Cabinet Office

Supplier Assurance Framework: Good Practice Guide

Version 1.1 – May 2018

Version History

SPF Version	Document Version	Date Published	Summary Of Changes
13.0	1.1	May 2018	Changes in data protection legislation reflected.

Contents

ANNEXES

Background to the Supplier Assurance Framework

In June 2012 the Information Working Group (IWG) established the Industrial Security Working Group (ISWG) to address a set of common issues reported by departments in their annual returns to the Cabinet Office. These were:

- A lack of consistency in government's approach to suppliers;
- The need for a common standards related question set;
- Greater transparency to drive up accountability;
- Standardised contractual terms;
- The acknowledgement that not all suppliers are the same and some services carry potentially greater risks than others so the degree of assurance required may be greater.

The ISWG was given a remit to develop a more **straightforward, proportionate** and **transparent** overall approach to supplier information assurance that will:

- Raise standards, enhance existing capabilities and generate capacity through shared service approaches in line with the '*do once, do it well and reuse'* philosophy;

- Reduce the cost and complexity of interacting with industry, helping to open up government markets to small and medium enterprises (SMEs);

- Minimise the compliance monitoring burden on departments through greater use of standard commercial approaches;

- Improve suppliers' understanding and application of information risk management and enhance accountability.

This good practice guidance has been developed by a group of experienced practitioners from across government including – BIS, CESG, DWP, Education/CLG, Government Procurement Service, HMRC, Home Office, Met Office, MoD, MoJ, National Police Improvement Agency (NPIA now part of Home Office), NHS/Dept of Health and SOCA.

In essence the Supplier Assurance Framework is an approach to managing supplier risk built around two tools and good management practice principles. It is intended to provide assistance to departments and government organisations and while it will be incorporated into the SPF its use is not mandated.

The supplier assurance framework delivers on its remit by:

✓Providing a flexible yet consistent approach to managing information risk in third party supplier contracts at the OFFICIAL level.

✓Being adaptable and light touch; it can accommodate an organisation's existing processes and governance structures and can be implemented in stages over time.

✓Providing corporate visibility of risk by bringing together **business, commercial** and **security** staff in aligning the proportionate management of information risk to the organisation's risk appetite and levels of risk tolerance.

Cabinet Office
October 2013

1. The Supplier Assurance Framework

Supplier Assurance Framework Overview

The supplier assurance framework applies to contracts at the OFFICIAL level. It should: enable the early identification of high risk projects; provide a framework for the risk management of contracts that is consistent, light touch but effective, understood by both government Stakeholders and suppliers and enable information sharing and accountability; and inform the assurance approach taken to high, medium and low risk contracts. It can be adapted for use in the wider government community as it allows organisations to interpret and apply it according to their business needs; it is particularly relevant where information is shared through contracts or agreements.

The Purpose of the Supplier Assurance Framework

The supplier assurance framework should provide corporate visibility of risks arising from OFFICIAL contracts with third party suppliers and confidence that they are being effectively identified and proportionately managed. It will facilitate better targeted risk management by:

- giving government **a consistent proportionate baseline** for risk assessment and approval of suppliers
- **providing a flexible framework** for departments and wider public sector organisations to adapt to suit their business needs
- facilitating **a co-ordinated and consistent approach** to assessing and determining security across business, commercial and security specialisms
- being **proportionate and cost effective** in terms of its application and in the security controls that are assessed as required from a supplier
- **assisting SIROs and IAOs** in better understanding and managing the risks to their information assets
- facilitating the **identification and proportionate management of risk in contracts**; and the better prioritisation of resources
- helping project teams to **determine proportionate security requirements** and supplier risk management arrangements
- **devolving responsibility** appropriately for business, commercial and security risk management **throughout the department/organisation**
- **including** physical security, business continuity, cyber, personnel and information security **aspects of outsourcing that all impact on the risk management of the asset**
- **helping suppliers to better understand** and work cooperatively with the business on proportionate security controls
- **providing Plain English guidance** for suppliers, including SMEs, and promoting healthier commercial offerings
- supporting a risk management **approach consistent with the HMT Orange Book** and provide evidence for Internal Audit to derive assurance

- **complementing other assurance and reporting processes** such as the Security Risk Management Overview (SRMO) and the Information Governance Toolkit reporting.

Supplier Assurance Framework

The framework is intended to bring together those areas of the organisation that have responsibility for or a business interest in the proportionate and consistent management of information risk. It supports de-duplication of effort and better targeting of resources; ;for example if a security unit had requested an SoA (Statement of Assurance) assessment but received no response then contracts branch would follow up with a reminder as part of their routine supplier contact. A consistent, co-ordinated approach would help to regularise suppliers' expectations and experience of the assurance process and would be likely to gain their buy-in.

It will help to identify good practice that could be adopted throughout organisations and widely shared across the community.

The framework provides a flexible structure capable of being adapted by organisations to meet their business needs, it is not prescriptive, overly detailed or process orientated. The structure has 8 key elements:

- **Identification of contracts or engagements with suppliers**
- **Identification of the contracts that need to be risk assessed**
- **Identification of who should be involved in and carrying out the Common Criteria for Assessing Risk (CCfAR) assessment**
- **Getting a strategic perspective on risk**
- **Moderation of CCfAR responses**
- **Summarisation of responses at relative risk levels**
- **Implementing an assurance programme**
- **Review of the process**

First steps – what already exists?

An initial assessment should be carried out to identify existing processes within the business, commercial and security units that can be adopted or adapted into the framework. Information sources such as – information asset registers (IARs), risk registers, contract lists – should be identified and existing governance structures, roles and responsibilities – IAOs, accreditation, annual SRMO reporting, procurement processes – highlighted and built into the framework.

Suggested areas to explore:

- How mature is the organisation's management of risk: Does it know what its information assets are? Does it have current risk registers? Does it have a corporate risk appetite?
- Are there any collated information stores: Are there lists of information assets or information asset registers (IARs). Who are the Information Asset Owners (IAOs)? Are there lists of contracts or suppliers? Who keeps or maintains these lists?
- Are there roles and responsibilities for reporting: Do IAOs have to provide risk assessments to the SIRO? Do accreditors routinely report major risks to the SIRO for their acceptance? Are IAOs involved in incident management?
- What assessment/assurance processes are already in place: Do business, commercial and security have assurance processes? How consistently are they used?
- What are the outcomes of assurance/assessment processes: Are reports produced? How widely are they shared? Are they routinely shared outside the unit for example with the Audit Committee or Board?

Researching these areas at the beginning may reduce duplication of effort later on and identify good practice already in place that can be replicated elsewhere.

A: Identification of contracts or engagements with suppliers

Some organisations have a considerable numbers of contracts with suppliers. The framework will be built up over time; a gradual approach will allow organisations to refine the key elements, bring others on board and build in any lessons learned while moving forward.

Lists of contracts may not be held centrally but within the individual project teams responsible for managing them. These lists provide a useful starting point and the people that manage them a valuable source of information.

B: Identification of the contracts that need to be risk assessed

Identify a small subset of these contracts. Attempting to tackle too large a group of contracts will be very resource intensive and allow no time to assess progress and make adjustments. A small set of high-risk contracts successfully managed through the framework will demonstrate to seniors the effectiveness of this approach.

To prioritise a contract set some criteria need to be agreed. Potential candidates for **inclusion** might be contracts that:

- handle personal data – in large quantities or include particularly sensitive personal data
- are business critical – they deliver key services to the public or would severely impact the organisation's ability to function if they were unavailable or their integrity was compromised
- manage departmental assets
- appear on corporate risk registers
- have suffered a serious incident, security breach or data loss.

Criteria for **exclusion** might be:

- the type of contract – e.g. facilities management where little or no data is involved or it is purely a goods type contract
- the contract has very little time left to run and will not be re-competed.

Once the criteria have been agreed they should be applied consistently to the contract set.

C: Identification of who should be involved in & carrying out the CCfAR assessment

Using the **Common Criteria for Assessing Risk** (CCfAR), a set of outline criteria for assessing risk in third party supplier contracts at the OFFICIAL level, organisations can broadly group them into 'high' 'medium' and 'low' risk services. For greater detail see related document, 'Using the CCfAR'. CCfAR assessments offer the greatest benefit where there is input from business, commercial and security representatives. Within each of these areas there maybe a variety of potential contributors for example:

Business – IAOs, key users, service/system SRO
Commercial – contracts managers, procurement team, legal
Security – DSO, IT manager, IA, accreditor

It is only important that there is a representative from each of these areas not that every role is represented. However security should be represented by someone with the relevant security experience.

D: Getting a strategic perspective on risk

Contracts need to be assessed in their strategic context. Specialist areas view risk from their particular perspective, contracts managers will focus on contractual issues, broadly the risk of non delivery or delay, the supplier going out of business, value for money etc.

There needs to be an overall assessment of the value of the contract to the organisation as a whole in relation to the integrity, availability and confidentiality of the service provided and the business impact on that organisation should that service be lost or compromised. The resultant risk mitigation strategy should align with the organisation's risk appetite.

For high risk contracts it may be the SIRO that provides a strategic perspective; however it is critical that the business has input to the CCfAR assessment.

E: Moderation of CCfAR responses

When all or a significant proportion of the contracts in the set have been CCfAR assessed their overall accuracy and outcomes should be subjected to a reality check. Expertise in carrying out this exercise will mature over time and be refined by experience.

- The first step is to be confident that the responses to the questions are accurate. This is to identify any major inconsistencies or inaccuracies, smaller inaccuracies are unlikely to be easily found and will most likely have little impact on the overall assessment
- The next step is to review the emerging results to ensure a similar approach has been adopted and to sanity-check them. Reviewing the scoring isn't essential as it will vary according to who has carried out the assessment. Concentrate on any which feel subjectively to be over or under-valued and examine these responses for consistency with others.
- Finally, map the contracts to the organisation's broad risk tolerance level/risk appetite; are these high risk contracts providing services or products ones that the organisation views as critical? If they are, are they on the risk register. If not then what impact might this have on how they are managed?

F: Summarisation of responses at relative risk levels

Following moderation the responses should be gathered together in one place in a ranked list, i.e. all the high risk contracts, all the medium risk contracts and all the low risk contracts.

The top 20% will provide a picture of who are the organisation's key suppliers and a review of these contracts will assist in identifying trends and flagging issues.

G: Implementing an assurance programme

A proportionate approach to the supplier assurance process can now be adopted based on the Statement of Assurance (SOA).

High risk contracts:

- IA self assessment - completion of the SoA by the supplier (including responses from suppliers regarding their measures employed to protect data against the key SoA areas).
- review of the return and any requests for further evidence
- an audit carried out to validate the response and evidence provided

Medium risk contracts:

- IA self assessment - completion of the SoA by the supplier (including responses from suppliers regarding their measures employed to protect data against the key SoA areas)
- review of the return and any requests for further evidence
- at an agreed period, e.g. every 3 years, an independent validation of the IA self assessment

Low risk contracts:

- *IA self assessment - completion of the SoA (simple responses to the key SoA areas)*

Using a common question set such as the SoA provides a consistent approach although it can be modified to meet the needs of the individual contracts. For instance, where delivery of a contract does not involve a technical element, other than incidental use of IT by a supplier; some technical elements may be removed. Further details on the SoA process are contained in the related document, 'Using the SoA'.

The SoA responses when reviewed will provide the basis for a report/submission to the SIRO that briefly:

- outlines the risks and implications of those risks to the business – confidentiality integrity and availability (CIA)
- demonstrates how the risks are being managed particularly in relation to CIA
- sets out the risk appetite that is being adopted in the management of risk in these contracts
- provides confidence that the risk management strategy is achievable and cost effective.

The submission will ask the SIRO to agree the approach including the acceptance of risk appetite assumptions. The board may want to approve the management of high risk systems.

SoA Tool

To manage high volumes of SoA returns, capture and analyse the responses and flag issues a paper or spreadsheet based approach may not be viable. A tool would provide consistency of approach and allow for information to be more readily shared, for example a supplier providing the same service to more that one organisation would only need to complete one return not one for each organisation. SoA returns captured on a widely available tool could provide a basic means of achieving supplier accountability. The dependency here is that the contracts are delivering the same service therefore the level of risk is comparable.

Currently there are no plans to develop a SoA tool centrally.

Presenting the SoA to suppliers

Suppliers should be briefed on the SoA, its purpose and role in the assurance process. This might be done during informal discussions or at supplier briefing days, though these events are often resource intensive to organise. Open and fair competition must prevail and can be achieved; for instance, as part of premarket engagement, however the organisation needs to ensure that the responses to any queries raised are shared among all the suppliers.

H: Review of the process

The assurance process (SoA) responses, in particular for high risk contracts, should be reviewed by business, commercial and security representatives.

Suppliers who have been part of this process should receive feedback, for low risk contracts it may be a thank you for taking part and a very brief summary of the risk management process and its importance to the organisation. If suppliers are managing the risks well it is important that this is acknowledged.

There may be several outputs from the assurance process, these might include:

- a residual risk statement
- a security plan template and subsequent completion by the supplier/a summary report to feed into the security plan
- a summary report for compliance processes, e.g. the SRMO
- a report to the SIRO – requesting acceptance of the risk appetite assumptions
- a trend analysis
- review of contract clauses (T&Cs) for future contracts
- actions/recommendations
- improvement plan
- supplier feedback

Overall the assurance process itself should be reviewed, lessons learned and changes implemented where necessary.

Information gained should be fed back into internal processes, for example the model terms and conditions (T&Cs) reviewed to include the requirement for suppliers to undertake and return annual assessments, or not to change service provision – putting data into the Cloud – without seeking the organisation's consent, etc.

It is important that the information generated from all elements of the supplier assurance framework **is organised and stored** in a central area, available to business, commercial and security staff. It should be used as a repository of information and evidence that can be drawn on by auditors, procurement teams, contract managers, IAOs, accreditors and others and have the potential to be shared with other organisations operating or looking to undertake similar contracts. The assumption is that information will be added to year on year.

Summary

The supplier assurance framework provides a flexible yet consistent and coordinated approach to managing information risk in third party supplier contracts. It is adaptable and can accommodate existing processes and governance structures. It unites business, commercial and security staff in aligning the proportionate management of information risk to the organisation's risk appetite.

Appendix A

Supplier Assurance Framework Checklist

Supplier Assurance Framework - Summary

The supplier assurance framework provides a flexible yet consistent approach to managing information risk in third party supplier contracts at the OFFICIAL level. It is adaptable, light touch, can accommodate an organisation's existing processes and governance structures and can be implemented in stages over time. It provides corporate visibility of risk by bringing together business, commercial and security staff in aligning the proportionate management of information risk to the organisation's risk appetite.

Supplier Assurance Framework Checklist

□ **FIRST STEPS - Identify existing processes**

- ✓ Are there any existing business, security, commercial processes or information sources that can be adopted or adapted into the framework?

□ **A: Identify contracts or engagements with suppliers**

- ✓ Identify a list of contracts;
- ✓ Identify who owns or managers that list.

□ **B: Identify the contracts that need to be risk assessed**

- ✓ Agree criteria to be used to prioritise the contract set;
- ✓ Apply the criteria consistently to the contract set.

□ **C: Identification of who should be involved in & carrying out the CCfAR assessment**

- ✓ Get representatives from the business, security and commercial areas for the CCfAR assessment;
- ✓ Explain the purpose of the CCfAR assessment and their role in ensuring that the risk is identified and properly managed;
- ✓ Conduct the CCfAR assessment and agree the outcome (high, medium, low risk);
- ✓ Inform the IAO of the outcome of the CCfAR assessment.

□ **D: Get a strategic perspective on the risk assessment**

- ✓ Seek the views of a senior business stakeholder(s) on whether the outcome of the CCfAR assessment, for high risk contracts, aligns with the organisation's risk appetite; what would be the business impact on the organisation if the service was unavailable or information was lost or compromised.

□ **E: Moderate CCfAR responses (compare a group of responses)**

- ✓ Identify any major inconsistencies in responses to the questions;
- ✓ Review the emerging results/outcomes to ensure a similar approach has been taken; identify any which appear to be over or under valued;
- ✓ Map the contracts to the organisation's risk appetite; are the high risk contracts providing products or services that the organisation regards as business critical?
- ✓ Check the risk register; are these contracts already listed or do they need to be entered on the risk register?

□ F: Summarize responses at relative risk levels

- ✓ List in one place in ranked order all the high, medium, low risk contracts;
- ✓ Review the top 20% to identify who are the organisation's key suppliers.

□ G: Implementing an assurance programme – Statement of Assurance (SoA)

- ✓ Agree format for the organisation's supplier assurance process, e.g.

  High risk contracts:
  - SoA self assessment
  - review return and request further evidence
  - audit to validate the response and evidence provided

  Medium risk contracts:
  - SoA self assessment
  - review return and request any further evidence
  - at an agreed period an independent validation of the SoA self assessment should be commissioned by the supplier

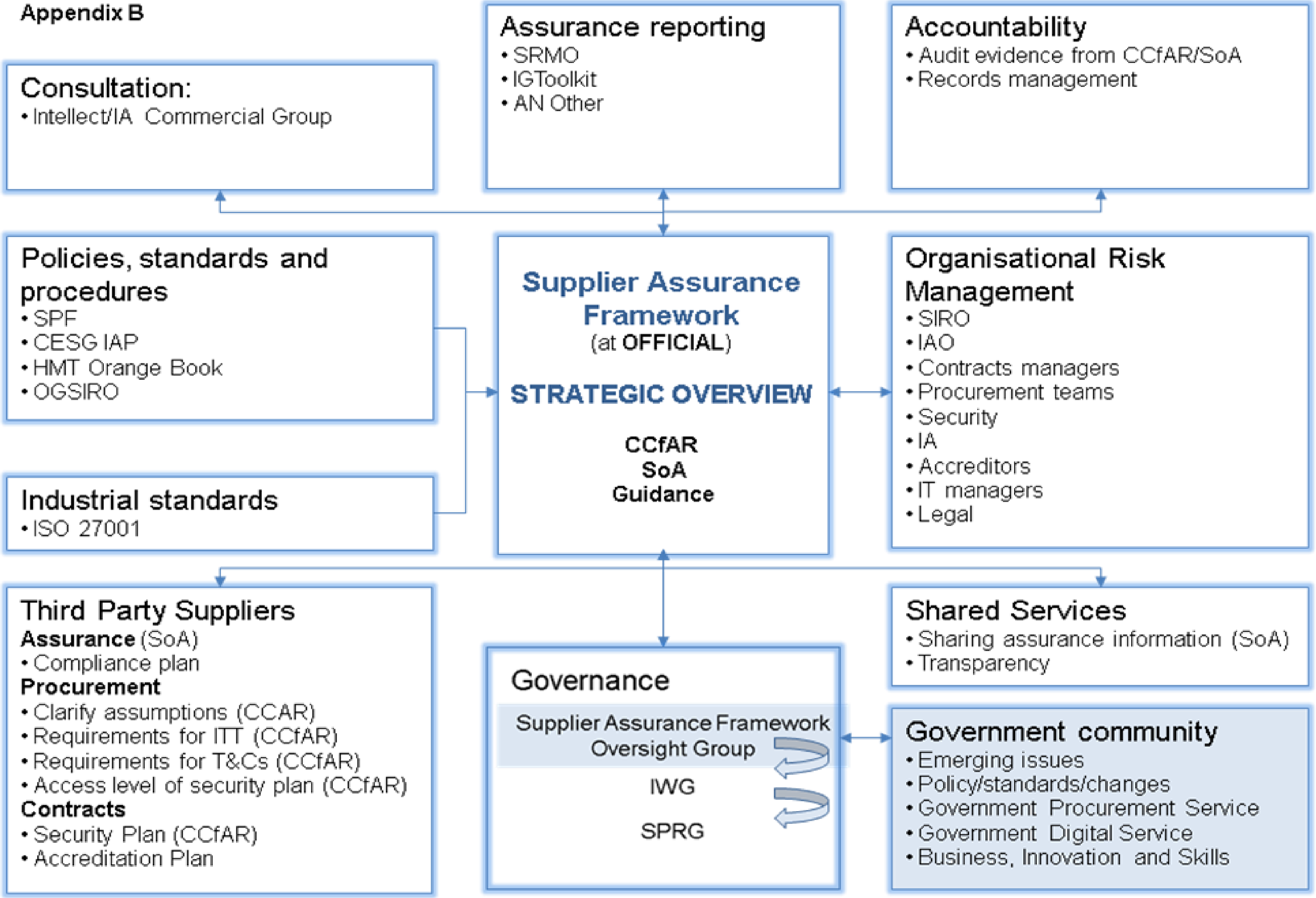
  Low risk contracts:
  - SoA self assessment;

- ✓ Identify a lead for managing the supplier assurance process;
- ✓ Prioritise contracts;
- ✓ Review available resources to carry out the supplier assurance process;
- ✓ Decide how the SoA will be made available to suppliers;
- ✓ Brief suppliers on the purpose of the SoA and the wider supplier assurance framework;
- ✓ Review SoA returns and other evidence from the supplier assurance process.

□ H: Review of the process

- ✓ Business, commercial and security representatives review the assurance process responses, particularly for high risk contracts;
- ✓ Suppliers receive feedback;
- ✓ SIRO receives an executive summary of the outcomes and the proposed approach to managing the risks going forward;
- ✓ SIRO agrees/challenges the approach and accepts/rejects risk assumptions
- ✓ Outputs produced including a summary report for compliance processes, e.g. the SRMO
- ✓ Participants review the process and implement necessary changes;
- ✓ Lessons learned fed back into internal processes, e.g. into model contract terms and conditions;
- ✓ Information generated from the supplier assurance process organised and stored in a central area available to business, security, commercial and procurement staff.

Appendix B



Consultation:

- Intellect/IA Commercial Group

Assurance reporting

- SRMO
- IGToolkit
- AN Other

Accountability

- Audit evidence from CCfAR/SoA
- Records management

Policies, standards and procedures

- SPF
- CESG IAP
- HMT Orange Book
- OGSIRO

Industrial standards

- ISO 27001

Supplier Assurance Framework
(at **OFFICIAL**)

STRATEGIC OVERVIEW

CCfAR
SoA
Guidance

Organisational Risk Management

- SIRO
- IAO
- Contracts managers
- Procurement teams
- Security
- IA
- Accreditors
- IT managers
- Legal

Third Party Suppliers

Assurance (SoA)

- Compliance plan

Procurement

- Clarify assumptions (CCAR)
- Requirements for ITT (CCfAR)
- Requirements for T&Cs (CCfAR)
- Access level of security plan (CCfAR)

Contracts

- Security Plan (CCfAR)
- Accreditation Plan

Governance

Supplier Assurance Framework Oversight Group

IWG

SPRG

Shared Services

- Sharing assurance information (SoA)
- Transparency

Government community

- Emerging issues
- Policy/standards/changes
- Government Procurement Service
- Government Digital Service
- Business, Innovation and Skills

2. Using the Common Criteria for Assessing Risk (CCfAR)

Purpose

The **Common Criteria for Assessing Risk** (CCfAR) is a set of outline criteria for departments and government organisations to use when assessing risk in third party supplier contracts at the OFFICIAL level (including OFFICIAL-SENSITIVE). Contracts at SECRET and above are subject to List X processes.

The criteria are intended to assist departments and government organisations in assessing the risk level in OFFICIAL contracts and broadly group them into ‘high’ ‘medium’ and ‘low’ risk services. Validation of these assessments will be gained over time depending on how the CCfAR is utilised as part of either the procurement cycle or the annual supplier assurance process.
The level of risk carried by a service or product will be an indicator of the level of assurance required by department or government organisation from the supplier on how that risk is being managed. For example a department or government organisations may accept an annual self assessment from a supplier providing a low risk service or product but will require more information from and interaction with a supplier providing a self assessment for a high risk service or product.

Principles

The CCfAR was designed by a group of departmental practitioners 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.

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

Using the CCfAR

To illustrate how the CCfAR might be implemented in government departments or organisations outlined below are two scenarios identified by the CCfAR working group.

Scenario A – **The CCfAR can be used by departments or government organisations to risk assess existing contracts at OFFICIAL, i.e. below the current List X criteria, and broadly group them into 'high' 'medium' and 'low' risk services. Those identified as 'high' risk should, as a priority, be included in the annual assurance report to the CO, the Security Risk Management Overview (SRMO).**

Broadly grouping all the contracts won't be achieved in one go (you may have more contracts than you realise), this is a progressive process and to get the most from it some planning is required before you begin.

:

- **Start** by deciding which part of the department/organisation is leading the CCfAR assessment e.g. Security, IA, Contracts etc. The lead branch/unit/area will probably be the one with the most to gain from undertaking this work.

- **Agree** the outcome, including: the number of contracts to be looked at, the timescale, the likely people involved, whether you are only concerned with particular or high risk contracts, what information you will have at the end, who you will share it with and what other processes it will inform or feed into. It is important to get the right scope and that it is achievable.

- **Initially select** a sample group of contracts that are likely to meet your requirements, to help develop an understanding of the process and gain confidence in using it.

- **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, as you are unlikely to have all the information you need.

- **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, below are some of the various options to consider:

    - How many of the key stakeholders (business, contracts, security, IT etc) are necessary for a productive discussion of the CCfAR for the contract(s)? What will be the impact of a key stakeholder not attending?

    - Where a key stakeholder is unavailable can you seek their views separately and feed them into the discussion?

    - DO NOT send the form out to stakeholders it is not designed for stand alone use.

    - The CCfAR has 20 criteria, 9 critical and 11 significant, will you:

        - Use all 20 criteria
        - Tailor them according to the contract
        - Use only the 9 critical criteria
        - Use or not use the scoring mechanism

    - Does the agenda allow participants sufficient time to produce an outcome and review it? Specifically – were the outcomes as expected, do they provide confidence that the process is effective, what did they gain from the process and who else could this information be usefully shared with e.g. IAO or SIRO?

- **Review** the information gathering process against the outcome, was it effective, can you repeat it, which stakeholders benefited, what did you learn that you didn't know before about your organisation, did you spot any trends emerging, who should you usefully share the information gathered with 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 have 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 are likely to be the business/IAO, security, IA, legal, IT, accreditors, etc. dependent on the level of risk identified in the contract.

As part of the risk assessment a discussion based around the CCfAR with the key stakeholders will provide information to support each of the 7 bullet points above.

For contracts likely to be assessed as high risk the IAO responsible for the information asset, as business risk owner, should be informed of the likelihood of the risk and its impact on the confidentiality, integrity and availability of the asset. They should consider whether this aligns to the organisation's risk appetite (if known) and if they accept the risk.

Contract award

At contract award the business will have fully understood and fleshed out the requirement, the assumptions will have been replaced by solutions and detail on how the service/product will be delivered; the organisation will have a better understanding of the risk.

Also the supplier will be known and the organisation can work with them 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

Key stakeholders at this stage are likely to include the contract manager, procurement, the business/IAO, security, legal, IA, accreditation and IT depending on the services/products provided under the contract.

The Procurement/Contract manager or security staff may lead a discussion with the key stakeholders to revisit the original CCfAR assessment and update it in the light of the contract award. The group

should consider an overall risk assessment for the contract – high, medium or low – and ensure all interested parties are kept informed of the status of high risk contracts, particularly the IAO, of the likelihood of the risk and its impact on the confidentiality, integrity and availability of the asset. For high risk contracts in particular the IAO should consider whether the assessment aligns with the corporate risk appetite and whether they accept the risk.
The outcomes of the CCfAR reassessment should be shared and stored for use in the next stage of the cycle.

Contract management
Contracts, particularly high risk contracts, are subject to an annual review process with the supplier. For example 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 in the Security Risk Management Overview (SRMO). The department or government organisation may review the security plan with the supplier or it may choose to request that the supplier completes a Statement of Assurance (SoA). The SRMO process is undertaken by the departmental security officer (DSO) in partnership with the SIRO.

It is important to review high risk contracts as part of a regular assessment process. To make best use of resources contract managers may select a group of high risk contracts by category e.g. all contracts that off shore information or manage very high volumes of data or employ a large subcontractor delivery chain or have had a number of data loss incidents over past year. In departments the review of these contracts should form part of the SRMO assurance process.

Key stakeholders are likely to include contract managers, security, IA, business/IAOs. Discussions with stakeholders following the assessment will be used to identify emerging trends, review the CCfAR risk assessment and update the CCfAR record for the contract.

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.

End of contract
Before the contract reaches its end, 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.
Contract managers and security staff will need to have input to a plan where high risk assets are involved.

Key stakeholders are likely to include contract managers, security staff, procurement, IA and IT. They should revisit the CCfAR and 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. SUPPLIER ASSURANCE FRAMEWORK – CCfAR 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 asset?			• **In the dept./organisation** • **In the supply chain**	See CCfAR guidance for further information	
Who is the data controller for the personal information assets?			• **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 data protection legislation 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 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 may be in **electronic** or **physical** form. Where will the information asset 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		**S**	• Less than 10 [**L**] 1		

read/write/update/delete/generate/transport the data?	**11**		- 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 data protection legislation 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	**16**	S	No **[L]** 0	Risk rating (**L M H)**:____	

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 .			At the start or end? [**M**] 2 At the start and end? [**H**] 3	**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:**_____________

4. SUPPLIER ASSURANCE FRAMEWORK – CCfAR Worksheet Guidance

CONTEXT

Who owns/is responsible for the information asset?

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

Departments/organisations should ensure that a named individual, an Information Asset Owner (IAO) for example, is responsible/accountable for understanding and managing the risks to that information asset. They should also be informed of any further risks to that 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 legislation requires every data controller to register with the ICO, unless they are exempt. This applies to both government organisations and suppliers. The Data Controller is frequently the Accounting Officer though for practical purposes this role may be delegated.

Suppliers handling personal data should be registered with the ICO if they are data controllers in their own right. 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 data protection legislation 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 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 recovery from any such failure. The supplier should have Disaster Recovery and Business Continuity plans in place in order 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.

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 legislation		The data protection legislation regulates the processing of personal data. *See ICO website for further information.*

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 off shore any data must be referred to OGSIRO.
Office of the Government SIRO	**OGSIRO**	The Office of the Government SIRO (Senior Information Risk Owner) has recently been 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.

5. Common Criteria for Assessing Risk – Scoring Model

Purpose
The **Common Criteria for Assessing Risk** (CCfAR) is a set of outline criteria for organisations to use when assessing risk in third party supplier contracts at the OFFICIAL level (including OFFICIAL-SENSITIVE) and broadly group them into 'high' 'medium' and 'low' (L, M, H) risk services. Validation of these assessments will be gained over time as part of a managed process.

Basic principles
The CCfAR has been designed by a group of departmental practitioners 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 – input from specialist areas, e.g. procurement, security, IA, business/customer, accreditors, IAO, legal etc. is essential to gain a good understanding of the risks within the context of the business and its risk appetite.

- 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**.

- 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.

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

Preparing for a CCfAR assessment
To get the most from using the CCfAR some initial planning is helpful.

- Start by deciding which part of the organisation is leading the CCfAR assessment e.g. Security, IA, Contracts, Procurement etc. The lead branch/unit/area will be the one with the most to gain from undertaking this exercise.
- Agree the scope:
  - whether you are looking at one or more contracts;
  - the timescale, including the time needed to carry out the assessment;
  - who will be involved – identify those areas of the organisation that are likely to have important input e.g. Contracts, Business/IAO, Security, IA, Procurement, Legal, IT, Accreditation etc. Include at least one representative from security, contracts and the business taking part;
- Agree the outcome:
  - what information you will have at the end;
  - what processes it will feed into, and
  - who you need to share it with.
- Compare the CCfAR assessment against existing contracts to establish a baseline for managing information risk in contracts.

Using the scoring model in a CCfAR assessment

The CCfAR worksheet is a collaborative assessment tool designed to be flexible as possible, as is its scoring mechanism. Before the assessment starts go through the criteria and remove or amend any that are not applicable to the contract in question. You may decide to replace them with your own criteria but keep these to a minimum, ensure they are relevant to assessing the risk and not overly detailed in nature. All changes should be recorded. However consistency will be lost if too many changes are made and the ability to compare assessments between contracts and build a common baseline for the management of information risk in supplier contracts will be impaired.

While the criteria are generic, it is difficult to achieve a completely generic risk assessment (H, M, L) or scoring model. For example the question – 'What is the value of the contract?' – offers a range of values from less than £50,000 [L] to over £5 million [H]. To a small organisation with a limited budget contract expenditure of £50,000 may constitute a very considerable risk while to a large organisation with a budget of possibly billions contract expenditure of £5 million may constitute a medium or low risk. Before carrying out a CCfAR assessment review the risk assessments and scoring to ensure they align with the organisation's business model and risk appetite and make any necessary adjustments.

If the CCfAR assessment is being carried out at an early stage of contract procurement when a number of the contract details are yet to be decided, risk assessments and scores can be flagged as assumptions **A** and scored on the basis of 'an intelligent guess'. This scoring can be revisited later when the details have been agreed. Not scoring or risk assessing CCfAR criteria is likely to unbalance the assessment.

The CCfAR worksheet is made up of 20 criteria (questions) grouped under three headings – Asset Identification (10 questions), Asset Management Processes (7 questions) and Impact (3 questions).

A simple weighting structure applies to the criteria; there are **8 critical** criteria – denoting areas of potentially highest risk – and **12 significant** criteria.

Critical criteria are allocated scores within the range **0 – 5** [L – H] and significant criteria score within the range **0 – 3** [L – H]. The overall score for each criterion should not exceed 5 (critical) or 3 (significant).

However the first two criteria are an exception:

The type of data/information processed by the contractor.
The number of data/ records processed/held over the lifetime of the contract?

They each represent key information risk factors and logically are linked; the resultant score is derived by multiplying the two individual scores. For example if the contract includes personal data **2**:

• 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**

and over ½ million records **5** are or will be being processed:

• Under 1,000	[?]	**1**
• 1,000 – 100,000	[?]	**2**
• Over 100,000	[?]	**3**
• Over ½ million	[?]	**4**

the resultant score would be **10** i.e. **(2 X 5).**

Please note if the contract concerns SECRET information or data it should be handled under List X procedures.

Each criterion can be given a score or a Low – Medium – High risk assessment, even a combination of the two. The awarding of a score or assessment should be the result of collaborative discussion. The overall outcome of the assessment process might be a numerical score, e.g. 73, or a risk assessment profile e.g. 12 Highs, 5 Mediums and 3 Lows risks, or both.

There is no centrally provided methodology for turning scores or assessment profiles into a High, Medium, or Low risk outcome. The purpose of the CCfAR question set is to guide and focus the assessors' discussions, allowing them to combine the breadth, depth, experience and expertise from a range of security, business and commercial practitioners to produce a practical and more consistent approach to risk assessment within supplier contracts.

7. Using the Statement of Assurance (SoA)

Purpose

The **Statement of Assurance** (SoA) is an assessment question set, based on ISO 27001:2005 criteria and aligned to the SPF, for completion by third party suppliers. It can be used by departments and government organisations as part their assurance process when assessing the management of information risk in third party supplier contracts at the OFFICIAL level (including OFFICIAL-SENSITIVE). Contracts at SECRET and above are subject to List X processes.

The level of risk carried by a contract, as assessed by the department or government organisation e.g. 'high', 'medium' or 'low', will be an indicator of the level of assurance required from the supplier on how that risk is being managed. For example a department or government organisation may accept an annual self assessment from a supplier providing a 'low' risk service or product but will require a more in depth validation of the SoA assessment and some interaction with a supplier for a 'high' risk service or product.

Operating Principles

The SoA has been designed as a flexible tool:

- Not all of the criteria may be valid for every contract; the SoA should be reviewed and amended to suit the business requirements of the contract. All amendments should be recorded.

- Suppliers should have a good understanding of the purpose of the SoA, its role in the assurance process and the use that will be made of the information they provide.

- It is critical that there is a range inputs to the assessment of a completed SoA from for example specialist areas such as contracts, procurement, security, IA, business/customer, accreditors, IAO, legal etc. as appropriate. By building a good understanding of the information risks in its contracts, the organisation can develop a consistent approach to managing those risks and ensure that they are aligned with the risk appetite of the SIRO and the OGSIRO.

- The scoring mechanism is NOT mandatory and cannot be the only consideration for assessing risk. Where issues are identified the organisation should follow up with the supplier and a way forward agreed on mitigating or managing the risk.

- A completed SoA is the record of an assessment carried out on a service or product and can be used as an audit trail over the life of the service or product provided.

- The SoA 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. Any major amendments should be subject to an approvals process.

- Government community use of a common set of assessment criteria (SoA) will support a consistent approach to managing information risk in third party suppliers.

The SoA Tool

The SoA question set has been developed as an Excel spreadsheet and currently it is only available in this format. Organisations will need to decide how they intend to make the content of the SoA available to their suppliers, but it is anticipated that most suppliers would prefer to receive an electronic version. At present there are no plans to develop a tool centrally.

Using the SoA
Scenario A – The SoA can be used by departments or government organisations to assess the management of information risk in existing contracts at OFFICIAL, as part of its assurance processes.
The organisation may have already used the CCfAR to broadly group its contracts into 'high', 'medium' or 'low' risk. Those identified as 'high' risk should, as a priority, be subject to a regular assurance process, e.g. as part of the annual assurance report to the CO, the Security Risk Management Overview (SRMO).
[Note: Organisations seeking assurance on a significant number of contracts, might consider staggering the SoA assessment process over a period of months rather than conducting it as a single exercise.]

- **Start** by deciding which part of the organisation is leading the SoA assessment process e.g. Security, IA, Contracts etc. The lead branch/unit/area will probably be the one with the most to gain from undertaking this work.

- **Agree** the process and outcomes, including: the contracts to be assessed, the timescale, the likely people involved, whether you are concerned with particular aspects of contracts, e.g. contract includes information held in the Cloud, what information you will have at the end, who you will share it with and what other processes it will inform or feed into. It is important to get the right scope and that it is achievable.

- **Identify** those areas of the organisation that are likely to have important input on these contracts, e.g. Contracts, Business/IAO, Security, IA, Procurement, Legal, IT, Accreditation etc, as you are unlikely to have all the information you need.

- **Contact** the suppliers concerned, identify a point of contact and ensure they have a good understanding of the purpose of the SoA.

- **Make** any necessary amendments to the SoA to tailor it to the contract and remove questions that don't apply.

- **Send** out the SoA to the supplier contact requesting the return of a completed SoA by an agreed date. Currently the SoA is only available as an Excel spreadsheet so organisations will need to decide whether they send it out in this format or devise another method of delivery.

- **Review** the completed assessments:

    - Circulate all or the relevant parts of the completed assessments to those who will have input to the assessment, e.g. security/IA, business/IAO, contracts, etc.

    - Consider whether all of the critical criteria been answered as expected.

    - Identify the key issues taking into account the overall level of information risk - 'high', 'medium' or 'low' – in the contract..

    - Decide whether any further clarification is required from the supplier, for high risk contracts this may be an iterative process.

    - Agree what further action is required to bring the supplier into compliance.

    - Record outcomes from the assessment and ensure key stakeholders are informed of significant outcomes.
    - Contact the supplier to inform them of the outcome.

- **Agree next steps with the supplier:**
    - **High risk** contracts may require some fairly detailed clarification of their assessment resulting in a further compliance check/visit. A compliance plan will then be agreed and may be followed up at any point with a pre-announced visit to assess progress.
    - **Medium risk** contracts, depending on the issue, may also require further clarification of their SoA response. Organisations may decide to agree a compliance plan with the supplier or request that the next SoA assessment be subject to independent validation. The company carrying out that validation should, as part of the process, compare the most recent SoA assessment with the preceding one.
    - **Low risk** contracts, depending on their risk management policy, organisations should at a minimum acknowledge the receipt of a completed SoA return from a supplier.
- **Review** the outcomes **–** as a result of the assessment it is possible the risk status of some contracts may be raised or lowered. At this point it may be beneficial to review the initial CCfAR assessment to identify changes or amendments to the contract.
- **Use** the SoA as part of a structured process to inform risk based decision making and to prioritise resources for assurance and compliance activities.

Scenario B – Using the SoA as part of the procurement or contract management process.

The SoA is adaptable and can be used at various stages in the procurement or contract management process.

Pre-requirement project stage: The SoA questions could be turned into a proportionate checklist and incorporated into the planning process, following the CCfAR.

Pre-contract: At the pre-contract stage the SoA questions can form part of the contractual requirements to be built into the Terms & Conditions, as an assessment of compliance capability or returned by the supplier with the tender document.

Compliance audits: The SoA can be used as an audit checklist or a pre-engagement document for Compliance Audits, reducing the burden on suppliers particularly if a number of organisations adopted this approach. If the supplier is delivering the same service to more than one organisation this would enable joint audits to take place.

On going contract management: SoA outcomes can also be used to inform regular, on-going and proportionate discussions between contract managers and suppliers to monitor their delivery of security as part of the wider assurance of value for money (VFM) in the contract.

8. Oversight of the Supplier Assurance Framework

Background

Departments and agencies are required by the Security Policy Framework (SPF) to seek annual assurance from their third party suppliers that any risks to government information assets are being appropriately managed and make an annual return (SRMO) to the Cabinet Office. The Supplier Assurance Framework provides good practice guidance on the information risk management of contracts at the OFFICIAL level. It is a light touch, flexible yet consistent approach designed to:

- Raise standards by improving suppliers' understanding and application of information risk management;
- Reduce the cost and complexity of interacting with suppliers through greater use of standard commercial approaches;
- Minimise the compliance monitoring burden on organisations, enhance existing capabilities and generate capacity through consistency of approach and the adoption of the '*do once, do it well and reuse'* philosophy;
- Enhance accountability and provide greater transparency.

The flexibility of the framework allows for the inclusion of existing processes and governance structures. It provides an audit trail for the corporate management of information risk and brings together business, security and contracts staff in the coordinated and proportionate management of information risk in contracts aligned to the organisation's risk appetite.

Risk Management Approach

The framework includes two tools that enable organisations to determine appropriate levels of compliance monitoring on the basis of business risk; The Common Criteria for Assessing Risk (CCfAR) and the Statement of Assurance (SoA.) The CCfAR criteria allow government organisations to broadly assess their contracts into 'high', 'medium' and 'low' information risk. The SoA is an ISO 27001:2005 and SPF aligned question set that allows suppliers to demonstrate the extent to which they are compliant with good practice commercial security standards.

Used together these two tools enable organisations to target their resources at areas of greatest concern:

- High risk contracts – supplier assessment (SoA), formal review/audit, compliance plan;
- Moderate risk contracts – supplier assessment (SoA), periodic independent verification (by commercial providers);
- Low risk contracts – supplier assessment (SoA).

Oversight

The strength of the Supplier Assurance Framework is the simplicity and flexibility of its approach and the adaptability of its tools. This adaptability is essential as the environment changes, e.g. Digital by Default, 'Cloud First', and as new and different risks emerge for example the potential to off shore data, even during the life of an existing contract.

While the ability to adapt and amend the CCfAR and SoA is beneficial it also potentially creates issues. The framework is intended to create a consistent approach to risk management and allow for the sharing of information from the supplier assurance process. If organisations are allowed wide ranging powers to amend the criteria in the tools without a moderation process then consistency and the ability to share will quickly be lost.

The Supplier Assurance Framework: Good Practice Guidance will be published on the GOV.UK website allowing organisations to download the tools and amend them to meet their business requirements. The master versions of the CCfAR and the SoA will be maintained centrally by the Supplier Assurance Framework Oversight Group, its membership is drawn from the cross government practitioner group that developed the framework and the tool set on behalf of the Industrial Security Working Group (ISWG). The oversight group will be chaired by the Cabinet Office.

Terms of Reference

The Supplier Assurance Framework Oversight Group will:

- Manage the CCfAR and SoA tool sets – review the criteria against emerging risks or changes in government policy and standards to maintain currency and relevance and reissue if amended to maintain central consistency;
- Review the guidance annually or as required;
- Feedback emerging issues to the Information Working Group (IWG);
- Hold meetings as necessary; initially meetings will be held quarterly but the requirement will be kept under review;
- Convene topic/issue focus groups as required;
- Share lessons learned;
- Report annually to the IWG.

The Supplier Assurance Framework Oversight Group stands up in October 2013 when the Supplier Assurance Framework is formally published.

SUPPLIER ASSURANCE FRAMEWORK – Annex 1

Frequently Asked Questions

SECTION 1: General Questions / Completion of the SoA Self-assessment

Q1. What is the purpose of the Statement of Assurance (SoA) self-assessment questionnaire?

A1. Good information assurance requires any organisation to understand the risks posed to their information assets within their third party supply chains. The Statement of Assurance (SoA) is designed as a basis to help suppliers, and their client organisations, to understand and have greater visibility of these risks in the supplier's own organisation throughout the contract

The SoA asks the supplier to self-assess what security policies, systems and processes they have implemented in order to ensure that they are handling government data and assets securely and in accordance with HMG security requirements, namely the Cabinet Office Security Policy Framework (SPF). https://www.gov.uk/government/publications/security-policy-framework

---

Q2. Is this SoA self-assessment compulsory?

A2. Some government contracts already specify in their Terms and Conditions a requirement for the supplier to comply with the department or organisation's information assurance (IA) regime. Some, probably older, contracts may not contain this provision.

The Government is fully committed to ensuring that its information assets are appropriately protected. A supplier invited by a department or organisation to complete a SoA self assessment is strongly encouraged to do so; its completion will provide the requester with a level of the assurance which is required to continue to share or host government information with the supplier.

If you have any queries or concerns about completing a SoA contact in the department or organisation's Procurement and/or Commercial team or equivalent.

Q3. A supplier has already completed a SoA self-assessment questionnaire for another Government Department (OGD). Do they still need to complete one for another government department or organisation?

A3. It is important to establish whether or not the supplier is providing the same or broadly similar product or service, carrying the same level of risk, to both organisations and if a previously completed SoA might be sharable. If the product or service being provided are very different and/or for example have different end-products or recipients, process or store data in different ways or locations, then a new self-assessment may be required.

However, if the products or services are comparable then the supplier should contact the security or IA unit in the department or organisation for whom they completed the first SoA to discuss how the information can be made available to the requesting organisation. Then the department or organisation should inform the requesting organisation that they are consulting with the supplier on the release of their previously completed SoA and indicate when to expect a response.

Both suppliers and government departments may benefit from sharing this information as it reduces their overheads and results in more effective governance.

Q4. Which individual in the company should complete the self-assessment for the specified contract?

A4. Ideally, the person in the company with the lead responsibility for information security and assurance should ensure that the information in the completed return is accurate and complete. They may complete parts of the questionnaire and co-ordinate input from their counterparts in other areas of the organisation who will be experts in their respective areas of security and have knowledge of the organisation’s policies in each of the security areas covered by the self-assessment

---

Q5. Does the SoA self-assessment cover just the prime supplier or does it include all the sub-contractors involved in providing the product or service?

A5. The SoA assessment applies to the prime supplier and all the subcontractors involved in delivering the product or service to the department or organisation.

Government organisations expect that their data will be protected appropriately throughout the supply chain. The expectation is that the prime supplier is responsible for ensuring that this requirement is built in throughout the supply chain.

Q6. How often will the supplier need to complete a SoA self-assessment?

A6. As often as agreed between the department or organisation and the supplier. The aim is to ensure that suppliers continue to ensure that their business processes and data handling policies are resilient and compliant with government security requirements and is an appropriate level of due diligence is applied.

Where there are any changes suppliers must inform the department or organisation and highlight their likely impact on the SoA assessment.

Q7. The supplier already has the necessary security policies in place and does not wish to complete the self-assessment.

A7. This is an ongoing programme of supplier self-assessment that provides suppliers with an opportunity to demonstrate, to their advantage, their capabilities to client departments or organisations including their ability to keep abreast of changing threats. In many cases this will already be a requirement of the contract

Q8. Where can a supplier get more information about completing the soa self-assessment?

A8. For existing contracts the supplier should contact their department or organisation’s contract manger.

If a supplier has been requested to complete a SoA as part of the tendering process then they should contact the department or organisation’s procurement/commercial team or their equivalent.

SECTION 2: Sensitive Information

Q9. What level (classification) of data does the SoA apply to?

A9. The SoA self assessment applies to information or data classified as OFFICIAL.

Data classified as above OFFICIAL is subject to the List X process.

If any supplier is unsure of the classification of the data/information assets covered by the contract they should contact one of the following; the security unit of the department or organisation that owns the information, their contact in its commercial or procurement team or an equivalent for guidance.

Q10. A supplier does not handle any information that might be considered sensitive as part of the contract. Do they still need to complete the SoA questionnaire?

A10. When assessing the risks to the department or organisation’s information assets it is not only the type of data that is considered but a number of related criteria, for example the volume of data, the number of transfers between sites where it is held, how many sub-contractors are involved and how it is processed.

Contracts supplying physical assets designed to hold data such as blank identity documents, for example passports, though not containing personal data are attractive items for criminals and should be appropriately protected.

If a supplier is unsure, they should contact the department or organisation’s security unit for further guidance.

Q11. The supplier is delivering a service on the department’s premises using the department’s own facilities, e.g. IT equipment. Does the supplier still need to complete the SoA questionnaire?

A11. Even when delivering a service on the department’s premises and using their equipment suppliers need to demonstrate that they have a clear understanding of the security policies and practices – both theirs and the departments - that apply to the delivery of the product or service and their responsibilities in complying with them.

SECTION 3: SoA Outcomes

Q12. Having completed the SoA self-assessment what happens next?

Q12. If the SoA self-assessment is for a current contract, the department or organisation will contact the supplier and work with them to agree any follow-up actions the supplier needs to take.

If the SoA self-assessment has been completed as part of the tendering process, the department or organisation may be in contact regarding any gaps and potential remedial action.

Q13. Will the results of the suppliers SoA self-assessment be shared with other government departments or organisations?

A13. Sharing of the supplier's self-assessment results would not occur without the supplier's permission.

Possible considerations where sharing the results would be beneficial are:

- If a government department or organisation invites the supplier to complete a self-assessment and the supplier has already completed one for another department where the supplier provides the same product or service. Both the department and the supplier's permission must be obtained before the information can be shared.
- This form of data sharing is good practice if the service or product being supplied to one department is the same as that provided to another government organisation.
- Sharing of this data prevents duplication of work across the department and its delivery partners and across the rest of Government; it allows available resources to be used as efficiently as possible.
- It will also help to reduce the impact on the supplier's time and resources and will provide the requesting department with relevant information on the supplier's capabilities and IA management.

Security Awareness & You

Protecting Government Assets at OFFICIAL

An Introduction for Suppliers' Employees
October 2013

Contents

1. What is an asset?

An asset is something that has value. It might be the information that you process or printouts giving details of personal information that could be used for fraud or identity theft. It might be a pass giving access to a secure building or some specific knowledge or information that a person has, for example a password that gives access to an IT system or large data stores. The building pass and the password are assets that protect, or could affect, an information asset.

Information and data assets

An information asset is any information, or collection of information, that is processed by you on behalf of a government organisation, as a part of the supply chain. Information assets include not just personal or sensitive data regarding individuals, staff records, medical records, legal or court records but also policy advice, financial data or other information being processed on behalf of government.

Information can be held in electronic form on an IT system, on media e.g. a USB stick, CD, back up tapes etc. Software can be an information asset. Information held in paper forms or documents is also an asset.

If you process personal information – anything from a name, address, date of birth, National Insurance Number – check your company's policy on compliance with its obligations under the data protection legislation.

You should be aware of the data protection principles and your obligations to comply with the information security obligations. Further information on the data protection principles is available at www.ico.org.uk. See also page 15.

Physical assets

Physical assets can be computers, laptops, mobile phones, machinery or buildings. Protecting these assets also helps to provide security for the government's information assets.

Personnel assets

Personnel assets can be the knowledge and access rights held by staff and used to process, and protect, information assets, e.g. access to information and the authority to add, amend or delete it.

2. Your responsibilities

Government takes the security of its assets, particularly information, very seriously. As part of the contract award process it requires suppliers to have in place security policies appropriate to the type of asset and the level of risk to that asset. These risks range from the loss or leaking of information, altering the information in some way to mislead or harm, staff with no valid reason having access to sensitive information or data, through to the stealing of ideas (intellectual property) or simply theft.

The loss or compromise of assets, particularly information, affects both government and the supplier. For government any loss or compromise of its assets impacts on its reputation, resulting in the public losing confidence in its ability to protect citizen data and / or deliver services. The same is true for the supplier – any loss or compromise of government assets is likely to have an impact on its business reputation and may influence whether or not it continues to do business not just with government but also with other companies in the future.

Your company will have put security policies in place to guard against these risks occurring. It is your responsibility to implement these policies in your working practices – **you** are responsible for the protection of the government assets you handle, process, transport, store, manage or guard.

Any loss or compromise of government assets is likely to result in disciplinary action being taken by the department against your company. If personal information is involved, the Information Commissioner's Office (ICO) will need to be informed and this may result in fines being imposed.

The aim of this short handbook is to explain what assets are, to outline the potential risks to those assets and to set out some of the measures you need to take to protect them. Many are common sense, e.g. locking your computer if you are leaving your desk so others cannot read your screen, ensuring information is being securely transferred to the correct recipient, not sharing your password or letting others have access to information they are not entitled to see, making sure no papers are left uncollected on the printer or left lying on your desk when you go for a coffee or go home at night.

3. Who can access an asset?

As an individual you are required to protect the assets you have access to in order to do your job.

Access to assets is protected by law; ranging from illegally entering your company's property to steal assets to, in the case of loss or misuse of personal data, the data protection legislation.

You are only allowed to access assets if you have a genuine business reason and the agreed authority to do so. Nor must you provide, share or allow access to assets to anyone who does not have a genuine business reason or agreed authority to do so.

By allowing unauthorised access or even accessing data or information without authority yourself, you may be in the uncomfortable position of breaking the law.

If you are unsure that you have appropriate authority or a genuine business reason to handle or share an asset – you should seek advice from your manager or supervisor or the person in your company responsible for security.

4. Consequences of not adequately safeguarding information assets

For You

Misuse of information or failure to follow correct policy may result in disciplinary action and possible dismissal.

For government

Loss of public confidence in government's ability to safeguard assets
Accountability to parliament and the citizen
Reputational damage
Theft of commercial/financial/citizen/ information

For the citizen

Stress, distress at personal details being known
Identity theft
Financial loss
Physical harm e.g. victims of domestic violence.

For your company

Reputational damage
Possible loss of government business
In the case of the loss or compromise of personal information, ICO fines

5. Why you need to protect information assets

Government information is valuable and should be protected.

It covers many areas and may include:

- Commercial information including contractual information and intellectual property

- Personal data requiring protection under the data protection legislation including court records, medical records, benefit records, case histories, citizen data, staff records including personnel and payroll records

- Government policy development and policy drafting.

How this information is handled and protected is set out in the contract agreed between your company and the government.

You must ensure that you are aware of and understand the processes that have been put in place to protect the information assets that you handle.

You, with guidance from your manager, supervisor or security manager, are under an obligation to make sure that the information you handle is given the level of protection that was agreed.

You must report any compromises or deviations from the agreed processes to your manager, supervisor or security manager.

6. Protecting information assets - basic checklist

These basic principles provide guidance on handling OFFICIAL information:

- Handle with care to avoid loss, damage or inappropriate access by those who don’t have permission or the authority to see the information.
- Make sure you are aware of and comply with any legal requirements that apply to your information e.g. the data protection legislation if you are handling personal data.
- If you share information with others in your company for legitimate business purposes ensure the information is sent on assured channels not via unsecured email (e.g. Gmail**)**, DropBox, unsecured memory sticks, personal devices etc.
- Store information securely when not in use. For example, lock your computer screen when away from your desk and place any papers in a drawer or cupboard that can be secured.
- If assets are taken outside the company environment they should be protected in transit, not left unattended and **must be** stored securely.
- If discussing HMG business in public or by telephone discretion should be exercised. Details of sensitive material should be kept to a minimum. Precautions should be taken to prevent overlooking, overhearing or inadvertent access when working remotely or in public places.
- Particular care should be taken when sharing information with others outside your company including sub-contractors. Permission should be gained from your manager, supervisor or security manager and procedures followed to ensure safe delivery through secure channels.
- At the end of the contract ensure the information assets are managed or disposed of as agreed between your company and the government department/organisation.
- Report any incidents involving theft, loss or inappropriate access to HMG assets as soon as possible to your manager, supervisor or security manager

7. Security in your working environment

Working securely means being alert though not necessarily suspicious of all situations that might impact on the business. Threats to you and your environment can come from a variety of sources; this includes threats to individuals and premises.

Controlling access to your site

Allowing unauthorised and unchecked access to sites may allow an intruder to cause damage to the premises, harm to individuals or steal valuables.
Visitors require access to premises for legitimate business reasons e.g. clients attending appointments, engineers to install equipment, colleagues for meetings. Without exception, they must all follow the correct security procedures for that site. The requirement for visitors to sign in will avoid unauthorised access and escorted, if required.
Don’t let anyone follow you into the office if it is unclear who they are.

Wearing a pass and/or name badge at work helps to identify authorised members of staff. If you see someone without a valid pass ask them politely if you can see their pass and if they don’t have one escort them back to reception.   Then report the incident to your manager.

If you have to enter a code into a digilock to get access to a secure area, do not let anyone else see the code as you enter it.

Leaving your site

Wearing identity passes away from your official premises may alert others to where you work and what you do. Wearing ID away from the office may also put your colleagues at risk alerting others to where they work or where they live.

A Clear Desk Policy is not just about clearing everything from your desk and locking papers away before leaving.

- Is there anything left on the printer, photocopier or fax machine?
- If you are last to leave, make sure windows and cupboards are locked and the keys are secure.
- Remove paper on faxes to avoid receiving messages when unattended. Switch off faxes, photocopiers and printers where possible. Are there any papers, files or information on desks or in post trays? Are all cabinets and cupboards locked and are keys removed and stored safely?

8. Working securely with IT

Access to your account

In most businesses when you log into your IT system your account will give you access to any of the systems you are authorised to use. Any unauthorised actions would be logged against you.

Allowing others to use your account would give them access to information they do not have the authority to see. They may use your account to send inappropriate emails or access inappropriate Internet sites exposing your company to viruses, malicious software or hacking.

Access to applications and information is controlled to protect you, your organisation and government assets.

Passwords

Your password:

- must be known only to you and should not be easily guessed
- must not be shared or displayed visibly on your desk or screen
- should contain a combination of upper and lower case letters and symbols
- avoid anything obvious like ‘password’ or ‘welcome’
- don’t use the same password for all your other log-ins.

Advice on strong memorable passwords can be found on the **Get Safe Online** website www.getsafeonline.org

If you need to write it down then make sure that you keep the note secure and try to disguise it so that it does not look like a password.

If you think someone knows your password then change it immediately.

Further information

A good source of information on working securely on the Internet, both at work and at home, is www.getsafeonline.org

9. Personnel security

Baseline Personnel Security Standard (BPSS)

All staff that work for government departments or government organisations and those with access to government assets are subject on recruitment to the requirements of the BPSS. The process involves a series of checks to confirm your identity, employment history, nationality, immigration status and a criminal records check. For further details about BPSS click on this link to the CO website.

National Security Vetting

If you are working on a government contract and have access to government assets, sites, individuals or systems that are considered sensitive for national security, you may be required to undergo a more detailed security vetting process. Further details on the CO website.

Training, induction and ongoing refresher training

Most government contracts require their suppliers to provide security training for their staff before they handle government assets (of which this booklet may be a part). They may also require you to attend refresher training on a regular basis during the time you are employed by the company.

Confidentiality

Suppliers are usually required to sign a confidentiality agreement as part of the contract.   This means that they agree not to discuss, share or give details of any aspect of the contract and the assets it concerns to anyone who does not have the right to know; this includes people outside of the company (friends and family) and the media.   It also covers information that you post on your social networking sites or tweets.   Depending on the contract you may have been asked to sign an individual confidentiality agreement as part of your employment contract.

Legal obligations

You **must make sure** you are aware of your legal obligations when handling **any data** not just government assets. They include: the data protection legislation, The Computer Misuse Act and the Freedom of Information Act.   More information is available on the Cabinet Office website.

Disciplinary procedures

It is important to understand that if any misuse, disclosure or loss of information/data occurs this could lead to disciplinary action being taken.

10. Making security a habit

Good security works anywhere

Much of what you do at home to keep your information safe applies to what you do in the office. Think about your bank/credit cards – where do you store them? Do you share your PIN numbers? How do you store valuable documents, for example passports, birth certificates or bank statements? Are they in a safe place and somewhere you can always find them? How do you dispose of letters or documents containing your name, address and personal details? How careful are you in ensuring that your identity and finances are protected? It is just as important that you take care of other people's information when you are at work.

Sending information by email

While there are times when you can safely respond to an email, for example confirming the date of an appointment, in general there are some basic rules that you need to consider:

- Do you have the authority to send the information?
- Does the recipient have the right to receive the information?
- Do you need to send the information – is there another way of dealing with it?
- Only send the bare minimum to satisfy the request and remove any information that is not required to answer the query.
- Never send multiple customer details in a single email reply.
- Is the requestor asking for details that **should already be known to them** e.g. their address, National Insurance Number, bank account details, medical history, court record etc.?
- Does the incoming email look odd or doesn't 'ring true'? Verify the sender's details by contacting them using contact details your company already holds for them. If in doubt notify your manager, supervisor or security officer.
- What is the likelihood that the information may go astray? What is the potential damage or embarrassment to the owner of the information? What would be the impact on you and your employer?

Sending information by post or courier

Again there are some basic rules to be considered:

- It is the sender's responsibility to assess the scale, volume and sensitivity of the information being sent and whether any additional security is required, such as a full 'Track and Trace' service

- It is the sender's responsibility to ensure that the package is correctly addressed and the correct courier used
- Is this a regular data transfer? Are there processes to be followed and/or authorisation/a signature needed?
- If it is a 'one off' transfer, particularly of bulk data, has the correct authorisation been obtained, the information and its destination checked and the correct address verified and clearly displayed?

Social networking

Nowadays many people have 'a presence on the Net'; this may be Facebook pages, on a business site such as LinkedIn, a Twitter feed or YouTube site.   Many companies also have a website, large companies even have a company Facebook page, and some allow staff to post information on these pages.

Posting information attracts the attention of friends and family but also people seeking to take advantage of the information that you may have access to.   It is similar to giving an interview to the media in that it advertises who you are and what you do.

If you are posting information or personal comments on-line – on your own site or the company's – or considering any television appearances or contributing to a newspaper or magazine articles, **you** must:

- **seek** permission before taking part in any media activity that may identify you as delivering a contract on behalf of the government
- **not** disclose any knowledge or government information, make commitments or engage in activities on behalf of or relating to the government department or its assets unless you are authorised to do so
- **not** represent the government department when expressing personal opinions
- **not** pass official information on or make it available to any person e.g.. newspapers, journalists or give interviews about the government department without appropriate authorisation
- **understand** that such unauthorised disclosure of information is very serious and disciplinary action will be taken for failing to comply.

11. Portable media & security

What is portable media?

Portable media includes laptops, memory sticks (USB), tablets, BLACKBERRY, mobile phones, smart phones etc.

Portable media can also be used to refer to paper, as information may be carried out of the office in documents.

You are responsible for ensuring that any equipment or papers containing government assets, particularly personal or sensitive data, are protected from unauthorised access, theft, interference or damage when you are travelling or working off site.

You must only use authorised encrypted removable media provided by your employer.

You must not use your own laptop, tablet, mobile, smart phone etc. to store, process, transfer or send information or data belonging to the government unless specifically authorised to do so.

Travelling

Train, bus or plane journeys are often used as a time to get work done.

If you are working on the move make sure that you cannot be overlooked or overheard. Many mobile phones have cameras and voice recording facilities, so take care what can be seen and heard by others.

Never leave any equipment i.e. laptops, phones, encrypted memory sticks or paperwork unattended. If you need to leave anything in a car it must be kept out of sight and locked away in the boot. Don’t leave any equipment in an unattended vehicle overnight.

Working off site

If you are planning to take official documents out of the office it is important to get approval from your manager or supervisor. Only take with you what you need to do the job. Make sure the information is kept secure, particularly when travelling and at your destination and away from prying eyes.

12. Data protection principles

Guidance on data protection legislation should be obtained from your Data Protection Officer, the Information Commissioner's Office (https://ico.org.uk/) and from the SIRO.

The data protection principles identified in the General Data Protection Regulation are:

Personal data shall be:

(1) processed lawfully, fairly and in a transparent manner in relation to the data subject.

(2) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

(3) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

(4) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

(5) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

(6) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

13. Security incidents

An incident can be described as any activity that affects or could potentially affect the availability, confidentiality or integrity of the physical or electronic information assets of the Data Controller (usually Government in a contracted service) or the Data Processor (the supplier usually when delivering contracted Government services).

Examples are: unauthorised disclosure or transfer of information, loss of data i.e. paper records or laptop/USB, misuse of information, lost or incorrectly addressed post, information not properly secured and stolen by an opportunistic thief, information being dumped in rubbish bins instead of being securely disposed of, accidental or inadvertent release of information, a disgruntled employee intentionally leaking information to the media or stealing equipment and selling it on online markets (e.g. eBay).

This can have very serious consequences for both the individuals concerned and your company. It could lead to identity theft causing anxiety and upset for the individuals and reputational damage to your company leading to the potential loss of business.

Do you know:

- Who is responsible for information/data security in your company?
- Where to find your company's security policy or guidance?
- How to report an information/data security incident and who you report it to?
- Your responsibilities under the data protection legislation?
- If your company provides regular updates or training on data security?
- If you can use your personal IT to transport, store or process government information assets?
- Whether your company has a whistle-blowing policy?
- Who has authorised access to the information assets that you handle?
- How to dispose securely of information assets?
- Where you can get more information on using the Internet safely?

www.getsafeonline.org