responses.

[1] This is available at www.cesg.gsi. gov.uk and through CPNI

Chapter 3 - Technical Approach

Key Principles

- Builds on the National Information Assurance Strategy.
- Focuses on informed risk taking rather than solution derivation.
- Primary emphasis is transaction assurance rather than data security.
- Emphasises balanced response to all stakeholder expectations.
- Presents logical steps to deriving a security case.

Introduction

16. In keeping with its evolutionary intent, this document builds on, but repositions, the approach adopted in the e-GSF whilst responding to external changes that have impacted on the technical approach.

Context

National Information Assurance Strategy

17. The current NIAS places much greater emphasis than its predecessor on informed information risk management by the information risk owner and hence reduces the opportunity to appeal to prescriptive standards, typically set by a central authority, that may not be well matched to the specific business environment. This moves the policy emphasis away from recommending solutions; rather it is expressed in a manner that requires information risk owners to develop an understanding of the risks to their business information, the requirements for solutions that will counter these risks, and the rationale behind the expression of those requirements.

18. This risk managed approach encourages information risk owners to develop a better understanding of the wider information risk picture, make balanced judgements that are relevant to their specific business environment, and present the evidence and rationale in support of an accreditation case. As compared to the consequences of more solution focussed policy, the current NIAS encourages the deployment of better and more feature rich solutions and services but demands greater engagement by the business, and continuing investment in developing awareness of, and responding to, challenges to security. This approach also recognises the reality that security measures will be tailored to the specific business needs and cannot necessarily be drawn directly from a catalogue of generic solutions.

Delivering Online Public Services

19. Current policy direction requires the delivery of online public services to place greater emphasis on the citizen viewpoint and experience, and stresses the sharing of service provision between departments and other bodies. Service elements will be provided by the organisation that can offer the most cost effective solutions, and service components will be re-used in the compilation of composite citizen facing services.

20. Architectural approaches to online public service provision are still being developed but the working assumption is that a distributed service model is likely to emerge. Departments are encouraged to offer service elements that best exploit their core expertise and resources. The citizen facing services will embody reusable service components accessed using a common presentation and delivery framework.

21. This document therefore presumes a distributed service model rather than the departmentally focussed client server model that underpinned the e-GSF and takes into account the expectations of a broader set of stakeholders than the more government centric perspective of the e-GSF.

Conceptual Model

22. IA policy and practice has typically focussed on the preservation of security properties of data held and operated on by the ICT. The principal information security properties have, historically, been Confidentiality (information visible only to those authorised to access it), Integrity (information modifiable only by those authorised to change it), and Availability (information always accessible when authorised).

23. This data centric approach to IA is most appropriate where the business purpose of the ICT can be treated as a data storage, preservation and processing function that maps readily onto a centralised client server system. For future service provision, the primary focus is on the transaction[2] that benefits the parties concerned and the ICT is the infrastructure over which the exchange takes place and supports the service.

[2] Ref [d], Para 7 “The specific opportunities lie in improving *transactional* services…..”

24. Future service provision implies a more balanced relationship between multiple service suppliers and service beneficiaries. The network infrastructure and end services combined become the pervasive fabric over which individuals and corporate bodies can remotely transact business that transfers value and commitment between parties and, in so doing, confers benefits and obligations on those parties. Proper attention to security will ensure that the rights and interests of the transacting parties are upheld, liabilities are clearly understood and that any damage incurred as a consequence of shortcomings of electronic service delivery will be repaired or compensated for.

25. Figure 1 below illustrates the conceptual model applicable when determining security requirements:

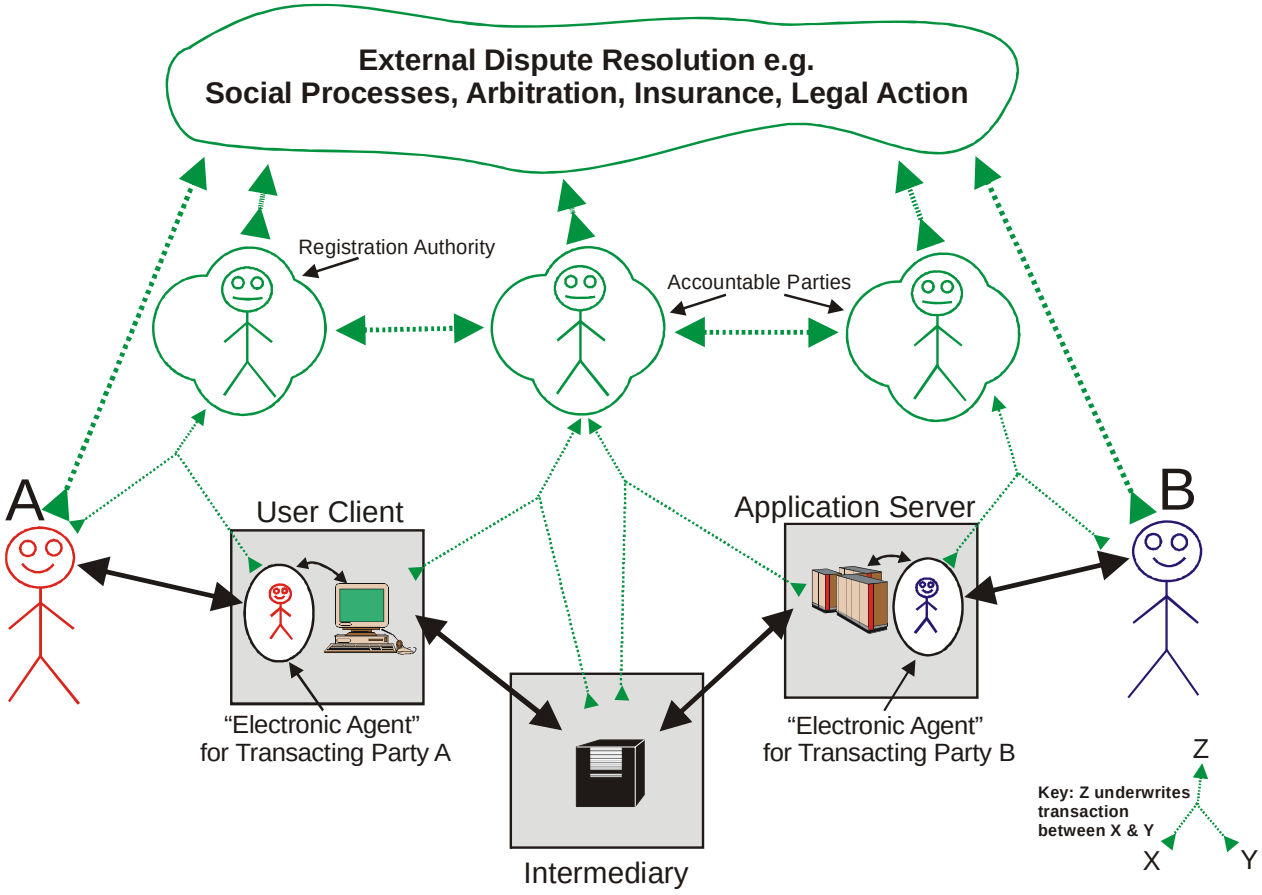


Figure 1 – Transactional Model

26. Under this model, party A (typically the individual or commercial business) transacts with party B (typically a public sector organisation or their service supplier) using the electronic infrastructure. The intended outcome is an exchange of value between the parties, where value is interpreted loosely to include property, payment, or benefit along with associated commitments and obligations, and takes place outside the ICT. The ICT facilitates the transaction (e.g. issuing a passport) but the value and obligations exist, and must be preserved, in the external environment.

27. For remote access (generally using public networks) the interaction will rely on ICT that spans multiple domains each with distinct ownership and accountabilities. As depicted in Figure 1, each party interacts with its local ICT, which creates an electronic process that serves as agent for the external parties within the electronic infrastructure. This appointed electronic agent inherits the rights of the transacting party to access and operate the services and associated resources, and assures the binding between the electronic operations and the external party. Additionally, if external parties are to be held accountable for their actions within the electronic systems, the transacting parties must be identified and their responsibilities defined to the extent that they can be held to account for their actions using external enforcement mechanisms such as legal or disciplinary measures.

28. The data held and operated on by the ICT can be treated as representing some real world object with value. Value can be equated to monetary value, but it may also reflect less tangible properties such as privacy, reputation, or health and well being. Analysis of the security requirements can then be based on the extent to which subsets of the ICT can be trusted to preserve, and correctly transact with, the information assets they hold, and the extent to which value and commitment are properly transferred between domains of accountability and, ultimately, to the transacting parties themselves.

29. Value preserving transfer of data objects between management or ownership domains requires a responsible party to underwrite the binding of the data to the value it represents and who can also act as the accountable authority for dispute resolution and route to recompense in the event of a disagreement. A responsible party exists, either explicitly or implicitly, in any transfer between independent domains, and the relationships and obligations may be explicit or implicit. In the absence of an identified responsible party, or a clear agreement, disputes may be resolved using other dispute resolution methods based on examination of evidence within some due process. Examples of such responsible party relationships include:

a. Transfer of signed objects between domains under a Public Key Infrastructure will require a Certification Authority that will attest to the authenticity (or otherwise) of the signatures under the terms of an explicit Certification Policy agreed to by both parties.

b. The binding between a real world user and the electronic system is underwritten by a registration authority that checks and attests to the identity of the individual and issues credentials that are used to subsequently authenticate that identity to the systems.

c. Transfer of payment authority and resulting payment requires a set of multi party agreements including both parties' banks, a payment service, and the parties (and their intermediaries) themselves.

d. An informal transfer (e.g. an e-mail) may imply a real world commitment without any obvious underwriters and may be enforced using external legal or other social processes that assess evidence at face value.

Process

30. The process for deriving security requirements for public service systems emphasises securing the transaction (as being directly experienced by and relevant to the parties) rather than the data (as the internal representation of the transaction). The aim is to derive a set of security requirements for the systems and services that fairly meets the expectations of the transacting parties. The proposed security response is supported by rationale that can be used to demonstrate that the security requirements demanded of systems are a reasoned and proportionate response to the threat and the expectations of the stakeholders (including customers), and that tradeoffs made are documented and explicitly accepted.

31. It is important that the initial analysis focuses on expectations and requirements rather than techniques and implementation. Security requirements will, in the first instance, be informed by stakeholder expectations and needs though it is inevitable that engineering and budgetary constraints will moderate the extent to which some stakeholder expectations can be met.

32. The technique proposed is not intended to derive the security solution directly, rather it is an approach to discussing and reasoning about the security problem and developing a shared understanding of its implications. It will help Information Risk Owners reach an understanding of the information risk implications of their business decisions and satisfy themselves that the security response is reasonable and measured, and fairly represents the concerns and expectations of the business and the customers for the service. It is not intended to substitute for the security engineering, rather it provides a foundation for the security engineering work. It will also offer a common language to communicate and negotiate security responses.

33. This approach actively discourages information risk transfer or dispersal without full knowledge, understanding, and acceptance of the implications. Public service systems will be of a scale, complexity, and fluidity that cannot be fully addressed by closed and static security solutions. Information risks must be confronted, understood, and actively managed by information risk owners within the business throughout the life of the systems.

34. This approach underpins rather than supplants standards based certification and accreditation schemes. Elements of online public service delivery will be well defined and amenable to a more static standards based approach. Where appropriate, the benefits of the standards based approach should be taken but this must not detract from the continuing need to directly manage the information risk in the context of the wider online service. Standards cited must be properly understood and shown to be relevant to the circumstances. Standards must not be used as a substitute for understanding the information risk or a pretext to transfer risk to those unqualified or unprepared to manage it.

35. The output is intended to demonstrate business understanding and appreciation of the information risk and planned responses and is not a catalogue of required security measures. The output will include:

    a. Contextual and descriptive material necessary to fully appreciate the intended service and the environment in which it will operate;

    b. Enumeration of the parties with an interest in the transaction and description of their involvement, capabilities, motivations, and responsibilities;

    c. Descriptions of the transactions to be safeguarded including key information assets;

    d. A statement of the security related expectations of parties to the transaction, derived from Chapter 4 – Stakeholder Expectations and set out in a way that can be referred to and tested against;

    e. A statement of the information risks that are relevant to the transaction including a discussion of source of threat, information assets at risk, potential harm, likelihood of damage arising, and the extent to which such damage can be sustained in the normal course of business;

    f. A target security profile calling out levels of the different components of security identifying any adjustments or refinements made;

    g. A security case that provides the rationale justifying the target security profile and which may be subject to independent scrutiny and challenge.

36. A six step process is proposed to develop these outputs.

Step 1, Identify and Describe the Security Challenge

37. Step 1 is the initial analysis that establishes the context for developing the security case. It is a narrative statement, largely descriptive, and presents the proposed service from a business perspective. Reference should be made to any existing business plans and proposals.

38. Proposed security critical transactions should be identified, accompanied by possible delivery approaches, critical information requirements, need for access to payment services, and other relevant material that affect the security requirements.

39. Any security issues and concerns that have been identified in the business case for the proposed service should be restated and amplified if necessary.

Step 2, Enumerate Participants and other concerned Parties

40. Step 2 identifies the participants and other interested parties in the principal transactions and any other parties that may be called upon to underwrite those transactions, implicitly or explicitly. The subset of those for whom determining the security requirements is relevant should be identified.

41. The aim is to build a stakeholder map identifying the parties involved in, or with an interest in, the transaction and the interactions between the principals and intermediaries.

Step 3, Enumerate Stakeholder Expectations and Engagement

42. Step 3 involves, for each significant party/stakeholder, enumerating their expectations, level of engagement, and motivations with respect to the system aims.

43. Expectations are essentially security requirements viewed from the stakeholder perspective and expressed in a way that emphasises their interests, expertise, and points of view. This will form the security agreement between the parties. If possible, stakeholders should be consulted and agreement sought as to their expectations.

44. This is where this approach diverges from more data centric approaches to deriving security requirements. The primary focus is on the real world users and their reasonable expectations rather than the data security that is indirectly, and often obscurely, related to the stakeholder concerns.

45. Stakeholder expectation tables at chapter 4 are presented as a guide and starting point and should be supplemented as required.

46. Stakeholders, in particular the target users, vary greatly in their capability to interact correctly with the system and their commitment to the aims of the offered service. Some assessment of the competence and motivations of the stakeholders and other actors is a necessary input to the risk assessment. The following categorisations can be used as a starting point for the analysis.

    a. Committed – The subject understands the aims and purpose of service, understands the rationale for measures and is trained to use the systems, aware of the pitfalls, and committed to making it work.

    b. Conscientious – The subject is motivated to make the service work, generally supportive but is untrained and unaware of dangers.

    c. Indifferent – The subject is not interested in aims, objectives, and outcomes of service, not interested in becoming an informed or competent user, and may resent being required to use service.

    d. Hostile – The subject may be actively committed to undermining the aims of the system motivated by ideology, financial gain, or personal circumstances.

Step 4, Enumerate Information Risks

47. Step 4 recasts the user expectation analysis in the form of a set of information risks to be countered. Information risks are characterised by:

    - The information asset under threat and its significance to stakeholders;
    - The potential threat sources and actors including assessment of motivation and capability;
    - The opportunity that will be exploited (where opportunity may be an unintentional vulnerability or a necessary property of the system);
    - The damage that may be experienced consequent on the risk materialising;
    - The assessed likelihood of the risk being realised;
    - Opportunities for recovery and compensation should the issue arise.

48. Whilst, this document does not contain, or reference, specific risk management guidance or process to be followed in order to enumerate and treat the risks to be managed. For those, but not all, parts of the public sector mandated by SPF to undertake risk management. Current HMG standards in this area (IS1, see Refs [e] and [f]) should be consulted but will need some interpretation to support the focus on transaction value and liability directly rather than indirectly through the Data Confidentiality, Integrity, and Availability perspective.

Step 5, Match the Risks to a Profile

49. Step 5 expresses security requirements for the service in the form of a profile of the levels of the components of security identified in this document. The aim is not to derive exact solutions and proposals, rather it is to set the ambition for security, declare the extent of the preparedness to invest in security, and provide a common vehicle for expressing, discussing and negotiating security proposals.

50. This step will require application of significant security and design skills. The description of the levels of the individual components of security contains some guidance, but there is no standardised approach that can map the risk profile and stakeholder expectations on to a cohesive set of security requirements. Businesses have diverse budgets, capabilities, motivations, and risk tolerances and must make, and be prepared to justify, their own information risk decisions.

Step 6, Develop and Validate the Security Case

51. The final step is to build a complete security case that takes the decisions and proposals from the previous steps and adds the rationale that shows how the selected profile will mitigate the risks identified and reconcile the fair expectations of the various parties.

52. This is not the final specification against which accreditation and certification will take place, nor should it be at this stage. It will declare the aspiration for security. The intent is that information risk remains a live issue throughout the system procurement and operational lifecycle. It will be part of the continuing risk management toolset and is a demonstration of understanding and commitment by the system and service owners. Online public services will be too complex and dynamic to support static security solutions, the security case must remain a live document that is used as part of the toolset for continuing security management.

THIS PAGE IS INTENTIONALLY LEFT BLANK

Chapter 4 - Stakeholder Expectations

Key Principles

- Stakeholder expectations for the system and services provided are the primary driver.
- Expectations, concerns and risks demand consideration whether well founded or not.
- All significant stakeholders views should be considered.
- Expectations inform system security requirements and measures.

Stakeholder Expectations

53. Security requirements are derived from the reasonable expectations of all significant stakeholders in respect of transaction security. The notion of transaction security is broader than (though closely related to) protective security of data held and processed by the systems. Analysis of security requirements for public systems should start with determining and agreeing the reasonable expectations of the interested parties in respect of security of their transactions.

54. The tables in this Chapter are a framework for setting out the expectations and provide pointers to the related threats and security requirements. These tables are designed to help demonstrate that the reasonable expectations of all those involved in a public service delivery are adequately addressed. It is essential that the citizen and business expectations as well as government requirements are addressed. The expectations are described by the columns:

    a. **Expectation** – Describes an expectation for security related behaviours viewed from that perspective. There is an assumption of reasonableness, but not that the viewpoint is of someone who understands information security. This policy is predicated on the assumption that these are reasonable expectations, and the systems must meet them or explain the shortfalls and how they might be addressed elsewhere. For example, it is a reasonable expectation that the systems will safeguard user information but it may not be a reasonable expectation that there will never be any system compromises. However, it is a reasonable expectation that, in the event of compromise, recovery action is possible, and that users will be recompensed for any harm experienced.

b. **Concern** – is the underlying belief, worry or unease that informs the expectation. Concerns may be valid, unjustified, or overstated, but they remain concerns that must be addressed. Concerns may be based on perceptions of risk and possible harm or they may reflect wider concerns about privacy and other softer issues.

c. **Risks** – identifies relevant information risks that will need to be managed. These are risks that relate to actions of external threat agents and other events over which the project has no influence.

Stakeholder Expectation Descriptions

55. The tables in this section offer a framework for setting out reasonable stakeholder expectations for the systems and services. These expectations are not intended to be prescriptive and should be referred to when developing the system security policies and responses.

56. Whilst not intended to be exhaustive, an initial analysis would respond to the expectations explaining how they are either:

a. Addressed, that is the expectation is fair and reasonable, and that the system has addressed this concern in its design.

b. Partially addressed, that is the expectation is fair and reasonable but cannot be fully addressed within the constraints of the proposed service. The security case should make it clear where the shortfalls are, and whether the risk is accepted or dealt with external to the system.

c. Not addressed, that is that the concern is reasonable but cannot be addressed directly by the system. The security case should show how such concerns are out of scope or addressed outside of the system, or make an explicit statement that such concerns are not addressed, and demonstrate that the implied transfer of risk is identified (i.e. risk from whom to whom) and reasonable, or underwritten in some way acceptable to the stakeholder.

d. Discounted, that is that the concern is not relevant or reasonable in the context of the proposed system or service, or that the associated risks are small enough to be accepted.

User Viewpoint

57. The user (general public, individual user, or business user) viewpoint mainly expresses concerns that their interests and information will not be safeguarded, failures and shortcomings will not be underwritten and, in the event of dispute or malfunction, there will be a presumption of guilt and inadequate or unfair redress processes.

Expectation	Concern	Risks
Privacy – Online public services will not unnecessarily compromise the privacy of actual or potential users, or the general public, in respect of their personal, financial, or business information.	Government will collect information for which it has no business need, and no rights of access. Government will accumulate information that leaves the user open to identity theft, fraud, invasion of privacy, or other personal distress. Personal information will be shared without explicit permission and will be collated with other sources of information in order to draw inferences about the subject that may be counter to their interests. Government will not look after personal information responsibly or will use it for purposes that were not agreed to.	Deliberate or accidental breaches of confidentiality by third parties will compromise the customer's privacy. Function creep and gradual accumulation of stored personal information presents new (and unmediated) opportunities for invasion of privacy. Analysis of large collected datasets may expose inferences about subjects that violate their reasonable expectations of privacy. Electronically delivered services will not be taken up by the public owing to their concerns about privacy.
Authenticity – Users can be assured that they are interacting with a genuine public service.	Users can be deceived by a plausible false presentation of a online public service and thereby reveal Personal Private Information (PPI) to a potential fraudster ('Phishing').	Personal and private information will be lost to a fraudulent operator with possible personal and financial consequences. The integrity and reputation of public sector services will be undermined.
Confidentiality – sensitive information will only be accessible to those with a legitimate need, and used for a legitimate purpose.	Sensitive information held by the government may be compromised through exposure (deliberate or otherwise) to those who have no need to see it, or may be intent on causing harm. Online public services present opportunities for 'ID Theft'.	Adversaries may exploit vulnerabilities to gain access to information without authority. Information may be accidentally or deliberately exposed to potential adversaries.

Expectation	Concern	Risks
Integrity – stored personal information will not be corrupted or changed incorrectly. It will be protected in a manner that reflects its intrinsic value to the individual.	Information held by the public sector could become corrupted or destroyed with undesirable or serious consequences. Information held by the public sector could become out of date or be inaccurate.	Adversaries may deliberately alter sensitive personal information and thereby disadvantage or damage the information subject. Information may be accidentally corrupted leading to damage or disadvantage to the information subject. Users may be unjustifiably accused of damaging or fraudulent activities. Circumstances of a user may change leading to information held becoming inaccurate.
Availability – critical services will always be available when they are needed.	Urgent service needs will not be met. Alternate service delivery opportunities will be withdrawn in favour of e-delivery without adequate accessibility, reliability and coverage. Time critical response demands, which may incur a penalty, cannot be supported by the e-systems	Users may be disadvantaged or damaged as a consequence of inability to access public sector services when needed owing to intentional acts by adversaries or accidental misuse of security functions by users.
Transparency – personal information is held by/supplied to the public sector for its agreed purpose only.	Once the public sector has possession of information, it will use it for purposes that were not declared when the information was supplied or as agreed subsequently.	Users will be harmed or perceive privacy violations through use of their information for a purpose they were not aware of, had not agreed to, or did not understand.
Identity – systems will confirm the identity of those with access to information before enacting a transaction. The strength of the identity measures will be appropriate to the value of the information, and the need for confirming true identity (as opposed to authority) when completing the transaction. Identity compromise by the public service will be admitted and repair properly supported.	Systems will have weak controls which will lay individuals open to identity fraud and malpractice. Identity controls will be applied insensitively, full identity will always have to be proved where it is not strictly necessary. Interactions will be unnecessarily intrusive leading to privacy concerns. Public authorities will offer poor support for identity repair following compromise and leave responsibility with the customer.	Adversaries will be able to impersonate legitimate users and cause damage through abusing their access rights. User privacy will be compromised through demanding full identity when not necessary for the business in hand. Users will continue to suffer the consequences of identity compromise and will not be supported in identity repair or compensated.
Reliance – it is safe to act upon the displayed service outcomes.	The online public sector services may not display the true situation, e.g. monies showing as transferred may not be accessible, or information may be misleading leading to later penalty.	Users will be harmed as a consequence of taking action on incorrect or inconsistent system information or instructions.

Expectation	Concern	Risks
Payment Safety – monetary transfers are correctly carried out between the correct parties and do not lay individual financial details open to exploitation.	Bank account details will be misused or not properly controlled leading to financial exposure. Erroneous transactions cannot be challenged or reversed.	Adversaries can exploit vulnerabilities in the systems to commit fraud. Fear over financial exposure and fraud will deter users from using the systems.
Accountability and Fairness – False accusations of fraud or unwarranted impositions of penalties will not be made and cannot be upheld. Any dispute will be easily and fairly resolved.	The liability model will not be fair to the individual, there will be a presumption of guilt in the event of a dispute and no evidence against which a case can be made and redress sought.	Fear over lack of transparency and fairness will deter users from using the systems. Users are unable to query transactions and resolve inconsistencies to their and the system owners' satisfaction.
Inclusivity – The advent of electronic access to public sector services will not disadvantage those with particular personal circumstances or disabilities.	Public sector service access will be more difficult and discriminatory and alternate access routes will be withdrawn	Users may be denied service through inability or incapability to access the electronic systems. Adversaries may harm users through exploitation of weaknesses in the fall back arrangements for the electronic systems.
None Discoverability – search or query access to systems and data will not be accessible to unauthorised individual or used for unauthorised purposes.	Unauthorised parties, or subverted authorised parties will gain search or unconstrained query access to large or complete datasets and thereby be able to discover or draw inferences about vulnerable subjects.	Query access to large datasets will be misused in order to locate individuals, or identify at risk individuals (e.g. witness protection) at an impact level in excess of the individual records.

Service Owner Viewpoint

58. The service owner viewpoint reflects the concerns of those charged with delivering business improvements and efficiencies through increased use of ICT, and reflects major concerns that the security measures will be intrusive or unaffordable, and that security failures in large business systems will lead to departmental sanction and failure.

Expectation	Concern	Risks
Compliance – systems are able to comply with an acceptable interpretation of relevant legislation and policies in regard of protecting official and personal information and managing information risk.	Compliance responsibilities are unclear and not closely related to the practical value and impact of security controls. Meeting the compliance requirements is infeasible or expensive and time consuming, and inhibits business delivery. Individuals may be held accountable for circumstances outside their control.	Information management controls will be held to be deficient through lack of clarity on roles, requirements, and responsibilities. Lack of clarity of roles and accountabilities will lead to an overly cautious interpretation of compliance requirements resulting in higher costs and/or unnecessary service limitations.
Available Measures – Suitable security measures are available on the market and widely accepted as reasonable, proportionate, and meeting the national and citizen interests.	The available policies, products, and knowledge, do not allow solutions to be built. Impractical and inappropriate solutions will be adopted to achieve administrative compliance.	Information risks will be improperly managed through inability to source the necessary measures. Legalistic focus on compliance will result in the acquisition of inappropriate or ineffective measures.
Affordability – Security processes and measures will not place an unsustainable cost burden on departments.	Affordable products and services do not exist, and development costs of new capability are high. Assurance requirements push costs up. A sustainable COTS market will not exist.	Information risks will be improperly managed through inability to afford the necessary measures or the acquisition of inappropriate measures.
Business Impact – Security measures do not impact the business to the extent that the desired business outcome is unachievable or unaffordable.	Policies and compliance regimes lead to unacceptable business impact. Regulatory and policy restrictions preclude the use of apparently suitable solutions.	Responding to IA regimes and processes will impact on the viability of the service offering. Proposed service is beyond the acceptable bounds of information risk.
Risk Awareness – Information risk awareness will be high and it will be possible to understand the efficacy of the risk mitigation measures and their value to the business.	There is a lot of material about managing information risk which concentrates on deriving the measures and testing their quality, but little on determining actual business harm and to what extent the measures affect it.	Untestable risk assumptions will result in the deployment of uneconomic or restrictive measures.

Expectation	Concern	Risks
Assurance – the value, utility, and quality of the installed security measures can be confirmed as suitable and VFM is clear.	It is hard for public sector security authorities to get a meaningful independent confirmation of the quality, effectiveness, and appropriateness of selected measures.	Poor appreciation of security will lead to inappropriate application of assurance schemes and processes and limit the opportunities for success.
Supply – Business services will most likely be delivered through third parties who can, and are able to, accept their part of the responsibility for information risk.	Security capability, processes and practices do not align with contracting practice for service provision. Service providers cannot accept risk transfer, or will price unrealistically.	Commercial and contractual drivers will dominate and information risks will not be properly managed.

Service Supplier Viewpoint

59. The Supplier viewpoint represents the interest and concerns of product and service suppliers who are contracted to deliver or otherwise involved in the delivery of electronic public services.

Expectation	Concern	Risks
Clarity – requirements and responsibilities for security of supplied systems and services are clear enough, and stable, to allow the commercial risk to be scoped and implemented.	Government IA policy, practices, processes and capabilities are inadequately described, opaque, and subject to change. Commercial risks in responding are unacceptably high leading to uncompetitive pricing or financial and business risk.	Misaligned expectations of service owners and suppliers with regard to security will lead to contractual difficulties.
Achievability – affordable equipment and assurance services will be available to meet contractual requirements.	It will not be possible to respond sensibly to procurements because the needs are unclear or excessive and the necessary products and services are unavailable.	Supply opportunities will be lost owing to inability to supply against (possibly unrealistic) requirements.
Positive Risk Culture – prevailing culture will be one of partnership in dealing with information risk, and not simply risk and cost transfer. Commercial risk associated with partnering with customer on information risk can be priced.	The department will seek to pass information risk to the supplier when it is not appropriate so to do.	Information risk management will suffer from lack of ownership.

Service Partner Viewpoint

60. Future electronic service provision presumes the widespread adoption of a Shared Service model to achieve the planned efficiencies. Under the Shared Service model, service components will be developed by a lead department and shared within a common infrastructure. The end user will see a composite and comprehensive service offering that draws on service components sourced from a number of different departments and suppliers.

61. Public sector organisations offering service components to be incorporated into composite end user services by others will have reasonable expectations of responsible and correct behaviour by the organisation incorporating the service component into their service offerings.

Expectation	Concern	Risks
Correct Usage – The service component aggregator will access the service component within its specified parameters at all times.	The service component aggregator will not adhere to the specified interface and thereby compromise the security and/or reliability of the service component.	Out of specification use, whether intentional or otherwise, will damage the integrity and security of the service component. Other services also dependent on that service component will be compromised.
Responsible Use – The service component aggregator will operate the service component responsibly and within its intended pattern and purpose of use.	The service component aggregator will make excessive demands on the service component and/or use the results from the service component in a way that undermines the intended purpose of the service.	Misapplication of the component may damage data security or the privacy of data subjects. The reputation of the service component owner might be undermined by the effects of irresponsible usage.

Accountable Authority Viewpoint

62. A transaction generally leads to transfer of benefit, commitment and value across accountability boundaries. Whenever that happens, and there is a possibility for the transaction to be disputed, there is a need for an accountable party to be identified as responsible for resolving the dispute. In a well regulated cross business transaction environment, this responsibility would be explicitly identified and the obligations defined. In practice, responsibilities are often not well defined in advance, and the dispute resolution processes appeal to existing constructs such as arbitration, negotiation, and resolution by legal process.

63. If citizen expectations for transparency and fairness are to be met, more attention must be paid to identifying the accountable parties in advance, and setting out their responsibilities and obligations. These parties may be formally recognised trusted third parties such as signing and certification authorities or, in the case of authentication services, the registration authorities – or they may be less formal entities such as one or both of the parties to the transaction defining dispute resolution processes to which the other subscribes.

64. Responsible parties will have reasonable expectations about system qualities and behaviours in order that they can quantify their risk exposure.

Expectation	Concern	Risks
Accountability – The systems will preserve accountability within their business logic.	Systems will not be able to furnish sufficient evidence, or good quality evidence, to permit responsibilities and liabilities to be properly assigned.	Third parties will be exposed to unknown or unscoped risk because the evidence is not available to properly determine and assign responsibilities.
Traceability – Business logic, and inter domain transfers, will maintain records that permit transactions to be audited, analysed, and potentially reversed.	Accounting and audit information will not be available, or not be trustworthy enough, to assign responsibility for system activities.	Third parties will be exposed to unknown or unscoped risk because the evidence is not available to properly determine responsibilities.
Credential Protection – systems will protect critical credentials from exposure, misuse, or corruption.	Systems will not provide sufficient protection to critical objects such as private keys and biometric templates leading to potential for deniability of user actions.	A claim of credential corruption or exposure will be used to deny accountable activities.
Security Mechanism Strength – critical security mechanisms will be strong enough for their intended purpose.	Cryptographic and other (such as biometric) mechanisms with finite strength will not be strong enough for the intended purpose.	Inherent weaknesses in protection mechanisms will allow accountable actions to be denied or users impersonated.

International Viewpoint

65. Identity and access to public sector services is not a uniquely national concern. It has a strong connection to border and immigration controls and the need to share personal information with, and trust the systems of, overseas governments and other organisations. The term International covers the UK centric viewpoint in relation to overseas systems, and the overseas viewpoint in respect of UK national systems and services.

Expectation	Concern	Risks
Interoperability – users in one jurisdiction will be able to use the service from another.	Systems and services developed within one jurisdiction will not be accessible or useable from other jurisdictions.	UK services cannot be extended to nationals overseas and other nationals (particularly EU) entitled to UK government services. Continuation of legacy systems will be expensive, discriminatory, and bypass security measures.
Legal Clarity – Users and owners of services delivered across borders will be confident about the legality of activities and the applicable law.	Users are uncertain about the legalities in relation to cross border transactions. System owners are unable to determine the legal implications of cross border access to their systems.	Users of systems will be exposed to legal action through use of public sector systems. Public services cannot be extended to nationals overseas and other nationals (particularly EU) entitled to UK government services. Continuation of legacy systems will be expensive, discriminatory, and bypass security measures.
Privacy and Safety – Citizens of any one nation (specifically the UK) will not be exposed to safety and privacy risks through the actions or inactions of other nations and national programmes.	Personal and private information will be exposed to, and may be misappropriated by, overseas governments and organisations.	Public sector systems and services present a risk to national security and safety of the population when extended to other administrations. Uptake of systems will be limited and legacy services will be continued.
Assurance and Quality – Online interactions with overseas governments and systems can be trusted to perform as specified.	Visibility of the security and quality of connected overseas systems will be limited thus reducing trust in their ability to protect national interests.	Personal and national information will be exposed and may be misused as a result of shortcomings of overseas systems.

THIS PAGE IS INTENTIONALLY LEFT BLANK

Chapter 5 - Summary of Security Components

Key Principles

- Security components are packages of security requirements that focus on a specific aspect of security.
- Security component requirements and outcomes are captured as a set of levels.
- Levels have no absolute significance in relation to components.
- Part 1 summary presents component intent and desired outcome, not content.

66. The Security Profile, which is the vehicle used to scope and agree the security response, is structured around a set of Security Components. These layered descriptions of different elements of security can be used to compose the overall description of security requirements for the public sector service. There is some overlap between the components, and there may be additional requirements not covered by the components defined. These components can be used when building a description of the required service security. The components can then be used for communication of the intentions in regard of service security and negotiating the detailed requirements.

67. The degree of attention to be given to each component of security is captured as a set of levels, where Level 0 generally represents 'no specific requirements' and the higher levels represent increasingly demanding requirements. Level 0 should generally be read as 'no specific requirements are expressed in this policy' or 'not relevant to this application', it should not be read as 'no attention is needed to this aspect'.

68. The levels are expressed as security requirements and outcomes with minimal reference to solutions. Reference to potential solutions is used to explain requirements but these need not constrain actual solutions unless necessary for other reasons such as interoperability.

69. The level numbering has no absolute significance, and different components describe different numbers of levels. The profile should select levels which are appropriate for the service and not necessarily favour the same numeric level for each component. The aim should be to build a comprehensive security case whilst avoiding over investment or excessive caution that might constrain the delivered solutions.

70. In assigning a level for a particular security component to a service, the service provider must consider the direct and indirect consequences of a failure in that particular component and interpret such terms as 'minor', 'significant, and 'substantial' in the context of that particular scenario. For example, a significant financial loss to an individual may be of little consequence to a large company.

71. Service providers must consider the assigned levels in terms of expectations of the various concerned parties, risks to the service as a whole, cost of implementation, practicality, and overall business benefit.

72. Part 2 of this guidance describes the security component set. The table below summarises the security components and their levels.

Security Component	Notes	Level 0	Level 1	Level 2	Level 3
End User Personal Registration	Personal Registration is the act of establishing the identity of an individual as a condition for issuing credentials that can be used to subsequently reaffirm that identity.	**Not required** The real identity of the individual is not relevant to the service. As a courtesy, users may be offered facilities to save preferences and other material but no personal information is solicited.	**Asserted** The user asserts an identity. This identity, which need not describe or imply a real identity, is not tested. Personal information solicited is not shared externally.	**Tested** The user asserts a real identity and provides information to enable the claimed identity to be tested. The evidence presented needs to support the real identity and can be tested independently of the immediate presence of the subject. Evidence presented might be offered in support of civil proceedings.	**Verified** The user claims a real identity and the claimed identity is subject to rigorous testing to independently verify the individual's identity and presence. The independent evidence of identity might be cited in support of criminal proceedings.
End User Corporate Registration	Corporate registration is the act of establishing the legal identity of a corporate body, the identity of the user registering the business identity and evidence that the user is an authorised representative of the organisation.	**Not required** The legal identity of the organisation is not relevant to the service. As a courtesy, users may be offered persistent storage to save preferences but no commercially sensitive information is solicited.	**Asserted** The user asserts an identity. This identity, which need not describe or imply a real corporate identity, is not tested. Any commercially sensitive information solicited is not shared externally. The user is assumed to be entitled to act on behalf of the corporate body.	**Tested** The user claims a corporate identity and provides information to enable the claimed identity to be tested. The evidence presented needs to be sufficient to confirm the legal identity of the business, the user's real identity and the user's claim to be a representative of the organisation. The requirement for traceable linkage to identity is not strong enough to warrant rigorous independent human review and testing of the evidence but it might be cited in support of civil proceedings.	

Security Component	Notes	Level 0	Level 1	Level 2	Level 3
End User Authorisation	Authorisation is the act of confirming that a registered user is entitled to access a service prior to permitting access.	**Implicit** There is no additional requirement to confirm that a user is entitled in order to grant the user authority to access the service. Additional courtesy registration may be offered and additional credentials issued.	**Tested** The user claims entitlement to access the service and provides evidence to enable their claim to be tested. Testing is within the 'balance of probabilities'. Additional service specific registration and credentials may be needed.		
End User Authentication	Authentication is the act of giving authorised users access to a service.	**Not required** No additional authentication actions are required to access the service. Implicit Authority by virtue of the access path may be inferred.	**Minimal** The user is required to demonstrate possession of an authentication credential that is issued or recognised by the service. An authentication secret may be directly quoted during authentication.	**Robust** The user is required to demonstrate possession of the authentication credential that is issued or recognised by the service. Robust measures are required to protect the credential during use. At this level, there is a presumption that the authorised user is generally cooperative and well intentioned and the primary threat is external. Evidence of user actions may be offered in support of civil proceedings.	**Accountable** The user is required to demonstrate possession and ownership of the authentication credential. The measures must be such that uncooperative or malicious authorised users can be held to account for their activities. Evidence of user actions and presumed identity may be offered in support of criminal actions against the authorised identity.

Security Component	Notes	Level 0	Level 1	Level 2	Level 3
End User Privacy	Privacy is a requirement for socially responsible handing of personal information by the system. Citizens or businesses have a reasonable expectation that measures are in place to ensure that information collected by a service is the minimum necessary to fulfil its purpose, is used only for the purposes for which it was collected, and is disposed of in a secure manner when no longer required.	**No Statement** Private or privacy relevant information is not collected by the system.	**Implicit** No stated requirement beyond the implicit requirement for protection of private information. At this level, only information directly solicited from the user will be processed, and will be visible to them.	**Explicit** The system, of necessity, collects and collates personal or sensitive information that could be directly linked to an individual or corporate body. Misuse of such information could be perceived as, or may actually be, detrimental to the well being of users.	**Protected** Bulk personal data and/or sensitive information is, of necessity, collected and collated. Misuse of the collected information would present a danger to the information subjects. Bulk compromise would present a threat to the safety of the wider community.
Server Information Access	The means by which assurance is gained that information can only be accessed by those who are authorised while it is received, stored, processed or otherwise disposed of within the service environment.	**Limited** In general, none of the information handled is sensitive and is not subject to any formal access control policy.	**Self Assessed Commercial** The information stored has some access limitations but no formal protective markings and the impact of disclosure is minimal.	**Assessed Commercial** The information stored has access control requirements but generally attracts no protective marking, or a subset is no higher than PROTECT. Impact of disclosure is largely reputational with limited potential for individual harm. Bulk data loss or damage could have significant implications.	**Assessed Government** The information stored has significant access control requirements that generally equate to PROTECT, Personally Identifiable Information, or RESTRICTED for subsets, aggregated or bulk data. Impact of unwarranted disclosure or damage is significant with scope for individual harm. Bulk or aggregated data compromise would have significant reputational and business impact.

Security Component	Notes	Level 0	Level 1	Level 2	Level 3
Server Information Availability	The means by which assurance is obtained that access to information and resources cannot be withheld in an unauthorised manner. This document does not address reliability in general; its specific focus is denial of access to resources as a result of malicious activity and the susceptibility of systems and services to such threats.	**Limited** No explicit requirements for availability over and above reasonable expectations of continuing service delivery.	**Commercial** Unavailability of service or information is an inconvenience to users but unlikely to cause harm. Extended down time risks reputational damage to the service provider.	**Critical** Unavailability of the service or associated information might cause harm to the individual user. Extended down time for the service as a whole risks serious reputational damage to the service provider and might lead to action for compensation for harm caused.	
Network Communications Security	Means by which assurance is gained that observation or interference with information cannot occur in transit to, from, and between components of services. Typically relates to the requirement for encryption of communications links.	**No specific measures** Limited requirements for communications security, typically because the information is non sensitive or network provider measures are adequate.	**Limited** Threat analysis leads to a requirement for explicit protective measures and demonstration that the threat has been addressed.	**Significant** Threat analysis suggests a need for strong measures to counter the threats to the system. The threat actor capability is however not sufficiently great to warrant the use of HMG specific encryption.	**Substantial** Threat analysis suggests a need for strong measures to counter well resourced and competent adversaries. The response may require government specific capabilities and assurance.
Network Authentication	The means by which assurance is obtained as to the authenticity of machines involved in inter-domain connections and data exchange.	**Limited** Low threat or limited opportunity for attack. In general, reliance on physical connectivity or network identifiers is sufficient**.**	**Active** Moderate threat and opportunity for attack for which standard commodity mitigating measures, when correctly configured, are a reasonable response.		

Security Component	Notes	Level 0	Level 1	Level 2	Level 3
Network Network protection	The means to assure that the service is protected from an adversary with network visibility and access.	**Limited** Service assessed as unlikely to be of heightened interest to attackers. No special measures beyond requirement for duty of care in the application of commonly accepted custom and practice.	**Baseline** Threat of network attack assessed as low for government systems but still likely to attract interest as a government system per se.	**Enhanced** An independent assessment made of the threat and vulnerabilities indicates potential heightened interest to attack community.	**Significant** An independent assessment by informed government assessors is carried out. Privileged sources used to inform the threat assessment which indicate significant interest to well resourced attackers.
Network Situational awareness	The practice of obtaining and maintaining awareness of the vulnerabilities of a service, incidence of attacks, and responding in a timely, coordinated and prioritised way to maintain service availability.	**Limited** Service assessed as unlikely to be of heightened interest to attackers. No special measures beyond requirement for duty of care in the application of commonly accepted custom and practice.	**Aware** Service assessed of being of interest to a class of adversaries but no specific threat identified.	**Active awareness and response** Service assessed as being of specific interest to identified capable adversaries.	**Informed awareness and coordinated response** Service assessed as being of interest to specific highly capable adversaries with evidence of ongoing activity against the service or its peers.
Business logic Internal accountability	Measures taken to establish the traceability and accountability of significant transaction steps and information assets managed.	**Limited** There are no specific internal accountability requirements other than those required to meet commercial and legal requirements for financial accounting and asset management.	**Auditable** A basic level of accountability for transactions is required but legal case against infringements would need additional evidence.	**Accountable** There is a strong requirement to be able to hold those involved in a transaction accountable, possibly with legal action to seek redress.	

Security Component	Notes	Level 0	Level 1	Level 2	Level 3
Business Logic External accountability	Measures taken to establish the accountable authority for, and provenance of, transfers of data to and from external sources.	**Limited** There are no specific external accountability requirements, information received or transmitted will be taken at face value without special mechanisms to support traceability.	**Auditable** Basic assurance as to the identity of the originator and receiver (if relevant) of the transaction is supported. Use of commercial and widely deployed measures is appropriate. Evidence of receipt of a transaction is provided by the service to the client.	**Accountable** Evidence of receipt of a transaction is provided by the service to the client. When a transaction spans multiple management domains, there is a strong defensible persistent binding between the transaction and the originator and recipient.	
Assurance Technical assurance	Covers the review of the service to ensure that it is designed, implemented, configured, maintained and operated in accordance with the security requirements and can be trusted to uphold the interests of the transacting parties.	**No statement**	**Independent assessment** Assurance obtained through independent assessment	**Government approved assessment** As Level 1 but assurance is obtained using a CESG approved method by a CESG approved supplier (e.g. CTAS)	
Assurance Organisational assurance	Covers the review of the organisations involved in the delivery of a service to ensure that the required management, procedural, personnel and physical arrangements are in place to secure the service.	**No statement**	**Independent assessment** Independent assurance required that those involved in the provision of the service and the locations from which they provide the service have appropriate (commercial best practice) organisational, personnel and physical controls in place.	**Government approved assessment** Independent assurance is required that those involved in the provision of the service and the locations from which they provide the service have appropriate (government best practice, see IA Maturity Model (IAMM) organisational, personnel and physical controls in place.	

References

[a] E-Government Security Framework, Cabinet Office, 2002.

[b] A National Information Assurance Strategy, Cabinet Office, June 2007.

[c] HMG Security Policy Framework, Tiers 1 – 3 (Not Protectively Marked). Available at: http://www.cabinetoffice.gov.uk.

[d] Transformational Government Enabled by Technology, Cabinet Office 2005.

[e] HMG Information Assurance Standard No. 1, Part 1, Technical Risk Assessment, issue 3.5, October 2009 (Not Protectively Marked). Available from the CESG IA Policy Portfolio.

[f] HMG Information Assurance Standard No. 1, Part 2, Technical Risk Treatment, issue 3.5, October 2009 (Not Protectively Marked). Available from the CESG IA Policy Portfolio.

[g] Manual of Protective Security, Cabinet Office, 2007.

Glossary

e-GSF	E-Government Security Framework
GCHQ	Government Communications Headquarters
IA	Information Assurance
IAMM	IA Maturity Model
IARTG	Information Assurance Requirements for Transformational Government
ICT	Information and Communications Technology
MPS	Manual of Protective Security
NIAS	National Information Assurance Strategy
PPI	Personal & Private Information
SPF	Security Policy Framework, replaces MPS

Customer Feedback

CESG Information Assurance Guidance and Standards welcomes feedback and encourage readers to inform CESG of their experiences, good or bad in this document. We would especially like to know about any inconsistencies and ambiguities. Please use this page to send your comments to:

Customer Support
CESG
A2j
Hubble Road
Cheltenham GL51 0EX
(for the attention of IA Policy Development Team)

Fax: (01242) 709193 (for UNCLASSIFIED FAXES ONLY)
Email: enquiries@cesg.gsi.gov.uk

For additional hard copies of this document and general queries please contact CESG enquiries at the address above

PLEASE PRINT

Your Name:

Department/Company Name and Address:

Phone number:
Email address:

Comments:

THIS PAGE IS INTENTIONALLY LEFT BLANK

IA
CESG
B2h
Hubble Road
Cheltenham
Gloucestershire
GL51 0EX

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