Government Security

GovAssure Guidance - Peer Review

When mentioned in this guidance, unless otherwise stated:
Organisation = the organisation being peer reviewed
Reviewer = individual(s) performing the peer review
LGD = Lead Government Department

2023

Government Security

Who is this guidance for?

- This guidance pack is for organisations undertaking GovAssure that are not subject to an Independent Assurance Review (IAR), and instead will be undergoing a form of peer review for their Cyber Assessment Framework (CAF) self-assessments.

- The guidance is advised for any organisation and individual involved in a form of review, including;
  - Review by the Lead Government Department (LGD)
  - Peer review by another organisation
  - Internal review

- This guidance is applicable to both the individual(s) performing the peer review as well as the organisation being peer reviewed.

- In addition to the information on the slides, supporting commentary will be provided in the **speaker notes** below where appropriate

Government Security

Aims of this Guidance

Following this guidance, you should:

- ★ Have a clear understanding of the CAF, and the target Government CAF Profiles that underpin the assessment
- ★ Be familiar with the end-to-end GovAssure process
- ★ Feel able to perform a peer review on another organisation's CAF return
- ★ Feel confident in the peer review process, including the roles and responsibilities of both the reviewer and the reviewee
- ★ Develop a broader understanding of the security practises implemented by peer organisations and share best practice
- ★ Know who to contact if there are any issues

Government Security

Peer review options

- Government Security Group (GSG) has created additional options for alternative GovAssure validation, beyond the formal Independent Assurance Review with a third party.

- Lead Government Departments in collaboration with their ALBs should select one of the following validation approaches to meet the assurance requirements:
  1. Certified third party Independent Assurance Review (IAR), procured through CSS3
  2. LGD Review
  3. Peer Review by another Organisation
  4. Internal Review by Organisation
  5. No review (agreed with GSG)

Peer review options

Review type	Description	Actions
LGD review	An organisation with existing engagement with their LGD may have their review conducted by the department.	➔ **Organisations should discuss with their LGD as early as possible in the GovAssure process if this is an approach that will be followed** ➔ **If agreed, the LGD should identify an individual with sufficient time and capability to dedicate to the review**
Peer review by another organisation	Peer review is conducted by a different organisation. They should be a government organisation that ideally has experience with GovAssure or cyber assurance more broadly. Organisation should consult and agree this approach with their LGD.	➔ **Organisations may select an organisation with whom they have an existing relationship as their reviewer.** ➔ **LGDs are expected to support their organisations identify a potential reviewer from within their sector**
Internal peer review	Peer review is performed by an individual from within the same organisation. Organisation should consult and agree this approach with their LGD.	➔ **Organisations will identify individual(s) not directly involved in the specific system return to perform the review, for example, an owner of a system that is not being assessed**

What do we mean by peer review?

- ➔ An assessment of an organisation's WebCAF returns by another individual that does not have a conflict of interest.
- ➔ An assessment focused at the contributing outcome (CO) level, where reviewers will assess whether the organisation has achieved the target CO level based on the self-assessment and evidence provided.
- ➔ Reviewers will use the Baseline profile to understand what target level the organisation is meeting or working towards.
- ➔ Reviewers should expect and account for flexibility in organisations' answers, since there is more than one way to meet an outcome.
- ➔ Where an organisation and reviewer CO answers are the same, no extensive commentary is required.
- ➔ Where the answers differ, reviewers should use the contributing outcome box to explain what and why they disagree with the organisation's CO assessment.
- ➔ See slide 21 for more information.

Government Security

Peer Review…

Is…	Is **Not**…
➔ For organisations participating in an alternative form of review as part of the GovAssure process. ➔ For systems assessed against the B**aseline** CAF profile. ➔ A cost-effective alternative to a third-party Independent Assurance Review. ➔ Going to provide organisations with a summary report and Targeted Improvement Plan (TIP). ➔ Undertaken at the organisation's discretion, following direction from LGD. ➔ An opportunity for you and your organisation to share information on security practise with peers.	➔ Appropriate for systems assessed against the **Enhanced** CAF profile. ➔ Going to provide as in-depth validation as the Independent Assurance Review. ➔ As structured and objective of a view as the IAR. ➔ Centrally coordinated by GSG - The peer review will be arranged and coordinated between the LGD and relevant organisations. ➔ A form of assurance to assess the overall cyber posture of organisations.

Government Security

Guidance Overview

Guidance on the CAF

GovAssure Process

Peer review end to end process

Government Security

Guidance on the CAF

- Information on NCSCs CAF can be found here.
- Before initiating peer review, GSG expects the reviewer to have a good understanding of the CAF and how it is being implemented in GovAssure.
- https://www.security.gov.uk/guidance/govassure/ contains all of the information and guidance on the CAF including its structure, how specific target Government CAF profiles have been developed and how they should be understood.
- GSG expects the peer reviewer to have read the detailed guidance on the relevant stages of the GovAssure process before proceeding:
  - Stage 1: Organisational context and services
  - Stage 2: In-scope systems and assignment to the Government CAF profiles
  - Stage 3: CAF self-assessment

Government Security

GovAssure Process with Peer Review

Describe strategic context of the organisation, to identify essential services

Identifying systems and define boundaries / dependencies

Prioritise systems for assessment in year

Assign the target CAF profile (Baseline or Enhanced).

Organisation completes self-assessment for each system in scope and collates evidence pack.

Self-assessment will be reviewed by a peer reviewer, providing additional verification of the assessment.

NB - for LGDs this will be an Independent Assurance Review provided by a third party

A final report will be produced, outlining recommendations to be implemented to reduce cyber risk. This will be a key mechanism to support investment and decision making.
The TIP is agreed separately with the organisation.

Government Security

End-to-end process for peer review

Peer Reviewer

Organisation

Steps		
1	Share GovAssure scoping document with Peer Reviewer	
	Understand and familiarise yourself with the Organisational Context and systems being assessed	
	Agree ways of working, timelines, document sharing	
	Provide access to Peer Reviewer for WebCAF	Provide self-assessment evidence / documentation to Peer Reviewer
2	Read example assessments and understand the requirements for the Baseline Profile	
3	Read NCSC CAF contributing outcomes and underpinning IGPs (e.g. what kind of answers and evidence would constitute achieved, partially achieved, not achieved at the contributing outcome level	
4	Read CAF self-assessment contributing outcome statements / justification / evidence	Identify any areas unclear or requiring more evidence
5	Evaluate CAF self-assessment contributing outcome statement considering underpinning IGP answers	
6	Indicate and **provide commentary** on WebCAF whether contributing outcome achievement statements apply to the system using dropdown boxes	
	Arbitration process (NB - optional)	

Conducting Peer Review

1. **Starting Peer Review**
2. Actions for Peer Review
3. Worked Example

1 **Starting Peer Review**

2 Actions for Peer Review

3 Worked Example

Starting Peer Review

- Once the peer reviewer(s) have been assigned to the organisation they will need to:
    - Be provided with the relevant Scoping Documents to understand the context of the organisation they are reviewing.
    - Be granted access to the self-assessment(s) that have been submitted to WebCAF for review as an ‘Assessor’.
    - Have access to the evidence referenced in the self-assessment, or an understanding of the relevant evidence.
    - Complete their review on WebCAF confirming achievement at IGP level and providing commentary at the contributing outcome level where required.
    - Perform a brief moderation of the review with the organisation before formal submission on WebCAF.

Note: GSG anticipate a full peer review to take around 1-2 days, however timescales are expected to vary depending on the organisation and number of systems being reviewed.

1 Starting Peer Review

2 **Actions for Peer Review**

3 Worked Example

Government Security

Step 1
Understand the Organisational Context

- The organisation being reviewed will have completed a GovAssure Scoping Document covering the following:
  - (1) Organisational context and essential services
  - (2) In-scope systems and assignment of the target Government CAF profile
- The reviewer should read and digest the contents of the Scoping Document to understand the systems for which they are reviewing CAF self-assessments.

Actions

- ➔ **The GovAssure Scoping Document will need to be shared at the earliest opportunity with the selected peer reviewer.**
- ➔ **The organisation and reviewer will agree a rough timeline and establish ways of working. This should include; access to the self-assessments, how supporting document and evidence will be shared, who will be involved and when discussions between reviewer and organisation should take place (where needed).**

Government Security

Step 2
CAF profiles and WebCAF examples

- As part of the scoping process, the organisation being reviewed will have assigned one of two Government CAF profiles to the systems in scope. **For the purpose of peer review, systems in scope for this type of review are those assigned the Baseline Profile only.**
- WebCAF has an example completed CAF assessment at Baseline. Peer reviewers should familiarise themselves with this as an indication of the kinds of answers organisations may provide as part of the self-assessment.

Actions:

➔ **The organisation will assign the reviewer(s) to the assessments being reviewed on WebCAF.**

➔ **The reviewer will read the example CAF assessment for Baseline to aid their review.**

Government Security

CAF Government Profiles - Summary

Baseline Profile
https://www.security.gov.uk/guidance/govassure/government-caf-profiles
All government organisations will need to meet the Baseline CAF Profile. The Baseline Profile has been developed and agreed by GSG, NCSC and CDDO. It was developed by modelling the most likely impactful attacks against government against MITRE and determining the indicators of good practice within the outcomes of CAF which would mitigate the attack.

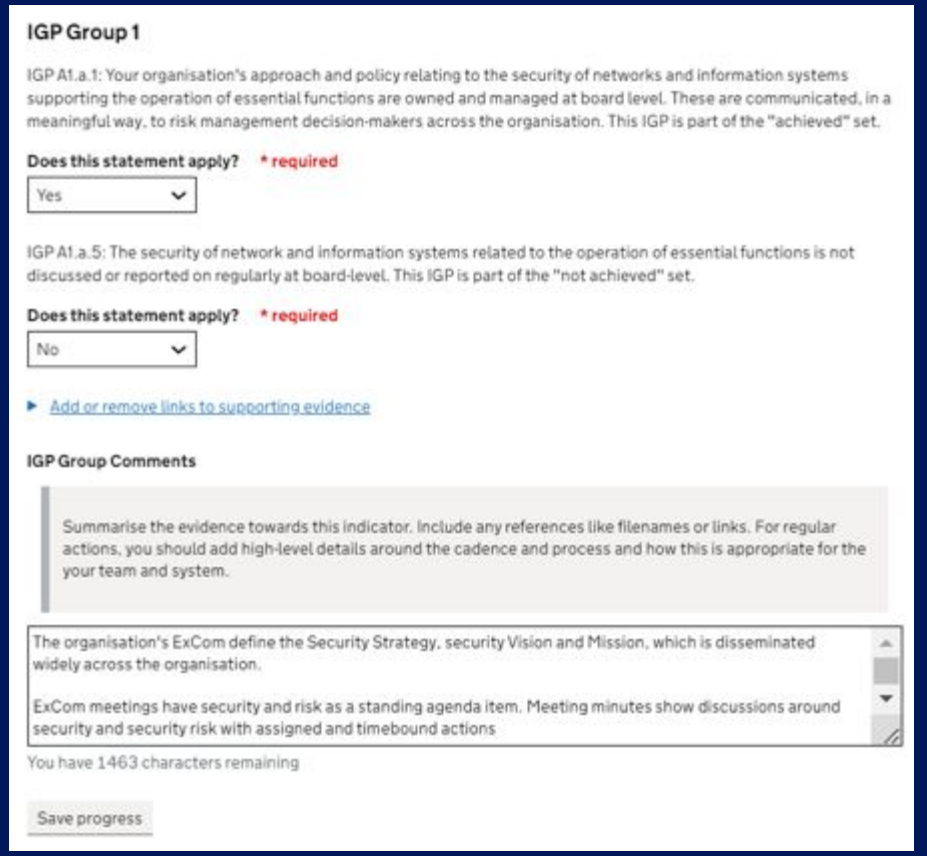
- ➔ **Peer reviewer should only be reviewing systems that have the Baseline Profile assigned. If this is not the case, then please contact GSG as soon as possible.**
- ➔ **The Baseline Profile is the target profile and there are number of ways for organisations to reach the target IGPs across the contributing outcomes.**
- ➔ **Reviewers are expected to account for flexibility in organisations answers to reflect the above.**

Government Security

Steps 3, 4 and 5

Understanding the organisations CAF self-assessment

- The reviewer(s) will be assigned a specific system assessment on WebCAF by the organisation lead.
- The self-assessment responses and supporting narrative will be ‘locked’ for the reviewer to work through systematically.
- Organisations will complete a CAF return focusing on assessment at contributing outcome (CO) level.
- Narrative is focused at the CO level, and reviewers should comprehend the CO and individual IGP statements before assessing the CO statement.
- Evidence will be referenced on WebCAF and reviewers should be provided access to the evidence that is stored separately.



Actions:

- ➔ **Stage 3 - reviewer reads NCSC’s CAF CO description and associated IGPs**
- ➔ **Stage 4 - reviewer reads organisations CO answer**
- ➔ **Stage 5 - reviewer reads the CO in the context of the given IGPs (if applicable)**

Government Security

Step 6
Reviewing the CAF self-assessment

- In step 6, reviewers will be expected to use expert judgement to complete the peer review.
- For peer review, commentary should be focused at the **contributing outcome level only.**
- On WebCAF, boxes will appear below each set of contributing outcome statements for the reviewer to populate (see following slides)
  - Where the organisation and reviewer are the same, there is no need to provide detailed commentary (see Slide 31)
  - Where organisation and reviewer comments differ, commentary should be provided as to what and why? Organisation may be contacted for further clarification by the reviewer.
- References to individual IGPs may be made in the CO statement review, however this is optional.

Actions:

- ➔ **Reviewer uses Y/N checkboxes to assess whether the contributing outcome statement applies to the system in question, and supporting commentary is provided if necessary (Slide 30-31)**
- ➔ **Where reviewer assessments differ from the organisations contributing outcome achievement, they should justify fully and with reference to the areas of difference.**
- ➔ **An agreement should be made on whether any additional (and optional) arbitration workshops and feedback are necessary**
- ➔ **Reviewer, organisation (and optionally LGD) should fully check quality of review before submission to GSG on WebCAF.**

Government Security

Steps 6 and 7
Reviewer commentary

		Organisation Self-assessment claims that Contributing Outcome…	
		…has been met	…has not been met
Assurance reviewer determines that Contributing Outcome…	…has been met	No detailed commentary is necessary unless reviewer sees exception	Summary explains why outcome has changed
	…has not been met	Summary needs to explain why and where reviewer has downgraded assessment	**Short** summary confirming why that system fails to meet chosen CO.

Government Security

Worked example for Peer Reviewers

3

Department of Artificial Intelligence and Robotics Technology

Department of Artificial Intelligence & Robotic Technologies

1. Starting Peer Review 
2. Actions for Peer Review 
3. **Worked Example** 

Step 1: familiarise yourself with the organisation scoping document and the background to system(s) being assessed

PART A: ORGANISATIONAL MISSION, OBJECTIVES AND PRIORITIES

Please consider and document the following 'about the organisation' aspects to help inform the organisational context that is presented to the independent assurance reviewer (Stage 4). ***Please keep all answers under 250 words.***

Strategic Context

What is the organisation fundamentally trying to achieve? What are the organisation's mission, objectives and priorities, and how do they support the delivery of Government services?

Please think about how an 'elevator pitch' about the organisation would look if written in in 2-3 sentences.

Mission: The Department of Artificial Intelligence and Robotic Technologies (DAIRT) was established in 2019. DAIRT is an expert policy Department following the growth of domestic and commercial Artificial Intelligence (A.I.) and robotic technologies. DAIRT works with industry and academia to make every day domestic tasks safer, more efficient, and inclusive. To do this, DAIRT aims to shape the safe and secure introduction of domestic and commercial A.I and robotics into households and service-oriented organisations leading the government's wider Future of A.I and Robotics programme.

Objectives: The objectives are to:

- Set strategic direction and provide investment certainty through policy and other interventions.
- Develop and implement the legislative and safety framework necessary to enable the safe domestic and commercial deployment of A.I. and Robotic Technologies (AIRT) across different areas including UK homes and the Hospitality sector.
- Engage with the public to gain an insight into public opinion and increase the public's understanding of the emergence of AIRT.
- Provide joint investment with industry through to 2025 to overcome the barriers to commercial deployment, thereby attracting, de-risking, and anchoring global investment.
- Creating jobs and strengthening our supply chain so that the UK is a maker of AIRT and not just a taker.
- Provision of the AIRT Safety Management System. Reporting on the performance of AIRT through use, and trial outcomes, which will include incidents or issues encountered, recalls and advisories. This includes:
  - Communication with the AIRT regulator, the A.I. and Robotics Authority.
  - Delivery of a communication platform for Universities and Research organisations.

3

PART D: IDENTIFYING THE IN-SCOPE CRITICAL SYSTEMS FOR GOVASSURE

Now you have identified the critical systems that support your organisation's essential services, please consider which critical systems will be assessed as part of GovAssure

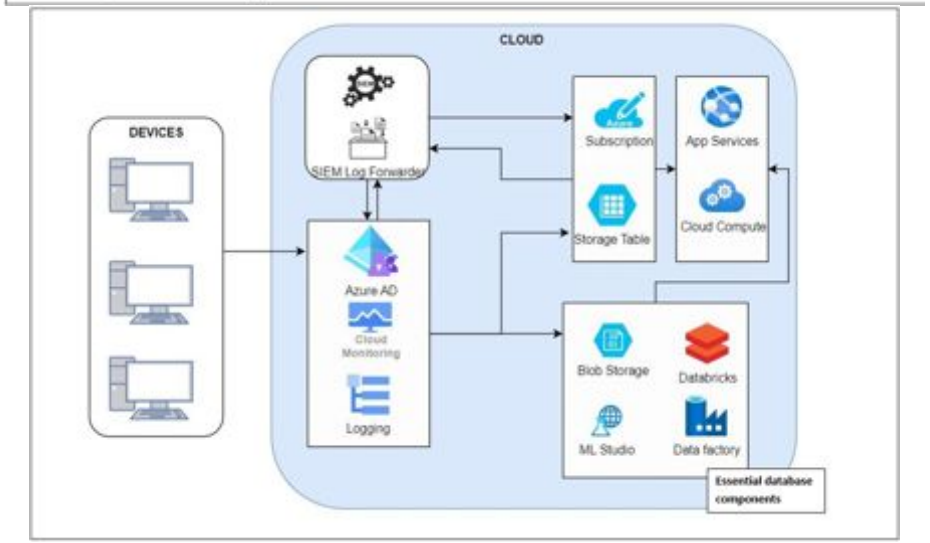
IN-SCOPE SYSTEM 1 DESCRIPTION

System name:	**IMS**
Essential service and function this supports	**Service:** AIRT Safety Management Recording and Reporting **Function:** Incident and event recording
Description – what does the system do and why do you consider it in scope for GovAssure:	IMS is DDCAIRT's primary system for capturing and recording AIRT incidents and events. It should be included in scope as without this system, it is not possible to record and communicate important events to the AIRT regulator and providers, the impact of this would be that we would be unable to issue urgent advisories and recall notices.

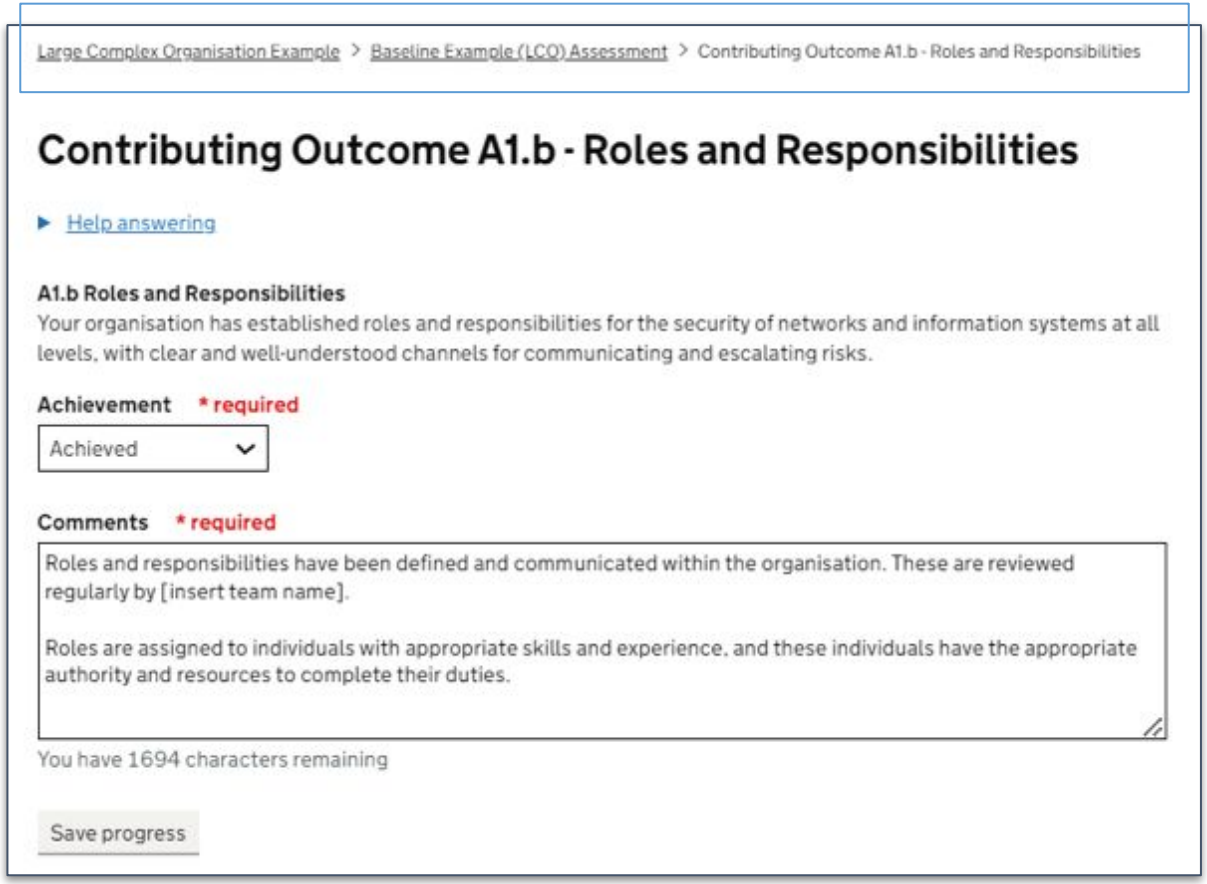
Breakdown of components (if appropriate)

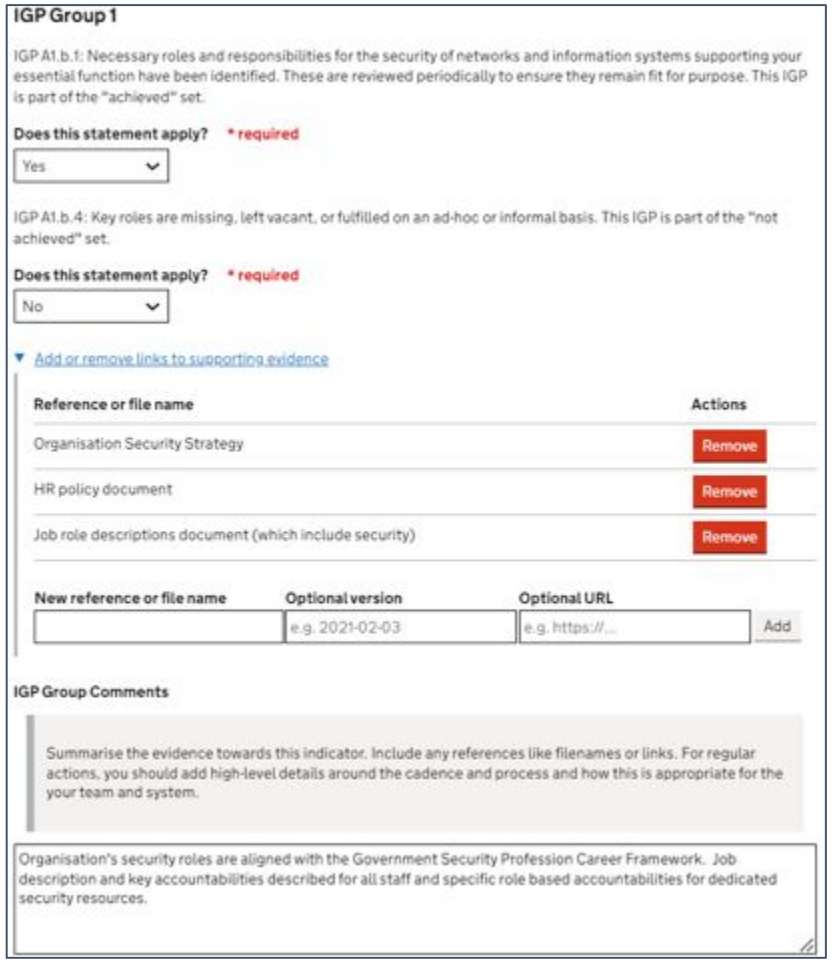
IMS consists of the following components:

- **SIEM** – The Security Information and Event Management (SIEM) component collects AIRT event log data from other components, which can then be analysed in real time to identify potential threats and vulnerabilities.



Step 2: familiarise yourself with the 'Example Assessments' on WebCAF which contain a (non-exhaustive) collection of the types of evidence and commentary for systems assessed at either Baseline or Enhanced





Reviewing DAIRT's return: Objective A

This is how a Peer Reviewer would approach and respond to DAIRT's assessment of A1.b Roles & Responsibilities.

A Objective - Managing security risk

Appropriate organisational structures, policies, and processes are in place to understand, assess and systematically manage security risks to the network and information systems supporting essential functions.

A1.b Contributing Outcome - Roles and Responsibilities

Your organisation has established roles and responsibilities for the security of networks and information systems at all levels, with clear and well-understood channels for communicating and escalating risks.

Achieved	Partially achieved	Not achieved
A1.b IGP Group 1		
Necessary roles and responsibilities for the security of critical systems have been identified. These are reviewed periodically to ensure they remain fit for purpose.		Key roles are missing, left vacant, or fulfilled on an ad-hoc or informal basis.
A1.b IGP Group 2		
Appropriately capable and knowledgeable staff fill those roles and are given the time, authority, and resources to carry out their duties.		Staff are assigned security responsibilities but without adequate authority or resources to fulfil them.
A1.b IGP Group 3		
There is clarity on who in your organisation has overall accountability for the security of the critical systems.		Staff are unsure what their responsibilities are for the security of the critical system.

Step 3: **Start by looking at the contributing outcome. Then look at the underpinning IGPs and what kind of answers and evidence would constitute achieved, partially achieved or not achieved at the contributing outcome level.**

Box 1 - Scoring of contributing outcomes

- ➔ COs should be scored according to the evidence provided.
- ➔ Scoring at CO level is dependent on the answers at the IGP level
- ➔ A CO can be scored 'Achieved' only when all relevant 'Achieved' IGPs are met (except those marked N/A).
- ➔ A CO can be scored "Partially Achieved" when all relevant "partially achieved" IGPs are met (except those marked N/A).
- ➔ A CO must be scored "not achieved" if **any** "not achieved" IGPs describe the system or organisation.
- ➔ Where "N/A" is chosen organisations should have explained sufficiently to justify its use, and therefore reviewers can exclude this from the CO scoring.
- ➔ As peer reviewers, IGPs do **not** need to be individually reviewed, but should be used alongside any evidence provided to inform the overall CO assessment.

Contributing Outcome A1.b - Roles and Responsibilities

▶ Help answering

A1.b Roles and Responsibilities

Your organisation has established roles and responsibilities for the security of networks and information systems at all levels, with clear and well-understood channels for communicating and escalating risks.

Organisation Achievement

Achieved

Organisation Comments

Overall, DAIRT has cybersecurity roles and responsibilities defined for all those working on the security of IMS. Communication channels are clear with risk governance processes stated clearly in security policy and guidance.

IMS organogram is updated on a quarterly basis to reflect changes in roles and responsibilities.

Regular refresher security training and education is provided for new DAIRT colleagues via a third-party provider. DAIRT employees receive a certificate upon completion. Comms are clear (e.g. Intranet) when there is a change in security policy or new security guidance for all DAIRT employees. We continually look at how we can improve our security education and training offer to DAIRT employees by engaging with external third-party learning leads.

As stated in DAIRT HR Policy, external contractors who are brought in to work on critical systems are required to complete the mandatory DAIRT security education and training. Upon completion all contractors receive a certification of completion.

Save progress

Note - in-line guidance on WebCAF is aimed at independent assurance reviewers. The following guidance should be followed instead.

Step 4: Read the organisation's contributing outcome achievement assessment as well as the justification, logic and decision making process along with supporting evidence. Also note any planned remediations.

IGP Group 1

IGP A1.b.1: Necessary roles and responsibilities for the security of networks and information systems supporting your essential function have been identified. These are reviewed periodically to ensure they remain fit for purpose. This IGP is part of the "achieved" set.

Organisation: Does this statement apply?

Yes *(Positive answer: "Yes")*

IGP A1.b.4: Key roles are missing, left vacant, or fulfilled on an ad-hoc or informal basis. This IGP is part of the "not achieved" set.

Organisation: Does this statement apply?

No *(Positive answers: "No" or "Not Applicable")*

▶ Add or remove links to supporting evidence

Organisation Comments

Overall, DAIRT has cybersecurity roles and responsibilities defined for all those working on the security of IMS.

This is evidenced in DAIRT Job role descriptions. This is held in IMS's organogram which is accessible to all those in the directorate. IMS organogram is updated on a quarterly basis to reflect changes in roles and responsibilities.

Business planning and a review of cyber security recruitment strategy is conducted on a quarterly basis to determine if appropriate amount of resource is available.

Step 5: Read the organisation's IGP level answers as further evidence to support contributing outcome level assessment.

Cross reference this with any evidence provided to help assessment of the overall contributing outcome statement and whether the evidence matches the statements made (see next slide)

IGP Group 1

IGP A1.b.1: Necessary roles and responsibilities for the security of networks and information systems supporting your essential function have been identified. These are reviewed periodically to ensure they remain fit for purpose. This IGP is part of the "achieved" set.

Organisation: Does this statement apply?

Yes *(Positive answer: "Yes")*

Assessor: Does this statement apply?

Yes

IGP A1.b.4: Key roles are missing, left vacant, or fulfilled on an ad-hoc or informal basis. This IGP is part of the "not achieved" set.

Organisation: Does this statement apply?

No *(Positive answers: "No" or "Not Applicable")*

Assessor: Does this statement apply?

No

▸ Add or remove links to supporting evidence

Organisation Comments

Overall, DAIRT has cybersecurity roles and responsibilities defined for all those working on the security of IMS. This is evidenced in DAIRT Job role descriptions. This is held in IMS's organogram which is accessible to all those in the directorate. IMS organogram is updated on a quarterly basis to reflect changes in roles and responsibilities.Business planning and a review of cyber security recruitment strategy is conducted on a quarterly basis to determine if appropriate amount of resource is available.

Assessor Comments

You have 2000 characters remaining

Step 5: Please note, for peer review, Y/N ratings are <u>not</u> expected at the IGP level, and can be left untouched. Functionality to score will be available however leaving them blank will not impact review progression.

Step 5: Please note, for peer review, comments are <u>not</u> expected at the IGP level. Functionality to comment will be available however they are optional boxes, and leaving them blank will not impact review progression.

Contributing Outcome A1.b - Roles and Responsibilities

▶ Help answering

A1.b Roles and Responsibilities
Your organisation has established roles and responsibilities for the security of networks and information systems at all levels, with clear and well-understood channels for communicating and escalating risks.

Organisation Achievement

The organisation has selected the following achievement rating:

Achieved

Organisation Comments

Organisations are asked to summarise the evidence towards this indicator, including any references like filenames or links. For regular actions, they should add high-level details around the cadence and process and how this is appropriate for the their team and system.

Overall, DAIRT has cybersecurity roles and responsibilities defined for all those working on the security of IMS. Communication channels are clear with risk governance processes stated clearly in security policy and guidance.

IMS organogram is updated on a quarterly basis to reflect changes in roles and responsibilities….

Assessor Achievement * required

Achieved

Assessor Comments * required

Roles and responsibilities are clearly defined supported by a defined organogram and defined job descriptions referencing responsibility for security of networks and information systems. The Governance structure is documented with a clear chain of escalation for Cyber issues and risks and regularly scheduled cadence of meetings which was evidenced to be meeting on a regular basis with clear actions. The organogram may need a review and update as it was almost a year old.

Step 6: Having read evidence and commentary at the IGP level, now re-read the contributing outcome statement and make a reviewers judgement on what you believe to be the organisation achievement level.

Contributing Outcome A1.b - Roles and Responsibilities

▶ Help answering

A1.b Roles and Responsibilities
Your organisation has established roles and responsibilities for the security of networks and information systems at all levels, with clear and well-understood channels for communicating and escalating risks.

Organisation Achievement

The organisation has selected the following achievement rating:

Achieved

Organisation Comments

Organisations are asked to summarise the evidence towards this indicator, including any references like filenames or links. For regular actions, they should add high-level details around the cadence and process and how this is appropriate for the their team and system.

Overall, DAIRT has cybersecurity roles and responsibilities defined for all those working on the security of IMS. Communication channels are clear with risk governance processes stated clearly in security policy and guidance.

IMS organogram is updated on a quarterly basis to reflect changes in roles and responsibilities….

Assessor Achievement * required

Achieved

Assessor Comments * required

Roles and responsibilities are clearly defined, supported by an organogram and defined job descriptions referencing responsibility for security of networks and systems. The Governance structure is documented with a clear chain of escalation for Cyber issues and risks The organogram may need a review and update as it was almost a year old.

You have 2000 characters remaining

Step 6a: In this example, the reviewer answer is the same as the organisation's assessment.

Therefore we would expect minimal commentary in the 'Assessor Comments' box. Small issues or improvements may be flagged.

Contributing Outcome A1.b - Roles and Responsibilities

▶ Help answering

A1.b Roles and Responsibilities
Your organisation has established roles and responsibilities for the security of networks and information systems at all levels, with clear and well-understood channels for communicating and escalating risks.

Organisation Achievement

The organisation has selected the following achievement rating:

Achieved

Organisation Comments

Organisations are asked to summarise the evidence towards this indicator, including any references like filenames or links. For regular actions, they should add high-level details around the cadence and process and how this is appropriate for the their team and system.

Overall, DAIRT has cybersecurity roles and responsibilities defined for all those working on the security of IMS. Communication channels are clear with risk governance processes stated clearly in security policy and guidance.

IMS organogram is updated on a quarterly basis to reflect changes in roles and responsibilities….

Assessor Achievement * required

Not Achieved

Assessor Comments * required

Agree that roles and responsibilities are clearly identified and staff have received appropriate training. However, there was no evidence of a nominated Board level member who has individual accountability for the delivery and operation of security across the organisation (IGP A1.b.3). Devolved responsibilities were not fully embedded in job descriptions, and these should be re-written to explicitly state responsibilities.

You have 2000 characters remaining

Step 6b: In this example, the reviewer answer is not the same as the organisation's assessment.

Therefore we would expect more commentary in the 'Assessor Comments' box. Specifically justifying *why* the answers are different.

Reviewers may wish to flag here the codes for the IGPs where the reviewer and organisation differ, however this is *optional*

Reviewers *do not* need to suggest remediations at this point (see Stage 5 of the GovAssure Process)

Reviewing DAIRT's return: Next Steps…

- After all contributing outcomes have been reviewed and comments provided where appropriate, the next steps are:

➔ The organisation and reviewer may wish to arrange a workshop to discuss the review. LGD and/or GSG can provide a third opinion if required as part of a streamlined arbitration process.

➔ When both organisations and the LGD are content the peer review has been completed, the reviewer will submit their review via WebCAF.

➔ Organisations **must** ensure they have exported a printout of their final reviewed CAF return as this will only remain on WebCAF for a short period of time.

WebCAF Submission

- Following submission, the reviewed CAF return will be stored in a SECRET environment and will not be accessible on WebCAF in the long term.
- The reviewed assessment will be collated into a report if multiple systems have been put through GovAssure by the organisation.
- Organisations, in combination with their LGDs, will also work up a Targeted Improvement Plan based on final CAF returns.
- Peer reviewers will not be expected to contribute to either product, unless they do so voluntarily.

Further Information

- Guidance on GovAssure is available to all on https://www.security.gov.uk/guidance/govassure/
- For any questions on the GovAssure process please contact your LGD.
- For additional questions on the GovAssure process or peer review, please contact cybergovassure@cabinetoffice.gov.uk
- For technical issues with WebCAF, please contact webcaf@cabinetoffice.gov.uk