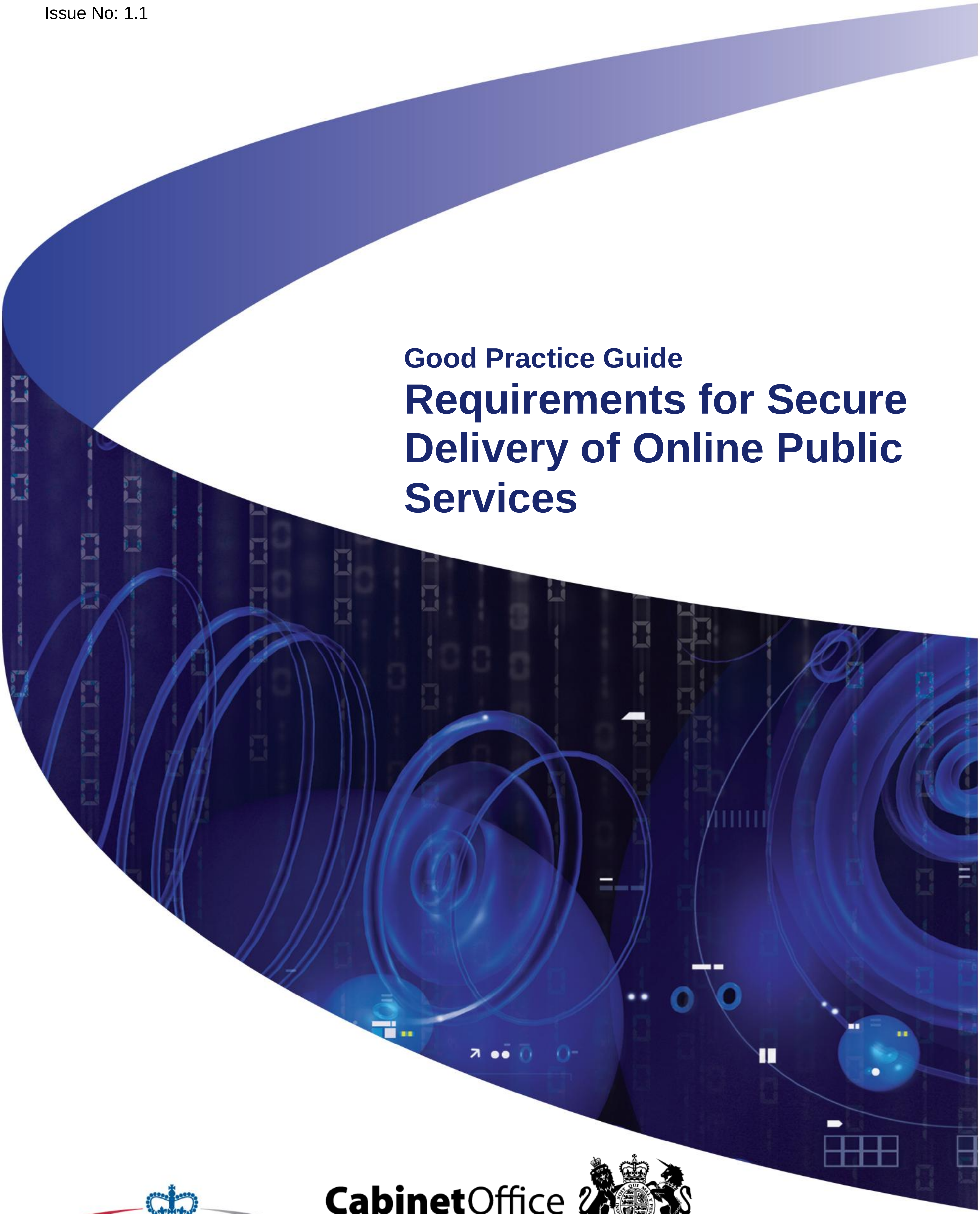
December 2012
Issue No: 1.1



Good Practice Guide

Requirements for Secure Delivery of Online Public Services

CabinetOffice

CESG

NATIONAL TECHNICAL AUTHORITY
FOR INFORMATION ASSURANCE

Good Practice Guide No. 43

Requirements for Secure Delivery of Online Public Services

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, then, 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.

The copying and use of this document for training purposes, is not permitted without the prior approval of CESG.

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

Intended Readership

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

Executive Summary

HMG service providers should understand that providing their services online will attract significant risk.

This document is a response to the challenge of delivering online public services and sets out an approach to determining the components needed to securely deliver public services online to individuals and businesses.

A transactional viewpoint is presented as a way of describing and reasoning about information risk. This approach takes account of the overall business function and its distributed service model.

A six step process is introduced that provides a systematic process to help inform the risk management of online public services.

The process takes into account the expectations of the key stakeholders and the risks to the service on the basis of the transactions that take place.

This generates a security profile that considers service delivery requirements and takes account of business goals and the organisations risk appetite.

The output is a security case that demonstrates that these aspects have been considered in a transparent way.

Changes from Previous Issue

This section documents any significant changes made from Issue 1.0 to 1.1.

- Added additional Chapters (3 & 4) covering generic threat, vulnerability, impact and risk
- Specific references to CESG IA Policy Portfolio documents removed to further comply with publication requirements
- Corporate Registration security component under review to consider completion of Level 3 (Verified)
- Organisational Assurance security component under review to consider completion of Level 1 (Self Assessment)
- Technical Assurance security component under review to consider completion of Level 1 (Self Assessment)
- Document update to reflect any general changes within review period to date (details added as completed)

THIS PAGE IS INTENTIONALLY LEFT BLANK

Contents:

THIS PAGE IS INTENTIONALLY LEFT BLANK

Chapter 1 - Introduction and Scope

Key Principles

- Aimed at those providing online public services
- Provides a means to understand what is needed to securely deliver online public services
- Takes a transactional viewpoint of services based on distributed delivery models
- Encourages an informed risk management approach whilst taking into account stakeholder expectations and concerns
- Produces a security case that transparently demonstrates that stakeholder expectations and information risk have been appropriately considered

Introduction

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

2. This Good Practice Guide (GPG) describes the scope, context, and a process for deriving security requirements for public sector systems and services.

3. Two supporting, but separate Annex are also provided, these are:

   - Annex A, Stakeholder Expectations - presents greater detail on stakeholder expectations and concerns (reference [a])
   - Annex B, Security Components – provides detailed descriptions in the form of security components that are to be used to express the system security requirements (reference [b])

Scope

4. This document is applicable when determining security requirements for Information and Communication Technology (ICT) systems that deliver public sector services to individuals and businesses.

Purpose

5. The purpose of this document is to provide HMG departments and the wider public sector with a means to understand what is needed from a security perspective to support delivery of an online public service.

6. The aim is not to derive exact solutions and proposals; rather it is to set the target for security and to declare the extent of the preparedness of the Service

Provider to invest in security. In addition this approach is intended to provide a common vehicle for expressing, discussing and negotiating security proposals with stakeholders that supports transparency in the decision making process.

7. The RSDOPS approach takes a transactional view of an online service and assumes there is a distributed service model rather than the departmentally focussed client server model that is used to deliver services today.

8. It is concerned with ensuring security of a transaction end to end and therefore takes account of not just technical security aspects but additionally the need to ensure security of the business processes and sometimes, complex stakeholder relationships that support the provision of an online service.

9. Architectural approaches to online public service provision are being developed and a number of distributed service models are starting to emerge.

10. For the purpose of this document a transaction is defined as a transfer or exchange of value between two or more parties. This transfer may take place outside of but is supported by an online system. Providers and consumers of online services need to consider the value of online transactions. This value is dependent on the nature of the service being provided and may be in the form of service related information, financial exchanges or other exchanges of value.

11. Current practice is to place greater emphasis on informed information risk management. RSDOPS is not intended to replace existing physical, business or technical risk assessment methods rather it should inform and complement their use. This approach is intended to allow appropriate risk managed choices to be made by the business.

12. This risk managed approach encourages Information Risk Owners to develop a better understanding of the wider information risk picture and make balanced judgements that are relevant to their specific business environment.

13. The intended outcome of the method sets out a target profile for security that the service should strive to achieve.

Chapter 2 - The Six Step Process

Key Principles

- Provides a means for online Service Providers to think about and analyse the security needs of their service
- Produces a security profile that sets out the security aims for the online service

Introduction

14. This document introduces a six step process that allows public Service Providers to better understand what is needed from a security perspective to support delivery of an online service.

15. The process is not intended to be a standalone assessment, rather it is intended to inform and consume other analysis and assessment conducted as part of a service delivery programme.

16. The process is intended to allow public Service Providers to think about secure delivery of their service in terms of:

    - What is the online service intended to do and what security challenges will it bring?
    - Who will be involved in delivery and consumption of the service and what expectations and concerns do they have?
    - What risks will be posed as a result of putting this service online?
    - What security profile should the service seek to achieve?

17. The six steps are not intended to enable the organisation to arrive at an immediate solution; rather they are to open a discussion on the security problem and to develop a shared understanding of its implications.

18. They will assist Information Risk Owners in reaching an understanding of the information risk implications of their business decisions and satisfy themselves that the security response is proportionate, and fairly represents the concerns and expectations of the business and the customers for the service. They are intended to provide a foundation for subsequent security engineering work. They will also offer a common language to communicate and negotiate security responses.

19. The resultant security profile is intended to be used as a statement of security intent that can be used in subsequent stages of a project to define technical and non-technical requirements.

20. A security case is developed that communicates the security profile in a way that demonstrates transparently that security has been considered fairly and proportionately to address business and stakeholder needs and expectations.

21. The output will demonstrate business understanding and appreciation of the information risk and planned responses and will not be a catalogue of required security measures. The output will include:

    a. A full description of the intended service and the environment in which it will operate;

    b. Identification of the parties with an interest in the transaction and consideration of their involvement, capabilities, motivations, and responsibilities in the context of the service;

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

    d. A statement of the security-related expectations of parties involved in the transaction, (as illustrated in Step 3) 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 source of threat, information assets at risk, potential harm, likelihood of damage arising, and the extent to which such damage could be sustained in the normal course of business;

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

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

22. The following diagram provides an overview of the six-step process and will be expanded upon throughout the remainder of this Chapter.

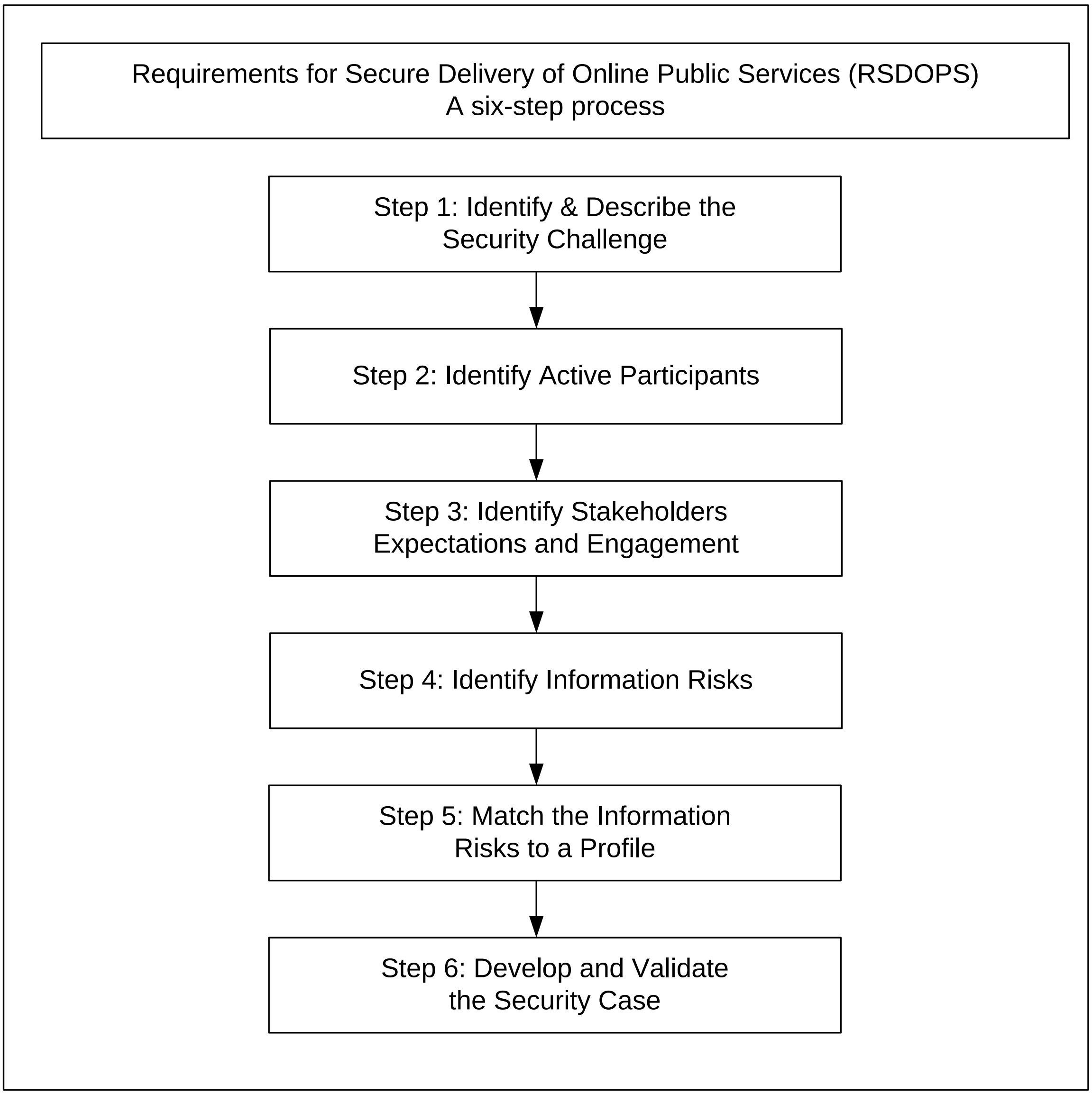

Requirements for Secure Delivery of Online Public Services (RSDOPS)
A six-step process
Step 1: Identify & Describe the Security Challenge
Step 2: Identify Active Participants
Step 3: Identify Stakeholders Expectations and Engagement
Step 4: Identify Information Risks
Step 5: Match the Information Risks to a Profile
Step 6: Develop and Validate the Security Case

Figure 1 - Diagram showing the six-step process

Step 1: Identify and Describe the Security Challenge

23. The objective of Step 1 is to provide the initial analysis that establishes the context for developing the security case.

24. The service description should consist of a narrative statement, largely descriptive to present the proposed service from a business perspective. Reference should be made to any existing business plans and proposals.

25. The following aspects should be identified and documented as part of this step:

- All assets identified and any agreed valuation (e.g. Business Impact Levels for Confidentiality, Integrity and Availability)
- All high-level business requirements for the service
- Any high-level information security requirements for the service (e.g. if facilities are provided for credit card payments then the service will need to take account of Payment Card Industry Data Security Standard (PCI DSS))
- Any need for access to 3rd party services (e.g. payment or identity assurance services)
- Any high-level use cases (and mis-use cases) or other business process models
- Any proposed security relevant transactions (e.g. financial transfers or changes to sensitive account information)
- All proposed delivery approaches (e.g. project management, development and implementation methods)
- Any other relevant material that will inform the subsequent security analysis

26. This step should clearly identify any security challenges for the project that have been identified at this early stage (e.g. balancing the need for pragmatic, appropriate and cost effective security with customer and business needs).

27. Finally, 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: Identify Active Participants (Including Stakeholders, Customers and Users) and any other Interested Parties

28. The objective of Step 2 is to identify and list the participants and other interested parties in the principal transactions and any other parties that may be called upon to support, underwrite or provide governance for those transactions, implicitly or explicitly.

29. Consider the service being offered end-to-end. The model shown in Figure 2 below, shows how a number of stakeholders and participants could be involved in providing and using a service. The relationships between these stakeholders and participants should be considered.

30. Under this model, party A (typically the individual or commercial business) transacts with party B (typically a public sector organisation or their service supplier). The intended outcome is an exchange of value between the parties. Consideration should be given to any effects posed by service failure and which stakeholder has responsibility for recovery or compensation.

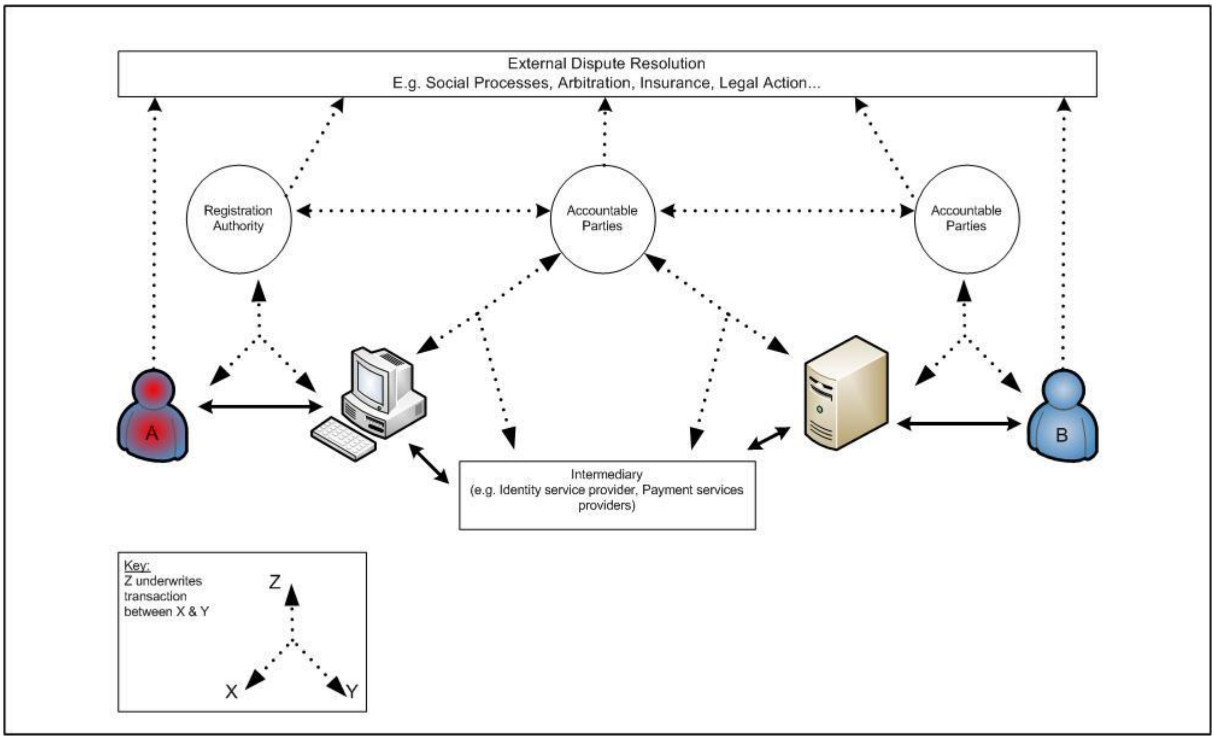

External Dispute Resolution
E.g. Social Processes, Arbitration, Insurance, Legal Action...
Registration Authority
Accountable Parties
Accountable Parties
A
B
Intermediary (e.g. Identity service provider, Payment services providers)
Key:
Z underwrites transaction between X & Y
Z
X
Y

Figure 2 – High-level Transactional model of an end to end online service including intermediaries and areas to consider

31. The following questions could help to identify potential participants, stakeholders and interested parties:

- Who will use the system?
- Who will deliver the system?
- Who will support the system?
- Who will manage the system?
- Who will regulate the system?

32. The following model provides a view of those stakeholders and participants that may be considered for an online public service. This model is indicative only and Service Providers should ensure that they clearly understand who is involved in the consumption of and delivery of their own specific service.

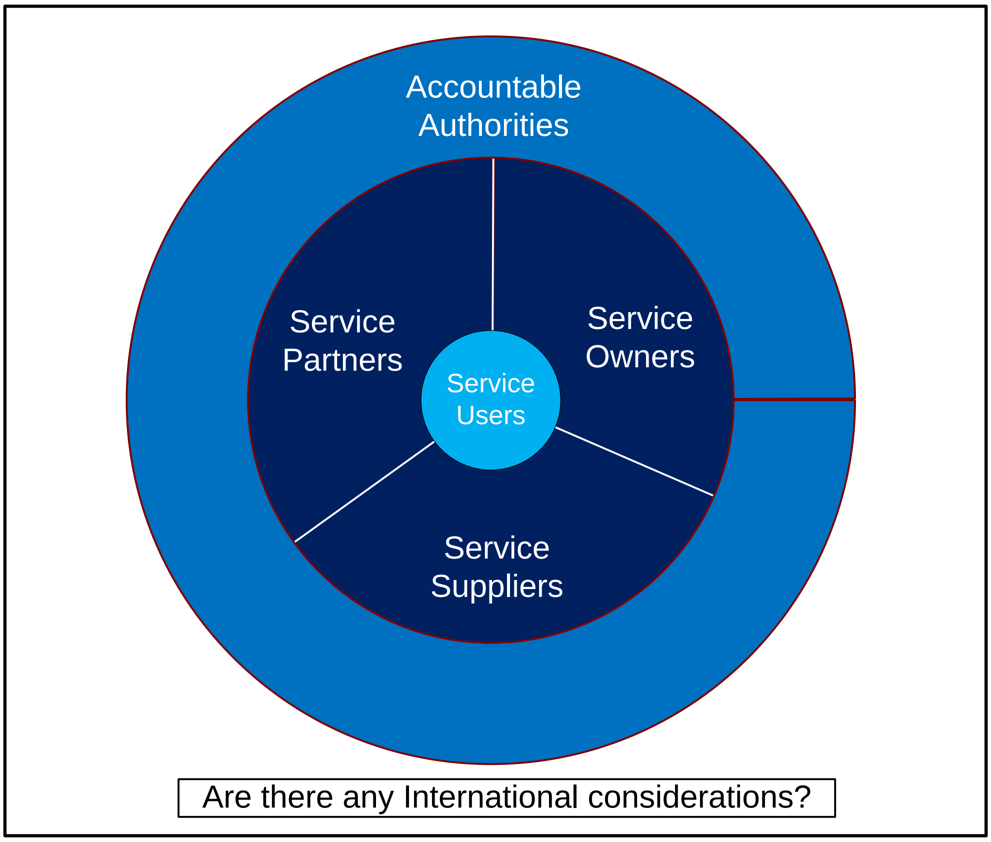


Figure 3 - Potential Stakeholders involved in the provision of an online service

33. These example groups are further defined below:

- Service Users: the general public, individual user, or business user that may use the service. It is important to note that users may be gaining access to the service from outside of the UK and therefore subject to local (non-UK) standards, regulations and legislation
- Service Owners: those charged with delivering business capabilities, improvements and efficiencies through the provision of an online public service
- Service Suppliers: product and service suppliers who are contracted to deliver or are otherwise involved in the delivery of service. It is important to note that suppliers to the service may be outside of the UK and therefore subject to local (non-UK) standards, regulations and legislation
- Service Partners: the providers of service components that are then used by others to provide their services. It is important to note that service partners may be located outside of the UK and therefore subject to local (non-UK) standards, regulations and legislation
- Accountable Authorities: those parties identified as being responsible for the overall governance of a service and owning the responsibility for resolving any disputes or issues within a defined aspect of the service. For example, if an aspect of the service fails who will be responsible for undertaking and funding remediation or for compensating stakeholders who have experienced a loss as a result of the failure

34. During this step it is important to clearly understand whether there are any international considerations that need to be taken into account.

Step 3: Identify Stakeholder Expectations and Engagement

35. The objective of Step 3 is to identify the expectations, level of engagement, and motivations with respect to the system aims for each significant party/stakeholder. Consideration should also be given to any international aspects identified.

36. 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.

37. The primary focus is on real world users and providers of an online service and their reasonable expectations. Some stakeholder expectations may be related to the design or the implementation of an online service and may not be partially or wholly addressed by security.

38. Stakeholder groups could express a large and varied number of expectations and concerns. The following list provides examples of subjects that should be considered. This list is indicative and therefore should not be considered as a reference list:

Technical

- System security
- Privacy
- Proof of transaction
- Accountability of actions
- Protection against fraud
- Integrity of information and services
- Confidentiality of information
- Availability of information & services
- Contingency
- Regulatory & legal compliance

Non-technical:

- Privacy
- Liability
- Protection against fraud

- Usability/Ease of use
- Customer engagement
- Dispute resolution
- Cost effectiveness
- Regulatory & legal compliance
- Timeliness of delivery and service

39. An explanation of stakeholder expectations, concerns and risks can be found in RSDOPS Annex A (reference [a]). Additionally, examples of stakeholder expectations and concerns are provided. These examples are categorised by stakeholder group and can be used when considering more specific expectations of stakeholder groups.

Step 4: Identify Information Risks

40. Delivering a public service online will attract significant levels of risk for public Service Providers. Risks can include those of fraud, loss of public confidence and information loss.

41. This step is intended to recast the user expectation analysis conducted in Step 3 in the form of a set of information risks that will need to be managed in order to deliver stakeholder expectations and mitigate their concerns. Information risks are usually characterised by:

    - The value and significance of the information asset under consideration to stakeholders
    - The potential threat sources and actors including assessment of motivation and capability that would either benefit from or conduct an attack
    - The opportunity to compromise an online public service that is presented to threat sources and actors as a result of vulnerabilities that exist in systems, services and processes
    - The damage that may be experienced as a consequence of a risk being realised

42. This document set does not mandate or recommend a specific risk management method, approach or process to be followed in order to identify the risks to be managed. It is recognised that in order to gain as complete as possible view of the risks to an online service it is likely that a number of different risk assessment approaches will need to be considered. The exception to this is where HMG Departments and Agencies are mandated to use the HMG Security Policy Framework (SPF) (reference [c]).

43. For example, where an online public service will make use of personal information a Privacy Impact Assessment must be carried out as mandated by the Information Commissioner Office. This will need to be taken into account to manage any privacy related risks identified.

44. It is therefore recommended that when completing this step Service Providers take a view of risk that includes:

    - Personnel Risks: These are the risks posed to the online service by the people who use and deliver the service

- Procedural Risks: These are the risks posed to the online service due to vulnerabilities in business processes and procedures that support delivery of the service
- Physical Risks: These are the risks posed to the online service due to physical locations from which services are delivered from and from where access is provided
- Technical Risks: These are the risks posed to the online service due to technical design, implementation and management of technical systems and services that deliver the online service. HMG Departments and Agencies that are mandated to use the SPF (reference [c]) **must** follow the relevant policy to assess technical risks to their services.

Step 5: Match the Information Risks to a Profile

45. The purpose of this step is to express the security requirements for the service in the form of a profile for the components of security identified in this document set. These security components are summarised in Chapter 5 with a complete description provided in Annex B (reference [b]).

46. The aim is not to derive exact solutions and proposals. It is to set the target for security that declares the extent of the organisation’s preparedness to invest in security, and to provide a common vehicle for expressing, discussing and negotiating security proposals.

47. Additionally 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 as well as to the expectations of the stakeholders (including customers), and that trade-offs made are documented and explicitly accepted.

48. There is a degree of interdependence between Security Components. For example, it may be difficult to achieve the desired level of accountability without suitably matched registration and authentication mechanisms.

49. This step will require the application of significant security and Information Assurance 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 should make, and be prepared to justify, their own information risk decisions.

50. Irrespective of what risk assessment method is used, it is reasonable to assume that there is a direct relationship between the risks that exist to a service or a transaction and what profile for security and assurance should be aspired to. The following table demonstrates this concept and provides a view of how levels of risk identified in Step 4 could be mapped to RSDOPS levels.

51. Table 1 provides an indicative mapping of risk levels to security components with levels 0–3. This mapping is provided simply to demonstrate the thinking required, that as levels of risk to a service or transaction increase then what needs to be done from a security and assurance perspective increases in proportion.

RSDOPS Levels	Level 0	Level 1	Level 2	Level 3
Levels of Risk				
High				✓
Medium			✓	
Low	✓	✓		

Table 1 - Mapping Risk Levels to RSDOPS Levels for Security components with levels 0-3

52. The risk assessment methodology chosen to support this step should ensure that threat, vulnerability and service or transaction value are considered in terms of a public service being provided online using the Internet.

53. The mapping of risk levels to RSDOPS levels is not absolute. When determining this mapping it is important to take into account the risk the security component is intended to treat along with the risk appetite, risk tolerance and business objectives of the business or the programme involved.

54. It is also important to determine thresholds for risk levels and how they relate to the RSDOPS levels for security components. These thresholds are dependent on the methodology being used, e.g. for example some methods may generate high risks where Level 3 for a security component is appropriate, whereas other methods may generate a medium level risk where Level 3 for a security component is equally as appropriate.

55. The objective is to identify a level for a security component that demonstrates that the risks identified in Step 4 for a business, service or a transaction are being managed by a security profile that is proportionate and appropriate for the business in the context of delivering online services.

56. With this understanding, of how levels of risk can be used to inform the choices made with respect to RSDOPS security component levels, then a security profile for a service or an individual transaction can be determined as shown in the example in Table 2 below. Annex B (reference [b]) provides greater detail of each security component, including examples, by individual level.

RSDOPS Components	End User Components					Server Components		Network Components				Business Logic		Assurance	
Service/Transaction Description	Personal Registration (End User)	Corporate Registration (End User)	Authentication (End User)	Authorisation (End User)	Privacy (End User)	Information Access (Server)	Information Availability (Server)	Communications Security (Network)	Network Authentication (Network)	Network Protection (Network)	Situational Awareness (Network)	Internal Accountability (Business Logic)	External Accountability (Business Logic)	Organisational Assurance (Assurance)	Technical Assurance (Assurance)
Example: Customer applies for payment to their online bank account	*3*	*N/A*	*3*	*1*	*3*	*2*	*2*	*2*	*1*	*2*	*2*	*2*	*2*	*2*	*2*

Table 2 - Example security profile for an example online transaction

Step 6: Develop and Validate the Security Case

57. The final step is to build a complete security case that captures the decisions and proposals from the previous steps. Also included is the rationale that shows how the proposed response to security will mitigate the risks identified and reconcile the fair expectations of the various parties and stakeholders.

58. This is not the final baseline against which accreditation and certification will take place, rather it sets an aspiration target for security. Information risk should remain a live issue under continuous review throughout system procurement and operation.

59. The following list provides potential subjects that could be included in the security case but this should not be considered a template. The content and complexity of the security case needs to be commensurate with the needs of the business and should be developed accordingly with the agreement of IA stakeholders from within the business (e.g. the SIRO and the Accreditor).

- Overview of the service or transaction
- Description of any security challenges identified
- Summary of stakeholders, their concerns and expectations
- Summary of risk assessment activities and key findings
- Security profile recommended and supporting rationale
- Analysis of consequences of failure of specific security component

60. The security case can then be used to communicate to the business and stakeholders alike what security is needed to successfully deliver an online service. This can be published if appropriate to provide transparency and assurance for all stakeholders with regard to security of the online service.

THIS PAGE IS INTENTIONALLY LEFT BLANK

Chapter 3 - Threats, Vulnerabilities and Impacts

Key Principles

- The threat to a HMG Online Service should be considered as anyone or any organisation that has the capability and motivation to attack a HMG online service
- When developing solutions that deliver online services care should be taken to ensure that as far as possible all vulnerabilities have been considered
- Attacks against online services can impact the service in a variety of ways. It is important to understand the impacts that would result should the service be compromised

The Threats

61. When considering the threats to a HMG Online Services, analysts should be aware that anyone or any organisation that has the capability and motivation to attack the service are highly likely to do so. Threats will seek to make use of lost, stolen, intercepted or hijacked identity information to gain unauthorised access to systems, information and services.

62. Any analysis carried out to determine the requirements for HMG Online Services should ensure that it has taken into account all potential sources of threat, e.g. from members of the public who may accidentally or deliberately seek to compromise a service through to serious and organised criminal groups who may seek to compromise the service for large scale financial gain.

63. Threat sources and threat actors should be considered in the context of the online service under consideration.

The Vulnerabilities

64. When developing solutions that deliver online services care should be taken to ensure that as far as possible all vulnerabilities have been considered. The following provides a high level view of the types of vulnerabilities that should be taken into account. This list is not exhaustive and the requirements for HMG Online Services should be continually reassessed (this may form part of a wider end-to-end service risk assessment) to ensure that it is appropriately treating existing or emerging vulnerabilities.

    a. **People** – Users and providers of an online service are vulnerable to social engineering attacks (e.g. phishing) and are vulnerable through lack of training and awareness.

    b. **Physical** – The physical storage of and handling of sensitive information used to support a service are vulnerable to a multitude of attacks including loss and theft. Users of an online service may, through lack of awareness,

leave their personal information and, or, authentication credentials vulnerable to loss or theft. The providers of online services, through weak physical protection of ICT systems and sensitive information, leave themselves vulnerable.

c. **Procedures** – Poor procedures for the use and provision of online services will leave HMG and the user vulnerable to attacks on their information.

d. **Technical** – HMG and the user are vulnerable to technical attacks on the systems used to provide online services. Vulnerabilities exist in technical systems due to poor development, design and implementation of systems and software and through failures to keep systems and applications patched and up to date. Systems should be tested for vulnerabilities prior to 'go live' and on a regular basis thereafter to ensure that security measures continue to appropriately treat existing and emerging vulnerabilities. For example:

   i. A poorly protected or un-patched endpoint will leave user systems vulnerable to keystroke loggers and other malicious attacks that could adversely affect systems and applications e.g. an un-patched browser could be vulnerable to man in the browser attacks;

   ii. Poor or weak communication security will leave communication between the user, the identity provider and the Service Provider vulnerable to interception and man in the middle attacks;

   iii. The use of weak authentication credentials will leave the user and the HMG Online System vulnerable to guessing, brute force attacks;

   iv. Weak authentication of services to the user (e.g. wrong website, misdirected or spoofed website);

   v. Fake or broken web certificates, Domain Name System (DNS) attacks etc.

Impacts

65. The impact of a compromise of a HMG Online Service on HMG and the user should be clearly understood. Public Service Providers who seek to deliver their services online should use an appropriate method to achieve this. For those mandated to do so, the relevant HMG Security Policy Framework (SPF) (reference [c]) Mandatory Requirements should be applied for assessing business impacts. For those not mandated to use the SPF, standards or guidance for assessing business impacts should be applied as specified by their business.

66. The following list provides a non-exhaustive indication of the types of significant impacts that should be considered if HMG online service is compromised:

a. **Loss of service availability:** A compromise of a HMG online service could lead to a loss of access to services for an individual or many users of the system.

b. **Loss of information integrity:** An attacker may seek to maliciously change information that is stored or consumed by a HMG online service.

c. **Individual loss of personal data:** A compromise of a HMG Online Service could lead to a loss or compromise of an individual's personal information.

d. **Individual financial loss:** A compromise of a HMG Online Service could lead to a compromise of an individual's financial information or their financial well being.

e. **Significant financial loss:** This can occur if a successful attack against one transaction no matter how complex or expensive to set up in itself, can be automated or repeated many times.

f. **Significant loss of personal data:** This can occur if an individual attack at compromising the personal data of an individual can be repeated many times, or if poor design or implementation of systems and architectures leave them vulnerable to online attacks.

g. **Reputation:** Any successful attack even if relatively insignificant in itself could result in a loss of customer confidence and the overall reputation of the service and all involved in its delivery.

THIS PAGE IS INTENTIONALLY LEFT BLANK

Chapter 4 - The Risks

Key Principles

- Providing HMG Online Services will attract significant risk for HMG Service Providers
- Service Providers should consider the risk to HMG Online Services carefully taking into account the threats to, the vulnerabilities of and the value of the transaction or service in terms of the impact a compromise would have on HMG, Service Providers and the user

Assessing the Risk

67. When considering delivering a public service, public Service Providers should determine the risks associated with delivery of an online service. Risks should be considered end-to-end to take account of all systems, services, processes and transactions involved in the provision of the online service. It is intended that this assessment of risk be used to support Step 4 of the RSDOPS method as defined in Chapter 2.

68. This understanding of risk should then be used to decide what measures need to be taken to maintain security of the online service, accountability of actions and inform the level of assurance required for all aspects of the service end-to-end.

69. For those HMG Service Providers who are mandated to do so, the relevant HMG Security Policy Framework (SPF) (reference [c]) Mandatory Requirements **must** be applied. For those not mandated to use the SPF, risk assessment standards or guidance should be applied as specified by their business to develop an understanding of the risks associated with an online public service.

THIS PAGE IS INTENTIONALLY LEFT BLANK

Chapter 5 - Summary of RSDOPS Process

Key Principle

- Provides a diagrammatic summary of the six step RSDOPS process to assist analysts

Process Summary

70. The following diagram is intended to provide a summary of the RSDOPS six step process and provide additional information to assist analysts. Provided are some recommended sources of input needed to complete each step and a view of the objectives of each step to assist the analyst in understanding what the output of each step should be.

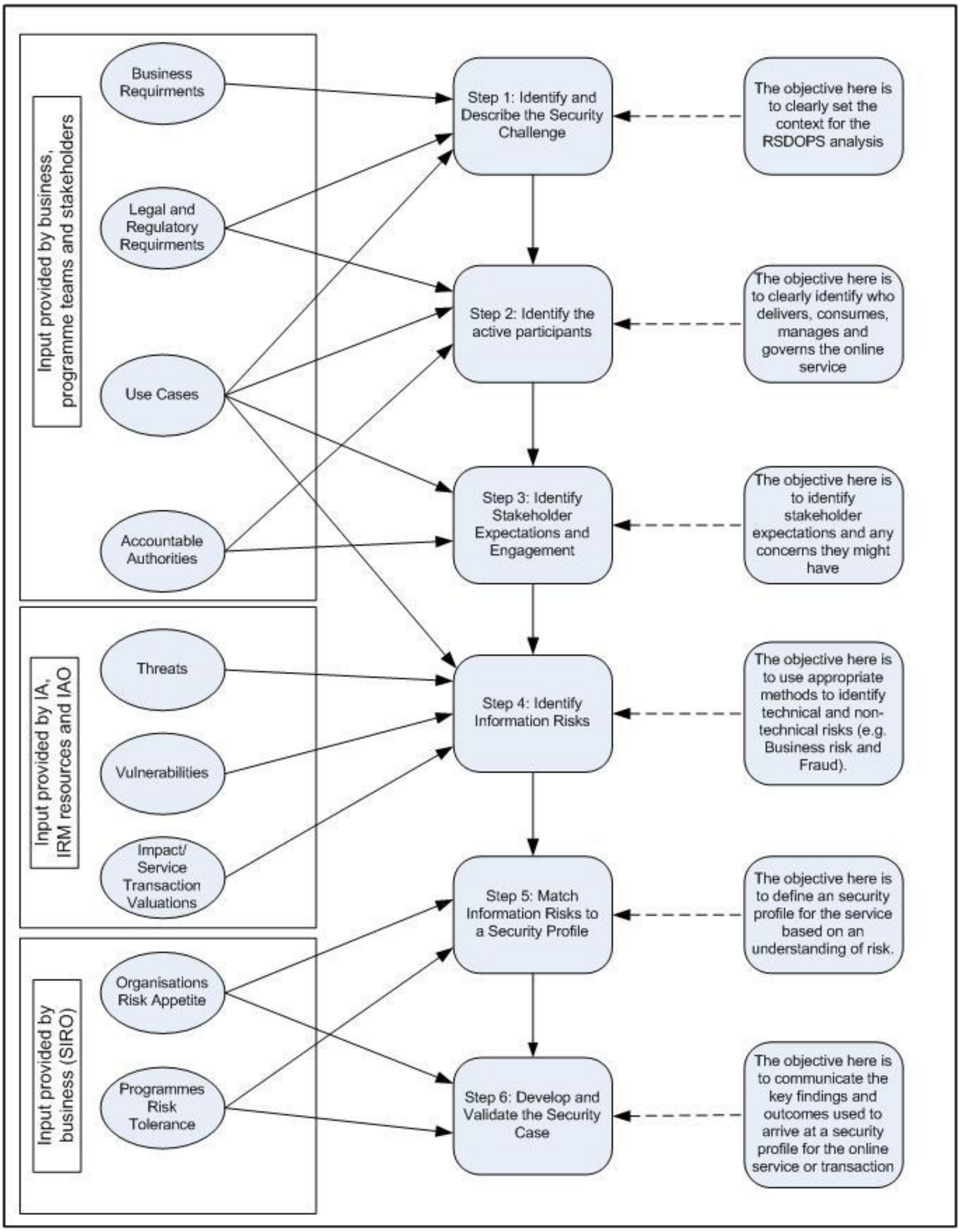

Input provided by business, programme teams and stakeholders
Business Requirments
Legal and Regulatory Requirments
Use Cases
Accountable Authorities
Input provided by IA, IRM resources and IAO
Threats
Vulnerabilities
Impact/ Service Transaction Valuations
Input provided by business (SIRO)
Organisations Risk Appetite
Programmes Risk Tolerance
Step 1: Identify and Describe the Security Challenge
Step 2: Identify the active participants
Step 3: Identify Stakeholder Expectations and Engagement
Step 4: Identify Information Risks
Step 5: Match Information Risks to a Security Profile
Step 6: Develop and Validate the Security Case
The objective here is to clearly set the context for the RSDOPS analysis
The objective here is to clearly identify who delivers, consumes, manages and governs the online service
The objective here is to identify stakeholder expectations and any concerns they might have
The objective here is to use appropriate methods to identify technical and non-technical risks (e.g. Business risk and Fraud).
The objective here is to define an security profile for the service based on an understanding of risk.
The objective here is to communicate the key findings and outcomes used to arrive at a security profile for the online service or transaction

Figure 4 - Summary of RSDOPS Process

Chapter 6 - Summary Security Components

Key Principles

- Security components are packages of security requirements that focus on a specific aspect of security
- Security component requirements and outcomes have been assigned levels 0–3
- The levels have no absolute significance in relation to components
- This summary presents component intent and desired outcome, not content

71. The Security Profile, which is the vehicle used to scope and agree the security response, is structured around a set of Security Components. There is some overlap between the components, and there may be additional requirements not covered by the components defined. The components can then be used for communication amongst stakeholders of the intentions of the service owner in regard of service security and negotiating the detailed requirements.

72. 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 guidance‘, or ’not relevant to this application’, it should **not** be read as ‘no attention is required to be given to this component’.

73. The security requirements and outcomes are broken down into levels with minimal reference to solutions. Reference to potential solutions is used to illustrate requirements but these need not constrain actual solutions unless necessary for other reasons such as interoperability.

74. The profile should select levels that 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.

75. In assigning a level for a particular security component to a service, the Service Provider should consider the direct and indirect consequences of a failure in that particular component and interpret such potential failures as:

    - Minor
    - Significant
    - 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.

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

77. A high-level summary of the security components and their levels can be found in the tables that follow.

78. Some boxes in the tables below have been left ‘intentionally blank’ as currently there are no pan-Government requirements. Some organisations may wish to undertake work equivalent to these particular levels to fulfil their own specific internal requirements.

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 subsequently to 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.	This box is intentionally blank.

Security Component	Notes	Level 0	Level 1	Level 2	Level 3
End User Authentication	Authentication is the act of ensuring or checking that a user of a service or system is the owner of the identity they claim to be. This is achieved through the provision of evidence usually in the form of credentials.	**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 should 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.
End User Authorisation	Authorisation is the act of confirming that a registered user is entitled to access a service prior to permitting that 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.	This box is intentionally blank.	This box is intentionally blank.

Security Component	Notes	Level 0	Level 1	Level 2	Level 3
End User Privacy	Privacy is a requirement for socially responsible handling 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. For further information see the Data Protection Act 1998 (reference [d]).	**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.	This box is intentionally blank.
Network Communications Security	Means by which assurance is gained that observation or interference with information cannot occur in transit to, from, or 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 public sector specific capabilities and assurance.	**Substantial** Threat analysis suggests a need for strong measures to counter well-resourced and competent adversaries. The response may require public sector specific capabilities and assurance.
Network 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.	This box is intentionally blank.	This box is intentionally blank.

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 public sector systems but still likely to attract interest as a public sector 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 public sector 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.	This box is intentionally blank.

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 and persistent binding between the transaction and the originator and recipient.	This box is intentionally blank.
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.	This box is intentionally blank	**Independent 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 (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.	This box is intentionally blank.
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.	This box is intentionally blank	**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. CPA and CESG Tailored Assurance Service, CTAS)	This box is intentionally blank.

References

[a] CESG Good Practice Guide No. 43, Requirements for the Secure Delivery of Online Public Services – Annex A, Stakeholder Expectations, Issue 1.1, December 2012, Available from the CESG IA Policy Portfolio.

[b] CESG Good Practice Guide No. 43 Requirements for the Secure Delivery of Online Public Services – Annex B, Security Components, Issue 1.1, December 2012, Available from the CESG IA Policy Portfolio.

[c] HMG Security Policy Framework Tiers 1-3, (Not Protectively Marked) are available at www.cabinetoffice.gov.uk

[d] Data Protection Act, 1998, available at www.ico.gov.uk/for_organisations/data_protection.aspx

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