2. The Common Criteria for Assessing Risk (CCfAR)

Purpose

The **Common Criteria for Assessing Risk** (CCfAR) is a set of outline criteria for government organisations to use when assessing risk in third party supplier contracts at the OFFICIAL level (including OFFICIAL-SENSITIVE).This will assist in ranking the risks of third party suppliers and determining the level of assurance required.

For example as part of the annual compliance process a government organisations may accept an annual self assessment from a supplier providing a low risk service or product but may require more information and a site audit from a supplier providing a high risk service or product.

Principles

The CCfAR is designed as a flexible tool:

- Not all of the criteria may be valid for every contract; the CCfAR should be amended and augmented to suit the business requirements of the contract.

- To use the CCfAR it is not necessary to know all the answers – assumptions can be made. Seeking to clarify these assumptions may further highlight or mitigate a risk.

- It is critical for the risk assessor to have a range of input to the CCfAR from specialist areas, e.g. procurement, security, IA, business/customer, accreditors, IAO, legal etc. as necessary. In this way a good understanding of the risks within the context of the risk appetite of the SIRO and the OGSIRO can be gained.

- The scoring mechanism is NOT mandatory and cannot be the only consideration for assessing risk, the discussions that take place when considering the business requirements, how they are or will be implemented in the contract and the resultant risks are the most valuable element of using the CCfAR.

- Information gathered for the CCfAR will provide a record, that can be updated, or an audit trail over the life of the service or product provided.

- The CCfAR template is a living document, it will need to reflect emerging risks such as increased supplier use of bring your own device (BYOD) and cloud services to remain relevant. A completed CCfAR is the record of an assessment carried out on a service or product and can be compared to the results of any future assessments.

- How they are or will be implemented in the contract and the resultant risks **are the most valuable element of using the CCfAR**.

- Use of a common set of criteria will support a consistent approach to managing information risk in third party suppliers.

Using the Common Criteria for Assessing Risk (CCfAR)

To illustrate how the CCfAR might be implemented in government organisations two scenarios are outlined below.

Scenario A – **The CCfAR can be used by government organisations to risk assess existing contracts, and rank and group them into the level of risk e.g. 'high' 'medium' and 'low' risk services. Those which are 'High' risk should, be included in the annual Departmental Security Health Check report to the Cabinet Office,** There may be more contracts than initially realised and therefore the assessment may require a progressive process and planning.

- **Start** by deciding which part of the department/organisation is leading the CCfAR assessment e.g. Security, IA, Contracts etc.
- **Agree** the outcome, including: the number of contracts to be looked at, the timescale, the likely people involved, the scope e.g. will it include specific or high risk contracts, and what other processes it will inform or feed into.
- **Identify** those areas of the dept./organisation that are likely to have important input on these contracts, e.g. Contracts, Business/IAO, Security, IA, Procurement, Legal, IT, Accreditation etc..
- **Outline** the information gathering process, it should have a structure yet be as light touch as possible. The best results are likely to come from stakeholder discussion sessions.
- **Review** the information gathering process against the outcome, was it effective, can it be repeated, which stakeholders benefited, what lessons were learnt, were there any trends, who would benefit from sharing the information and how could it be stored for future use?
- **Use** the CCfAR as an initial part of a structured process to inform risk based decision making and to prioritise resources for assurance and compliance activities.

Scenario B – **Using the CCfAR as an integral part of the procurement cycle**

The CCfAR has a role to play at 4 main stages in the procurement cycle:

1. **Identifying the need**
2. **Contract award**
3. **Contract management**
4. **End of contract**

Below is a proposed outline of how the criteria could be used at each stage of the cycle.

Identifying the need

At this stage the business has identified / defined a requirement and had tasked procurement with drafting some outline proposals on how the requirement might be met.
Procurement will complete a risk assessment in order to:

- Engage key stakeholders
- Identify major risks and assess an overall likely risk rating for the contract
- Clarify where assumptions need to be made
- Capture requirements for the ITT
- Capture requirements for the terms and conditions of the contract
- Assess the level of security plan required
- Capture and record information necessary for the life cycle of the contract.

The key stakeholders may include the business, IAO, security, IA, legal, IT, accreditors, etc. dependent on the level of risk identified in the contract. The CCfAR can be used to form the basis on the discussion about risk with the key stakeholders and will provide information to support each of the 7 bullet points above. For high risk contracts the relevant IAO responsible should be informed of the likelihood of the risk and its impact on the confidentiality, integrity and availability. The IAO should consider whether this aligns to the organisation's risk appetite and if they can accept the risk or will need to escalate to the SIRO.

Contract award

At contract award the business will have a complete set of requirements, any assumptions will have been replaced by solutions and detail how the service/product will be delivered and there will be a better understanding of the risk.

The organisation can work with the supplier to ensure the proportionality of the contract and the:

- Security Plan
- Accreditation Plan
- Assurance Plan, and
- Roles and Responsibilities of the various stakeholders within the organisation

A review of the CCfAR assessment can be undertaken and updated in the light of the contract award. If there is any change to the risk the relevant parties should be informed. The outcomes of the CCfAR reassessment should be shared and stored for use in the next stage of the cycle.

Contract management

The Security Policy Framework (SPF) requires departments to conduct an annual compliance review that includes delivery partners (executive agencies, NDPBs) and third party suppliers and report exceptions or areas of concern or high risk in the Departmental Security Health Check report. Reviews may include a review of the security plan with the supplier or request that the supplier completes a Statement of Assurance (SoA).

The impact of any changes to the supplier's delivery methodology or security measures should be considered in the review of the CCfAR risk assessment and the documentation should be amended where required e.g. security plan amendments. Stakeholders including IAOs should be informed of any high risk changes to the delivery of the contract. Analysis of the assessments can be used to identify emerging trends.

End of contract

Before the end of the contract, particularly for high risk contracts or where there is a forced termination, the exit strategy should be reviewed, including for example whether any information held by the supplier needs to be returned, securely destroyed or archived.

The CCfAR should be reviewed to ensure it provides an accurate assessment of the current risks. This then can form the basis of the risk mitigation plan. Stakeholders including IAOs should be informed of any risks likely to impact on the information asset prior to the termination of the contract.

3. COMMON CRITERIA FOR ASSESSING RISK - Worksheet

Project/contract name: ______________________ Date of Assessment: ________ Score:_____ Risk Outcome (L M H)**:** _____

Criteria	Risk No		Response & Scoring	Score	Assumption
CONTEXT					
Who owns/is responsible for the information processed by the contractor?			• **In the dept./organisation** • **In the supply chain**	See CCfAR guidance for further information	
Who is the data controller for the personal information processed by the contractor?			• **In the dept./organisation** • **In the supply chain**	See CCfAR guidance for further information	
Asset Identification					
The type of data/information processed by the contractor. When considering these categories you may wish to refer to the DPA definitions of personal and sensitive personal data. In almost all cases this information will be held in OFFICIAL.	**1A**	C	• OFFICIAL – contains no personal or policy information **[L]** 1 • OFFICIAL – may contain personal or policy information **[M]** 2/3 • OFFICIAL-SENSITIVE **[H]** 4 • SECRET (List X) **[H]** 5	These criteria are inextricably linked so the proposal is to combine them, so for example if personal data [2] was being processed and there were over ½ million records [5] – then the resultant score would be 10 ([2] **x** [5]) Risk rating (**L M H**):_____ **Score**:_________	
The number of data records processed**/**held over the lifetime of the contract?	**1B**	C	• Under 1,000 **[?]** 1 • 1,000 – 100,000 **[?]** 2 • Over 100,000 **[?]** 3 • Over ½ million **[?]** 4		
The information asset(s) may be in **electronic** or **physical** form. Where will the information asset(s) be held?	**2**	C	• UK Mainland (Onshore) – includes storage of physical assets **[L]** 0/1 • Inside EEA (Near shore) [M] 2 • Offshore with EU DP equivalence **[M]** 3 • Offshore elsewhere **[H]** 5	Risk rating (**L M H**):_____ **Score**:_________	A
Where will the data be accessed from/processed?	**3**	C	• UK Mainland (Onshore) includes supplier or subcontractor's Data centre **[L]** 0/1 • Inside EEA (Near shore) **[M]** 2 • Offshore with EU DP	Risk rating (**L M H**):_____ **Score**:_________	A

			equivalence [M] 3 • Offshore elsewhere [H] 5		
What is the sensitivity or impact of compromise of physical assets being either provided under the contract or being protected under the contract?	4	S	• Low [L] 0 • Medium [M] 2 • High [H] 3	Risk rating (**L M H**):____ **Score**:_________	A
Will the data be processed on a single site or a number of sites?	5	S	• Single [L] 1 • Few [M] 2 • Many [H] 3	Risk rating (**L M H**):____ **Score**:_________	A
The information asset may be processed in **electronic** or **physical** form. Will the supplier process the information as hardcopy? How will the supplier process the data – on what systems?	6	S	• Processed as hardcopy [L] 1 • Dept's own systems [L] 1 • Supplier's systems [M] 2 • G-Cloud [M] 2 • Shared asset [M] 2 • **Other** [H] 3	Risk rating (**L M H**):_____ **Score**:_________	A
Does the supplier use subcontractors in the delivery of the service?	7	S	• None [L] 1 • Some [M] 2 Completely outsourced [H] 3	Risk rating (**L M H**):____ **Score**:_________	A
Does the supplier allow the use of **portable media/devices**?	8	S	• No [L] 0 • Yes [H] 3	Risk rating(**L M H**):____ **Score**:_________	A
Does the supplier allow the use of bring your own device (BYOD) e.g. supplier's staff can use their own ICT?	9	S	• No [L] 0 • Yes [H] 3	Risk rating (**L M H**):____ **Score**:_________	A
Notes, comments: *Use this free text area to note anything relating to Asset Identification, particularly areas that have or will have an impact on how the risks will be or are managed and also to note where any modifications to, additions or deletions of criterion have been made.*					
Asset Management Processes					
Will the supplier have access to a live departmental system/database or to an offline extract, and is that data modified updating departmental systems, master records, ledger balances etc?	10	C	• No [L] 0 **Yes** • Read only access [L] 1 • Delete departmental record [M] 3 • Generate data for department [M] 4 • Update departmental record [H]4/5	Risk rating (**L M H**):____ **Score**:_________	A

How many of the supplier's staff will have access to read/write/update/delete/generate/transport the data?	**11**	S	- Less than 10 [L] 1 - Less than 50 [**M**] 2 - More than 100 [**H**] 3	Risk rating (**L M H**):____ **Score**:_________	A
Are there any existing accreditations or certifications that can provide evidence of information security controls e.g. RMADs, ISO27001, PSN CoCo, G-Cloud Accreditation, Information Security Management Systems (ISMS) etc?	**12**	S	Yes **[L]** 1 Working towards with executive support and plan [**M**] *2* No [**M**] 3	Risk rating (**L M H**):____ **Score**:_________	A
Is data transferred between the department/govt organisation and suppliers during the life of the contract? Consider whether the transfers are: In bulk or small amounts; regular or ad hoc. In electronic form or hard copy/paper. Only between the dept and the supplier or between the supplier and one or more subcontracts. During the transfers are there any risks to: **Confidentiality** e.g. loss of data and DPA consequences **Integrity** e.g. potential for data to be altered/tampered with **Availability** e.g. loss of service to provision, business continuity	**13**	C	No [L] 1 Yes [**L M H**] **1 - 5**	Risk rating (**L M H**):____ **Score**:_________	A
Will the supplier need to provide secure retention/storage/archiving and destruction of Authority data/documentation from completion of customer deliverable or beyond the end of the contract for a set period of time? For how long? For what reason?	**14**	S	No: **[L]** 0 No: return to the Authority or destroy in house **[L]** 0 *Yes* - ***Yes***: *for up to 6 months* **[L]** 1 - ***Yes***: *6 – 18 months* **[M]** 2 - ***Yes***: *over 18 months* **[H]** 3	Risk rating (**L M H**):____ **Score**:_________	A
The numbers of transfers down the supply chain for this contract, i.e. starting from the prime supplier down to the final subcontractor.	**15**	S	- 1 **[L]** 1 - 2 **[M]** 2 - 3 etc **[H]** 3	Risk rating (**L M H**):____ **Score**:_________	A

Are there particular risks or concerns relating to volume, confidentiality, integrity or availability of data being transferred at the start or the end of the contract? Consider whether: There will be a parallel run and how long will this be It will involve one or more government bodies. How much data will need to be migrated and the complexity of migration. Updates are required and their frequency.	**16**	S	No **[L]** 0 At the start or end? **[M]** 2 At the start and end? **[H]** 3	Risk rating (**L M H**):____ **Score**:_________	A
Notes, comments: *Use this free text area to note anything relating to the Asset Management Process, particularly areas that have or will have an impact on how the risks will be or are managed and also to note where any modifications to, additions or deletions of criterion have been made.*					
Impact					
Significance of the contract to the department, will disruption impact on delivery of a high profile service? Consider the following: **Confidentiality** – the reputational impact on the dept of a loss or compromise of information/data **Integrity** – impact of a compromise to the quality of service delivered **Availability** - the impact on customers/business of a loss of service	**17**	C	• **No** **[L]** 0 • Minor – small user group **[L]** 1 • Significant – many users **[M]** 3 • Major departmental system **[H]** 4 • National significance **[H]** 4 • National finances **[H]** 5 • National security **[H]** 5 • International significance **[H]** 6	Risk rating (**L M H**):____ **Score**:_________	A
Reputational impact of failure?	**18**	C	• Minor **[L]** 1 • Significant **[M]** 3 • Major **[H]** 5	Risk rating (**L M H**):____ **Score**:_________	A
What is the value of the contract? Consider the range of financial risk carried by your department – you may need to consult the finance dept	**19**	S	• Less than £50,000 **[?]** • Less than ½ million **[?]** • Up to 5 million **[?]** • Over 5 million **[?]**	Risk rating (**L M H**):____ **Score**:_________	A
Notes, comments: *Use this free text area to note anything relating to Impact and also to note where any modifications to the criterion have been made.*					

Overall Risk Rating:____________ Overall Score:____________

COMMON CRITERIA FOR ASSESING RISK - Worksheet Guidance

CONTEXT

Who owns/is responsible for the information asset?

- **In the dept./organisation**
- **In the supply chain**

Departments/organisations should ensure that there are named individuals, Information Asset Owners (IAOs), responsible/accountable for understanding and managing the risks to the information processed by the supplier. They should also be informed of any further risks to their information when it is handled, stored or processed by the supplier during the lifecycle of the contract.
The supplier should also name an individual to be responsible/a point of contact for managing the Information risks to that information asset during the life cycle of the contract.

Who is the data controller for the personal information assets?

- **In the dept./organisation**
- **In the supply chain**

The Data Protection Act 1998 requires every Data Controller to register with the ICO, unless they are exempt. This applies to both government organisations and suppliers. If a supplier processes personal data under contract for a department (or other organisation) the department is the Data Controller even if the personal data is collected directly by the supplier.

Suppliers may often be data controllers in their own right (for example if they employ staff) and if so should be registered with the ICO. Procurement, contract or security officers may wish to should check that the supplier is registered.

Asset Identification

The type of data/information processed by the contractor (CRITICAL)

All Government information is of value. It is important to consider the sensitivity of the information asset to be handled by the contractor, the nature of the threat to that information, its likelihood and impact. The majority of all personal information/data will be handled within OFFICIAL without any caveat or descriptor. Further information on the sensitivity of the information asset should be sought from the IAO or the individual responsible for managing the risks to that information asset.

The number of data/ records processed/held over the lifetime of the contract? (CRITICAL)

In assessing the risk you should take into account not only the number of data records processed on a daily, weekly or monthly basis to deliver the service but also the total number of records that will be handled, processed and/or stored by the supplier over the life of the contract. Potentially is the threat any different to large volumes of aggregated data that may accumulate over the life of the contract?

The contract should also have an agreed exit strategy setting out how any information held by the supplier will be returned, securely destroyed or archived at the end of the contract.

The information asset may be in electronic or physical form - where will the information asset be held? (CRITICAL)

You should be aware of the location where the supplier is/will be holding your information assets. If it is in electronic form will it be held in the UK or will it be off shored. Departments/organisations proposing to off shore personal information must submit their proposal to the Office of the Government SIRO (OGSIRO) and seek their approval.
There are various off shoring options available, each with differing levels of protection depending on the threat to the information asset. It is important that a risk assessment has been undertaken on the asset before an off shoring option is selected.

The information asset may be in paper format; does the supplier have the required controls necessary to ensure the information asset is adequately protected, e.g. secure storage, access control processes, etc.

Where will the data be accessed from/processed? (CRITICAL)

The information asset may be located on the UK mainland but the supplier may be accessing it from another location in order to deliver the service or process the data. For example if the supplier is delivering a service that customers need access to 24/7 then it is possible that the supplier may have staff or sub-contractors in other countries to provide that service or support services. It is important to establish who will be accessing that data, for what purpose, from where and how, e.g. a cloud service, over the Internet, etc. How these activities are carried out will impact on the risk assessment.

What is the sensitivity or impact of compromise of physical assets being either provided under the contract or being protected under the contract? (Significant)

Contracts for the supply of goods or products should also be assessed for potential sensitivity. For example if a supplier were providing official documentation such as passport blanks or driving licence blanks that would have significant value to criminals or serious organised crime then these assets may be considered as at greater risk.

Will the data be processed on a single site or a number of sites? (Significant)

Services outsourced to a contractor may not always be processed on a single site and may involve the primary contractor or a chain of sub-contractors resulting in information being transferred between sites perhaps on a regular basis, either electronically or in paper format, sometimes without the knowledge of the department/government organisation. The transfer of data, either in electronic or paper format, introduces further risk into the process that will need to be assessed and managed. All sites must provide the required level of protection.

The information asset may be processed in electronic or physical form. (Significant)
Will the supplier process the information as hardcopy?
How will the supplier process the data – on what systems?

Information may be provided to the supplier in hardcopy format for processing/delivery of the service. Will the supplier only process the paper version or will the information be entered electronically onto the suppliers system for processing? Will hardcopy processing be carried out at the supplier's premises or the department/government organisation?
The supplier may process the data in various ways, for example using the department/government organisation's own systems on their site, this will reduce the risk of processing information off site but the department/government organisation will need to assure itself that the supplier's staff are suitably cleared, trained and monitored. The risk assessment should focus on the sensitivity of the information asset and where and how it is processed.

Does the supplier use subcontractors in the delivery of the service? (Significant)

In general a contract for the delivery of a service is between a government organisation and the prime contractor. To deliver that contract the prime contractor may sub-contract some or all of the service delivery. It is important to establish whether the department/government organisation will specify in the terms and conditions that the use of sub-contractors is acceptable/not acceptable and that the supplier undertakes to ensure that the information asset is handled, stored, processed, transmitted, shared and destroyed according to HMG requirements/standards and that they are audited to ensure that they comply with the contract. In addition the prime contractor must agree to notify the department/government organisation of any changes in the supply chain, for example a change in sub-contractor or a change to the service delivery for example a sub-contractor may hold/process information in the cloud.

Does the supplier allow the use of portable media/devices? (Significant)

It is important to establish whether the supplier will use portable media/devices in the delivery of the service. More importantly whether the supplier allows staff and sub-contractors to use portable media/devices in the workplace and whether they have a policy that defines their use and processes and controls in place to manage the risk.

Does the supplier allow the use of bring your own device (BYOD) e.g. supplier's staff can use their own ICT? (Significant)

Organisations need to consider whether the supplier and any sub-contractor allow the use of privately owned devices (BYOD) to store or access information assets. BYOD presents a number of challenges, including how the device will be managed, whether the data held on the device can be adequately protected and if the data held on the personal device can be securely sanitised. There are also a number of legal issues surrounding the use of privately owned devices to store or process personal data for work purposes, which are discussed on the ICO website. Departmental/organisational information is still subject to FOIA even if held on a personally owned device. The risks associated with privately owned devices are explained in greater detail in CESG Good Practice Guide 10 (GPG 10), Remote Working.

Notes, comments:

Use this free text area to note anything relating to Asset Identification, particularly areas that have or will have an impact on how the risks will be or are managed and also to note where any modifications to, additions or deletions of criterion have been made.

Asset Management Processes

Will the supplier have access to a live departmental system/database or to an offline extract, and is that data modified updating departmental systems, master records, ledger balances etc? (CRITICAL)

If the supplier and/or any of the subcontractor's staff are to be granted direct access to the organisation's live systems this will increase the risks to the integrity and confidentiality of the data. You should ensure that sufficient background checks are carried out all employees, by your supplier. If you have any sensitive data you need to ensure it will not be put at risk. It is vital to put in place control measures to manage how the supplier will access your information ensuring limited access rights are given to supplier's staff.

How many of the supplier's staff will have access to read/write/update/delete/generate/transport the data? (Significant)

The higher the number of the supplier's staff handling your information the greater the threat posed to your information. You should know precisely what information is being handled by the supplier and the impact should there be any breaches or loss in terms of CIA.   You also need to be clear about what the supplier's employees will be doing with your information. If they are going to update or modify your records how will you check the integrity of the information once it has been handled/processed by the supplier? If the supplier's employees will be modifying data the level of access granted must only support the business activities in regard to the contract, whether it is to access, transfer or process information. Access rights must apply to individual staff and their roles only. If the data is to be transferred you need to check how it will be done.

Consideration around the security of that information whether it is electronic or in paper format must be given.

It also important to ensure proper management of unauthorised access including management of user accounts e.g. joiners, leavers and internal moves. When staff move on are their access rights revoked? Protective monitoring is one method to help prevent breaches in security. You should also ensure that all your supplier staff receive information security risk awareness training and that it is current.

Are there any existing accreditations or certifications that can provide evidence of information security controls e.g. RMADs, ISO27001, PSN CoCo, G-Cloud Accreditation, Information Security Management Systems (ISMS) etc? (Significant)

Organisations should consider whether the supplier has any existing and relevant accreditation or certification from one of the commercially recognised standards for information security management. Organisations must consider the scope of the accreditation/certification held, and whether it is relevant or appropriate or proportionate for the service which they will be or are delivering and whether additional controls or requirements are needed to strengthen existing controls for the secure delivery of the contract

Is data transferred between the department/govt organisation and suppliers during the life of the contract? (CRITICAL)

If data or information is transferred between the organisation and the supplier, the type and quantity of the data transfer needs to be assessed. If the transfer is regular and in bulk then the process is likely to be better controlled and understood than if it were small amounts transferred ad hoc.

Consideration needs to be given on how the data will be transferred; over secure networks or unsecured networks or via removable media. Key areas to consider are the appropriate level of security and grade of encryption used. A risk managed decision should be taken and the permission of the SIRO or IAO obtained. This requirement is applicable to all information types where there is a need to protect the confidentiality and/or integrity of the data. It is vital to know how much data will be transferred, to whom, and the frequency of the transfers.

A risk assessment must be undertaken to determine the specific technical controls needed to protect aggregated data sets – this will include an understanding of how aggregation affects threat. Technical controls to protect an aggregated data set should be robust and risk owners may decide that they require a higher level of assurance or additional technical capability.

Another important consideration is the number of transfers down the supply chain from prime contractor to sub-contractor(s).

Consider whether the transfers are:

- In bulk or small amounts; regular or ad hoc.
- In electronic form or hard copy/paper.
- Only between the dept and the supplier or between the supplier and one or more subcontracts.

During the transfers are there any risks to:

- Confidentiality e.g. the loss of data and DPA consequences
- Integrity e.g. the potential for data to be altered/tampered with

- Availability e.g. loss of service, failure to maintain business continuity

Will the supplier need to provide secure retention/storage/archiving and destruction of Authority data/documentation from completion of customer deliverable or beyond the end of the contract for a set period of time? For how long? For what reason? (Significant)

You must consider treatment of the information at the end of the contract i.e. when the data is no longer required for its intended use or purpose and, after the contract has ended, whether the supplier will retain, return or destroy the data/information. The organisation should also consider where or whether it has space to store any returned data.

If the supplier is retaining the data how will it be stored and digital continuity maintained. If the data is being returned, in what format and by which method and will proof be needed that the data has been removed from the suppliers systems. If the data is to be destroyed, will it be disposed of in accordance with HMG IS 5 and how will this be verified.

The numbers of transfers down the supply chain for this contract, i.e. starting from the prime supplier down to the final subcontractor. (Significant)

Many prime suppliers also sub-contract. If your supplier intends to subcontract you need to be aware of how far down the supply chain your information assets or physical asset will be transferred. Taking into account the risks, the further down the supply chain the further removed from your organisation and there is potential for less control of risk. You need to consider how you will gain assurance from your supplier that there is sufficient risk management in place further down the supply chain and you may request that you are kept informed when changes take place, i.e. a new subcontractor replaces an existing one.

Are there particular risks or concerns relating to volume, confidentiality, integrity or availability of data being transferred at the start or the end of the contract? (Significant)

Organisations need to consider the life cycle of information assets in terms of C, I, A from the start of the contract up to the end of the contract. Key areas to be considered are; what information was given to the supplier at the start of the contract? What information has been processed, changed or updated and is the organisation getting back the complete information asset from the supplier at the end of the contract. Is it complete during migration? Is it usable? Is it like for like and how can this be tested?

Consider whether:

- There will be a parallel run and how long will this be
- It will involve one or more government bodies.
- How much data will need to be migrated and the complexity of migration

- Any updates required and their frequency
- What happens if the contract needs to be terminated prior to the end of the contract due date, for example due to major incidents or take over or insolvency of the company.

Impact

Significance of the contract to the department, will disruption impact on delivery of a high profile service? (CRITICAL)

From your organisation's viewpoint what is the significance of the contract in terms of business criticality and the impact on delivery of the service, for example for DWP payments of Universal Credit is business critical. Should an online service fail or be disrupted the impact on its customers might be critical, e.g. customers would not receive their payments on time. If this were to happen it would perhaps also attract attention from the press. Consider how critical the service is to your organisation and what would be the impact if the service was to fail.

Consider the following:

- **Confidentiality –** the potential harm/distress to individuals and reputational impact on the dept of a loss or compromise of information/data
- **Integrity –** impact of a compromise to the quality of service delivered, e.g. incorrect patient information given to a doctor
- **Availability** - the impact on customers/business of a loss of service

Reputational impact of failure? (CRITICAL)

Security breaches and failure of service can result in significant negative visibly for HMG and other organisations. The reputational and financial damage that incidents can cause highlights the need to manage the risks. You should consider the impact on your organisation in terms of its reputation should there be a failure in service or significant security breach during the delivery of the service. You need to ensure your supplier has a strategy in place to effectively recover from any such failure. The supplier should have Disaster Recovery and Business Continuity plans in place so that the service can be restored within the shortest time possible following the failure.

What is the value of the contract? (Significant)

Consider the value of the contract in terms of the overall budget of the organisation. The values given will represent a variable amount in terms of the risks for individual organisations. For example MOD may consider an amount of less than ½ million as a rather small amount in comparison to its overall expenditure. Consider the range of financial risk carried by your organisation – you may need to consult your finance department.

Glossary

Accreditation		Accreditation is a formal independent recognition of competence to perform specific tasks.
Assurance		Information Assurance (IA) describes the steps taken to gain confidence that the control measures protecting the confidentiality, integrity and availability of systems and services are effective and that these systems and services will protect the information they carry and will function as they need to, when they need to, under the control of legitimate users.
BYOD	**BYOD**	Bring your Own Device – the policy of permitting employees to bring personally owned mobile devices (laptops, tablets and smart phones) to their workplace and use those devices to access the organisation's information and applications.
Certification		Certification is a comprehensive evaluation of the technical and non-technical security controls on an information system to support the accreditation process. It establishes the extent to which a particular design and implementation of an approved set of technical, managerial, and procedural security controls have been implemented.
CIA	**CIA**	Confidentiality – preventing the disclosure of information to unauthorised individuals or systems. Integrity – maintaining and assuring the accuracy and consistency of data over its entire life cycle. Availability – the information must be available when it is needed.
CoCo	**CoCo**	Code of Connection – The CoCo is a mandatory set of technical and procedural requirements that must be demonstrated to have been met before systems can connect to a government system, e.g. PSN.
Data Controller		Data Controller means a person who (either alone or jointly or in common with other persons) determines the purposes for which and manner in which personal data, are, or are to be, processed. Data Controllers must ensure that any processing of personal data for which they are responsible complies with the Act.
Data Protection Act	**DPA**	The Data Protection Act regulates the processing of personal data. *See 'Key Definitions of the Data Protect Act'* @ www.ico.org.uk.
Government Cloud	**G-Cloud**	A cloud is a collection of computers and servers accessed via the internet or a private network. It includes Infrastructure, Platforms and Applications that can be accessed from a range of devices and locations. The G-Cloud is an ongoing programme of work that will enable the use of a range of cloud services throughout the public sector.
ICT	**ICT**	Information and communications technology often used as a synonym for IT, it refers specifically to the integration of telecoms, computers, software, storage and audio-visual systems that enable users to access, store, transmit and manipulate information.

Information Asset		A body of information, defined and managed as a single unit so it can be understood, shared protected and exploited effectively. Information assets have recognisable and manageable value, risk, content and lifecycles.
Information Asset Owners	**IAO**	Information Asset Owners are senior individuals involved in running the organisation's business. Their role is to understand what information is held, what is added and what is removed, how information is moved, and who has access and why. As a result they are able to understand and address risks to the information.
Information Security Management Systems	**ISMS**	A set of policies concerned with information security management or IT related risks (e.g. ISO 27001). The governing principle is that an organisation should design, implement and maintain a coherent set of policies, processes and systems to manage risks to its information assets, ensuring acceptable levels of information security risk.
ISO 27001	**ISO 27001**	An international standard that formally specifies a management system intended to bring information security under explicit management. It has 11 domains or topic sections and mandates specific requirements.
Off shoring		Offshoring is the term often used to describe the sourcing of technical or administrative services outside of the home country. It is also frequently used to refer to the processing and storage of data in locations other than in the country of original or in the cloud. Proposals to offshore any data must be made according to the guidance published by the Office of the Government SIRO (OGSIRO) on GOV.UK website.
Office of the Government SIRO	**OGSIRO**	The Office of the Government SIRO (Senior Information Risk Owner) was established to support the Government in setting and managing its appetite for information and cyber risk.
Public Sector Network	**PSN**	A UK Government programme to unify the provision of network infrastructure across the public sector into an interconnected 'network of networks' to increase efficiency and reduce overall public expenditure.
RMADS	**RMADS**	The Risk Management and Accreditation Document Set should provide justification and accountability for risk management decisions, the basis for risk management, accreditation and day to day security procedures and a benchmark for compliance
Senior Information Risk Owner	**SIRO**	The SIRO is a Board member who is accountable for the organisation's management of information risk.
The European Economic Area	**EEA**	The European Economic Area (EEA) comprises the countries of the European union plus Iceland, Liechtenstein and Norway.