

**Assessor guidance note:**

Please note: All pre-completed wording is to provide an example of suggested content, is indicative and subject to change.

This version 1.0 template is subject to change - please check security.gov.uk for the latest version of this template.

The document contains guidance notes and placeholder comments for reviewers in the form of:

- [Text to be replaced]

- Assessor guidance notes – tips and guidance to aid completion (delete prior to issuing)

- ## Comments to support completion (delete prior to issue).

The report has been designed to support it being split up to provide sections to service / systems owners on an needs basis which is why you will find some duplication between content at the Executive Summary level and at the System Detail level, so the system level reporting can be self-contained.

**GovAssure Independent Assurance Review Report (IARR)**

**[Organisation]**

**(Draft for discussion / Final report – ##delete as appropriate##)**

**[Month] [Year]**

**Contents ##To be automatically updated through table update based on headings##**

[Introduction 4](#_Toc150358814)

[Executive summary 6](#_Toc150358815)

[Summary of recommendations 12](#_Toc150358816)

[Summary of Contributing Outcomes and Target Government CAF Profile Achievement 15](#_Toc150358817)

[[System 1] Detailed findings 19](#_Toc150358818)

[[System 1] Summary 20](#_Toc150358819)

[[System 1] CAF Objective A - Contributing outcome achievement status 23](#_Toc150358820)

[[System 1] CAF Objective A - Detailed observations and recommendations 24](#_Toc150358821)

[[System 1] CAF Objective B - Contributing outcome achievement status 28](#_Toc150358822)

[[System 1] CAF Objective B - Detailed observations and recommendations 32](#_Toc150358823)

[[System 1] Objective C - Contributing outcome achievement status 37](#_Toc150358824)

[[System 1] CAF Objective C - Detailed observations and recommendations 38](#_Toc150358825)

[[System 1] CAF Objective D - Contributing outcome achievement status 42](#_Toc150358826)

[[System 2] Detailed findings 44](#_Toc150358827)

[[System 2] Summary 45](#_Toc150358828)

[[System 2] CAF Objective A - Contributing outcome achievement status 48](#_Toc150358829)

[[System 2] CAF Objective A - Detailed observations and recommendations 49](#_Toc150358830)

[[System 2] CAF Objective B - Contributing outcome achievement status 53](#_Toc150358831)

[[System 2] CAF Objective B - Detailed observations and recommendations 55](#_Toc150358832)

[[System 2] CAF Objective C - Contributing outcome achievement status 60](#_Toc150358833)

[[System 2] CAF Objective C - Detailed observations and recommendations 61](#_Toc150358834)

[[System 2] CAF Objective D - Contributing outcome achievement status 65](#_Toc150358835)

[[System 2] CAF Objective D - Detailed observations and recommendations 65](#_Toc150358836)

[[System 3] Detailed findings 67](#_Toc150358837)

[[System 3] Summary 68](#_Toc150358838)

[[System 3] CAF Objective A - Contributing outcome achievement status 71](#_Toc150358839)

[[System 3] CAF Objective A - Detailed observations and recommendations 72](#_Toc150358840)

[[System 3] CAF Objective B - Contributing outcome achievement status 76](#_Toc150358841)

[[System 3] CAF Objective B - Detailed observations and recommendations 78](#_Toc150358842)

[[System 3] CAF Objective C - Contributing outcome achievement status 83](#_Toc150358843)

[[System 3] CAF Objective C - Detailed observations and recommendations 84](#_Toc150358844)

[[System 3] CAF Objective D - Contributing outcome achievement status 88](#_Toc150358845)

[[System 3] CAF Objective D - Detailed observations and recommendations 88](#_Toc150358846)

[Appendix A: CAF Self-assessment – Managing the Completion of the CAF – Observations and Suggest Improvements 90](#_Toc150358847)

[Appendix B: Scope of the work undertaken 91](#_Toc150358848)

[Appendix C: Staff interviewed & evidence reviewed 92](#_Toc150358849)

# Introduction

In [Month] and [Year], [Organisation] commissioned [Provider] to perform an Independent Assurance Review (IAR) of [Organisation’s] GovAssure Cyber Assessment Framework (CAF) self-assessment in support of GovAssure’s Stage 4: Independent Assurance Review.

[Provider] conducted the assessment between the period of [Date from] and [Date to] and a close out meeting discussion was held on [Date] with [Team / Roles].

The GovAssure Scoping Document for [organisation] was used to provide an understanding of the context of the organisation as well as supporting the understanding of the scope of essential services and critical systems included within the scope of the self-assessment. The GovAssure Scoping Document for [organisation] was dated [Month] [Year].

The scope of this assessment was to perform a point in time assessment of [Organisations] CAF self-assessment to:

* Review, validate and report on the organisations own self-assessment as to the achievement against the target government CAF profile assigned to each system (Baseline or Enhanced).
* Consider the design, implementation and operation of key controls supporting the completion of the indicators of good practice and achievement of overarching contributing outcomes based on supporting narrative statements and evidence to justify the narrative.
* Undertake a combination of desk-based review as well as group workshops or individual one-to-one interviews with [organisation] personnel, to analyse and determine the information gaps against the GovAssure and Government Functional Standard GovS 007: Security and other related guidance.

Organisation overview

The [organisation’s] mission is to [XXX].

**Assessor guidance note:**

Summarised version to be extracted from the GovAssure Scoping Document.

The [organisation] is the lead government department for [XXX], [XXX] and [XXX]. It supports the delivery of government services using several missions and capabilities that fall within [XXX] directorates and is supported by [XXX] agencies and public bodies. These include [XXX].

The [organisation] has an annual budget in excess of [£XXX] with more than [XXX] civil servants operating in a wide range of roles across [locations].

Systems in scope and links to essential services

**Assessor guidance note:**

Summarised version to be extracted from the GovAssure Scoping Document.

The scope for the [organisations] GovAssure self-assessment consisted of [No.] of systems which were to be assessed based on the self-assessment performed by [organisation]. The version of the CAF used was 3.1, and the [organisation] used [Method e.g. WebCAF] to complete the self-assessment.

After initial review of the [organisations] CAF submission by [Independent Assurance Provider name], it was decided that the [No.] systems in scope were fit for review, in regards to the quality of evidence and narrative in the self-assessment responses provided.

The [organisation’s] systems were [first reviewed off-line using the evidence provided, then subject to a more formal assessment and reported upon] – full details can be found in the detailing findings section of this report and in the [WebCAF system report].

The scope of the IAR covered the following systems detailed as follows, along with the target CAF government profile they were assigned and assessed against:

* **[System 1 – NAME (Insert CAF target profile)]** – [Description – this can be sourced from the GovAssure scoping Document]
* **[System 2 - NAME]** - [Description]
* **[System 3 - NAME]** – [Description]

**Assessor guidance note:**

Number of systems – this template has been mocked up on the basis of three systems with two under the Baseline Target CAF Profile and one at Enhanced. If your client has a higher number of systems in scope then this will need to be reflected within the template. It may be appropriate to separate baseline and enhanced systems within tables used within this template.

# Executive summary

[High level overall summary that takes a holistic snapshot view of the organisation and its self-assessment return – intended to act as a ‘state of the nation’ style introduction that clearly identifies the key themes and issues that have been identified from a positive and negative perspective – if you only read this one paragraph, it would give you an overall snapshot as to the organisation’s cyber security posture and overall achievement against the target government CAF profile].

Areas of good practice

[Detail examples of good practice both around the approach and completion of the self-assessment as well as areas of good practice at an Objective / principle / contributing outcome level].

CAF Completion

[High level summary narrative covering the organisations approach to completing the CAF / quality of evidence etc. Can be expanded upon in Appendix A. Reference “For full details, please see Appendix A for more in-depth detail covering quality and completeness of the CAF self-assessment”].

Priority areas for remediation / key recommendations

[Highlight key areas to remediate – for example where there are common issues that have been identified across systems or where issues are considered ‘foundational’ control gaps that would need to be remediated as a priority].

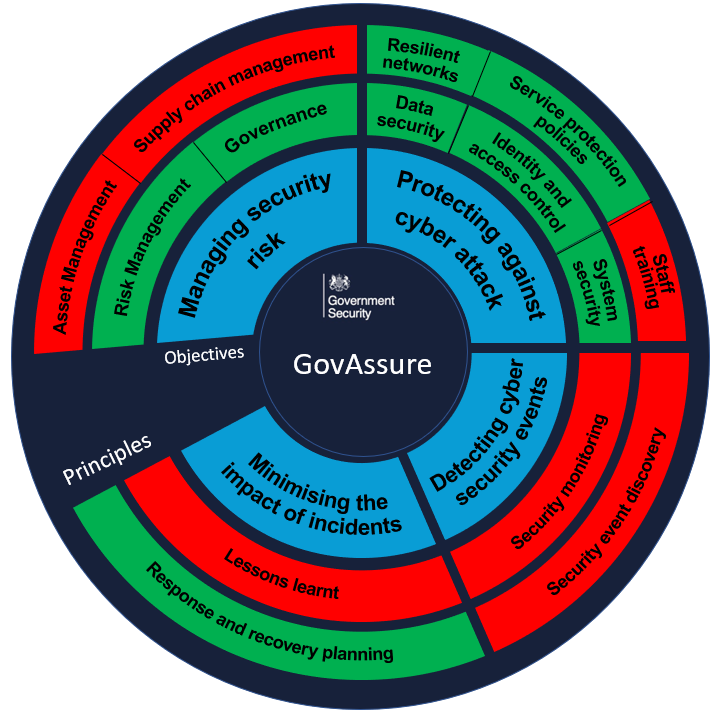
Example – ##Independent Assessor Guidance Page for the GovAssure dashboard dial view##

CAF Objective and Principle View: System level themes and key observations

The following GovAssure dashboard dial provides a view of the CAF principle areas and their level of achievement of the target CAF profile on the following basis:

**##Notes for reviewer completion##**

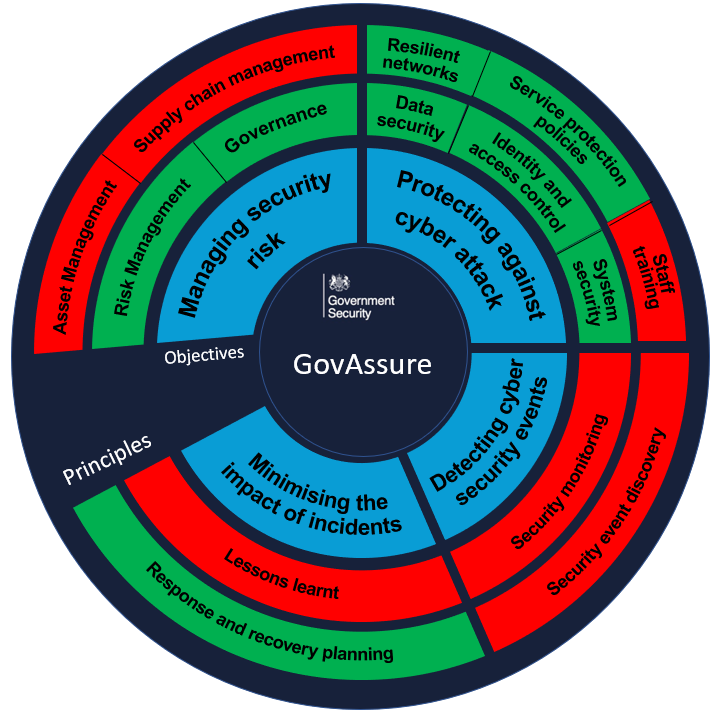
* The infographic has been designed with Executive level members in mind to bring contributing outcomes up a level to provide a visual as to where contributing outcomes are either supporting achievement of security principles or to identify where there are control gaps leading to security principles being let down by contributing outcomes not meeting the respective target CAF government profile on a system level basis.
* It reports on the basis of ‘met’ or ‘not met’ in respect of the target government CAF profile. For example, if contributing outcomes under the ‘Governance’ profile have not met the target defined profile, then the principle should be colour coded ‘red’ to represent contributing outcome not being ‘met’. If all contributing outcomes have met target, then this should be colour coded ‘green’ to represent achievement of the overall principle, ‘met’.
* GovAssure infographics are stored in a separate PowerPoint deck and are to be customised based on the results of the Assurance Review – either copy and paste, or snip and copy and paste in to this Word document.
* It is suggested that the approach taken includes a high-level themes and issues view at an organisational level and then on a per systems basis.
* The per system dial should be duplicated within the respective system section of the Part C: Detailed Findings to allow for this section to be extracted and issued on a need to know basis.



**Assessor guidance note:**

This page is for reviewer guidance only and should be deleted prior to issuing to your client.

CAF Objective and Principle View – How to read and interpret the GovAssure dashboard dial view



The GovAssure dashboard dials on the following pages provide an ‘at a glance’ overview of the CAF principles and whether the underlying contributing outcomes have met the assigned target CAF government profile (Baseline or Enhanced). It then summarises the key themes and issues according to each CAF objective.

These are arranged on a system by system basis (one dial per system), illustrating key themes and observations specific to the system.

The following provides a key as to how to interpret the dashboard:

**Green – ‘Met’:** All of the contributing outcomes supporting the overall CAF principle were met or exceeded when compared to the target CAF government profile.

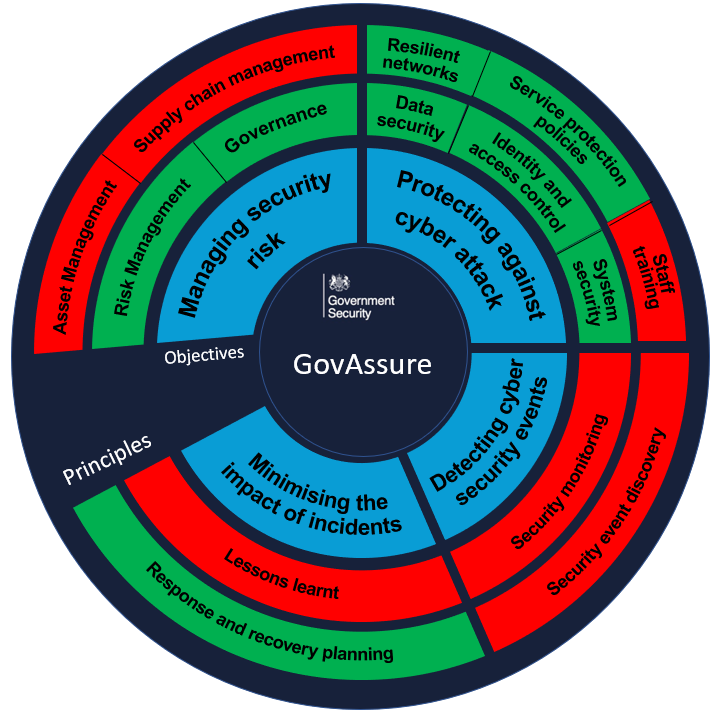
**Red – ‘Not met’:** One or morecontributing outcomes supporting the overall CAF principle were not met when compared to the target CAF government profile.

**Assessor note:**

Mock up for illustrative purposes only – this diagram should be updated to reflect contributing outcomes and control gaps

CAF Objective and Principle View: [System 1] themes and key observations

The following dashboard dial provide a view of the CAF principle areas and their level of achievement of the target CAF government profile for [System 1 - [target CAF government profile].



**CAF Objective A: Managing security risk**

* [Summarise high level key observations and themes relevant to the CAF Objective A]

**CAF Objective B: Protecting against cyber attack**

* [Summarise high level key observations and themes relevant to the CAF Objective B]

**CAF Objective C: Detecting cyber security events**

* [Summarise high level key observations and themes relevant to the CAF Objective C]

**CAF Objective D: Minimising the impact of incidents**

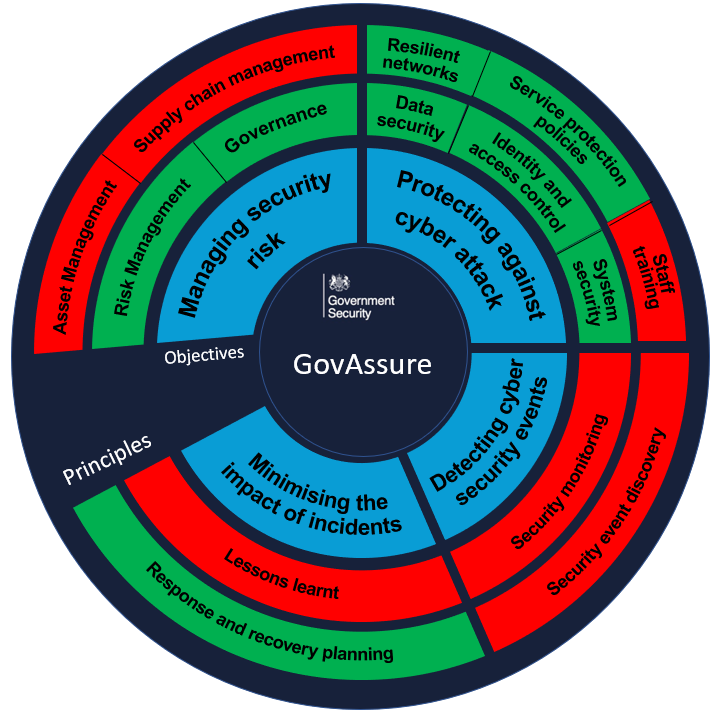
* [Summarise high level key observations and themes relevant to the CAF Objective D]

**Assessor note:**

Dial provided as an example for illustrative purposes only – this diagram should be updated to reflect contributing outcomes and control gaps.

CAF Objective and Principle View: [System 2] themes and key observations

The following dashboard dial provide a view of the CAF principle areas and their level of achievement of the target CAF government profile for [System 2 – [target CAF government profile].



**Assessor note:**

Dial provided as an example for illustrative purposes only – this diagram should be updated to reflect contributing outcomes and control gaps.

**CAF Objective A: Managing security risk**

* [Summarise high level key observations and themes relevant to the CAF Objective A]

**CAF Objective B: Protecting against cyber attack**

* [Summarise high level key observations and themes relevant to the CAF Objective B]

**CAF Objective C: Detecting cyber security events**

* [Summarise high level key observations and themes relevant to the CAF Objective C]

**CAF Objective D: Minimising the impact of incidents**

* [Summarise high level key observations and themes relevant to the CAF Objective D]

CAF Objective and Principle View: [System 3] themes and key observations

The following dashboard dial provide a view of the CAF principle areas and their level of achievement of the target CAF government profile for [System 3 – [target CAF government profile]

**CAF Objective A: Managing security risk**

* [Summarise high level key observations and themes relevant to the CAF Objective A]

**CAF Objective B: Protecting against cyber attack**

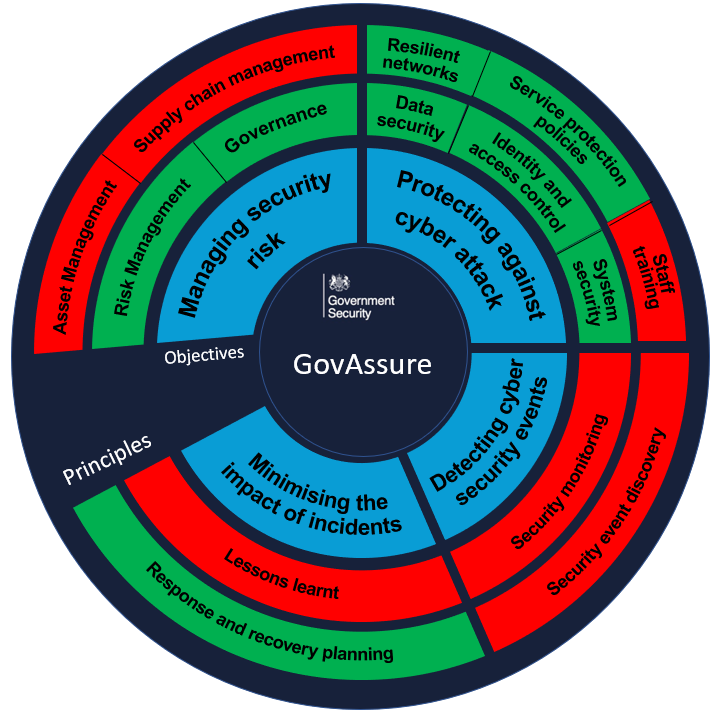
* [Summarise high level key observations and themes relevant to the CAF Objective B]

**CAF Objective C: Detecting cyber security events**

* [Summarise high level key observations and themes relevant to the CAF Objective C]

**CAF Objective D: Minimising the impact of incidents**

* [Summarise high level key observations and themes relevant to the CAF Objective D]



**Assessor note:**

Dial provided as an example for illustrative purposes only – this diagram should be updated to reflect contributing outcomes and control gaps.

## Summary of recommendations

The following table provides a summary of the recommendations raised against each CAF objective at a system level.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **System and Target CAF Profile** | **Coverage** | **Principle** | **Number of recommendations** | **Recommendations**  **Assessor note:**  This table is intended to provide an executive level member with a holistic summary of recommendations raised. |
| **[System 1]**  **(Baseline)** | **Objective A** | Governance |  | R01: [Recommendation title] – [Summary]  R02: [Recommendation title] – [Summary] |
| Risk Management |  | R03: [Recommendation title] – [Summary]  R04: [Recommendation title] – [Summary] |
| Asset Management |  |  |
| Supply chain |  |  |
| **Objective B** | Service Protection Policies and Processes |  |  |
| Identity and Access Controls |  |  |
| Data Security |  |  |
| System Security |  |  |
| Resilient Networks and Systems |  |  |
| Staff Awareness and Training |  |  |
| **Objective C** | Security Monitoring |  |  |
| Proactive Security Event Discovery |  |  |
| **Objective D** | Response and Recovery Planning |  |  |
| Lessons learned |  |  |
| **[System 2]**  **(Baseline)** | **Objective A** | Governance |  |  |
| Risk Management |  |  |
| Asset Management |  |  |
| Supply chain |  |  |
| **Objective B** | Service Protection Policies and Processes |  |  |
| Identity and Access Controls |  |  |
| Data Security |  |  |
| System Security |  |  |
| Resilient Networks and Systems |  |  |
| Staff Awareness and Training |  |  |
| **Objective C** | Security Monitoring |  |  |
| Proactive Security Event Discovery |  |  |
| **Objective D** | Response and Recovery Planning |  |  |
| Lessons learned |  |  |
| **[System 3]**  **(Enhanced)** | **Objective A** | Governance |  |  |
| Risk Management |  |  |
| Asset Management |  |  |
| Supply chain |  |  |
| **Objective B** | Service Protection Policies and Processes |  |  |
| Identity and Access Controls |  |  |
| Data Security |  |  |
| System Security |  |  |
| Resilient Networks and Systems |  |  |
| Staff Awareness and Training |  |  |
| **Objective C** | Security Monitoring |  |  |
| Proactive Security Event Discovery |  |  |
| **Objective D** | Response and Recovery Planning |  |  |
| Lessons learned |  |  |
| **Total** |  |  |  |  |

## Summary of Contributing Outcomes and Target Government CAF Profile Achievement

**Assessor guidance note:**

This table has been provided as an example and will need to be customised based on the systems in scope for the particular organisations. In this example, the organisation has included two systems in scope. Two systems have been assessed using the Baseline target CAF profile and one system using the Enhanced profile.

Add more columns as required to reflect the scope of the Department. If there are a large number of systems, it may be sensible to split Baseline and Enhanced systems in to two separate tables.

The table below compares whether the CAF target government profile (Baseline or Enhanced) has been met across all individual systems in scope. A breakdown of the compliance against the CAF target government profile for each individual area is provided in the detailed findings section of this report detailing findings on a per system basis.

* **“Yes”** means that the individual system assessed has achieved its respective target government CAF profile for each contributing outcome.
* **“No”** means that the individual system assessed has not achieved its respective target government CAF profile for the individual contributing outcome.
* **“N/A” or “Not applicable”** means the contributing outcome is considered exempt from the assessment or there is a compensating control in place.

|  |  |  | **Has the system met the Baseline profile?** | | **Has the system met the Enhanced profile?** |
| --- | --- | --- | --- | --- | --- |
| **Objective** | **CAF Principle** | **Contributing outcome** | **System 1** | **System 2** | **System 3** |
| **Objective A: Managing security risk** | **Governance** | A1.a Board Direction | **No** | **Yes** | **Yes** |
| A1.b Roles and Responsibilities | **No** | **Yes** | **No** |
| A1.c Decision Making | **No** | **Yes** | **Yes** |
| **Risk Management** | A2.a Risk management process | **No** | **Yes** | **No** |
| A2.b Assurance | **No** | **Yes** | **Yes** |
| **Asset Management** | A3.a Asset management | **No** | **Yes** | **No** |
| **Supply Chain** | A4.a Supply chain | **No** | **Yes** | **Yes** |
| **Objective B: Protecting against cyber attack** | **Service Protection Policies and Processes** | B1.a Policy and process development | **[Yes / No / N/A]** | **[Yes / No / N/A]** | **[Yes / No / N/A]** |
| B1.b Policy and process implementation | **[Yes / No / N/A]** | **[Yes / No / N/A]** | **[Yes / No / N/A]** |
| **Identity and Access Controls** | B2.a Identity verification, authentication, and authorisation | **[Yes / No / N/A]** | **[Yes / No / N/A]** | **[Yes / No / NA]** |
| B2.b Device management | **[Yes / No / N/A]** | **[Yes / No / N/A]** | **[Yes / No / N/A]** |
| B2.c Privileged user management | **[Yes / No / N/A]** | **[Yes / No / N/A]** | **[Yes / No / N/A]** |
| B2.d IDAC management and maintenance | **[Yes / No / N/A]** | **[Yes / No / N/A]** | **[Yes / No / N/A]** |
| **Data Security** | B3.a Understanding data | **[Yes / No / N/A]** | **[Yes / No / N/A]** | **[Yes / No / N/A]** |
| B3.b Data in transit | **[Yes / No / N/A]** | **[Yes / No / N/A]** | **[Yes / No / N/A]** |
| B3.c Stored data | **[Yes / No / N/A]** | **[Yes / No / N/A]** | **[Yes / No / N/A]** |
| B3.d Mobile data | **[Yes / No / N/A]** | **[Yes / No / N/A]** | **[Yes / No / N/A]** |
| B3.e Media/equipment sanitisation | **[Yes / No / N/A]** | **[Yes / No / N/A]** | **[Yes / No / N/A]** |
| **System Security** | B4.a Secure by design | **[Yes / No / N/A]** | **[Yes / No / N/A]** | **[Yes / No / N/A]** |
| B4.b Secure by configuration | **[Yes / No / N/A]** | **[Yes / No / N/A]** | **[Yes / No / N/A]** |
| B4.c Secure management | **[Yes / No / N/A]** | **[Yes / No / N/A]** | **[Yes / No / N/A]** |
| B4.d Vulnerability management | **[Yes / No / N/A]** | **[Yes / No / N/A]** | **[Yes / No / N/A]** |
| **Resilient Networks and Systems** | B5.a Resilience preparation | **[Yes / No / N/A]** | **[Yes / No / N/A]** | **[Yes / No / N/A]** |
| B5.b Design for resilience | **[Yes / No / N/A]** | **[Yes / No / N/A]** | **[Yes / No / N/A]**  **Assessor guidance note:**  C2.a and C2.b are greyed out due to the target profile being ‘not achieved’ at both baseline and enhanced. |
| B5.c Backups | **[Yes / No / N/A]** | **[Yes / No / N/A]** | **[Yes / No / N/A]** |
| **Staff Awareness and Training** | B6.a Cyber security culture | **[Yes / No / N/A]** | **[Yes / No / N/A]** | **[Yes / No / N/A]** |
| B6.b Cybersecurity training | **[Yes / No / N/A]** | **[Yes / No / N/A]** | **[Yes / No / N/A]** |
| **Objective C:** **Detecting cyber security events** | **Security Monitoring** | C1.a Monitoring coverage | **[Yes / No / N/A]** | **[Yes / No / N/A]** | **[Yes / No / N/A]** |
| C1.b Securing logs | **[Yes / No / N/A]** | **[Yes / No / N/A]** | **[Yes / No / N/A]** |
| C1.c Generating alerts | **[Yes / No / N/A]** | **[Yes / No / N/A]** | **[Yes / No / N/A]** |
| C1.d Identifying security incidents | **[Yes / No / N/A]** | **[Yes / No / N/A]** | **[Yes / No / N/A]** |
| C1.e Monitoring tools and skills | **[Yes / No / N/A]** | **[Yes / No / N/A]** | **[Yes / No / N/A]** |
| **Proactive Security Event Discovery** | C2.a System abnormalities for attack detection |  |  |  |
| C2.b Proactive attack discovery |  |  |  |
| **Objective D: Minimising the impact of cyber security incidents** | **Response and Recovery Planning** | D1.a Response plan | **[Yes / No / N/A]** | **[Yes / No / N/A]** | **[Yes / No / N/A]** |
| D1.b Response and recovery capability | **[Yes / No / N/A]** | **[Yes / No / N/A]** | **[Yes / No / N/A]** |
| D1.c Testing and exercising | **[Yes / No / N/A]** | **[Yes / No / N/A]** | **[Yes / No / N/A]** |
| **Lessons Learned** | D2.a Incident root cause analysis | **[Yes / No / N/A]** | **[Yes / No / N/A]** | **[Yes / No / N/A]** |
| D2.b Using incidents to drive improvements | **[Yes / No / N/A]** | **[Yes / No / N/A]** | **[Yes / No / N/A]** |

# [System 1] Detailed findings

## [System 1] Summary

**Introduction**

* [Introduction to the system]]
* [Context: Approach, process, any further detail on system assessment]
* [Supporting narrative]

**Target Government CAF Profile**

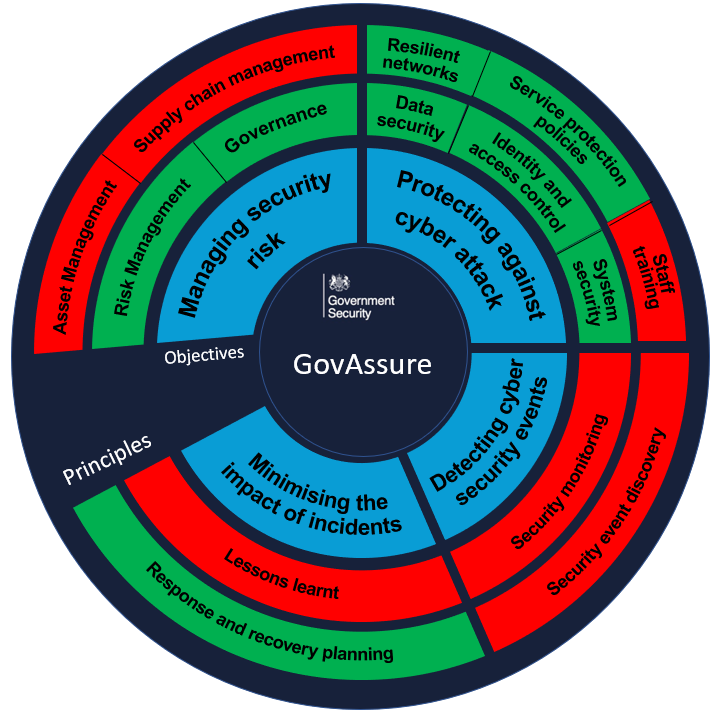
The system was assigned the [Baseline] target government CAF profile on the basis that [XXX]

**Summary of themes**

* [Summary of high-level themes]

**Assessor note:**

Dial provided as an example for illustrative purposes only – this diagram should be updated to reflect contributing outcomes and control gaps.

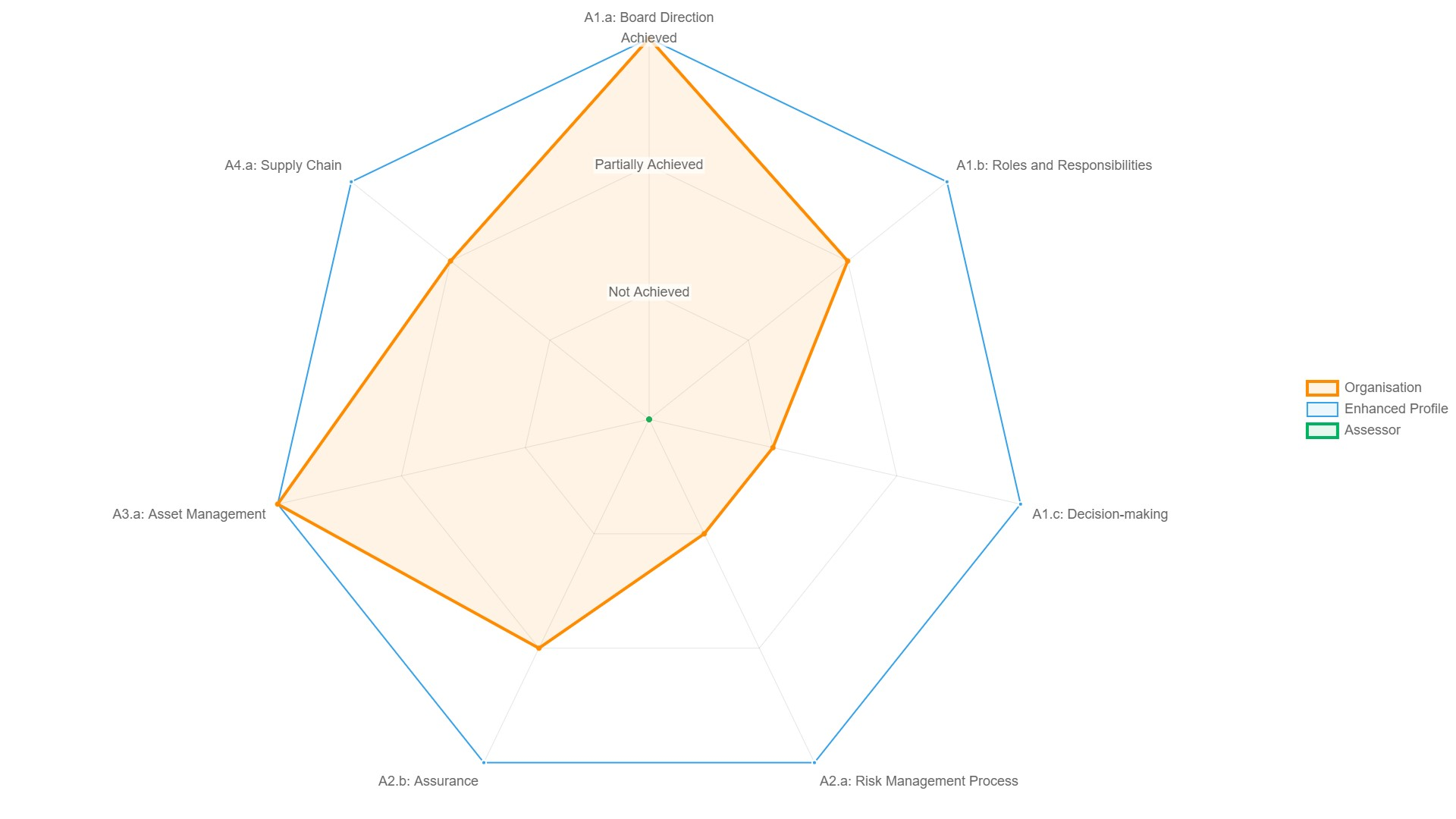


[System 1] CAF Objective A - Contributing outcome achievement status radargram

Following the detailed examination of documentation and evidence in support of [organisation’s] CAF self-assessment, the following radargram provides a high-level summary of the independently assessed status of each contributing outcome for the [System 1]. The subsequent pages detail any exceptions or recommendations raised, as well as contributing outcomes that were insufficiently supported by evidence (where applicable).

**Assessor note:**

Example provided for illustrative purposes only. This is a placeholder for a radargram produced by WebCAF as part of the Report (HTML) functionality. It should be copied and pasted here.



[System 1] Summary – CAF Objective A: Managing security risk

**A1 Governance:**

* **A1.a Board Direction -** [Exception based contributing outcome level summary]
* **A1.b Roles and Responsibilities** - [Exception based contributing outcome level summary]
* **A1.c Decision-making** - [Exception based contributing outcome level summary]

**A2 Risk Management:**

* **A2.a Risk Management Process** - [Exception based contributing outcome level summary]
* **A2.b Assurance** - [Exception based contributing outcome level summary]

**Assessor note:**

Delete contributing outcome references where no comments are being made.

**A3 Asset Management:**

* **A3.a Asset Management** - [Exception based contributing outcome level summary]

**A4 Supply Chain:**

* **A4.a Supply Chain** - [Exception based contributing outcome level summary]

## [System 1] CAF Objective A - Contributing outcome achievement status

**Assessor note:**

For the ‘non-compliant IGPs’ column – Provide references to the non-compliant IGPs.

**Assessor note:**

For the ‘profile met’ column - -compliant IGPs column – If the profile has not been met, a detailed observation and recommendation should be raised in the following ‘detailed observations and recommendations’ table.

The following table provides a summary of the contributing outcomes achievement status and whether the target CAF government profile has been achieved. **##Completed example for reference purposes only – data in the table below to be updated##**

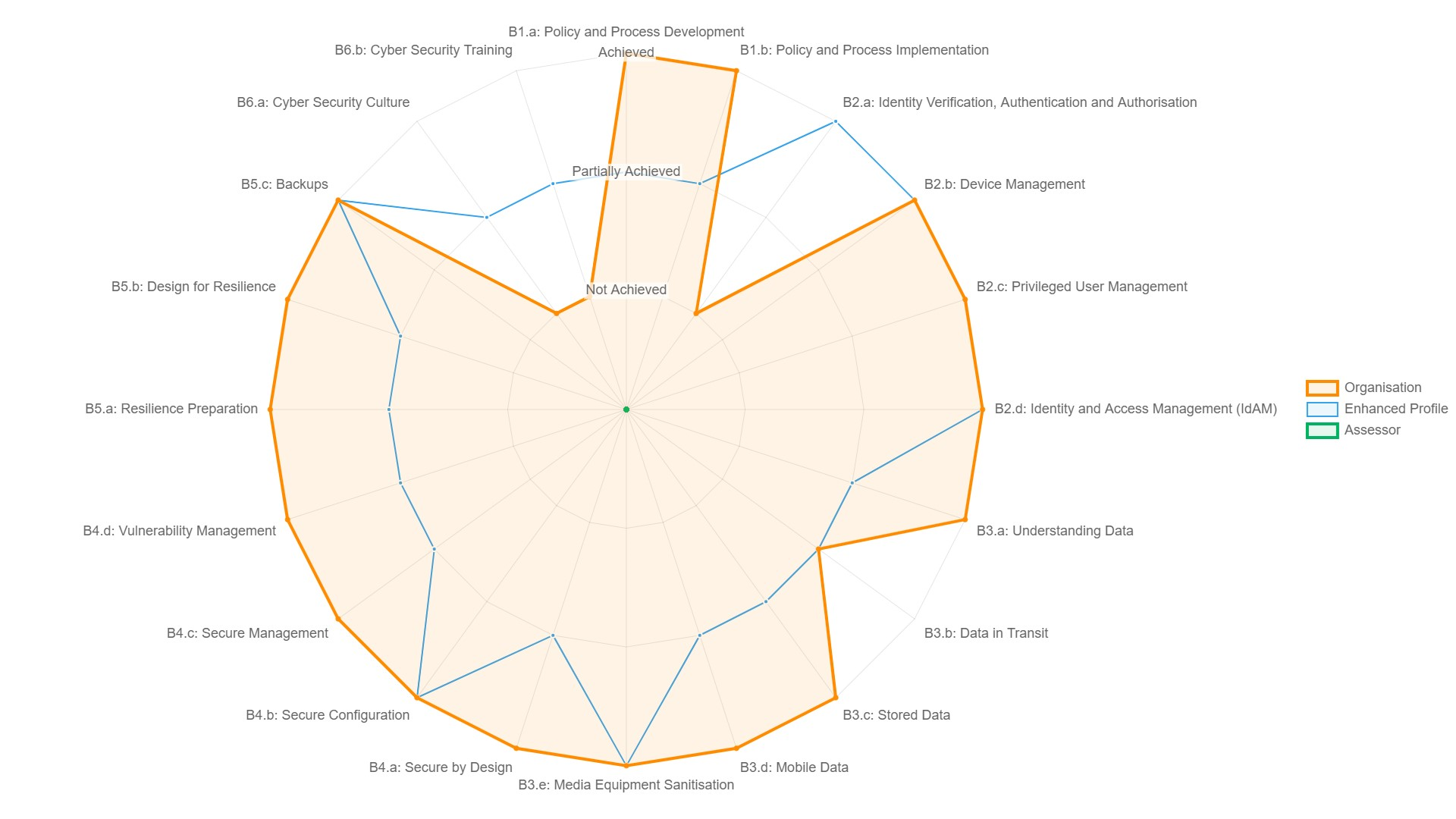
| **Objective** | **CAF principle** | **Contributing outcome** | **Target profile**  **(Baseline)** | **Self-assessment** | **Independent assurer assessment** | **Non-compliant IGPs** | **Profile met?** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Objective A: Managing security risk** | **Governance**  **Assessor note:**  For the ‘independent assurer assessment’ column – Does the independent assurance reviewer agree with the organisations assessment of the contributing outcome based on the commentary and available evidence? | A1.a Board Direction | **Achieved** | **Achieved** | **Not achieved** | A1.a.5  A1.a.6 | **No** |
| A1.b Roles and Responsibilities | **Achieved** | **Achieved** | **Not achieved** | A1.b.4 | **No** |
| A1.c Decision Making | **Achieved** | **Achieved** | **Not achieved** | A1.c.5 | **No** |
| **Risk Management** | A2.a Risk management process | **Partially achieved** | **Partially achieved** | **Not achieved** | A2.a.10 | **No** |
| A2.b Assurance | **Achieved** | **Achieved** | **Not achieved** | A2.b.7  A2.b.6 | **No** |
| **Asset Management** | A3.a Asset management | **Achieved** | **Achieved** | **Not achieved** | A3.a.6 | **No** |
| **Supply Chain** | A4.a Supply chain | **Partially achieved** | **Partially achieved** | **Not achieved** | A4.a.15 | **No** |

## 

## [System 1] CAF Objective A - Detailed observations and recommendations

| **Obs. ref.** | **Contributing outcome** | **Detailed observations** | **Risk** | **Recommendation**  **Assessor note:**  Delete contributing outcome lines where no observations or recommendations are being raised. |
| --- | --- | --- | --- | --- |
| **Objective A: Managing security risk** | | | | |
| **[Ref]** | **A1.a Board Direction** | **##Detailed observation reporting is by exception only and against the target CAF government profile. For example, if a target is ‘partially achieved’, generally we expect observations to be raised where they fall short of the target, but it is possible to include ‘improvement opportunity’ observations. ‘Improvement opportunity’ recommendations should be flagged as such##**  **##Detail can be copied, pasted and refined here from the original assurance reviewer report output from WebCAF to identify the observation/control gap##** | **##Identify the risk associated with the issue observed##** | **##Detail the recommended action as a result of the observation##** |
|  | **A1.b Roles and Responsibilities** |  |  |  |
|  | **A1.c Decision-making** |  |  |  |
|  | **A2.a Risk Management Process** |  |  |  |
|  | **A2.b Assurance** |  |  |  |
|  | **A3.a Asset Management** |  |  |  |
|  | **A4.a Supply Chain** |  |  |  |

[System 1] CAF Objective B - Contributing outcome achievement status radargram

Following the detailed examination of documentation and evidence in support of [organisation’s] CAF self-assessment, the following radargram provides a high-level summary of the independently assessed status of each contributing outcome for the [System 1]. The subsequent pages detail any exceptions or recommendations raised, as well as contributing outcomes that were insufficiently supported by evidence (where applicable). 

**Assessor note:**

Example provided for illustrative purposes only. This is a placeholder for a radargram produced by WebCAF as part of the Report (HTML) functionality. It should be copied and pasted here.

[System 1] Summary – CAF Objective B: Protecting against cyber attack

**B1 Service Protection Policies and Processes:**

* **B1.a Policy and Process Development -** [Exception based contributing outcome level summary]
* **B1.b Policy and Process Implementation -** [Exception based contributing outcome level summary]

**B2 Identity and Access Controls:**

* **B2.a Identity Verification, Authentication and Authorisation -** [Exception based contributing outcome level summary]
* **B2.b Device Management -** [Exception based contributing outcome level summary]
* **B2.c Privileged User Management -** [Exception based contributing outcome level summary]
* **B2.d Identity and Access Management (IdAM**) **-** [Exception based contributing outcome level summary]

**B3 Data Security:**

* **B3.a Understanding Data -** [Exception based contributing outcome level summary]
* **B3.b Data in Transit -** [Exception based contributing outcome level summary]
* **B3.c Stored Data -** [Exception based contributing outcome level summary]
* **B3.d Mobile Data -** [Exception based contributing outcome level summary]
* **B3.e Media Equipment Sanitisation -** [Exception based contributing outcome level summary]

**Assessor note:**

Delete contributing outcome references where no comments are being made.

**B4 System security:**

* **B4.a Secure by Design -** [Exception based contributing outcome level summary]
* **B4.b Secure Configuration -** [Exception based contributing outcome level summary]
* **B4.c Secure Management -** [Exception based contributing outcome level summary]
* **B4.d Vulnerability Management -** [Exception based contributing outcome level summary]

**B5 Resilient Networks and Systems:**

* **B5.a Resilience Preparation -** [Exception based contributing outcome level summary]
* **B5.b Design for Resilience -** [Exception based contributing outcome level summary]
* **B5.c Backups -** [Exception based contributing outcome level summary]

**B6: Staff awareness and training:**

* **B6.a Cyber Security Culture -** [Exception based contributing outcome level summary]
* **B6.b Cyber Security Training** **-** [Exception based contributing outcome level summary]

## [System 1] CAF Objective B - Contributing outcome achievement status

**Assessor note:**

For the ‘non-compliant IGPs’ column – Provide references to the non-compliant IGPs.

The following table provides a summary of the contributing outcomes achievement status and whether the target CAF government profile has been achieved.

| **Objective** | **CAF Principle** | **Contributing outcome** | **Target profile**  **(Baseline)** | **Self-assessment** | **Independent assurer assessment** | **Non-compliant IGPs** | **Profile met?** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Objective B: Protecting against cyber attack** | **Service Protection Policies and Processes** | B1.a Policy and process development | **Partially achieved** | **Achieved / Partially achieved / Not achieved / N/A** | **Achieved / Partially achieved / Not achieved / N/A** | **Achieved / Partially achieved / Not achieved / N/A** | **Yes / No / N/A** |
| B1.b Policy and process implementation | **Partially achieved** | **Achieved / Partially achieved / Not achieved / N/A** | **Achieved / Partially achieved / Not achieved / N/A** | **Achieved / Partially achieved / Not achieved / N/A** | **Yes / No / N/A** |
| **Identity and Access Controls** | B2.a Identity verification, authentication, and authorisation | **Partially achieved** | **Achieved / Partially achieved / Not achieved / N/A** | **Achieved / Partially achieved / Not achieved / N/A** | **Achieved / Partially achieved / Not achieved / N/A** | **Yes / No / N/A** |
| B2.b Device management | **Partially achieved** | **Achieved / Partially achieved / Not achieved / N/A** | **Achieved / Partially achieved / Not achieved / N/A** | **Achieved / Partially achieved / Not achieved / N/A** | **Yes / No / N/A** |
| B2.c Privileged user management | **Partially achieved** | **Achieved / Partially achieved / Not achieved / N/A** | **Achieved / Partially achieved / Not achieved / N/A** | **Achieved / Partially achieved / Not achieved / N/A** | **Yes / No / N/A** |
| B2.d IDAC management and maintenance | **Partially achieved** | **Achieved / Partially achieved / Not achieved / N/A** | **Achieved / Partially achieved / Not achieved / N/A** | **Achieved / Partially achieved / Not achieved / N/A** | **Yes / No / N/A** |
| **Data Security** | B3.a Understanding data | **Partially achieved** | **Achieved / Partially achieved / Not achieved / N/A** | **Achieved / Partially achieved / Not achieved / N/A** | **Achieved / Partially achieved / Not achieved / N/A** | **Yes / No / N/A** |
| B3.b Data in transit | **Partially achieved** | **Achieved / Partially achieved / Not achieved / N/A** | **Achieved / Partially achieved / Not achieved / N/A** | **Achieved / Partially achieved / Not achieved / N/A** | **Yes / No / N/A** |
| B3.c Stored data | **Partially achieved** | **Achieved / Partially achieved / Not achieved / N/A** | **Achieved / Partially achieved / Not achieved / N/A** | **Achieved / Partially achieved / Not achieved / N/A** | **Yes / No / N/A** |
| B3.d Mobile data | **Partially achieved** | **Achieved / Partially achieved / Not achieved / N/A** | **Achieved / Partially achieved / Not achieved / N/A** | **Achieved / Partially achieved / Not achieved / N/A** | **Yes / No / N/A** |
| B3.e Media/equipment sanitisation | **Partially achieved** | **Achieved / Partially achieved / Not achieved / N/A** | **Achieved / Partially achieved / Not achieved / N/A** | **Achieved / Partially achieved / Not achieved / N/A** | **Yes / No / N/A** |
| **System Security** | B4.a Secure by design | **Partially achieved** | **Achieved / Partially achieved / Not achieved / N/A** | **Achieved / Partially achieved / Not achieved / N/A** | **Achieved / Partially achieved / Not achieved / N/A** | **Yes / No / N/A** |
| B4.b Secure by configuration | **Partially achieved** | **Achieved / Partially achieved / Not achieved / N/A** | **Achieved / Partially achieved / Not achieved / N/A** | **Achieved / Partially achieved / Not achieved / N/A** | **Yes / No / N/A** |
| B4.c Secure management | **Partially achieved** | **Achieved / Partially achieved / Not achieved / N/A** | **Achieved / Partially achieved / Not achieved / N/A** | **Achieved / Partially achieved / Not achieved / N/A** | **Yes / No / N/A** |
| B4.d Vulnerability management | **Partially achieved** | **Achieved / Partially achieved / Not achieved / N/A** | **Achieved / Partially achieved / Not achieved / N/A** | **Achieved / Partially achieved / Not achieved / N/A** | **Yes / No / N/A** |
| **Resilient Networks and Systems** | B5.a Resilience preparation | **Partially achieved** | **Achieved / Partially achieved / Not achieved / N/A** | **Achieved / Partially achieved / Not achieved / N/A** | **Achieved / Partially achieved / Not achieved / N/A** | **Yes / No / N/A** |
| B5.b Design for resilience | **Partially achieved** | **Achieved / Partially achieved / Not achieved / N/A** | **Achieved / Partially achieved / Not achieved / N/A** | **Achieved / Partially achieved / Not achieved / N/A** | **Yes / No / N/A** |
| B5.c Backups | **Partially achieved** | **Achieved / Partially achieved / Not achieved / N/A** | **Achieved / Partially achieved / Not achieved / N/A** | **Achieved / Partially achieved / Not achieved / N/A** | **Yes / No / N/A** |
| **Staff Awareness and Training** | B6.a Cyber security culture | **Partially achieved** | **Achieved / Partially achieved / Not achieved / N/A** | **Achieved / Partially achieved / Not achieved / N/A** | **Achieved / Partially achieved / Not achieved / N/A** | **Yes / No / N/A** |
| B6.b Cybersecurity training | **Partially achieved** | **Achieved / Partially achieved / Not achieved / N/A** | **Achieved / Partially achieved / Not achieved / N/A** | **Achieved / Partially achieved / Not achieved / N/A** | **Yes / No / N/A** |

## [System 1] CAF Objective B - Detailed observations and recommendations

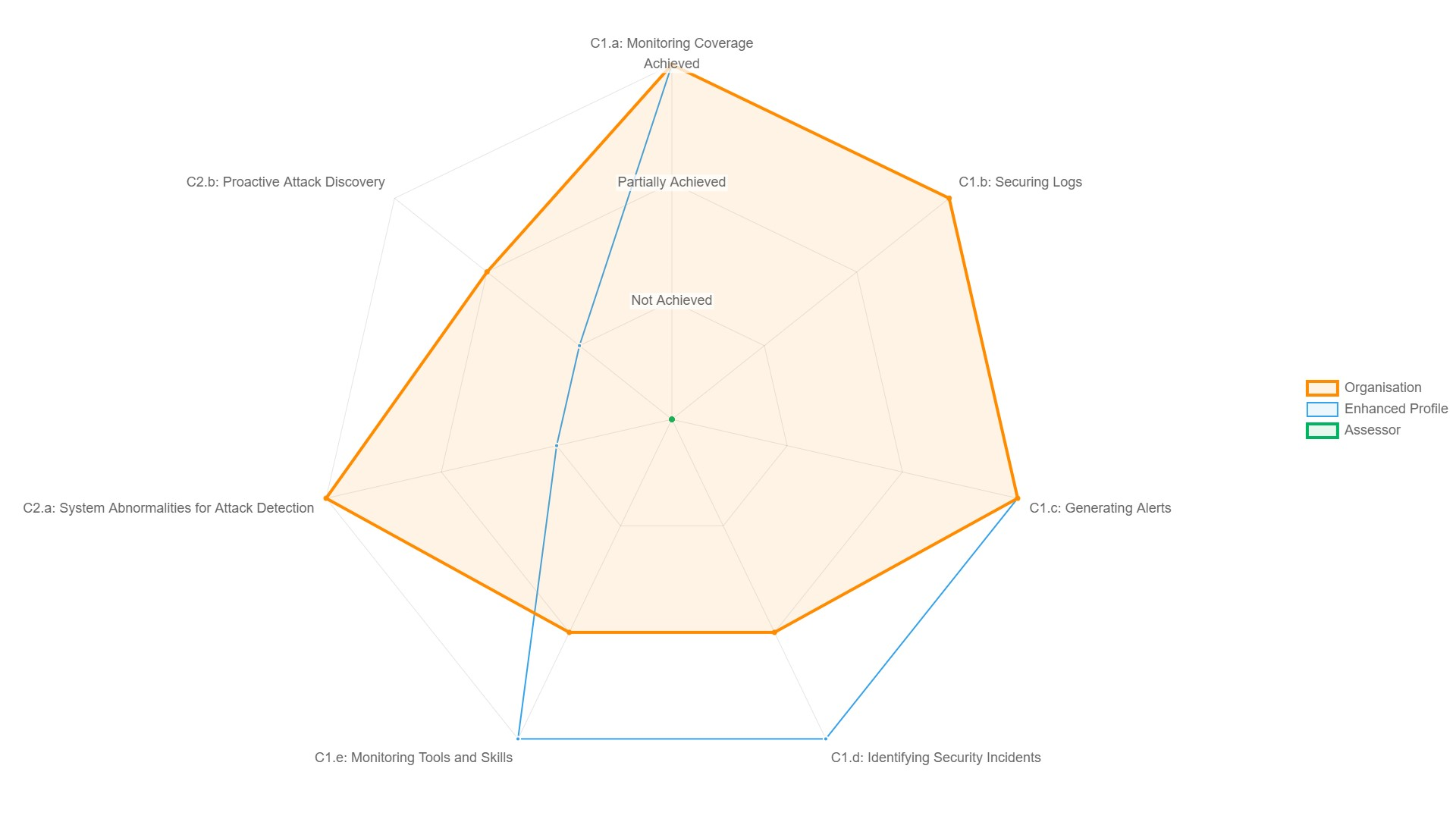
| **Obs. ref.** | **Contributing outcome** | **Detailed observations** | **Risk** | **Recommendation** |
| --- | --- | --- | --- | --- |
| **Objective B: Protecting against cyber attack** | | | | |
| **[Ref]** | **B1.a Policy and Process Development** | **##Detailed observation reporting is by exception only and against the target CAF government profile. For example, if a target is ‘partially achieved’, generally we expect observations to be raised where they fall short of the target, but it is possible to include ‘improvement opportunity’ observations. ‘Improvement opportunity’ recommendations should be flagged as such##**  **##Detail can be copied, pasted and refined here from the original assurance reviewer report output from WebCAF to identify the observation/control gap##** | **##Identify the risk associated with the issue observed##** | **##Detail the recommended action as a result of the observation##** |
|  | **B1.b Policy and process implementation** |  |  |  |
|  | **B2.a Identity Verification, Authentication and Authorisation** |  |  |  |
|  | **B2.b Device Management** |  |  | **Assessor note:**  Delete contributing outcome lines where no observations or recommendations are being raised. |
|  | **B2.c Privileged User Management** |  |  |  |
|  | **B2.d Identity and Access Management (IdAM)** |  |  |  |
|  | **B3.a Understanding Data** |  |  |  |
|  | **B3.b Data in Transit** |  |  |  |
|  | **B3.c Stored Data** |  |  |  |
|  | **B3.d Mobile Data** |  |  |  |
|  | **B3.e Media Equipment Sanitisation** |  |  |  |
|  | **B4.a Secure by Design** |  |  |  |
|  | **B4.b Secure Configuration** |  |  |  |
|  | **B4.c Secure Management** |  |  |  |
|  | **B4.d Vulnerability Management** |  |  |  |
|  | **B5.a Resilience Preparation** |  |  |  |
|  | **B5.b Design for Resilience** |  |  |  |
|  | **B5.c Backups** |  |  |  |
|  | **B6.a Cyber Security Culture** |  |  |  |
|  | **B6.b Cyber Security Training** |  |  |  |

[System 1] CAF Objective C - Contributing outcome achievement status radargram

Following the detailed examination of documentation and evidence in support of [organisation’s] CAF self-assessment, the following radargram provides a high-level summary of the independently assessed status of each contributing outcome for the [System 1]. The subsequent pages detail any exceptions or recommendations raised, as well as contributing outcomes that were insufficiently supported by evidence (where applicable).

**Assessor note:**

Example provided for illustrative purposes only. This is a placeholder for a radargram produced by WebCAF as part of the Report (HTML) functionality. It should be copied and pasted here.



[System 1] Summary – CAF Objective C: Detecting cyber security events

**Assessor note:**

Delete contributing outcome references where no comments are being made.

**C1 Security Monitoring:**

* **C1.a Monitoring Coverage -** [Exception based contributing outcome level summary]
* **C1.b Securing Logs -** [Exception based contributing outcome level summary]
* **C1.c Generating Alerts -** [Exception based contributing outcome level summary]
* **C1.d Identifying Security Incidents -** [Exception based contributing outcome level summary]
* **C1.e Monitoring Tools and Skills -** [Exception based contributing outcome level summary]

**C2 Proactive Security Event Discovery:**

* **C2.a System Abnormalities for Attack Detection -** [Exception based contributing outcome level summary]
* **C2.b Proactive Attack Discovery -** [Exception based contributing outcome level summary]

## [System 1] Objective C - Contributing outcome achievement status

The following table provides a summary of the contributing outcomes achievement status and whether the target CAF government profile has been achieved.

| **Objective** | **CAF principle** | **Contributing outcome** | **Target profile**  **(Baseline)** | **Self-assessment** | **Independent assurer assessment** | **Non-compliant IGPs** | **Profile met?** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Objective C:** **Detecting cyber security events** | **Security Monitoring** | C1.a Monitoring coverage | **Partially achieved** |  |  |  | **Yes / No / N/A** |
| C1.b Securing logs | **Partially achieved** |  |  |  | **Yes / No / N/A** |
| C1.c Generating alerts | **Achieved** |  |  |  | **Yes / No / N/A** |
| C1.d Identifying security incidents | **Partially achieved** |  |  |  | **Yes / No / N/A** |
| C1.e Monitoring tools and skills | **Achieved** |  |  |  | **Yes / No / N/A** |
| **Proactive Security Event Discovery** | C2.a System abnormalities for attack detection | **Not achieved** |  |  |  | **Yes / No / N/A** |
| C2.b Proactive attack discovery | **Not achieved** |  |  |  | **Yes / No / N/A** |

## 

## [System 1] CAF Objective C - Detailed observations and recommendations

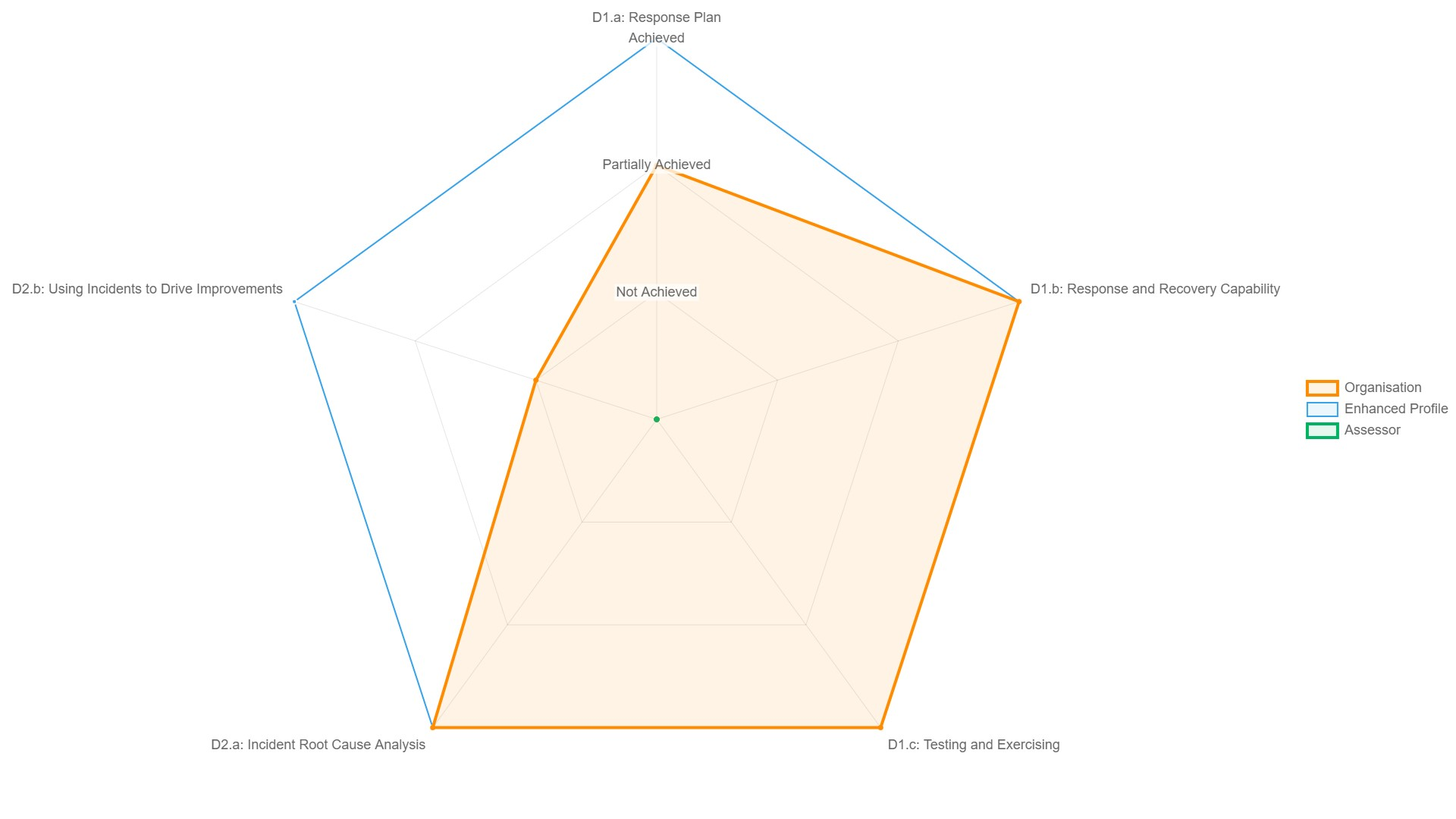
| **Obs. ref.** | **Contributing outcome** | **Detailed observations** | **Risk** | **Recommendation** |
| --- | --- | --- | --- | --- |
| **Objective C: Detecting security events** | | | | |
| **[Ref]** | **C1.a Monitoring Coverage** | **##Detailed observation reporting is by exception only and against the target CAF government profile. For example, if a target is ‘partially achieved’, generally we expect observations to be raised where they fall short of the target, but it is possible to include ‘improvement opportunity’ observations. ‘Improvement opportunity’ recommendations should be flagged as such##**  **##Detail can be copied, pasted and refined here from the original assurance reviewer report output from WebCAF to identify the observation/control gap##** | **##Identify the risk associated with the issue observed##** | **##Detail the recommended action as a result of the observation##** |
|  | **C1.b Securing Logs** |  |  |  |
|  | **C1.c Generating Alerts** |  |  |  |
|  | **C1.d Identifying Security Incidents** |  |  |  |
|  | **C1.e Monitoring Tools and Skills** |  |  |  |
|  | **C2.a System Abnormalities for Attack Detection** |  |  | **Assessor note:**  Delete contributing outcome lines where no observations or recommendations are being raised. |
| **C2.b.1** | **C2.b Proactive Attack Discovery** |  |  |  |

[System 1] CAF Objective D - Contributing outcome achievement status radargram

Following the detailed examination of documentation and evidence in support of [organisation’s] CAF self-assessment, the following radargram provides a high-level summary of the independently assessed status of each contributing outcome for the [System 1]. The subsequent pages detail any exceptions or recommendations raised, as well as contributing outcomes that were insufficiently supported by evidence (where applicable).

**Assessor note:**

Example provided for illustrative purposes only. This is a placeholder for a radargram produced by WebCAF as part of the Report (HTML) functionality. It should be copied and pasted here.



[System 1] Summary – CAF Objective D: Detecting cyber security events

**Assessor note:**

Delete contributing outcome references where no comments are being made.

**D1 Response and Recovery Planning**

* **D1.a Response Plan** - [Exception based contributing outcome level summary]
* **D1.b Response and Recovery Capability** - [Exception based contributing outcome level summary]
* **D1.c Testing and Exercising** - [Exception based contributing outcome level summary]

**D2 Lessons Learned**

* **D2.a Incident Root Cause Analysis** - [Exception based contributing outcome level summary]
* **D2.b Using Incidents to Drive Improvements** - [Exception based contributing outcome level summary]

## [System 1] CAF Objective D - Contributing outcome achievement status

The following table provides a summary of the contributing outcomes achievement status and whether the target CAF government profile has been achieved.

| **Objective** | **CAF principle** | **Contributing outcome** | **Target profile**  **(Baseline)** | **Self-assessment** | **Independent assurer assessment** | **Non-compliant IGPs** | **Profile met?** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Objective D: Minimising the impact of cyber security incidents** | **Response and Recovery Planning** | D1.a Response plan | **Achieved** |  |  |  | **Yes / No / N/A**  **Assessor note:**  For the ‘non-compliant IGPs’ column – Provide references to the non-compliant IGPs. |
| D1.b Response and recovery capability | **Achieved** |  |  |  | **Yes / No / N/A** |
| D1.c Testing and exercising | **Achieved** |  |  |  | **Yes / No / N/A** |
| **Lessons Learned** | D2.a Incident root cause analysis | **Achieved** |  |  |  | **Yes / No / N/A** |
| D2.b Using incidents to drive improvements | **Achieved** |  |  |  | **Yes / No / N/A** |

[System 1] CAF Objective D - Detailed observations and recommendations

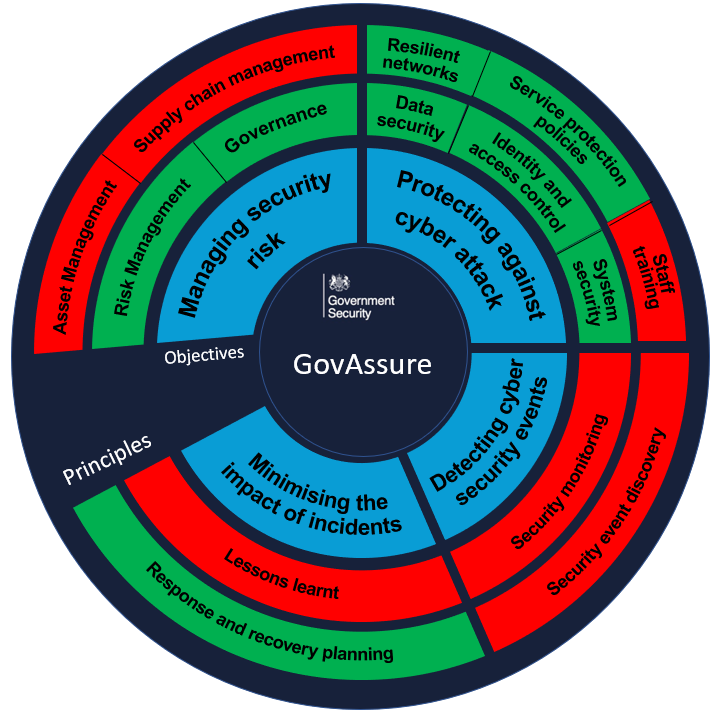
| **Obs. Ref.** | **Contributing outcome** | **Detailed Observations** | **Risk** | **Recommendation** |
| --- | --- | --- | --- | --- |
| **Objective D: Minimising the impact of incidents** | | | | |
| **[Ref]** | **D1.a Response Plan** | **##Detailed observation reporting is by exception only and against the target CAF government profile. For example, if a target is ‘partially achieved’, generally we expect observations to be raised where they fall short of the target, but it is possible to include ‘improvement opportunity’ observations. ‘Improvement opportunity’ recommendations should be flagged as such##**  **##Detail can be copied, pasted and refined here from the original assurance reviewer report output from WebCAF to identify the observation/control gap##** | **##Identify the risk associated with the issue observed##** | **##Detail the recommended action as a result of the observation##** |
| **D1.b.1** | **D1.b Response and Recovery Capability** |  |  |  |
| **D1.c.1** | **D1.c Testing and Exercising** |  |  |  |
| **D2.a.1** | **D2.a Incident Root Cause Analysis** |  |  |  |
| **D2.b.1** | **D2.b Using Incidents to Drive Improvements** |  |  |  |

**Assessor note:**

Delete contributing outcome lines where no observations or recommendations are being raised.

# [System 2] Detailed findings

## [System 2] Summary



**Introduction**

* [Introduction to the system]]
* [Context: Approach, process, any further detail on system assessment]
* [Supporting narrative]

**Target Government CAF Profile**

The system was assigned the [Baseline] target government CAF profile on the basis that [XXX]

**Assessor note:**

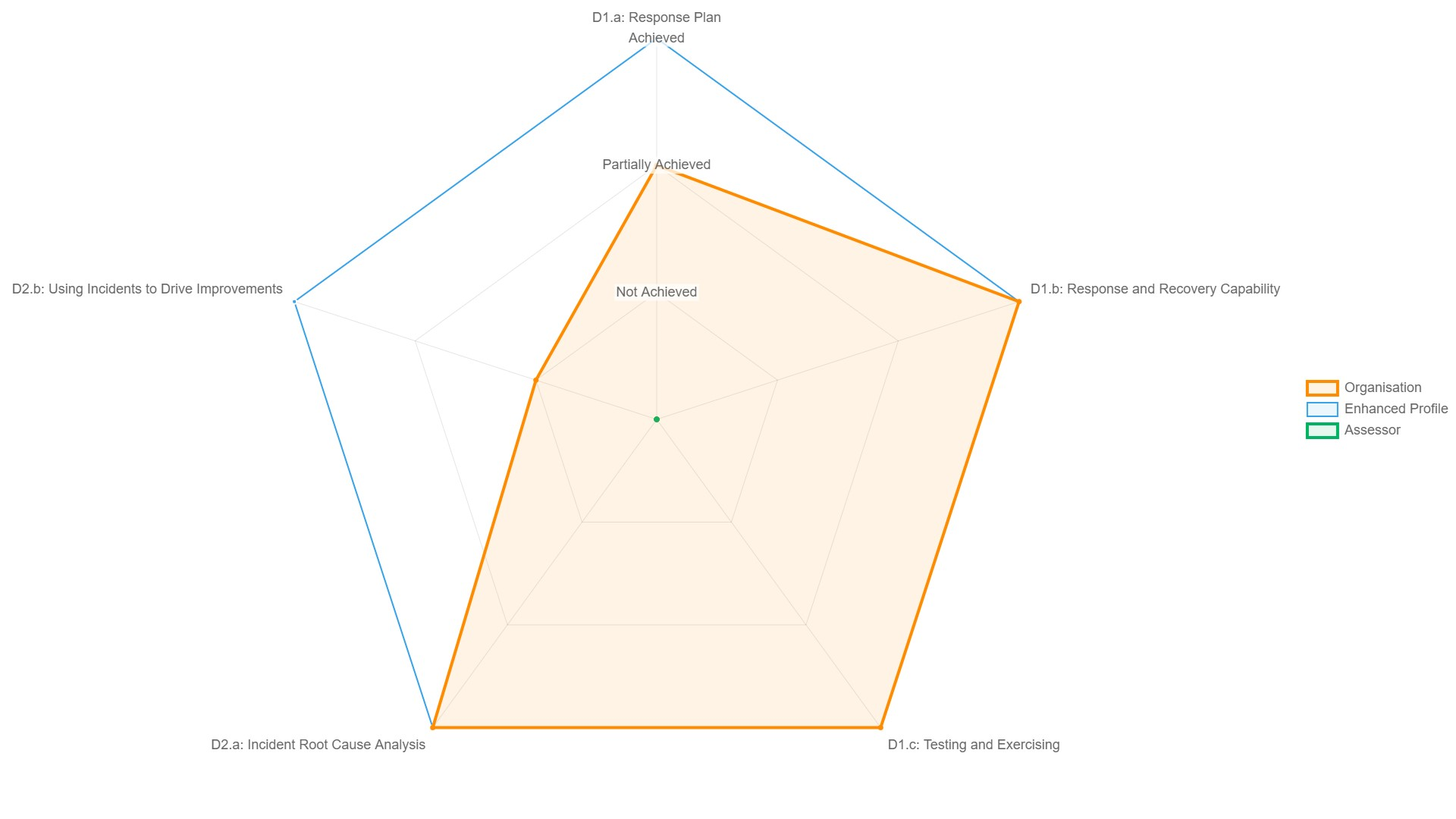
Dial provided as an example for illustrative purposes only – this diagram should be updated to reflect contributing outcomes and control gaps.

**Summary of themes**

* [Summary of high-level themes]

[System 2] CAF Objective A - Contributing outcome achievement status radargram

Following the detailed examination of documentation and evidence in support of [organisation’s] CAF self-assessment, the following radargram provides a high-level summary of the independently assessed status of each contributing outcome for the [System 2]. The subsequent pages detail any exceptions or recommendations raised, as well as contributing outcomes that were insufficiently supported by evidence (where applicable).



**Assessor note:**

Example provided for illustrative purposes only. This is a placeholder for a radargram produced by WebCAF as part of the Report (HTML) functionality. It should be copied and pasted here.

[System 2] Summary – CAF Objective A: Managing security risk

**A1 Governance:**

* **A1.a Board Direction -** [Exception based contributing outcome level summary]
* **A1.b Roles and Responsibilities** - [Exception based contributing outcome level summary]
* **A1.c Decision-making** - [Exception based contributing outcome level summary]

**A2 Risk Management:**

* **A2.a Risk Management Process** - [Exception based contributing outcome level summary]
* **A2.b Assurance** - [Exception based contributing outcome level summary]

**A3 Asset Management:**

* **A3.a Asset Management** - [Exception based contributing outcome level summary]

**A4 Supply Chain:**

* **A4.a Supply Chain** - [Exception based contributing outcome level summary]

## [System 2] CAF Objective A - Contributing outcome achievement status

The following table provides a summary of the contributing outcomes achievement status and whether the target CAF government profile has been achieved.

| **Objective** | **CAF principle** | **Contributing outcome** | **Target profile**  **(Baseline)** | **Self-assessment** | **Independent assurer assessment** | **Non-compliant IGPs** | **Profile met?** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Objective A: Managing security risk** | **Governance** | A1.a Board Direction | **Achieved** |  |  |  | **Yes / No / N/A** |
| A1.b Roles and Responsibilities | **Achieved** |  |  |  | **Yes / No / N/A** |
| A1.c Decision Making | **Achieved** |  |  |  | **Yes / No / N/A** |
| **Risk Management** | A2.a Risk management process | **Partially achieved** |  |  |  | **Yes / No / N/A** |
| A2.b Assurance | **Achieved** |  |  |  | **Yes / No / N/A** |
| **Asset Management** | A3.a Asset management | **Achieved** |  |  |  | **Yes / No / N/A** |
| **Supply Chain** | A4.a Supply chain | **Partially achieved** |  |  |  | **Yes / No / N/A** |

## 

## [System 2] CAF Objective A - Detailed observations and recommendations

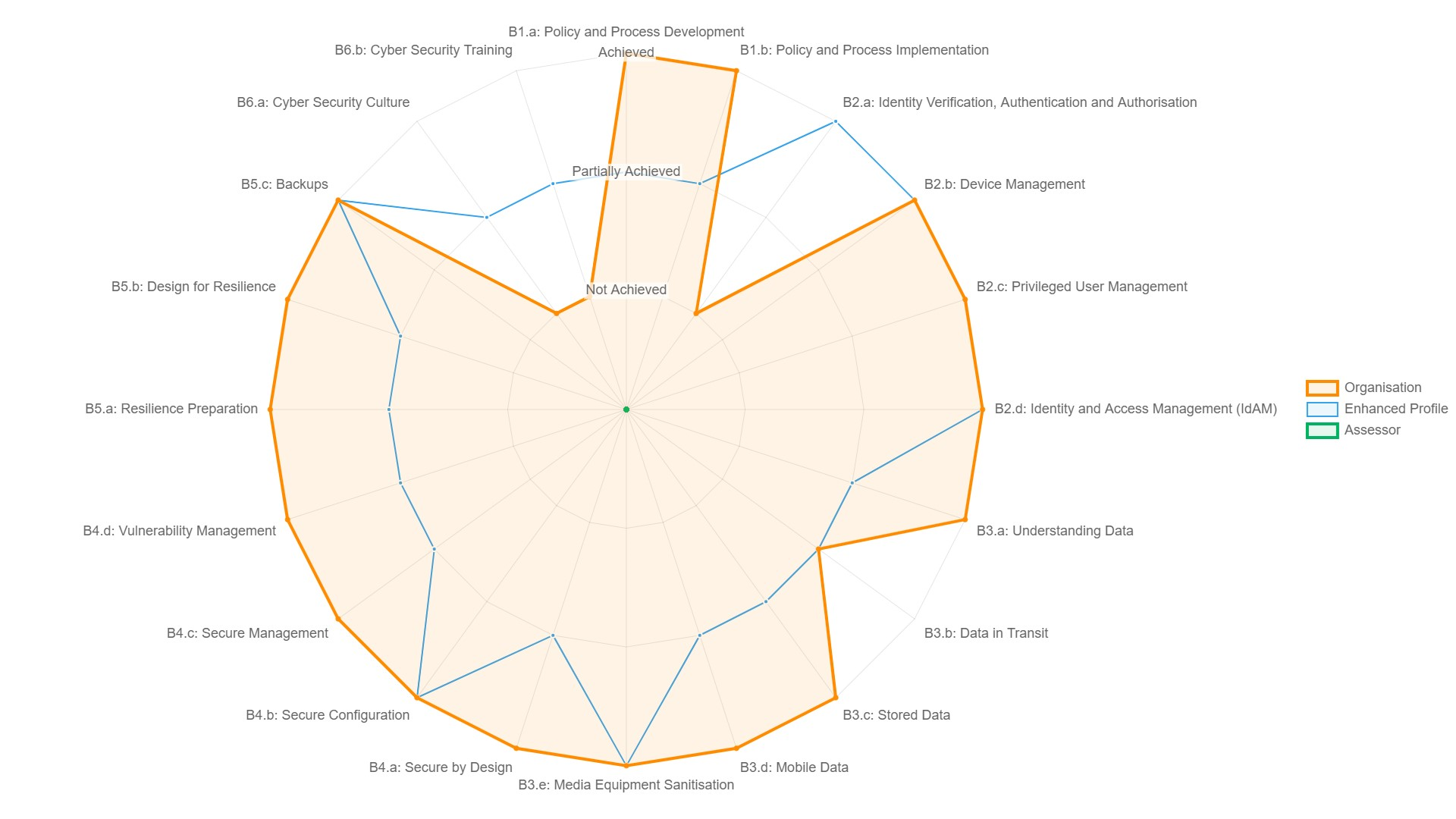
| **Obs. ref.** | **Contributing outcome** | **Detailed observations** | **Risk** | **Recommendation** |
| --- | --- | --- | --- | --- |
| **Objective A: Managing security risk** | | | | |
| **[Ref]** | **A1.a Board Direction** | **##Detailed observation reporting is by exception only and against the target CAF government profile. For example, if a target is ‘partially achieved’, generally we expect observations to be raised where they fall short of the target, but it is possible to include ‘improvement opportunity’ observations. ‘Improvement opportunity’ recommendations should be flagged as such##**  **##Detail can be copied, pasted and refined here from the original assurance reviewer report output from WebCAF to identify the observation/control gap##** | **##Identify the risk associated with the issue observed##** | **##Detail the recommended action as a result of the observation##** |
|  | **A1.b Roles and Responsibilities** |  |  |  |
|  | **A1.c Decision-making** |  |  |  |
|  | **A2.a Risk Management Process** |  |  |  |
|  | **A2.b Assurance** |  |  |  |
|  | **A3.a Asset Management** |  |  |  |
|  | **A4.a Supply Chain** |  |  |  |

[System 2] CAF Objective B - Contributing outcome achievement status radargram

Following the detailed examination of documentation and evidence in support of [organisation’s] CAF self-assessment, the following radargram provides a high-level summary of the independently assessed status of each contributing outcome for the [System 2]. The subsequent pages detail any exceptions or recommendations raised, as well as contributing outcomes that were insufficiently supported by evidence (where applicable).

**Assessor note:**

Example provided for illustrative purposes only. This is a placeholder for a radargram produced by WebCAF as part of the Report (HTML) functionality. It should be copied and pasted here.



[System 2] Summary – CAF Objective B: Protecting against cyber attack

**B1 Service Protection Policies and Processes:**

* **B1.a Policy and Process Development -** [Exception based contributing outcome level summary]
* **B1.b Policy and Process Implementation -** [Exception based contributing outcome level summary]

**B2 Identity and Access Controls:**

* **B2.a Identity Verification, Authentication and Authorisation -** [Exception based contributing outcome level summary]
* **B2.b Device Management -** [Exception based contributing outcome level summary]
* **B2.c Privileged User Management -** [Exception based contributing outcome level summary]
* **B2.d Identity and Access Management (IdAM**) **-** [Exception based contributing outcome level summary]

**B3 Data Security:**

* **B3.a Understanding Data -** [Exception based contributing outcome level summary]
* **B3.b Data in Transit -** [Exception based contributing outcome level summary]
* **B3.c Stored Data -** [Exception based contributing outcome level summary]
* **B3.d Mobile Data -** [Exception based contributing outcome level summary]
* **B3.e Media Equipment Sanitisation -** [Exception based contributing outcome level summary]

**B4 System security:**

* **B4.a Secure by Design -** [Exception based contributing outcome level summary]
* **B4.b Secure Configuration -** [Exception based contributing outcome level summary]
* **B4.c Secure Management -** [Exception based contributing outcome level summary]
* **B4.d Vulnerability Management -** [Exception based contributing outcome level summary]

**B5 Resilient Networks and Systems:**

* **B5.a Resilience Preparation -** [Exception based contributing outcome level summary]
* **B5.b Design for Resilience -** [Exception based contributing outcome level summary]
* **B5.c Backups -** [Exception based contributing outcome level summary]

**B6: Staff awareness and training:**

* **B6.a Cyber Security Culture -** [Exception based contributing outcome level summary]
* **B6.b Cyber Security Training** **-** [Exception based contributing outcome level summary]

## [System 2] CAF Objective B - Contributing outcome achievement status

The following table provides a summary of the contributing outcomes achievement status and whether the target CAF government profile has been achieved.

| **Objective** | **CAF principle** | **Contributing outcome** | **Target profile**  **(Baseline)** | **Self-assessment** | **Independent assurer assessment** | **Non-compliant IGPs** | **Profile met?** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Objective B: Protecting against cyber attack** | **Service Protection Policies and Processes** | B1.a Policy and process development | **Partially achieved** |  |  |  | **Yes / No / N/A** |
| B1.b Policy and process implementation | **Partially achieved** |  |  |  | **Yes / No / N/A** |
| **Identity and Access Controls** | B2.a Identity verification, authentication, and authorisation | **Partially achieved** |  |  |  | **Yes / No / N/A** |
| B2.b Device management | **Partially achieved** |  |  |  | **Yes / No / N/A** |
| B2.c Privileged user management | **Partially achieved** |  |  |  | **Yes / No / N/A** |
| B2.d IDAC management and maintenance | **Partially achieved** |  |  |  | **Yes / No / N/A** |
| **Data Security** | B3.a Understanding data | **Partially achieved** |  |  |  | **Yes / No / N/A** |
| B3.b Data in transit | **Partially achieved** |  |  |  | **Yes / No / N/A** |
| B3.c Stored data | **Partially achieved** |  |  |  | **Yes / No / N/A** |
| B3.d Mobile data | **Partially achieved** |  |  |  | **Yes / No / N/A** |
| B3.e Media/equipment sanitisation | **Partially achieved** |  |  |  | **Yes / No / N/A** |
| **System Security** | B4.a Secure by design | **Partially achieved** |  |  |  | **Yes / No / N/A** |
| B4.b Secure by configuration | **Partially achieved** |  |  |  | **Yes / No / N/A** |
| B4.c Secure management | **Partially achieved** |  |  |  | **Yes / No / N/A** |
| B4.d Vulnerability management | **Partially achieved** |  |  |  | **Yes / No / N/A** |
| **Resilient Networks and Systems** | B5.a Resilience preparation | **Partially achieved** |  |  |  | **Yes / No / N/A** |
| B5.b Design for resilience | **Partially achieved** |  |  |  | **Yes / No / N/A** |
| B5.c Backups | **Partially achieved** |  |  |  | **Yes / No / N/A** |
| **Staff Awareness and Training** | B6.a Cyber security culture | **Partially achieved** |  |  |  | **Yes / No / N/A** |
| B6.b Cybersecurity training | **Partially achieved** |  |  |  | **Yes / No / N/A** |

## 

## [System 2] CAF Objective B - Detailed observations and recommendations

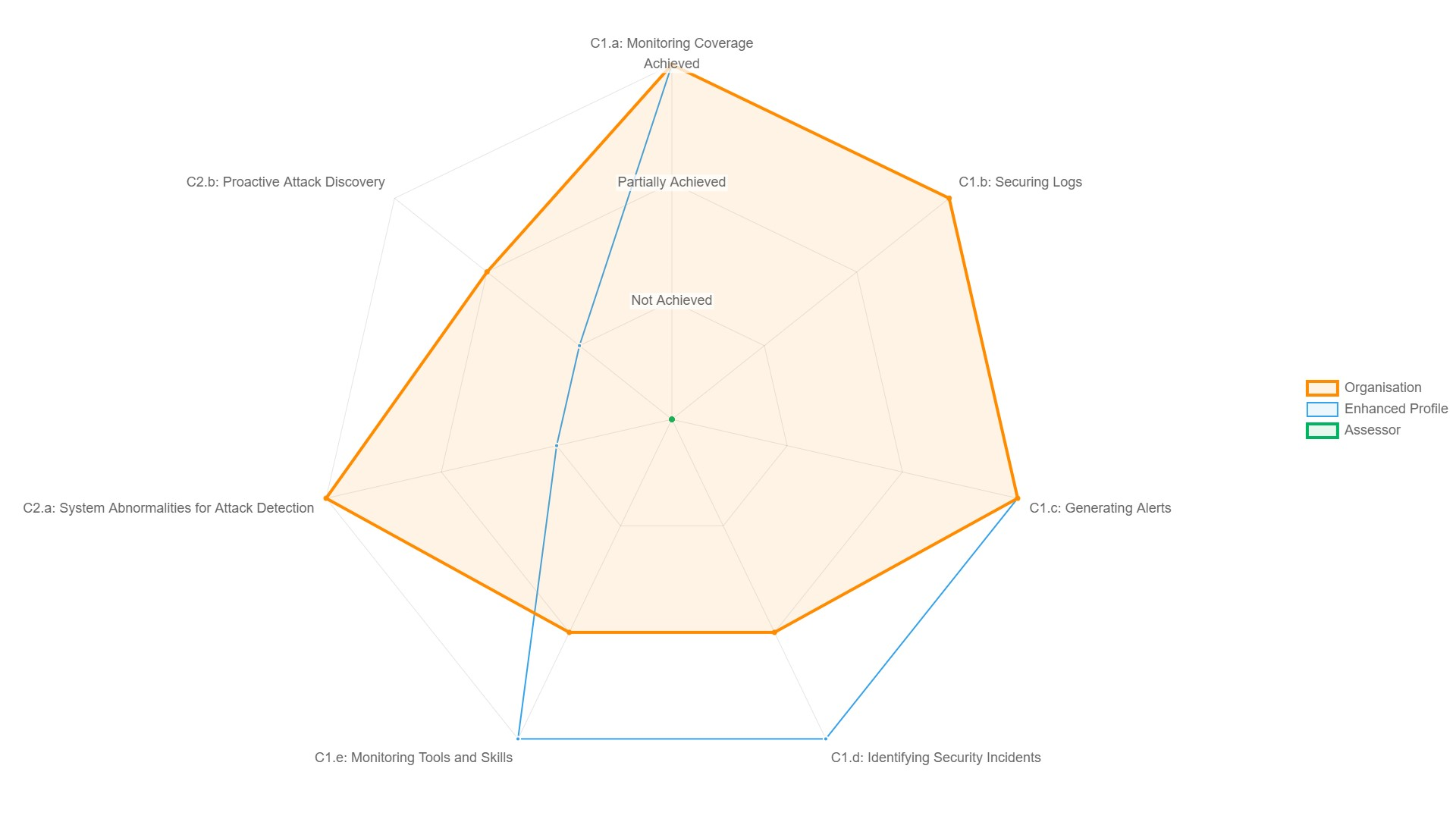
| **Obs. Ref.** | **Contributing outcome** | **Detailed observations** | **Risk** | **Recommendation** |
| --- | --- | --- | --- | --- |
| **Objective B: Protecting against cyber attack** | | | | |
| **[Ref]** | **B1.a Policy and Process Development** | **##Detailed observation reporting is by exception only and against the target CAF government profile. For example, if a target is ‘partially achieved’, generally we expect observations to be raised where they fall short of the target, but it is possible to include ‘improvement opportunity’ observations. ‘Improvement opportunity’ recommendations should be flagged as such##**  **##Detail can be copied, pasted and refined here from the original assurance reviewer report output from WebCAF to identify the observation/control gap##** | **##Identify the risk associated with the issue observed##** | **##Detail the recommended action as a result of the observation##** |
|  | **B1.b Policy and process implementation** |  |  |  |
|  | **B2.a Identity Verification, Authentication and Authorisation** |  |  |  |
|  | **B2.b Device Management** |  |  |  |
|  | **B2.c Privileged User Management** |  |  |  |
|  | **B2.d Identity and Access Management (IdAM)** |  |  |  |
|  | **B3.a Understanding Data** |  |  |  |
|  | **B3.b Data in Transit** |  |  |  |
|  | **B3.c Stored Data** |  |  |  |
|  | **B3.d Mobile Data** |  |  |  |
|  | **B3.e Media Equipment Sanitisation** |  |  |  |
|  | **B4.a Secure by Design** |  |  |  |
|  | **B4.b Secure Configuration** |  |  |  |
|  | **B4.c Secure Management** |  |  |  |
|  | **B4.d Vulnerability Management** |  |  |  |
|  | **B5.a Resilience Preparation** |  |  |  |
|  | **B5.b Design for Resilience** |  |  |  |
|  | **B5.c Backups** |  |  |  |
|  | **B6.a Cyber Security Culture** |  |  |  |
|  | **B6.b Cyber Security Training** |  |  |  |

[System 2] CAF Objective C - Contributing outcome achievement status radargram

Following the detailed examination of documentation and evidence in support of [organisation’s] CAF self-assessment, the following radargram provides a high-level summary of the independently assessed status of each contributing outcome for the [System 2]. The subsequent pages detail any exceptions or recommendations raised, as well as contributing outcomes that were insufficiently supported by evidence (where applicable).

**Assessor note:**

Example provided for illustrative purposes only. This is a placeholder for a radargram produced by WebCAF as part of the Report (HTML) functionality. It should be copied and pasted here.



[System 2] Summary – CAF Objective C: Detecting cyber security events

**C1 Security Monitoring:**

* **C1.a Monitoring Coverage -** [Exception based contributing outcome level summary]
* **C1.b Securing Logs -** [Exception based contributing outcome level summary]
* **C1.c Generating Alerts -** [Exception based contributing outcome level summary]
* **C1.d Identifying Security Incidents -** [Exception based contributing outcome level summary]
* **C1.e Monitoring Tools and Skills -** [Exception based contributing outcome level summary]

**C2 Proactive Security Event Discovery:**

* **C2.a System Abnormalities for Attack Detection -** [Exception based contributing outcome level summary]
* **C2.b Proactive Attack Discovery -** [Exception based contributing outcome level summary]

## [System 2] CAF Objective C - Contributing outcome achievement status

The following table provides a summary of the contributing outcomes achievement status and whether the target CAF government profile has been achieved.

| **Objective** | **CAF principle** | **Contributing outcome** | **Target profile**  **(Baseline)** | **Self-assessment** | **Independent assurer assessment** | **Non-compliant IGPs** | **Profile met?** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Objective C:** **Detecting cyber security events** | **Security Monitoring** | C1.a Monitoring coverage | **Partially achieved** |  |  |  | **Yes / No / N/A** |
| C1.b Securing logs | **Partially achieved** |  |  |  | **Yes / No / N/A** |
| C1.c Generating alerts | **Achieved** |  |  |  | **Yes / No / N/A** |
| C1.d Identifying security incidents | **Partially achieved** |  |  |  | **Yes / No / N/A** |
| C1.e Monitoring tools and skills | **Achieved** |  |  |  | **Yes / No / N/A** |
| **Proactive Security Event Discovery** | C2.a System abnormalities for attack detection | **Not achieved** |  |  |  | **Yes / No / N/A** |
| C2.b Proactive attack discovery | **Not achieved** |  |  |  | **Yes / No / N/A** |

## 

## [System 2] CAF Objective C - Detailed observations and recommendations

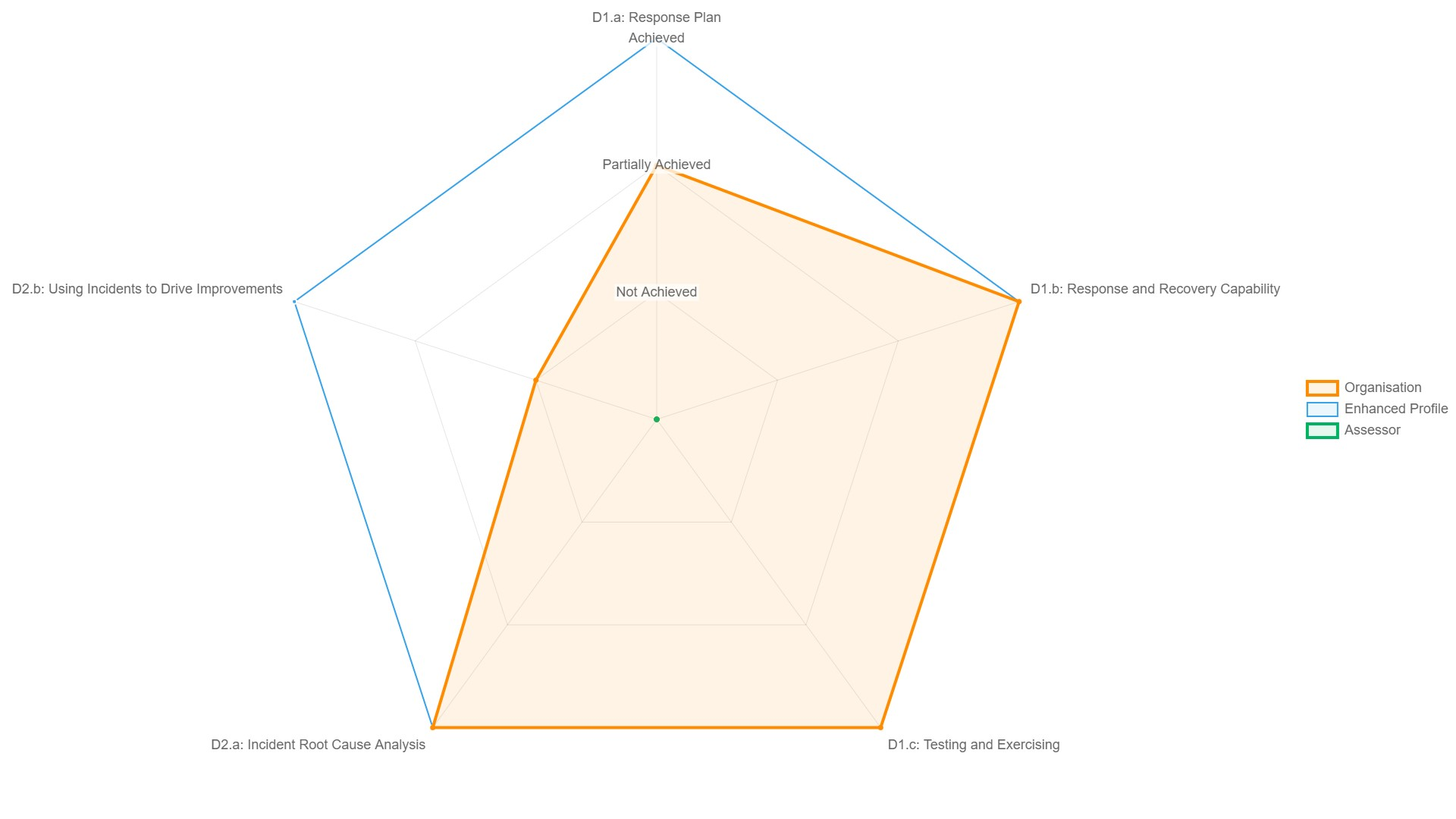
| **Obs. ref.** | **Contributing outcome** | **Detailed observations** | **Risk** | **Recommendation** |
| --- | --- | --- | --- | --- |
| **Objective C: Detecting security events** | | | | |
| **[Ref]** | **C1.a Monitoring Coverage** | **##Detailed observation reporting is by exception only and against the target CAF government profile. For example, if a target is ‘partially achieved’, generally we expect observations to be raised where they fall short of the target, but it is possible to include ‘improvement opportunity’ observations. ‘Improvement opportunity’ recommendations should be flagged as such##**  **##Detail can be copied, pasted and refined here from the original assurance reviewer report output from WebCAF to identify the observation/control gap##** | **##Identify the risk associated with the issue observed##** | **##Detail the recommended action as a result of the observation##** |
|  | **C1.b Securing Logs** |  |  |  |
|  | **C1.c Generating Alerts** |  |  |  |
|  | **C1.d Identifying Security Incidents** |  |  |  |
|  | **C1.e Monitoring Tools and Skills** |  |  |  |
|  | **C2.a System Abnormalities for Attack Detection** |  |  |  |
|  | **C2.b Proactive Attack Discovery** |  |  |  |

[System 2] CAF Objective D - Contributing outcome achievement status radargram

Following the detailed examination of documentation and evidence in support of [organisation’s] CAF self-assessment, the following radargram provides a high-level summary of the independently assessed status of each contributing outcome for the [System 2]. The subsequent pages detail any exceptions or recommendations raised, as well as contributing outcomes that were insufficiently supported by evidence (where applicable).

**Assessor note:**

Example provided for illustrative purposes only. This is a placeholder for a radargram produced by WebCAF as part of the Report (HTML) functionality. It should be copied and pasted here.



[System 2] Summary – CAF Objective D: Detecting cyber security events

**D1 Response and Recovery Planning**

* **D1.a Response Plan** - [Exception based contributing outcome level summary]
* **D1.b Response and Recovery Capability** - [Exception based contributing outcome level summary]
* **D1.c Testing and Exercising** - [Exception based contributing outcome level summary]

**D2 Lessons Learned**

* **D2.a Incident Root Cause Analysis** - [Exception based contributing outcome level summary]
* **D2.b Using Incidents to Drive Improvements** - [Exception based contributing outcome level summary]

## [System 2] CAF Objective D - Contributing outcome achievement status

The following table provides a summary of the contributing outcomes achievement status and whether the target CAF government profile has been achieved.

| **Objective** | **CAF principle** | **Contributing outcome** | **Target profile**  **(Baseline)** | **Self-assessment** | **Independent assurer assessment** | **Non-compliant IGPs** | **Profile met?** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Objective D: Minimising the impact of cyber security incidents** | **Response and Recovery Planning** | D1.a Response plan | **Achieved** |  |  |  | **Yes / No / N/A** |
| D1.b Response and recovery capability | **Achieved** |  |  |  | **Yes / No / N/A** |
| D1.c Testing and exercising | **Achieved** |  |  |  | **Yes / No / N/A** |
| **Lessons Learned** | D2.a Incident root cause analysis | **Achieved** |  |  |  | **Yes / No / N/A** |
| D2.b Using incidents to drive improvements | **Achieved** |  |  |  | **Yes / No / N/A** |

## [System 2] CAF Objective D - Detailed observations and recommendations

| **Obs. Ref.** | **Contributing outcome** | **Detailed observations** | **Risk** | **Recommendation** |
| --- | --- | --- | --- | --- |
| **Objective D: Minimising the impact of incidents** | | | | |
| **D1.a.1** | **D1.a Response Plan** | **##Detailed observation reporting is by exception only and against the target CAF government profile. For example, if a target is ‘partially achieved’, generally we expect observations to be raised where they fall short of the target, but it is possible to include ‘improvement opportunity’ observations. ‘Improvement opportunity’ recommendations should be flagged as such##**  **##Detail can be copied, pasted and refined here from the original assurance reviewer report output from WebCAF to identify the observation/control gap##** | **##Identify the risk associated with the issue observed##** | **##Detail the recommended action as a result of the observation##** |
| **D1.b.1** | **D1.b Response and Recovery Capability** |  |  |  |
| **D1.c.1** | **D1.c Testing and Exercising** |  |  |  |
| **D2.a.1** | **D2.a Incident Root Cause Analysis** |  |  |  |
| **D2.b.1** | **D2.b Using Incidents to Drive Improvements** |  |  |  |

# [System 3] Detailed findings

## [System 3] Summary

**Introduction**

* [Introduction to the system]]
* [Context: Approach, process, any further detail on system assessment]
* [Supporting narrative]

**Target Government CAF Profile**

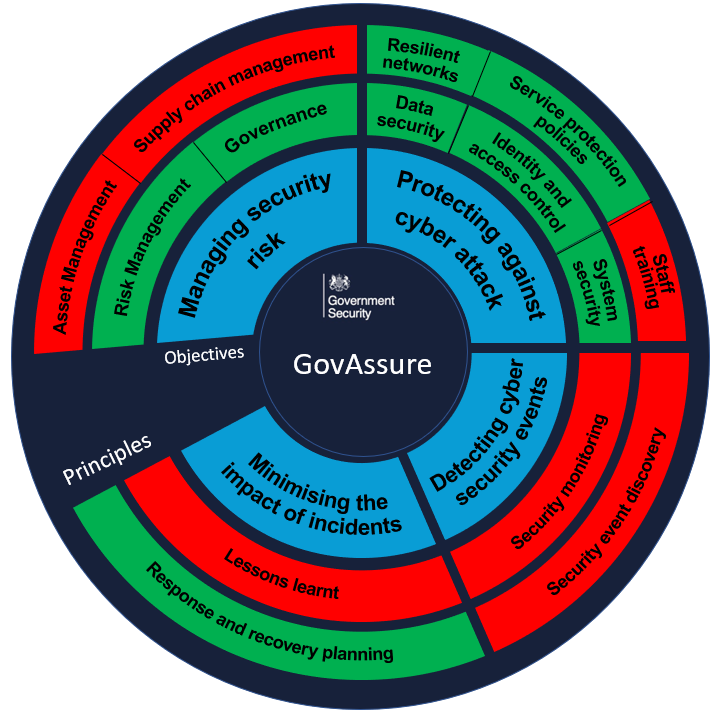
The system was assigned the [Enhanced] target government CAF profile on the basis that [XXX]

**Assessor note:**

Dial provided as an example for illustrative purposes only – this diagram should be updated to reflect contributing outcomes and control gaps.

**Summary of themes**

* [Summary of high-level themes]

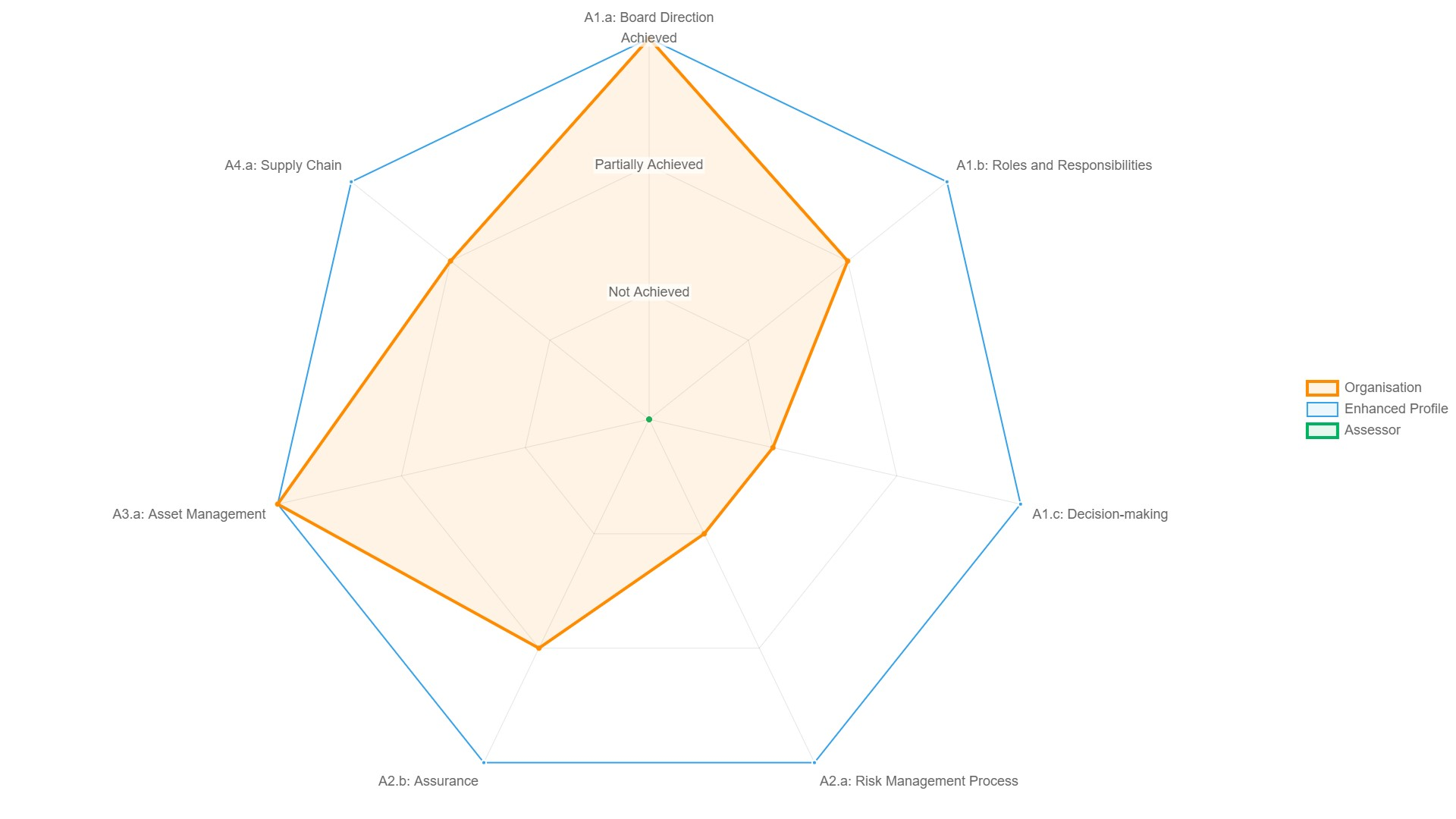


[System 3] CAF Objective A - Contributing outcome achievement status radargram

Following the detailed examination of documentation and evidence in support of [organisation’s] CAF self-assessment, the following radargram provides a high-level summary of the independently assessed status of each contributing outcome for the [System 3]. The subsequent pages detail any exceptions or recommendations raised, as well as contributing outcomes that were insufficiently supported by evidence (where applicable).

**Assessor note:**

Example provided for illustrative purposes only. This is a placeholder for a radargram produced by WebCAF as part of the Report (HTML) functionality. It should be copied and pasted here.



[System 3] Summary – CAF Objective A: Managing security risk

**A1 Governance:**

* **A1.a Board Direction -** [Exception based contributing outcome level summary]
* **A1.b Roles and Responsibilities** - [Exception based contributing outcome level summary]
* **A1.c Decision-making** - [Exception based contributing outcome level summary]

**A2 Risk Management:**

* **A2.a Risk Management Process** - [Exception based contributing outcome level summary]
* **A2.b Assurance** - [Exception based contributing outcome level summary]

**A3 Asset Management:**

* **A3.a Asset Management** - [Exception based contributing outcome level summary]

**A4 Supply Chain:**

* **A4.a Supply Chain** - [Exception based contributing outcome level summary]

## [System 3] CAF Objective A - Contributing outcome achievement status

The following table provides a summary of the contributing outcomes achievement status and whether the target CAF government profile has been achieved.

| **Objective** | **CAF principle** | **Contributing outcome** | **Target profile**  **(Enhanced)** | **Self-assessment** | **Independent assurer assessment** | **Non-compliant IGPs** | **Profile met?** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Objective A: Managing security risk** | **Governance** | A1.a Board Direction | **Achieved** | **Achieved** | **Not achieved** |  | **No** |
| A1.b Roles and Responsibilities | **Achieved** |  |  |  | **Yes / No / N/A** |
| A1.c Decision Making | **Achieved** |  |  |  | **Yes / No / N/A** |
| **Risk Management** | A2.a Risk management process | **Achieved** |  |  |  | **Yes / No / N/A** |
| A2.b Assurance | **Achieved** |  |  |  | **Yes / No / N/A** |
| **Asset Management** | A3.a Asset management | **Achieved** |  |  |  | **Yes / No / N/A** |
| **Supply Chain** | A4.a Supply chain | **Achieved** |  |  |  | **Yes / No / N/A** |
|  | D2.b Using incidents to drive improvements | **Achieved** |  |  |  | **Yes / No / N/A** |

## [System 3] CAF Objective A - Detailed observations and recommendations

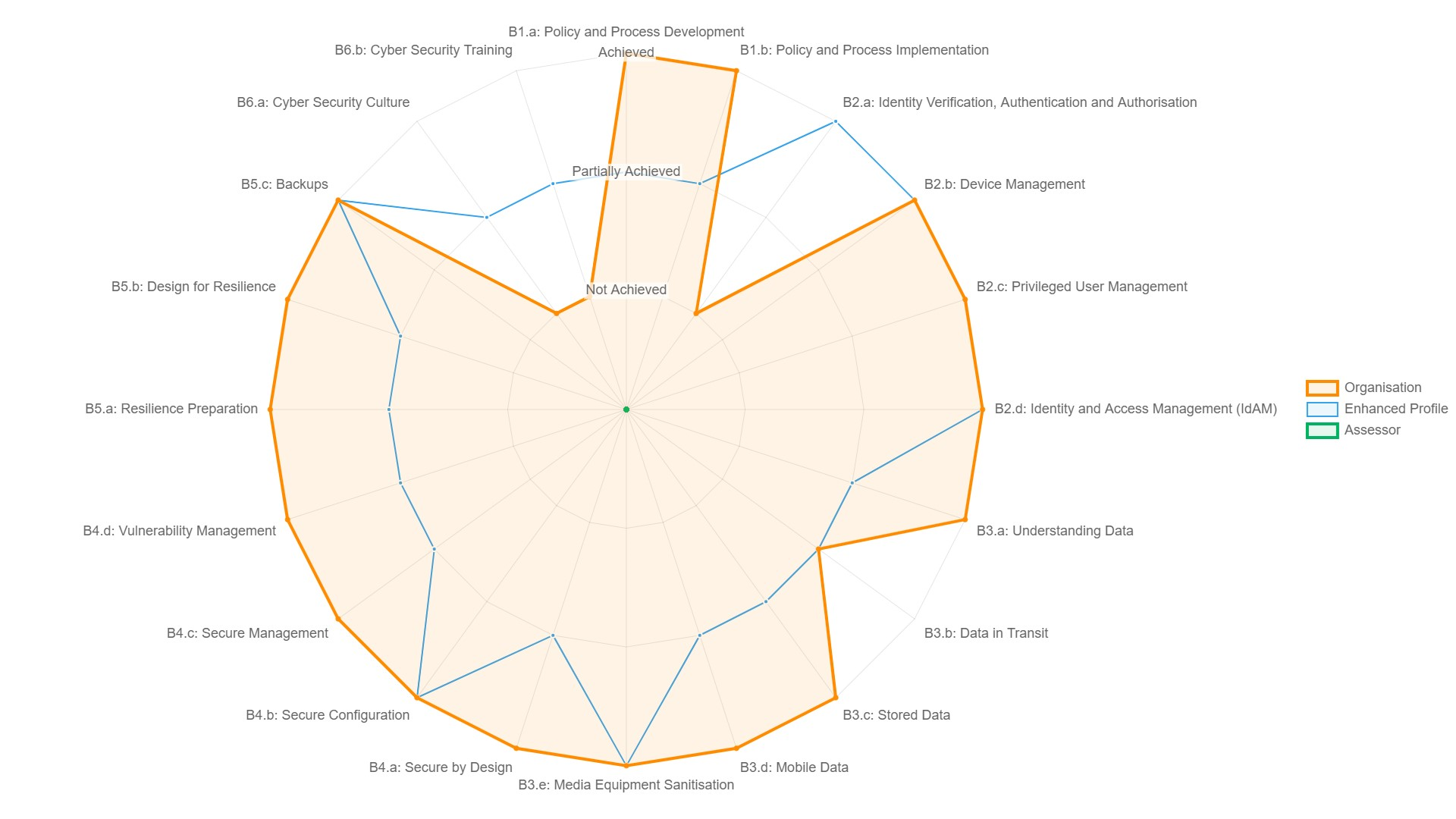
| **Obs. Ref.** | **Contributing outcome** | **Detailed observations** | **Risk** | **Recommendation** |
| --- | --- | --- | --- | --- |
| **Objective A: Managing security risk** | | | | |
| **[Ref]** | **A1.a Board Direction** | **##Detailed observation reporting is by exception only and against the target CAF government profile. For example, if a target is ‘partially achieved’, generally we expect observations to be raised where they fall short of the target, but it is possible to include ‘improvement opportunity’ observations. ‘Improvement opportunity’ recommendations should be flagged as such##**  **##Detail can be copied, pasted and refined here from the original assurance reviewer report output from WebCAF to identify the observation/control gap##** | **##Identify the risk associated with the issue observed##** | **##Detail the recommended action as a result of the observation##** |
|  | **A1.b Roles and Responsibilities** |  |  |  |
|  | **A1.c Decision-making** |  |  |  |
|  | **A2.a Risk Management Process** |  |  |  |
|  | **A2.b Assurance** |  |  |  |
|  | **A3.a Asset Management** |  |  |  |
|  | **A4.a Supply Chain** |  |  |  |

[System 3] CAF Objective B - Contributing outcome achievement status radargram

Following the detailed examination of documentation and evidence in support of [organisation’s] CAF self-assessment, the following radargram provides a high-level summary of the independently assessed status of each contributing outcome for the [System 3]. The subsequent pages detail any exceptions or recommendations raised, as well as contributing outcomes that were insufficiently supported by evidence (where applicable).

**Assessor note:**

Example provided for illustrative purposes only. This is a placeholder for a radargram produced by WebCAF as part of the Report (HTML) functionality. It should be copied and pasted here.



[System 3] Summary – CAF Objective B: Protecting against cyber attack

**B1 Service Protection Policies and Processes:**

* **B1.a Policy and Process Development -** [Exception based contributing outcome level summary]
* **B1.b Policy and Process Implementation -** [Exception based contributing outcome level summary]

**B2 Identity and Access Controls:**

* **B2.a Identity Verification, Authentication and Authorisation -** [Exception based contributing outcome level summary]
* **B2.b Device Management -** [Exception based contributing outcome level summary]
* **B2.c Privileged User Management -** [Exception based contributing outcome level summary]
* **B2.d Identity and Access Management (IdAM**) **-** [Exception based contributing outcome level summary]

**B3 Data Security:**

* **B3.a Understanding Data -** [Exception based contributing outcome level summary]
* **B3.b Data in Transit -** [Exception based contributing outcome level summary]
* **B3.c Stored Data -** [Exception based contributing outcome level summary]
* **B3.d Mobile Data -** [Exception based contributing outcome level summary]
* **B3.e Media Equipment Sanitisation -** [Exception based contributing outcome level summary]

**B4 System security:**

* **B4.a Secure by Design -** [Exception based contributing outcome level summary]
* **B4.b Secure Configuration -** [Exception based contributing outcome level summary]
* **B4.c Secure Management -** [Exception based contributing outcome level summary]
* **B4.d Vulnerability Management -** [Exception based contributing outcome level summary]

**B5 Resilient Networks and Systems:**

* **B5.a Resilience Preparation -** [Exception based contributing outcome level summary]
* **B5.b Design for Resilience -** [Exception based contributing outcome level summary]
* **B5.c Backups -** [Exception based contributing outcome level summary]

**B6: Staff awareness and training:**

* **B6.a Cyber Security Culture -** [Exception based contributing outcome level summary]
* **B6.b Cyber Security Training** **-** [Exception based contributing outcome level summary]

## [System 3] CAF Objective B - Contributing outcome achievement status

The following table provides a summary of the contributing outcomes achievement status and whether the target CAF government profile has been achieved.

| **Objective** | **CAF principle** | **Contributing outcome** | **Target profile**  **(Enhanced)** | **Self-assessment** | **Independent assurer assessment** | **Non-compliant IGPs** | **Profile met?** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Objective B: Protecting against cyber attack** | **Service Protection Policies and Processes** | B1.a Policy and process development | **Partially Achieved** |  |  |  | **Yes / No / N/A** |
| B1.b Policy and process implementation | **Partially Achieved** |  |  |  | **Yes / No / N/A** |
| **Identity and Access Controls** | B2.a Identity verification, authentication, and authorisation | **Achieved** |  |  |  | **Yes / No / N/A** |
| B2.b Device management | **Achieved** |  |  |  | **Yes / No / N/A** |
| B2.c Privileged user management | **Achieved** |  |  |  | **Yes / No / N/A** |
| B2.d IDAC management and maintenance | **Achieved** |  |  |  | **Yes / No / N/A** |
| **Data Security** | B3.a Understanding data | **Partially Achieved** |  |  |  | **Yes / No / N/A** |
| B3.b Data in transit | **Partially Achieved** |  |  |  | **Yes / No / N/A** |
| B3.c Stored data | **Partially Achieved** |  |  |  | **Yes / No / N/A** |
| B3.d Mobile data | **Partially Achieved** |  |  |  | **Yes / No / N/A** |
| B3.e Media/equipment sanitisation | **Achieved** |  |  |  | **Yes / No / N/A** |
| **System Security** | B4.a Secure by design | **Partially Achieved** |  |  |  | **Yes / No / N/A** |
| B4.b Secure by configuration | **Achieved** |  |  |  | **Yes / No / N/A** |
| B4.c Secure management | **Partially Achieved** |  |  |  | **Yes / No / N/A** |
| B4.d Vulnerability management | **Partially Achieved** |  |  |  | **Yes / No / N/A** |
| **Resilient Networks and Systems** | B5.a Resilience preparation | **Partially Achieved** |  |  |  | **Yes / No / N/A** |
| B5.b Design for resilience | **Partially Achieved** |  |  |  | **Yes / No / N/A** |
| B5.c Backups | **Achieved** |  |  |  | **Yes / No / N/A** |
| **Staff Awareness and Training** | B6.a Cyber security culture | **Partially Achieved** |  |  |  | **Yes / No / N/A** |
| B6.b Cybersecurity training | **Partially Achieved** |  |  |  | **Yes / No / N/A** |

## 

## [System 3] CAF Objective B - Detailed observations and recommendations

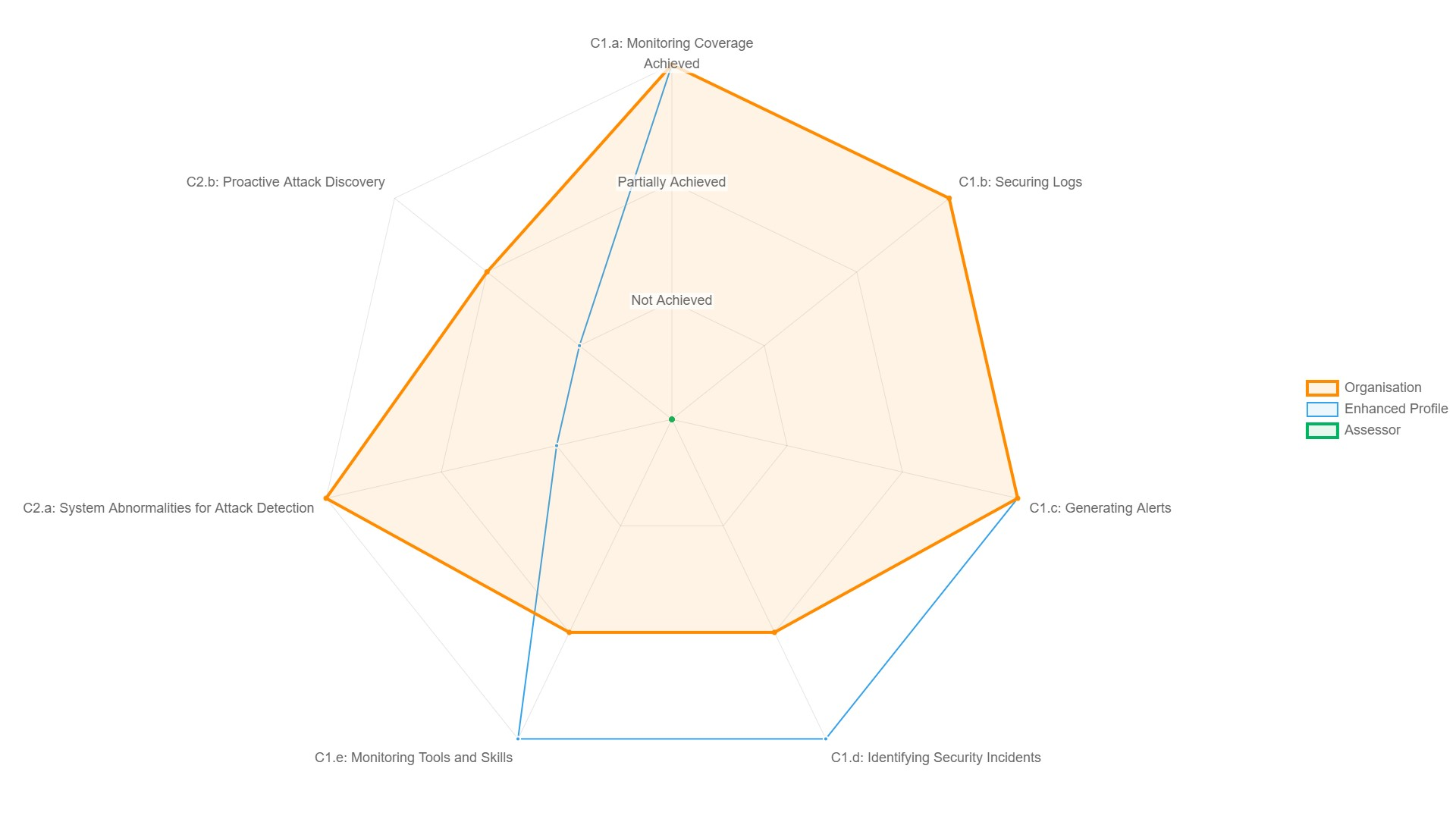
| **Obs. Ref.** | **Contributing outcome** | **Detailed observations** | **Risk** | **Recommendation** |
| --- | --- | --- | --- | --- |
| **Objective B: Protecting against cyber attack** | | | | |
| **[Ref]** | **B1.a Policy and Process Development** | **##Detailed observation reporting is by exception only and against the target CAF government profile. For example, if a target is ‘partially achieved’, generally we expect observations to be raised where they fall short of the target, but it is possible to include ‘improvement opportunity’ observations. ‘Improvement opportunity’ recommendations should be flagged as such##**  **##Detail can be copied, pasted and refined here from the original assurance reviewer report output from WebCAF to identify the observation/control gap##** | **##Identify the risk associated with the issue observed##** | **##Detail the recommended action as a result of the observation##** |
|  | **B1.b Policy and process implementation** |  |  |  |
|  | **B2.a Identity Verification, Authentication and Authorisation** |  |  |  |
|  | **B2.b Device Management** |  |  |  |
|  | **B2.c Privileged User Management** |  |  |  |
|  | **B2.d Identity and Access Management (IdAM)** |  |  |  |
|  | **B3.a Understanding Data** |  |  |  |
|  | **B3.b Data in Transit** |  |  |  |
|  | **B3.c Stored Data** |  |  |  |
|  | **B3.d Mobile Data** |  |  |  |
|  | **B3.e Media Equipment Sanitisation** |  |  |  |
|  | **B4.a Secure by Design** |  |  |  |
|  | **B4.b Secure Configuration** |  |  |  |
|  | **B4.c Secure Management** |  |  |  |
|  | **B4.d Vulnerability Management** |  |  |  |
|  | **B5.a Resilience Preparation** |  |  |  |
|  | **B5.b Design for Resilience** |  |  |  |
|  | **B5.c Backups** |  |  |  |
|  | **B6.a Cyber Security Culture** |  |  |  |
|  | **B6.b Cyber Security Training** |  |  |  |

[System 3] CAF Objective C - Contributing outcome achievement status radargram

Following the detailed examination of documentation and evidence in support of [organisation’s] CAF self-assessment, the following radargram provides a high-level summary of the independently assessed status of each contributing outcome for the [System 3]. The subsequent pages detail any exceptions or recommendations raised, as well as contributing outcomes that were insufficiently supported by evidence (where applicable).

**Assessor note:**

Example provided for illustrative purposes only. This is a placeholder for a radargram produced by WebCAF as part of the Report (HTML) functionality. It should be copied and pasted here.



[System 3] Summary – CAF Objective C: Detecting cyber security events

**C1 Security Monitoring:**

* **C1.a Monitoring Coverage -** [Exception based contributing outcome level summary]
* **C1.b Securing Logs -** [Exception based contributing outcome level summary]
* **C1.c Generating Alerts -** [Exception based contributing outcome level summary]
* **C1.d Identifying Security Incidents -** [Exception based contributing outcome level summary]
* **C1.e Monitoring Tools and Skills -** [Exception based contributing outcome level summary]

**C2 Proactive Security Event Discovery:**

* **C2.a System Abnormalities for Attack Detection -** [Exception based contributing outcome level summary]
* **C2.b Proactive Attack Discovery -** [Exception based contributing outcome level summary]

## [System 3] CAF Objective C - Contributing outcome achievement status

The following table provides a summary of the contributing outcomes achievement status and whether the target CAF government profile has been achieved.

| **Objective** | **CAF principle** | **Contributing outcome** | **Target profile**  **(Enhanced)** | **Self-assessment** | **Independent assurer assessment** | **Non-compliant IGPs** | **Profile met?** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Objective C:** **Detecting cyber security events** | **Security Monitoring** | C1.a Monitoring coverage | **Achieved** |  |  |  | **Yes / No / N/A** |
| C1.b Securing logs | **Achieved** |  |  |  | **Yes / No / N/A** |
| C1.c Generating alerts | **Achieved** |  |  |  | **Yes / No / N/A** |
| C1.d Identifying security incidents | **Achieved** |  |  |  | **Yes / No / N/A** |
| C1.e Monitoring tools and skills | **Achieved** |  |  |  | **Yes / No / N/A** |
| **Proactive Security Event Discovery** | C2.a System abnormalities for attack detection | **Not achieved** |  |  |  | **Yes / No / N/A** |
| C2.b Proactive attack discovery | **Not achieved** |  |  |  | **Yes / No / N/A** |

## [System 3] CAF Objective C - Detailed observations and recommendations

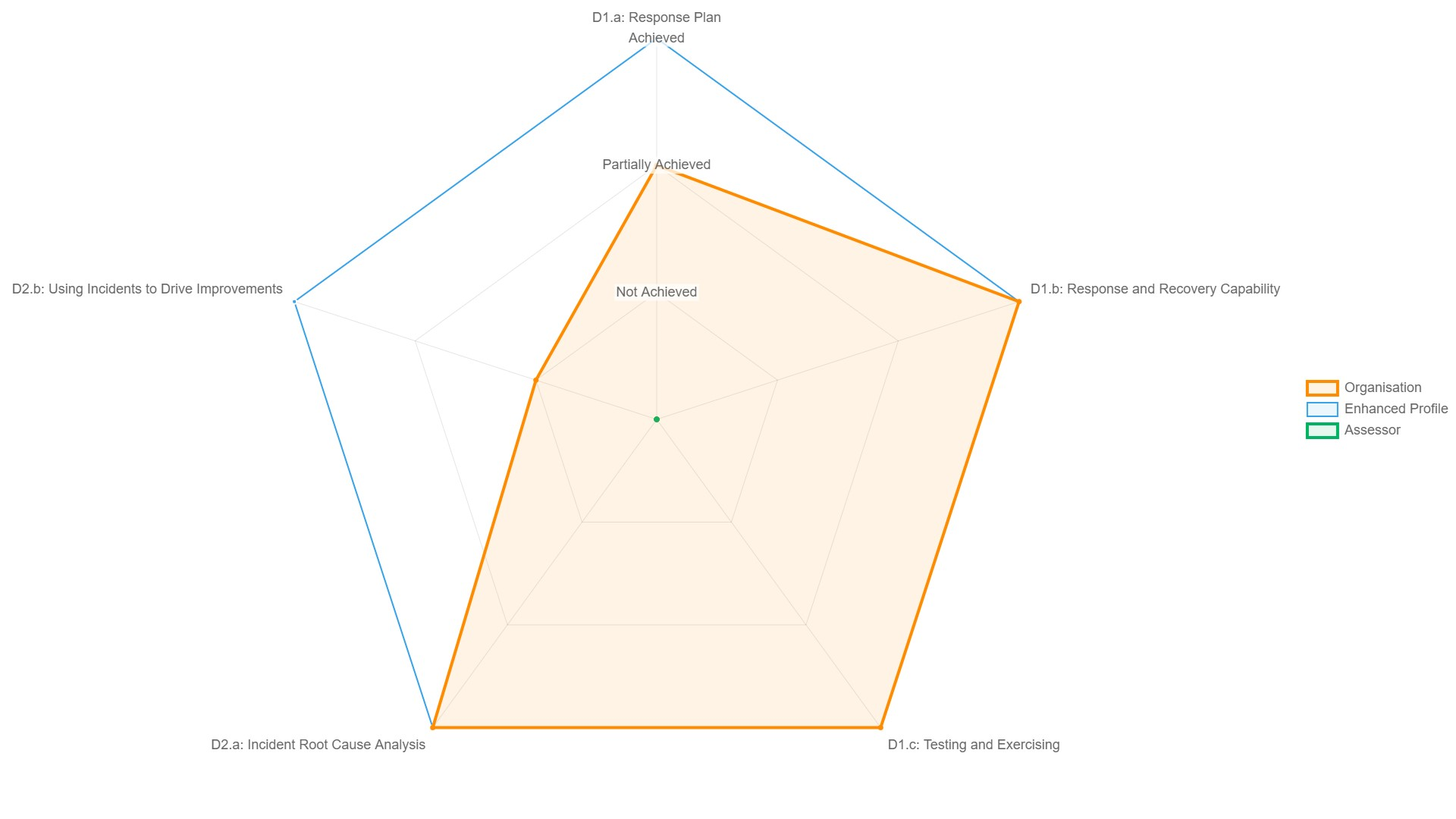
| **Obs. Ref.** | **Contributing outcome** | **Detailed observations** | **Risk** | **Recommendation** |
| --- | --- | --- | --- | --- |
| **Objective C: Detecting security events** | | | | |
| **[Ref]** | **C1.a Monitoring Coverage** | **##Detailed observation reporting is by exception only and against the target CAF government profile. For example, if a target is ‘partially achieved’, generally we expect observations to be raised where they fall short of the target, but it is possible to include ‘improvement opportunity’ observations. ‘Improvement opportunity’ recommendations should be flagged as such##**  **##Detail can be copied, pasted and refined here from the original assurance reviewer report output from WebCAF to identify the observation/control gap##** | **##Identify the risk associated with the issue observed##** | **##Detail the recommended action as a result of the observation##** |
|  | **C1.b Securing Logs** |  |  |  |
|  | **C1.c Generating Alerts** |  |  |  |
|  | **C1.d Identifying Security Incidents** |  |  |  |
|  | **C1.e Monitoring Tools and Skills** |  |  |  |
|  | **C2.a System Abnormalities for Attack Detection** |  |  |  |
|  | **C2.b Proactive Attack Discovery** |  |  |  |

[System 3] CAF Objective D - Contributing outcome achievement status radargram

Following the detailed examination of documentation and evidence in support of [organisation’s] CAF self-assessment, the following radargram provides a high-level summary of the independently assessed status of each contributing outcome for the [System 3]. The subsequent pages detail any exceptions or recommendations raised, as well as contributing outcomes that were insufficiently supported by evidence (where applicable).

**Assessor note:**

Example provided for illustrative purposes only. This is a placeholder for a radargram produced by WebCAF as part of the Report (HTML) functionality. It should be copied and pasted here.



[System 3] Summary – CAF Objective D: Detecting cyber security events

**D1 Response and Recovery Planning**

* **D1.a Response Plan** - [Exception based contributing outcome level summary]
* **D1.b Response and Recovery Capability** - [Exception based contributing outcome level summary]
* **D1.c Testing and Exercising** - [Exception based contributing outcome level summary]

**D2 Lessons Learned**

* **D2.a Incident Root Cause Analysis** - [Exception based contributing outcome level summary]
* **D2.b Using Incidents to Drive Improvements** - [Exception based contributing outcome level summary]

## [System 3] CAF Objective D - Contributing outcome achievement status

The following table provides a summary of the contributing outcomes achievement status and whether the target CAF government profile has been achieved.

| **Objective** | **CAF principle** | **Contributing outcome** | **Target profile**  **(Enhanced)** | **Self-assessment** | **Independent assurer assessment** | **Non-compliant IGPs** | **Profile met?** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Objective D: Minimising the impact of cyber security incidents** | **Response and Recovery Planning** | D1.a Response plan | **Achieved** |  |  |  | **Yes / No / N/A** |
| D1.b Response and recovery capability | **Achieved** |  |  |  | **Yes / No / N/A** |
| D1.c Testing and exercising | **Achieved** |  |  |  | **Yes / No / N/A** |
| **Lessons Learned** | D2.a Incident root cause analysis | **Achieved** |  |  |  | **Yes / No / N/A** |
| D2.b Using incidents to drive improvements | **Achieved** |  |  |  | **Yes / No / N/A** |

## [System 3] CAF Objective D - Detailed observations and recommendations

| **Obs. Ref.** | **Contributing outcome** | **Detailed observations** | **Risk** | **Recommendation** |
| --- | --- | --- | --- | --- |
| **Objective D: Minimising the impact of incidents** | | | | |
| **[Ref]** | **D1.a Response Plan** | **##Detailed observation reporting is by exception only and against the target CAF government profile. For example, if a target is ‘partially achieved’, generally we expect observations to be raised where they fall short of the target, but it is possible to include ‘improvement opportunity’ observations. ‘Improvement opportunity’ recommendations should be flagged as such##**  **##Detail can be copied, pasted and refined here from the original assurance reviewer report output from WebCAF to identify the observation/control gap##** | **##Identify the risk associated with the issue observed##** | **##Detail the recommended action as a result of the observation##** |
|  | **D1.b Response and Recovery Capability** |  |  |  |
|  | **D1.c Testing and Exercising** |  |  |  |
|  | **D2.a Incident Root Cause Analysis** |  |  |  |
|  | **D2.b Using Incidents to Drive Improvements** |  |  |  |

# Appendix A: CAF Self-assessment – Managing the Completion of the CAF – Observations and Suggest Improvements

[Detailed narrative around the approach to the management and completion of the self-assessment – consider inclusion of the following (where relevant)]

* [Approach to completing the CAF]
* [Provision of evidence, relevance and quality]
* [Contributing outcome and IGP completion]
* [Quality and detail of responses]
* [Key learnings and suggested improvements to the approach for subsequent years]

# Appendix B: Scope of the work undertaken

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **IDENTIFYING ESSENTIAL SYSTEMS** | | | | |
| **Essential system** | **Function this supports (from Part B)** | **Core IT infrastructure underpinning the service (e.g. Network/Cloud Provider)** | **Breakdown of backend systems/applications (where applicable)** | **In scope?**  **Assessor guidance note:**  Summarised version to be extracted from the GovAssure Scoping Document |
| **[System 1 – NAME]** |  |  |  |  |
| **[System 2 – NAME]** |  |  |  |  |
| **[System 3 – NAME]** |  |  |  |  |

# Appendix C: Staff interviewed & evidence reviewed

**Interviewees**

The table below lists the [organisation] stakeholder that took part in interviews as part of this GovAssure Assurance review. In some cases, secondary follow-up interviews took place with these stakeholders.

|  |  |  |
| --- | --- | --- |
| **Name** | **Title** | **Coverage** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Evidence**

The table below lists the [organisation] evidence that was provided as part of this GovAssure Assurance review.

|  |  |  |
| --- | --- | --- |
| **Document** | **Date** | **Coverage** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |