Cabinet Office

Government Security Classifications
FAQ Sheet 2: Managing Information Risk at OFFICIAL

v2.0 – March 2014

This FAQ describes how risk management activities should be conducted for the new OFFICIAL classification. It outlines the typical circumstances where OFFICIAL information can be securely managed on specific types of ICT infrastructure. These circumstances are directly informed by the Threat Model for OFFICIAL (Annex A) and ICT use cases are provided as examples to help inform departmental risk decisions (Annex B).

There are more detailed technical standards and guidance available for the relevant ICT Strategy Programmes (End User Devices, Public Services Network and G-Cloud) and the wider body of protective security policy advice is set out in the HMG Security Policy Framework alongside any statements of residual risk associated with the use of a particular product or service.

Key Principles

The OFFICIAL classification will contain a wide range of information of varying sensitivities, and with differing consequences resulting from compromise or loss.

It is for risk owners to properly understand the value and sensitivity of their information, and the ways in which they work with it, in order to make informed, risk management decisions.

At OFFICIAL, government-wide security standards will generally be achieved by delivering common security outcomes rather than via generic controls. Risks must always be effectively managed but there will opportunities for organisations to develop innovative solutions and take advantage of good commercial practices and tools.

Security measures must always be proportionate and driven by the business requirement. The Threat Model for OFFICIAL will provide the broad parameters in which security should be designed and implemented.

How do we accredit OFFICIAL systems?

Accreditation is the process whereby an organisation makes an informed business decision on whether they wish to accept the risks associated with a given capability, balanced against the business opportunities that it brings. The responsibility to manage this process is usually delegated from the senior risk owning executive, to an accreditor. The Government Security Classifications Policy does not change this principle.

Will we need to re-accredit existing or legacy systems?

No. Risk assessments will remain applicable under the new classifications policy as long as your system architecture and business processes have not changed as a result. Organisations may wish to re-evaluate existing accreditations against the approaches which have been developed to complement the new policy (e.g. CPA Foundation Grade, End User Device Platform Guidance, Cloud Security Principles), as there may be opportunities to streamline processes or realise efficiencies.

Will IA Standard (IS) 1/2 change?

No. IS1/2 provides a common approach for information risk assessment, management and assurance activities. Used properly, IS1/2 remains an appropriate method for assessing and managing risk and therefore will not change for the launch of the Government Security Classifications Policy.

How do I use IS1/2 for assessing risk to OFFICIAL systems?

IS1/2 remains unchanged under the new classifications policy. The fundamental aim of an IS1/2 risk assessment is to assess impact, threat and vulnerability in order to produce qualitative, business driven, risk statements. These principles apply equally, regardless of the classification regime in use. The output from the risk assessment process then forms a basis for the effective management of risk.

When practitioners assess risk they can continue to use the existing IS1/2 risk assessment method. However, they should ensure that the analysis fully takes account of business requirements; the Threat Model for OFFICIAL and doesn't simply step through the IS1/2 method without considered application. The output from an IS1/2 risk assessment should always be a business focused risk narrative and not a list of generic or meaningless statements.

What is happening to Business Impact Levels (BILs)?

IS1/2 provides security professionals with a method for conducting a risk assessment, which includes an assessment of 'impact' should a risk be realised. BILs were originally conceived as a means of normalising and articulating the output of such an impact assessment in the course of an overall risk assessment. However, BILs have been widely misused beyond their intended purpose, which has led to significant negative outcomes.

There is no longer any mandatory or policy requirement for the use of BILs and they do not map to the new classifications.

Reference by a security professional to the BIL tables in IS1/2 remains acceptable in the course of a comprehensive risk assessment provided that:

a) They are used appropriately and as intended. In particular, BILs should not be used to describe the security offered by an IT system, service or device, or as a level of accreditation. BILs should never be used as a proxy for specifying contractual security requirements.

b) The assessment uses the BIL tables for reference only as part of the overall IS1/2 risk assessment process. It is essential that the security professional conducts analysis and enumerates the actual business impact. This should be the output of the impact analysis and not simply a 'number' based on a broadly applicable statement from the BIL tables.

c) Effective impact and risk assessment is a business process and therefore the outputs from these activities should be specified in business language.

How will I know how secure an ICT system is without BILs?

BILs have never provided a level of security in themselves; rather they can indicate the impact of loss or compromise of information, stored or processed by a particular system. In the past people have misused BIL value as a proxy for security requirements, often leading to assumptions of the security measures which are present in that system. Interpretation of security requirements, defined solely by a BIL value, can vary considerably so assumptions such as these can cause confusion, add cost or potentially even increase risk.

Rather than attempt to create a shorthand or label to describe the implementation of security, practitioners should aim to be as clear and explicit as possible about the controls they apply and the risks that they are mitigating in any given system. It should always be possible to articulate this in plain English and without recourse to jargon.

At OFFICIAL, risk owners should expect compliance with any relevant legislation, the Classification Policy Controls Framework and alignment with good commercial practice and common standards – typically provided by pan-Government frameworks such as the PSN and G-Cloud.

Will the new classification policy affect my organisation's appetite for information risk?

We do not anticipate organisations accepting more information risk as a result of the Classification Policy, however there are a number of areas where the focus differs from current arrangements. For example the new policy places far greater emphasis on personal responsibility amongst staff and enables increased access to commodity technology rather than bespoke 'government-only' solutions. This shift could mean that the risk profile of the organisation will change e.g. more dependency on training and awareness and less reliance on purely technical mitigations.

How will Government find a common baseline of security?

Government interoperability and information sharing is founded on mutual trust that organisations will apply a consistent approach to security and that information will receive broadly equivalent levels of protection. At OFFICIAL, a common baseline of protection is provided via a number of means, including:

- The Classification Policy Controls Framework and Threat Model for OFFICIAL
- Any legal obligations (e.g. DPA) or regulatory requirements
- The broad risk appetite for OFFICIAL (see the Office of the Government SIRO *HMG Information Risk Directive)*
- The Security Policy Framework and CESG/CPNI advice and guidance
- Common assurance and accreditation methodologies
- Common security compliance regimes (e.g. GSI Codes of Connection / PSN IA Conditions)
- Common trusted infrastructure provided by the PSN and other ICT Strategy programmes (End User Devices and G-Cloud)
- Information-sharing agreements between organisations to provide detailed handling requirements for specific business exchanges

How does the security of an OFFICIAL ICT system differ from a RESTRICTED one?

It is a common misconception that there is a standard template for the security of a RESTRICTED ICT system – there is not. Organisations are expected to refer to any relevant policy and guidance (e.g. the Security Policy Framework, CESG/CPNI advice) and use it to inform local risk management activities and business decision-making. This body of policy, advice and guidance will remain largely current but where appropriate, geared more explicitly toward the new classifications over the next 12-18 months.

On this basis, the new Classification Policy will not provide a detailed technical specification for ICT systems but has been developed to complement the objectives of the ICT Strategy and associated programmes. In real terms, this means increased adoption of commoditised technology and services, use of the cloud and greater emphasis on devices that allow mobile or flexible working.

The ICT Programmes (e.g. PSN, G-Cloud, End User Devices) have detailed assurance and security frameworks which you will need to carefully consider in parallel to your implementation of the new Classification Policy.

Can we use commercial off-the-shelf security products for OFFICIAL?

Yes - the new Classification Policy describes the use of 'good' commercial security products for use at OFFICIAL. This means commercially available products that have been independently validated against a well defined set of characteristics for that particular product type. The level of assurance required is Foundation Grade, which will typically be provided by CESG's Commercial Product Assurance (CPA) scheme. While CPA is strongly recommended, organisations may also conduct other suitably-scoped assurance activities to provide further options - in the first instance your security practitioners should familiarise themselves with CESG's Security Characteristics which describe the attributes that they would expect to see in a range of good commercial security products.

CESG are working with vendors to increase the range of assured products in the CPA scheme, however, departments should also encourage their industry vendors to seek Foundation Grade assurance to speed this process.

This change in approach will enable the public sector to take advantage of a wider range of modern, lower cost (commodity) security products rather than defaulting to expensive, bespoke or augmented technologies.

When should we be using encryption to protect OFFICIAL information?

The new policy allows organisations to make risk-managed decisions on the protection of OFFICIAL information (by encryption or another method), provided the principles are agreed at SIRO level and are in line with departmental/HMG's risk appetite and with due consideration to any overriding legal obligations (e.g. DPA).

Local business requirements will drive your decision-making about when it is necessary to encrypt but organisations should be mindful of the inherent vulnerability of unencrypted information while in transit over un-trusted networks or at rest within a device or service.

Other considerations will be:

- PSN will provide central government organisations with the means to communicate securely with one another. This encrypted layer will be enabled by default and transparent to the end user.

- The UK communications infrastructure is increasingly global in nature. This includes overseas management and routing of communications as well as a truly global supply chain.

- Nearly all modern Internet based services that transact with users or hold sensitive/personal data are secured in transit (e.g. online banking and webmail).

- Use of encrypted VPN technologies enable simple and seamless mobile working while ensuring corporate networks remain protected. The user's choice of access (corporate network, home WiFi, WiFi hotspot) and choice of platform becomes

irrelevant to their experience. Good security makes it easy for users to concentrate on their job and makes it hard for them to do the wrong things.

- Encryption doesn't only protect confidentiality. Accessing personal information via a secure website provides us with a level of authentication and integrity of the service provider – something which is impossible to achieve through standard unencrypted email.

Who can we share OFFICIAL information with?

There is no distinct or bounded group that is permitted access to OFFICIAL information and this classification will contain a wide variety of information types. Any restrictions on sharing will be defined by particular sensitivities or the specific requirements of the information itself.

Considerations for sharing will include:

- The need-to-know principle
- Any legal obligations (e.g. DPA)
- The way the information is shared (e.g. via unencrypted email)
- Any assurance required in the person(s) receiving the information (e.g. security clearances)
- Where the shared information will be stored and whether you are able to gain any confidence in the security of the recipient organisation?
    - Other government departments are likely to be subject to similar security compliance regimes (e.g. GSI Code of Connection or PSN IA Conditions)
    - Commercial organisations may also have undergone comparable levels of scrutiny and assurance (e.g. an appropriately scoped ISO27001 certification)
    - It must be assumed that there is no assurance on privately-owned systems, unless you have gained this assurance through other means.

Can we email OFFICIAL information over the internet?

Yes - Organisations will send and receive OFFICIAL information via a number of channels and with a variety of partners, both internally and externally to government. The PSN will be the default and trusted bearer for information sharing within the public sector but, there will be a substantial and enduring requirement to share OFFICIAL information beyond this protected space.

The trust required in any recipient body for receiving OFFICIAL information will be as the considerations outlined in the previous questions but organisations will also have to carefully consider the mechanisms that they use to share. Email will continue to be the convenient communication tool for most staff and in many cases entirely appropriate for sharing information with external partners, however, you should be aware that an unencrypted email sent over the internet has no inherent protection.

Above all, you will need to ensure that the people within your organisation have received sufficient training, have access to clear policies and guidance and understand how they should share the information that they work with.

When should we be using the OFFICIAL-SENSITIVE caveat?

The OFFICIAL-SENSITIVE caveat should not be confused with a separate classification; it is tool to denote OFFICIAL information that is of a particular sensitivity but that can be managed on OFFICIAL systems and infrastructure.

Organisations and staff should use their discretion to determine those instances where the OFFICIAL-SENSITIVE caveat will provide value and this will vary depending on the subject area, context and in some cases, any statutory or regulatory requirements.

In order to maintain currency the handling caveat should be used by exception and in limited circumstances where there is a clear and justifiable requirement to reinforce the 'need to know.' This is where compromise or loss could have particularly damaging consequences for an individual (or group of individuals), an organisation, or for HMG more generally.

The handling caveat may not be necessary for sensitive OFFICIAL information that is already managed through clear and well understood business processes and where there is no requirement or benefit for this sensitivity to be explicitly highlighted through an additional marking. In all other cases handling instructions should be included.

What additional security controls should be used with OFFICIAL-SENSITIVE?

Any additional security controls for OFFICIAL-SENSITIVE information will be largely procedural rather than technical and designed to enforce particular need-to-know requirements. Examples could include:

- Well communicated and understood handling processes
- Clearly defined and bounded copy lists
- More granular access controls within document stores or databases
- Increased monitoring and compliance auditing

Management of OFFICIAL-SENSITIVE information should not require a separate ICT

infrastructure or additional security products. All OFFICIAL information can be managed on a single End User Device that is configured in accordance with the End User Device Platform Guidance.

Is Bring Your Own Device (BYOD) possible with OFFICIAL?

A BYOD model is possible at OFFICIAL but not recommended for a number of technical and non-technical reasons. The risks, complexities and costs involved with introducing BYOD could potentially negate any perceived benefits.

A risk owner will need to consider the following:

- Whether the personally-owned device can be under management authority of the organisation for the complete duration that it is permitted access to OFFICIAL information
- Whether sufficient separation can be achieved between personal and professional compartments on the device – currently there are no assured solutions to provide this
- The implications of OFFICIAL information saved to personally-owned devices (risk of data leakage, compliance with FOIA and DPA)
- The implications of untrusted devices connecting directly to your network (risk of malware, stolen login credentials)
- Any associated business implications (HR, IT Support or software licensing issues)
- How a security incident or breach would be managed without direct control of a device

ICO guidance on BYOD and personal data can be found here

Can we use smart phones and tablets for OFFICIAL?

Yes, detailed configuration guidance for all major mobile platforms can be found here

How will I know if G-Cloud services are secure enough for our OFFICIAL data?

The current G-Cloud Framework offers services against three levels of assurance, aligned with the Business Impact Levels (BILs) system. While use of BILs in this context will be discontinued in the next framework, organisations may continue to procure and use these services based on the following:

- Unassured Cloud services. These services (formerly Impact Level 00x) may be appropriate for a limited amount of information where there is little or no

confidentiality requirement, such as marketing and communications data intended for public consumption. However, organisations will also have to consider their integrity and availability requirements.

- Assured Public Cloud (formerly Impact Level 22x) services will be subject to a suitably scoped ISO27001 certification and assurance level based on good commercial standards. Such services may be appropriate for most OFFICIAL information, although organisations should carefully consider the scope of the IS027001 certification, the geographic location of the hosting, and any other residual risks identified as part of the G-Cloud Accreditation Statement. Many of these services may not be suitable for more sensitive information.

- Accredited Public Cloud (formerly Impact Level 33x) or Private Cloud services will be subject to full HMG accreditation and will be hosted within the UK. These services will be appropriate for all OFFICIAL information, although organisations should still be mindful of any risks involved in outsourcing services and data to the cloud (including those set out in the G-Cloud Accreditation Statement).

Future iterations of the G-Cloud Framework will ask suppliers to present the security of their service in a far clearer and more meaningful way. The basis of this approach can be found in the 14 Principles of Cloud Security and organisations are advised to start using these principles when selecting cloud services.

Can we off-shore OFFICIAL information?

Off-shoring of OFFICIAL information is permitted, however organisations should be aware of the following:

- There are certain information types (e.g. information relating to national security or sensitive international issues) where off-shoring may not be a suitable option

- Personal data held off-shore should be kept within the EEA, Safe Harbor or the limited number of countries with positive findings of adequacy from the European Commission. Organisations may conduct their own assessments of adequacy, however this approach carries the inherent risk that in the event of a breach, the Information Commissioner may not agree with their findings.

- It is important that you can satisfy your security requirements in the locations chosen to off-shore to. The local political, legislative or cultural environment may make satisfaction of your normal security requirements challenging.

The Office of the Government SIRO will review and advise on off-shoring proposals for HMG information.

How should we manage aggregated OFFICIAL information?

Aggregated datasets of OFFICIAL information should typically be managed within the same infrastructure and there is no threshold where increased volume will cause an uplift in the classification level e.g. a database containing 100,000 OFFICIAL records does not become a SECRET database.

Organisations will need to carefully consider the impact of aggregation on confidentiality, integrity and availability of information and implement security controls accordingly.

Aggregation could result in the following conditions being realised:

- The business impact of an aggregated data compromise is likely to be higher than the compromise of a single item.
- Existing threats will remain relevant but these threats may be more motivated to mount an attack as the benefit to them of compromising a large number of data objects is more appealing.
- New threats may be attracted to attack the aggregated data set or service because the return on investment may be sufficiently increased.

Access to aggregated datasets of OFFICIAL information should be carefully managed and this may include technical controls which physically limit the amount of data that can be accessed or presented to a user or device. Storage of aggregated data on mobile devices should always be minimised as far as business requirements will allow.

ANNEX A – The Threat Model for OFFICIAL

For the generality of its business and to deliver services in a modern, accessible and cost-effective fashion, HMG needs to work in the same way as any large and well run UK commercial organisation. This means adopting a commercial threat model that protects information and services against attackers with bounded resources and capabilities, including hactivists, single-issue pressure groups, investigative journalists, competent individual hackers and most criminals.

HMG is satisfied that this model will mean, amongst other things, that the confidentiality of citizen data and routine commercial dealings is assured. This does not imply that OFFICIAL information will not be targeted by sophisticated and determined threats (including Foreign Intelligence Services) but a decision has been taken to manage these risks in order to ensure efficiencies and allow government organisations to operate effectively. This approach is underpinned by an understanding that the majority of information risks can be successfully managed by getting the basics right: good governance, staff awareness and well maintained, modern IT systems.

There is no silver bullet for mitigating all threats at OFFICIAL and organisations should provide layered security across their businesses. People, technology and environmental controls should be mutually enforcing and given equal consideration as part of a holistic approach to security.

This model is not intended to provide an exhaustive list of threats and mitigations; instead it will describe the broad parameters in which threats should be managed. Organisations should also look to other sources of threat guidance and best practice to inform their decision-making.

Organisations should note that threats to large aggregated volumes of OFFICIAL information may not conform to this model - a significantly higher return on investment could attract more sophisticated or determined attackers (e.g. to conduct attacks against large transaction or online payment systems). Controls for aggregated data should be directly informed by a risk assessment and this will include an understanding of how aggregation affects threat.

There will also be occasions where threats to highly aggregated OFFICIAL systems and data extend beyond the profile of a single organisation and merit a government-wide or even national response. Typically these threats will be managed centrally and via pan-government programmes.

People

People will provide the strongest defence but will be the most significant vulnerability to OFFICIAL information. This model anticipates that almost all security incidents will have a decisive human factor and that often the most important mitigations will be training, clear policies and effective HR processes.

People working with OFFICIAL information will be vulnerable to social engineering, often designed to elicit information or compromise IT systems or business processes. These attacks will utilise a range of methods and techniques but the following (or combinations of)

should be considered within scope for OFFICIAL:

- Unsolicited approaches, via electronic means, by telephone or in person
- Targeted approaches developed from open source information (e.g. unsecured social media or professional networking profiles, corporate websites)
- Emails harbouring malware (as attachments or web links)
- Malicious or compromised websites
- Removable devices carrying malware

Organisations should protect against threats from wilful or careless misuse of OFFICIAL information and systems. Controls should be implemented to mitigate against people motivated by financial gain, coercion and disaffection.

Technology

IT systems used for OFFICIAL information will typically be internet-facing and protected by assured, commercially available products and services. Attacks will be designed to exploit vulnerabilities in software, network architectures, poor management and misconfiguration of systems and devices.

These attacks will utilise a range of methods and techniques but the following (or combinations of) should be considered within the scope for OFFICIAL:

- Widely available exploits for known software vulnerabilities
- Exploitation of misconfigured or poorly implemented boundary defences (e.g. firewalls, content filtering tools)
- Exploitation of poorly implemented user account management, rights and privileges
- Exploitation of poorly implemented system hardening or configuration management
- Exploitation of poorly architected networks and services, including insufficient separation from more vulnerable or exposed systems (e.g. web servers)

Commercial encryption products will be the default protection for OFFICIAL information in transit or at rest. Since commercial encryption products will vary in effectiveness it is recommended that they are independently validated, typically using a scheme such as CPA. At OFFICIAL, attacks against commercial encryption products will attempt to exploit weak algorithms or flaws in the design and implementation of cryptography.

Environment

OFFICIAL information will be managed in a range of environments and attackers will normally seek to take advantage of weaknesses in processes and procedures in order to gain access to information and services.

This unauthorised access will utilise a range of methods and techniques but the following (or combinations of) should be considered within scope for OFFICIAL:

- Exploitation of poorly implemented and managed perimeter security measures
- Exploitation of poor security awareness among staff (e.g. tailgating)
- Compromise of unsecured IT systems or physical documents

ANNEX B - ICT Services and Use Cases

Example Information Types

- **Non-Sensitive Information**: This information will typically be public knowledge or intended for public consumption; for example, marketing material, open consultations, information to be published under transparency/open data or even routine communications with members of the public or third parties where there is no confidentiality requirement. There may be a requirement to protect the integrity and availability of this information.

- **Transactional**: This includes one-off (potentially) sensitive exchanges with external partners, (citizens, industry, third sector etc), and online transactional services where the loss of a small number of instances is tolerable, but systematic or large scale compromise is unacceptable. Loss of confidentiality, integrity or availability of this data will result in disruption to HMG service delivery and may have a commercial or financial impact. Organisations may also need to comply with external compliance obligations such as the Payment Card Industry Data Security Standard (PCI DSS).

- **Routine Public Sector Business**: Information of varying sensitivity that supports the routine business, operations and services of the Public Sector. There is a requirement to protect the confidentiality, integrity and availability of this information.

- **Legally Defined (e.g. Personal)**: Information which is subject to legal and / or regulatory requirements. For example, personal information that relates to an identifiable individual as defined by the Data Protection Act (DPA). Legal or regulatory requirements must be met and additional controls may be required in line with HMG risk appetite tolerances. There is a clear requirement to protect the confidentiality, availability and integrity of such information.

- **OFFICIAL-SENSITIVE**: The loss, compromise or misuse of information marked with the OFFICIAL-SENSITIVE caveat has been assessed as being likely to have damaging consequences for an individual, an organisation or HMG more generally. Risk owners will typically require additional assurance that the need-to-know is strictly enforced, and there is a clear requirement to protect the confidentiality, integrity and availability of this information. However, note that this example is intended to illustrate where heightened technical protections may be appropriate; in most cases it will be more proportionate to risk manage access to limited amounts of OFFICIAL-SENSITIVE information on corporate systems using more stringent procedural controls instead.

ICT Services and Use Cases

Note, these use cases describe specific business scenarios to identify appropriate levels of assurance in each instance; they do not create distinct sub-tiers within OFFICIAL.

	End User Device (EUD)	Network	Service and Hosting
Non-Sensitive Information	No specific assurance requirement as the information is public knowledge or for public consumption.	Risk owners should consider availability needs. No other specific assurance requirement as the information is public knowledge or for public consumption.	Risk owners should consider integrity and availability needs when considering service offerings. Un-assured (public) services may be appropriate.
Transactional	No specific assurance requirement as transactional information will be exchanged with the citizen and therefore processed on the citizen's un-managed device. Transactional services should be presented via GOV.UK to ensure a common interface and to benefit from centralised resilience.	Risk owners should consider confidentiality, integrity and availability needs. The confidentiality and integrity of transactional data should be protected, e.g. by utilising a secure TLS connection as it traverses the Internet.	Risk owners should consider confidentiality, integrity and availability needs. The end-to-end service must be appropriately protected; assurance requirements for the system as well as the data at rest will depend on the nature of the information, and should aim to protect against loss of data or disruption to service. Many such financial services will also be subject to non-government security standards e.g. PCI-DSS
Routine Public Sector Business	Risk owners should consider confidentiality, integrity and availability needs. End user devices are expected to be appropriately protected and managed by the enterprise, and should be configured in accordance with the EUD Platform Guidance. Aggregation of information or the	Risk owners should consider confidentiality, integrity and availability needs. The bulk of public sector information in transit will be via accredited shared infrastructure (such as PSN) or protected using encryption Routine information may be emailed / shared with external partners / citizens,	Risk owners should consider confidentiality, integrity and availability needs. Assurance requirements will vary depending on the nature of the information. However services and hosting should be assured at a minimum based upon a well scoped ISO 27001 assessment. Risk owners must read and understand the scope and associated residual risk statements.

	presentation of aggregated information should be avoided at the end device.	subject to local business policies and procedures. Where more sensitive information must be shared with external partners organisations should consider using alternative secure mechanisms.	Refer to the Cloud Security Principles and make a determination as to what security requirements you have in reference to these principles.
Legally Defined	Risk owners must ensure that their organisation, as a minimum, fulfil their legal and regulatory obligations such as the principles of the Data Protection Act (1998).		
	End user devices are expected to be appropriately protected and managed by the enterprise, and should be configured in accordance with the EUD Platform Guidance. In addition follow ICO guidance. Aggregation of personal information or the presentation of aggregated personal information should be avoided at the end device.	Organisations should take all reasonable steps to ensure that personal information in transit is protected and such information would normally be encrypted where there are confidentiality requirements. Where sensitive personal information must be shared with external partners (e.g. citizens), organisations should consider providing access via secure, encrypted mechanisms (e.g. browser sessions using SSL / TLS)	Services and hosting should be assured at a minimum based upon an ISO 27001 assessment. Risk owners must read and understand the scope and associated residual risk statements. Aggregated or sensitive personal information should not normally be processed in unencrypted public cloud solutions. Personal data held off-shore should be kept within the EEA, Safe Harbour or in countries with positive findings of adequacy from the European Commission.
OFFICIAL-SENSITIVE Information	Risk owners should consider confidentiality, integrity and availability needs. End user devices are expected to be appropriately protected and managed by the enterprise, and should be configured in accordance with the EUD Platform Guidance. Risk owners may chose to put in place specific additional procedural measures.	Risk owners should consider confidentiality, integrity and availability needs. OFFICIAL-SENSITIVE information in transit must be protected by default, and should normally be encrypted when in transit or stored on mobile devices. Limited information exchange with appropriate and trusted external	Risk owners should consider confidentiality, integrity and availability needs. Services and hosting must be subject to accreditation by Departmental SIRO representatives or (for shared services) the Pan-Government Accreditor. Risk Owners should carefully consider the risks before off-shoring OFFICIAL-SENSITIVE information.

	Aggregation of OFFICIAL-SENSITIVE information or the presentation of such aggregated information should be minimised at the end device	partners. Risk owners should apply the "need to know" principle when considering access to such data.	