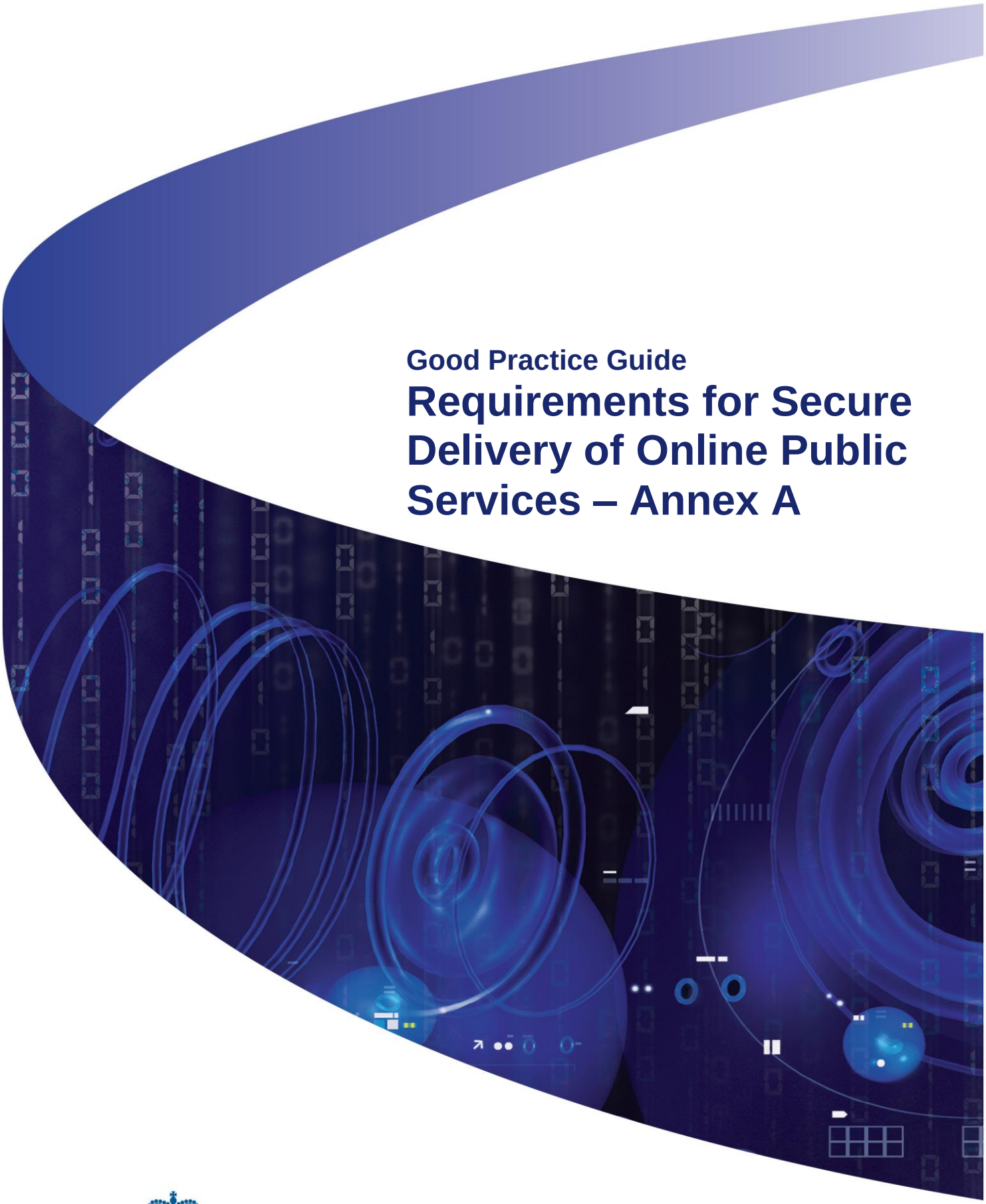
December 2012
Issue No: 1.1

Good Practice Guide

Requirements for Secure Delivery of Online Public Services – Annex A



CESG

NATIONAL TECHNICAL AUTHORITY
FOR INFORMATION ASSURANCE

CabinetOffice

Good Practice Guide No. 43 – Annex A

Requirements for Secure Delivery of Online Public Services

Stakeholder Expectations

Issue No: 1.1
December 2012

This document is issued by CESG, the UK's National Technical Authority on Information Assurance. It is provided "as is" as an example of how specific requirements could be met, but it is not intended to be exhaustive, does not act as endorsement of any particular product or technology and is not tailored to individual needs. It is not a replacement for independent, specialist advice. Users should ensure that they take the appropriate technical and legal advice in using this document (and others accessed from the GCHQ/CESG website).

This document is provided without any endorsement and without any warranty of any kind whether express or implied. It is provided without any representation as to the accuracy, completeness, integrity, consent, quality or fitness for purpose of all or any part of it. CESG cannot accept any liability whatsoever for any loss or damage suffered or costs incurred by any person as a result of, or arising from, either the disclosure of this document to you, or your subsequent use of this document.

Document History

Version	Date	Comment
1.0	April 2012	First issue
1.1	December 2012	Produced for IDAP review. Minor presentational changes

Requirements for Secure Delivery of Online Public Services – Annex A

Intended Readership

This Annex is aimed at IA practitioners, project managers, system and business architects who are responsible for defining and delivering system, service and information risk management requirements to meet stakeholder expectations.

Aim

This Annex provides additional information to assist in determining and capturing various stakeholder expectations, concerns and risks. These can be used in support of a Requirements for Secure Delivery of Online Public Services (RSDOPS) assessment.

This Annex supports CESG Good Practice Guide No. 43 (GPG 43), Requirements for Secure Delivery of Online Public Services (reference [a]).

Changes from Previous Issue

No significant changes made.

THIS PAGE IS INTENTIONALLY LEFT BLANK

Contents

THIS PAGE IS INTENTIONALLY LEFT BLANK

Chapter 1 - Introduction

Key Principles

- Introduces a framework for analysis of stakeholder expectations, concerns and associated risks
- Supports the development of a rationale for system and security requirement choices

Introduction

1. This document provides supplementary guidance in the area of stakeholder expectations in support of GPG 43 (reference [a]).

2. A framework is introduced that allows the stakeholders identified during a RSDOPS assessment to be assigned to one of the defined stakeholder viewpoints group.

Stakeholder Expectations

3. The tables in Chapter 2 provide an example framework for consideration of stakeholder expectations, concerns and associated risks. These tables are designed to help demonstrate that the reasonable expectations of all those involved in a public service delivery have been appropriately captured. These can then be assessed and appropriately addressed. It is essential that user and business expectations, as well as Government requirements, are taken into account. The expectations are described by the columns:

    - **Expectation** – Describes an expectation for security related behaviours viewed from the stakeholder perspective. There is an assumption of reasonableness, but not that the viewpoint is of someone who understands information security. This is based on the assumption that these are reasonable expectations, and the systems and services 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
    - **Concern** – Is the underlying belief, worry or unease that informs the expectation. Concerns may be valid, unjustified, or overstated, but they remain concerns that should be considered. Concerns may be based on perceptions of risk and possible harm or they may reflect wider concerns about privacy and other softer issues

- **Risks** – Identifies relevant information risks that could lead to stakeholder concerns being realised. These risks can then be used to inform and be taken into account in Step 4 where there is a need to conduct further risk assessment activity.

Stakeholder Expectation Descriptions

4. Stakeholder expectations are not intended to be prescriptive and should be referred to when developing the rationale for system and security requirement choices. For example, these stakeholder expectations should be referred to when defining the rationale for security profile choices when developing the security case in Step 6.

5. 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 the concern is reasonable but cannot be addressed directly by the system. The security case should show how such concerns are out of scope, addressed outside of the system, or make an explicit statement that such concerns are not addressed.

   d. Discounted, that is 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.

Viewpoint and Consideration Groups

6. The following stakeholder viewpoint and consideration groups are covered in Chapter 2:

   a. User;

   b. Service Owner;

   c. Service Supplier;

   d. Service Partner;

   e. Accountable Authority;

   f. International Considerations.

Chapter 2 - Stakeholder Expectations

Key Principle

- Provides example stakeholder groups and illustrates potential stakeholder expectations, concerns and associated risks

Introduction

7. The following sections are intended to provide examples of each stakeholder group viewpoint or consideration. A short explanation of the group is provided along with a table providing examples of various expectations, concerns and risks.

8. The stakeholder groups and their expectations documented in this Chapter should not be considered as fully exhaustive and businesses should consider their own stakeholder groups appropriately.

User Viewpoint

9. The user (general public, individual user, or business user) mainly expresses concerns over the fact 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 on the part of the user, as well as inadequate or unfair processes for redress.

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.	The public sector will collect information for which it has no business need, and no rights of access. The public sector 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. The public sector 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 could be deceived by a plausible false presentation of an 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 ensuing 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 public sector may be compromised through exposure (deliberate or otherwise) to those who have no need to see it, or to those who 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. The 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. Alternative 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 their 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 is in 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 will 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 and will not be compensated.

Expectation	Concern	Risks
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.
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.
Non Discoverability – search or query access to systems and data will not be accessible to an 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 will 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

10. The service owner viewpoint reflects the concerns of those charged with delivering business improvements and efficiencies through an increased use of ICT, and may outline any major concerns around the security measures as to whether they are deemed to be intrusive or unaffordable. Security failures in large business systems may lead to departmental sanction and closure.

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 unfeasible 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 user 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 an inability to carry out 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 Commercial Off The Shelf (COTS) market will not exist.	Information risks will be improperly managed through an inability to afford the necessary measures or through the acquisition of inappropriate measures.
Business Impact – Security measures do not impact upon 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. The proposed service is beyond the acceptable bounds of information risk.

Expectation	Concern	Risks
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.
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 will 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

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

Expectation	Concern	Risks
Clarity – requirements and responsibilities for the security of supplied systems and services are clear enough, and stable enough to allow the commercial risk to be scoped and implemented.	The public sector 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 an inability to supply against (possibly unrealistic) requirements.
Positive Risk Culture – The 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 the customer on information risk can be priced.	The department will seek to pass information risk to the supplier when it is not appropriate to do so.	Information risk management will suffer from a lack of ownership.

Service Partner Viewpoint

12. The provision of electronic services in the future will likely see 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.

13. Public sector organisations offering service components to be incorporated into composite end user services will reasonably expect the organisation incorporating the service component into their service offerings to behave responsibly.

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

14. A transaction generally leads to transfer of benefit, commitment and value across accountability boundaries. If it is possible for the transaction to be disputed, an accountable party should be identified as owning the responsibility 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.

15. If user expectations for transparency and fairness are to be met, sufficient attention should 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.

16. Responsible parties have reasonable expectations concerning system qualities and behaviours so as to 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 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 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 Consideration

17. 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.

Expectation	Concern	Risks
Interoperability – users in one jurisdiction will be able to use the service from another jurisdiction.	Systems and services developed within one jurisdiction will not be accessible or usable from other jurisdictions.	UK services cannot be extended to nationals overseas and other nationals (particularly EU) entitled to UK public sector services. Continuation of legacy systems will be expensive, discriminatory, and will 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 public sector services. Continuation of legacy systems will be expensive, discriminatory, and will bypass security measures.
Privacy and Safety – Users 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.

References

[a] CESG Good Practice Guide 43, Requirements for Secure Delivery of Online Public Services, Issue 1.1, December 2012. Available from the CESG website.

THIS PAGE IS INTENTIONALLY LEFT BLANK

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
A2b
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
A3e
Hubble Road
Cheltenham
Gloucestershire
GL51 0EX

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