NIS | Competent Authority

Department of Finance
An Roinn Airgeadais
www.finance-ni.gov.uk

GUIDANCE ON THE IMPLEMENTATION OF THE NETWORK AND INFORMATION SYSTEMS (NIS) REGULATIONS 2018

DOF CYBER ASSESSMENT FRAMEWORK (CAF) - 2022

DOCUMENT CONTROL

The only controlled version of this document can be accessed on the DoF NIS CA Website

Printed copies of this document, together with electronic copies held on local computers and other storage devices are uncontrolled.

Contents

1 Introduction and purpose

1.1 This guidance is developed by the Department of Finance pursuant to, and in satisfaction of, Regulation 3(3)(b) and the competent authority obligation to prepare and publish guidance.

1.2 The Department of Finance is the designated Network and Information Systems (NIS) competent authority within Northern Ireland for Operators of Essential Services (OES) in the health, drinking water supply and distribution, road and rail transport and energy sectors.

1.3 This guidance is for operators of essential services (OES) for which the Department of Finance is designated as the NIS competent authority within the health, water supply and distribution, road and rail transport and energy sectors.

1.4 The purpose of this guidance document is to outline a framework to enable organisations as OES under the NIS Regulations to create and be able to review the scope of their essential service(s) relevant to the NIS regulations 2018.

1.5 This Guidance Document will also provide guidelines to an OES on the completion of the Cyber Assessment Framework (CAF) to ensure that relevant information and evidence is provided to demonstrate confidence to the Department of Finance, as the NIS competent authority, that appropriate and proportionate measures, with regard to state of the art security are used in protecting the continued delivery of the essential service(s) of that OES.

1.6 These guidance documents will be amended as required to ensure they remain accurate and up to date. Additional guidance may be added to these documents if necessary or made available in another individual document if required.

1.7 This document is specific to a DoF NIS competent authority adapted version of the National Cyber Security Centre (NCSC) CAF reporting tool (CAF v3.1).

2 Identification of Network and Information Systems

2.1 The NIS Regulations aims to improve the security of network and information systems that support or have a direct effect on the delivery of the essential services you provide within your sector.

2.2 The definition of a network and information system is outlined under regulation 1(2) and is considered to include, electronic communications networks; any device or group of interconnected or related devices which perform automatic processing of digital data; or digital data stored processed,

retrieved or transmitted by an electronic network or device.

2.3 For most sectors this definition can apply to both Operational Technology (OT) systems and Information Technology (IT) systems.

2.4 Regulation 10 outlines the responsibilities of an operator of essential services (OES), specifically regarding taking appropriate and proportionate measures to manage the risks to their network and information systems and to prevent and/or minimise the impact of incidents to those systems.

2.5 Therefore, to understand the level of security and where measures should be applied, it is important to identify what network and information systems fall within the scope of the Regulations.

3 Defining the NIS Essential Service

3.1 To create a NIS scope the OES must first have a present and clear understanding as to what essential services they deliver under the NIS regulations within the overall context of the business services provided within an organisation and from this determine what underpinning IT, OT systems that are needed to protect the continued delivery of that service.

3.2 Companies should engage the wider business in creating their NIS scope to ensure the correct systems are identified to build an accurate reflection of its operating and continual delivery of the essential service. Companies should ensure appropriate representation from the departments best placed to aid these discussions.

3.3 OES should note that some systems may only come into scope on a time bound basis, i.e. if an underpinning service was disrupted for 1 hour the essential services through business tolerance or continuity measures would be different than if the essential service was to be maintained for a disruption for 4-6 weeks or longer. This is normally determined through conducting a Business Impact Assessment (BIA) for each business function providing a level of criticality for each and determining a recovery time objective (RTO) i.e. how long can a business system or process be out of service before it has a significant impact, and a maximum tolerable downtime (MTD) i.e. the time at which point systems and service disruption will be catastrophic and would not be able to be fully restored. These figures feed into business and disaster recovery plans.

3.4 OES should take cognisance of threat intelligence sources to inform their own threat and risk analysis. It is widely published that recent increases across many sectors of ransomware attacks can leave organisations disrupted for 21

days on average[1] with some systems being disrupted longer than this.

3.5 Once the essential service is defined draw a boundary around this and identify the underpinning IT and OT systems, including any 3rd party services that support this service.

4 Creating the NIS Scope

4.1 NIS regulations relate to the network and information systems necessary in the continued delivery of the essential service. This can also bring in physical controls that are necessary to provide proportionate and appropriate protection to these systems e.g., a locked server room, vandal proof distribution cabinet etc.

4.2 The systems identified in the NIS Scope are then included as part of the company's Cyber Assessment Framework (CAF) return.

4.3 As with defining the scope of the essential service companies should engage the wider business in creating their NIS Scope to ensure the correct systems are identified and to build an accurate reflection of its operating and continued delivery of their essential service(s). Companies should ensure appropriate representation from the departments best placed to aid these discussions form a business and IT/OT perspective.

4.4 In the first instance, a company should identify the systems that underpin and support the production and delivery of their essential service(s), understand their key functions and how these systems interact with other systems. This can include:

- A description of the essential service(s);
- A brief description of each system and its function;
- A high level diagrammatic overview of the systems and their interconnectivity;
- Indication of the major dependencies between these systems;
- Indication of which systems are operated by third parties;
- Key data and system inputs and outputs necessary for the essential service; and
- For each of the systems identified, companies should understand the implications if that system fails or is compromised and what impact that disruption would have on the production and delivery of essential service(s).

4.5 Whilst it is appreciated that a NIS Scope will be dependent on the network and information systems in operation at each company, DoF NIS competent authority expects, as a minimum that companies include any system that has a **direct impact** on the production and delivery of essential service(s), this

[1] Ransomware Payments Decline in Q4 2020 (coveware.com)

should include, but not limited to:

- IT Systems
- SCADA
- HMI
- PLCs
- RTUs
- IP Sensors
- IP Controllers
- Telemetry Master Stations.

4.6 A NIS Scope will form part of the company's overall CAF submission and DoF NIS competent authority will review and where necessary challenge the level and depth of the Scope where appropriate during the assessments of company's submissions.

4.7 A company's NIS Scope is designed to be an evolving document and therefore will change over time. This can be due to increased knowledge of how systems support or directly affect how the essential service is provided or through changes in the network and information systems used. DoF NIS competent authority therefore expects companies to keep their NIS Scope under regular review (at least annually) and certainly it should be reviewed as part of any significant changes to a company's operating systems or following a cyber incident. Any changes to a NIS Scope are to be highlighted and explained within an updated NIS scope submitted with any subsequent CAF return to the NIS competent authority.

5 Objective of the Cyber Assessment Framework (CAF)

5.1 The key security duties of each company is to manage risks to their network and information systems and to prevent and/or minimise the impact of incidents to those systems, through appropriate and proportionate technical and organisational measures.

5.2 This is achieved by working towards 4 top-level objectives:

- Objective A. Managing security risk
- Objective B: Protecting against cyber attack
- Objective C: Detecting cyber security events
- Objective D: Minimising the impact of cyber security incidents

5.3 These four objectives will be realised through the implementation of a set of 14 cyber security principles as outlined in Figure 5.1. These principles are designed to be outcome focused and therefore outline what needs to be achieved rather than exactly what needs to be completed.

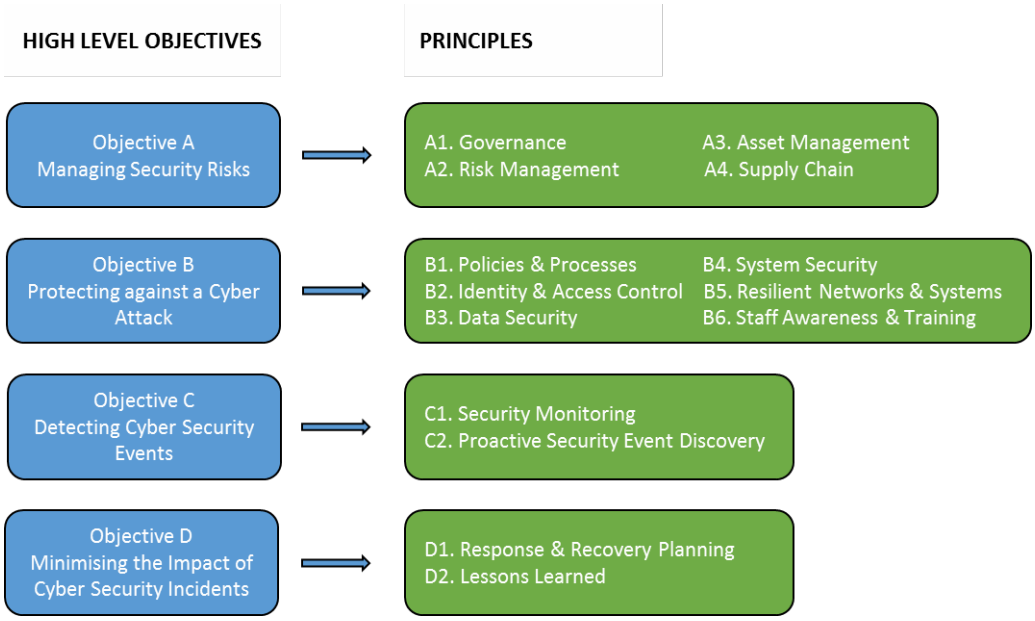


Figure 5.1: NIS Objectives and underlying Cyber Security Principles

5.4 The aim of the CAF therefore is to:

- Provide each company with a framework to assess and evidence how cyber security risks are being managed within their business in relation to the production and delivery of essential service(s).
- Allow the DoF NIS competent authority to assess the extent to which each company is achieving the outcomes specified by the cyber security principles.

5.5 The results of the CAF will enable companies to identify cyber security improvement plans in line with the above objectives, principles and contributing outcomes, and will form discussions with DoF NIS competent authority in demonstrating commitment by the organisation to compliance with the NIS regulations. Importantly this conveys a level of confidence with the NIS competent authority to the protection and continual delivery of essential service through effective risk management activities and the use of proportionate and appropriate technical and organizational controls.

6 CAF Structure

6.1 The 14 cyber security principles each have a collection of lower level contributing outcomes (CO). The extent to which a principle is being achieved is dependent on the status of all the COs under that principle.

6.2 The status of each CO is characterised as either being ‘achieved’ (Green), ‘not achieved’ (Red) and in some cases ‘partially achieved’ (Amber), dependent on the assessment of the indicators.

6.3 These indicators are considered the basis of the CAF profile, as outlined in Figure 5.1.

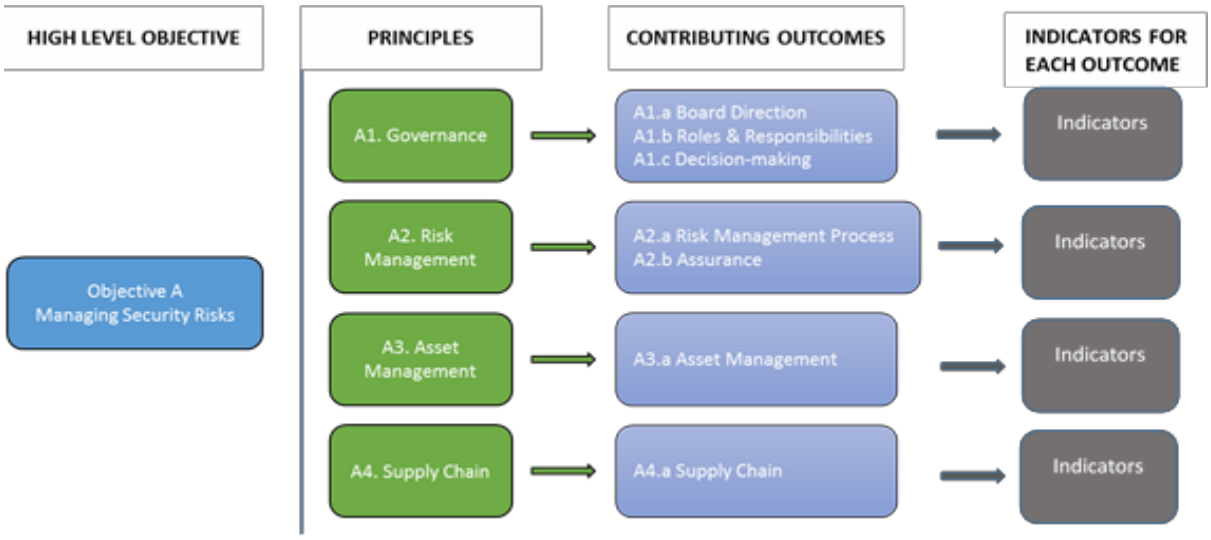


Figure 6.1: CAF Hierarchical Structure for Objective A

6.4 The results for all contributing outcomes create a CAF profile for the organisation. Whilst there is the obvious expectation that companies should be aiming for 'achieved' across all contributing outcomes, the CAF has been designed in such a way that a result in which all contributing outcomes were assessed as 'achieved' would indicate a mature level of cyber security. DoF NIS competent authority recognises that this may be some way beyond where most organisations are and may not be proportionate and appropriate for all sectors depending on prevailing threat and risk factors.

6.5 DoF NIS competent authority recognises the prevailing NCSC baseline CAF profile as the minimum level of cyber security an OES needs to be aiming to achieve. Where appropriate DoF NIS competent authority will work with NCSC and other UK sector NIS competent authorities to present a sector specific CAF profile referred to as an advanced CAF profile based on current threat intelligence information. Where an advanced profile is developed this will be the sector specific minimum target profile. Either the basic or advanced CAF profiles will consist of a mixture of contributing outcomes to be met at 'achieved', 'partially achieved', and some more advanced security measures where a "not achieved" determine acceptable minimum levels of cyber security for an OES.

6.6 Companies are expected to manage their own security strategies and plans and must be able to justify and evidence their stated CAF positions. The justifications should clearly show the risk assessment that supports the

declared contributing outcome position and how this is mitigated to a point that sits within their company risk appetite.

7 Information Technology (IT) and Operational Technology (OT)

7.1 Dependent on how a company's NIS Scope is completed, systems from both IT and OT networks may be included as part of the CAF.

7.2 A single completed CAF covering both networks may therefore influence the status of the indicators dependent on the strengths/weaknesses from each.

7.3 DoF NIS competent authority acknowledges that companies may wish to complete separate CAFs for both the IT and OT networks on the basis that the information could be more beneficial to the company as it will provide a holistic assessment for each.

7.4 However, DoF NIS competent authority expects a single CAF to be completed combining the systems in scope for both IT and OT networks as the company's submission. The combined CAF should be completed using the lowest status of each corresponding contributing outcome as this is a more representative profile of the company's overall cyber security. For example if an IT network has a contributing outcome deemed "Green - achieved" and an OT network has the same contributing outcome deemed "Amber – partially achieved" then the status should be "Amber – partially achieved" as the lowest status.

7.5 If completed, a company may still include the individual IT and OT CAFs as part of the overall CAF submission. DoF NIS competent authority are happy to reference these assessments if applicable during the discussions around future work planning.

8 CAF completion for affiliated companies

8.1 The definition of an affiliated company is where two companies or more, operating in different geographical regions, are managed by the same board of directors.

8.2 DoF NIS competent authority appreciates that, dependent on the operational alignment of the two companies, a single completed CAF may not reflect the true status of each company.

8.3 Companies therefore have the option to either submit a single CAF that combines the two affiliate companies, or two individual CAF submissions for each affiliate. Companies should consider the benefits each option will provide,

as well as ensuring a consistent assessment is taken to any common technologies. DoF NIS competent authority reserve the right to request that separate CAFs are provided should the need arise to capture and analyse individual positions more clearly.

8.4 A combined CAF should be completed using the lower status of each contributing outcome as this is a more representative profile of the company's overall cyber security.

8.5 DoF NIS competent authority will continue to discuss both profiles and aspects of performance separately where present. This will ensure appropriate measures are being taken to achieve the CAF profile for both companies, and to understand the company's long-term strategy for technological alignment.

8.6 Where changes to affiliation arrangements have occurred, this should be highlighted within the accompanying updated NIS Scope document and proactively communicated as soon as practicable to the NIS Team's shared-email address given in paragraph 14.3 this includes any corporate name changes or changes in designated contact points.

9 Completing the CAF

9.1 DoF NIS competent authority expects companies to complete the CAF using input from several staff to ensure the most accurate assessment is reflected. As with the NIS scope, companies are best placed to choose the relevant staff required and so DoF NIS competent authority will not publish a prescriptive list. DoF NIS competent authority proposes that the following roles should be represented as a minimum:

- Essential service business owners
- Data owners
- IT staff and OT staff
- Resilience/Emergency Planners
- Security Managers
- Operations staff.

9.2 The National Cyber Security Centre (NCSC) has also published a collection of guidance documents and reference links on their website which provides further information on how a OES may achieve the outcomes specified in the principles. It is recommended that companies refer to this guidance whilst completing the CAF.

9.3 For a consistent approach, companies should use the DoF CAF Reporting Tool. The latest version will be available on the competent authority website. Guidelines for using the tool are outlined in Annex 2: Guidelines for the CAF Reporting Tool

9.4 Companies understand their own systems and operations and so DoF NIS competent authority expects each company should be capable of using expert judgement to take informed and balanced decisions about how they assess each contributing outcome.

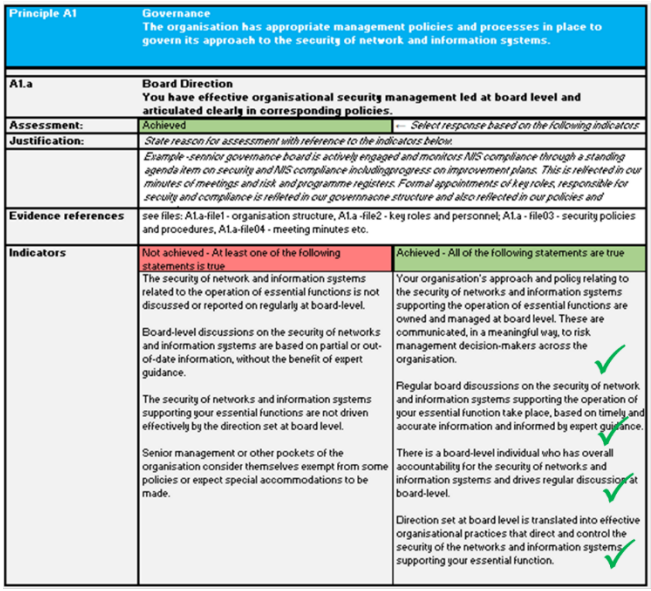
10 Reaching a CAF Contributing Outcome (CO) assessment

10.1 Interpretation of each indicator column is standalone, and therefore there is no direct correlation between each column for a CO. The indicators should be read vertically and not applied horizontally see Annex 3: Guidance for Reading Indicator Tables.

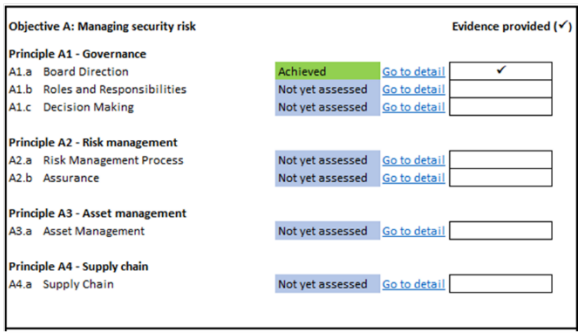
10.2 In terms of the detailed scoring for a CO, for a green RAG status, the GREEN ‘achieved’ column of an indicator table defines the typical characteristics of an organisation fully achieving that outcome. It is intended that ***all*** the indicators would normally be present and evidenced to support an assessment of ‘achieved’. See the example below.

Objective A tab – Managing Security Risk
A1.a - Board direction
assessed as "achieved" as all indicators met

On Summary tab
A1.a - Board direction
marked as "achieved" automatically
Evidence box is for OES to ensure evidence has been provided to justify assessment



Principle A1	Governance The organisation has appropriate management policies and processes in place to govern its approach to the security of network and information systems.	
A1.a	Board Direction You have effective organisational security management led at board level and articulated clearly in corresponding policies.	
Assessment:	Achieved	← Select response based on the following indicators
Justification:	State reason for assessment with reference to the indicators below.	
	Example -senior governance board is actively engaged and monitors NIS compliance through a standing agenda item on security and NIS compliance including progress on improvement plans. This is reflected in our minutes of meetings and risk and programme registers. Formal appointments of key roles, responsible for security and compliance is reflected in our governance structure and also reflected in our policies and	
Evidence references	see files: A1.a-file1 - organisation structure, A1.a -file2 - key roles and personnel; A1.a - file03 - security policies and procedures, A1.a-file04 - meeting minutes etc.	
Indicators	Not achieved - At least one of the following statements is true	Achieved - All of the following statements are true
	The security of network and information systems related to the operation of essential functions is not discussed or reported on regularly at board-level. Board-level discussions on the security of networks and information systems are based on partial or out-of-date information, without the benefit of expert guidance. The security of networks and information systems supporting your essential functions are not driven effectively by the direction set at board level. Senior management or other pockets of the organisation consider themselves exempt from some policies or expect special accommodations to be made.	Your organisation's approach and policy relating to the security of networks and information systems supporting the operation of essential functions are owned and managed at board level. These are communicated, in a meaningful way, to risk management decision-makers across the organisation. Regular board discussions on the security of network and information systems supporting the operation of your essential function take place, based on timely and accurate information and informed by expert guidance. There is a board-level individual who has overall accountability for the security of networks and information systems and drives regular discussion at board-level. Direction set at board level is translated into effective organisational practices that direct and control the security of the networks and information systems supporting your essential function.



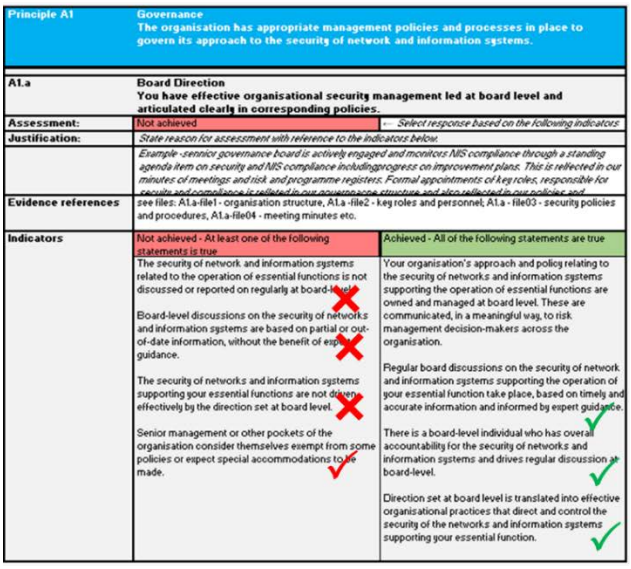
Objective A: Managing security risk			Evidence provided (✓)
Principle A1 - Governance			
A1.a Board Direction	Achieved	Go to detail	✓
A1.b Roles and Responsibilities	Not yet assessed	Go to detail	
A1.c Decision Making	Not yet assessed	Go to detail	
Principle A2 - Risk management			
A2.a Risk Management Process	Not yet assessed	Go to detail	
A2.b Assurance	Not yet assessed	Go to detail	
Principle A3 - Asset management			
A3.a Asset Management	Not yet assessed	Go to detail	
Principle A4 - Supply chain			
A4.a Supply Chain	Not yet assessed	Go to detail	

10.3 When present for a CO, the AMBER 'Partially achieved' column of an indicator table defines the characteristics of partially achieving that CO. If at least one amber statement is classified as being met, there are no red statements met, and not all green statements are met, then that CO will be assessed as 'partially achieved' overall.

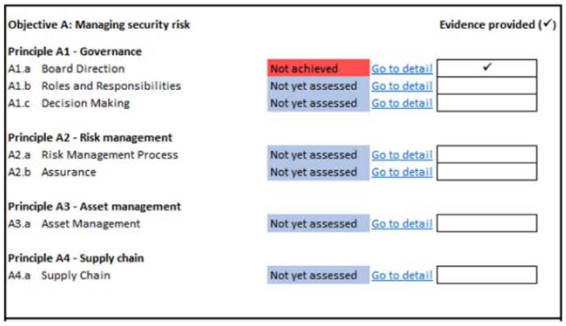
10.4 The RED 'Not achieved' column of the indicator table defines the characteristics of not achieving that CO. If a single red statement is characterised as *true* then this would justify an overall assessment of 'not achieved' for that CO, as outlined below:-

Objective A tab – Managing Security Risk
A1.a - Board direction
assessed as "not achieved"

On Summary tab
A1.a - Board direction
marked as "not achieved" automatically
Evidence box is for OES to ensure evidence has been provided to justify assessment and improvement plans



Principle A1	Governance The organisation has appropriate management policies and processes in place to govern its approach to the security of network and information systems.	
A1.a	Board Direction You have effective organisational security management led at board level and articulated clearly in corresponding policies.	
Assessment:	Not achieved	← Select response based on the following indicators
Justification:	State reason for assessment with reference to the indicators below.	
	Example -senior governance board is actively engaged and monitors NIS compliance through a standing agenda item on security and NIS compliance including progress on improvement plans. This is reflected in our minutes of meetings and risk and programme registers. Formal appointments of key roles, responsible for security and compliance is reflected in our governance structure and also reflected in our policies and	
Evidence references	see files: A1.a-file1 - organisation structure, A1.a -file2 - key roles and personnel; A1.a - file03 - security policies and procedures, A1.a-file04 - meeting minutes etc.	
Indicators	Not achieved - At least one of the following statements is true	Achieved - All of the following statements are true
	The security of network and information systems related to the operation of essential functions is not discussed or reported on regularly at board-level. Board-level discussions on the security of networks and information systems are based on partial or out-of-date information, without the benefit of expert guidance. The security of networks and information systems supporting your essential functions are not driven effectively by the direction set at board level. Senior management or other pockets of the organisation consider themselves exempt from some policies or expect special accommodations to be made.	Your organisation's approach and policy relating to the security of networks and information systems supporting the operation of essential functions are owned and managed at board level. These are communicated, in a meaningful way, to risk management decision-makers across the organisation. Regular board discussions on the security of network and information systems supporting the operation of your essential function take place, based on timely and accurate information and informed by expert guidance. There is a board-level individual who has overall accountability for the security of networks and information systems and drives regular discussion at board-level. Direction set at board level is translated into effective organisational practices that direct and control the security of the networks and information systems supporting your essential function.



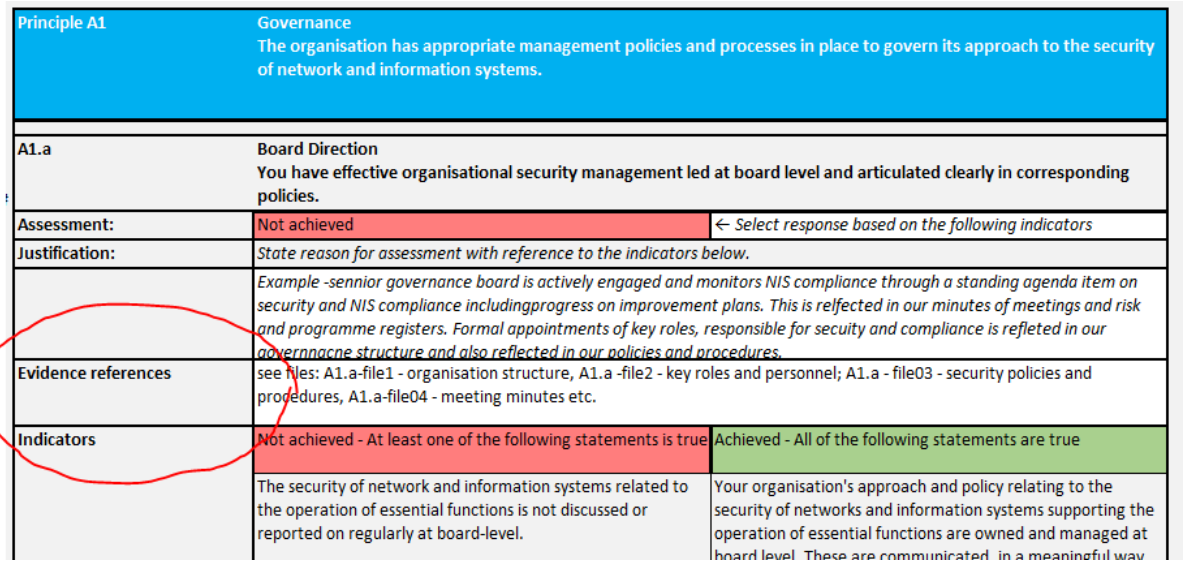
Objective A: Managing security risk			Evidence provided (✓)
Principle A1 - Governance			
A1.a Board Direction	Not achieved	Go to detail	✓
A1.b Roles and Responsibilities	Not yet assessed	Go to detail	
A1.c Decision Making	Not yet assessed	Go to detail	
Principle A2 - Risk management			
A2.a Risk Management Process	Not yet assessed	Go to detail	
A2.b Assurance	Not yet assessed	Go to detail	
Principle A3 - Asset management			
A3.a Asset Management	Not yet assessed	Go to detail	
Principle A4 - Supply chain			
A4.a Supply Chain	Not yet assessed	Go to detail	

10.5 A company may assess an indicators table as having individual statements that fall into each of the three of ‘not / partially / achieved’ columns. In this instance, the Red / Not-achieved column would have to be the final assessment.

10.6 Some contributing outcomes have the option to be characterised as ‘not relevant’. Whilst DoF NIS competent authority strongly recommends companies do not use this option as the assessment for a contributing outcome, it is recognised that there could be a justification for this option to be selected. If a company decides to use this option, then sufficient justification should be provided against that contributing outcome and evidence provided.

11 Providing evidence

11.1 Companies should be able to justify and provide evidence as to the reasoning behind the assessment of each contributing outcome. This evidence should be referenced under the evidence section in the CAF Reporting Tool (Figure 11.1) and should be able to be forwarded to DoF NIS competent authority in a separate data submission.



Principle A1	Governance The organisation has appropriate management policies and processes in place to govern its approach to the security of network and information systems.	
A1.a	Board Direction You have effective organisational security management led at board level and articulated clearly in corresponding policies.	
Assessment:	Not achieved	← *Select response based on the following indicators*
Justification:	*State reason for assessment with reference to the indicators below.*	
	Example -sennior governance board is actively engaged and monitors NIS compliance through a standing agenda item on security and NIS compliance includingprogress on improvement plans. This is relfected in our minutes of meetings and risk and programme registers. Formal appointments of key roles, responsible for secuity and compliance is refleted in our governnacne structure and also reflected in our policies and procedures.	
Evidence references	see files: A1.a-file1 - organisation structure, A1.a -file2 - key roles and personnel; A1.a - file03 - security policies and procedures, A1.a-file04 - meeting minutes etc.	
Indicators	Not achieved - At least one of the following statements is true	Achieved - All of the following statements are true
	The security of network and information systems related to the operation of essential functions is not discussed or reported on regularly at board-level.	Your organisation's approach and policy relating to the security of networks and information systems supporting the operation of essential functions are owned and managed at board level. These are communicated, in a meaningful way

Figure 11.1 Evidence box for each Contributing Outcome

11.2 Companies can choose to enter this as plain text, insert a file structure picture or document that indexes all documents and files sent. It is important that the information contained in the CAF tool evidence boxes and the files and documents returned in the evidence template (shown is figure 12.1 and 12.2) reconcile providing clear auditable link between the two elements of the CAF return.

12 Evidence template

12.1 To simplify the process of analysing supporting evidence, DoF NIS competent authority has developed a folder structure template which must be used by

the OES to structure any supporting evidence to be provided. The template is a hierarchy of folders which follows the structure of the CAF principles as shown below:

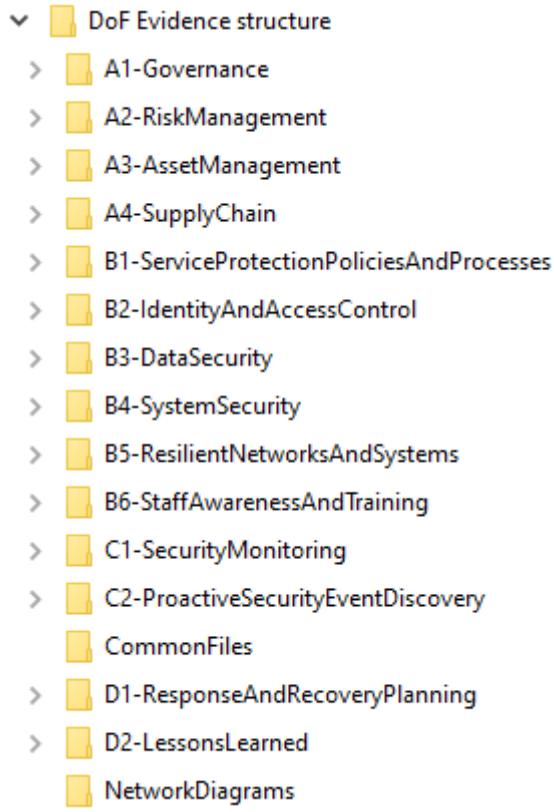


figure 12.1 –Evidence Template - CAF principles folder structure

12.2 Each CAF principle has a corresponding folder which is sub divided into the corresponding contributing outcomes as shown below for A1 – Governance (A1.a – Board Direction, A1.b – RolesAndResponsibilities etc) and A2 – Risk Management (A2.a – RiskManagement etc).

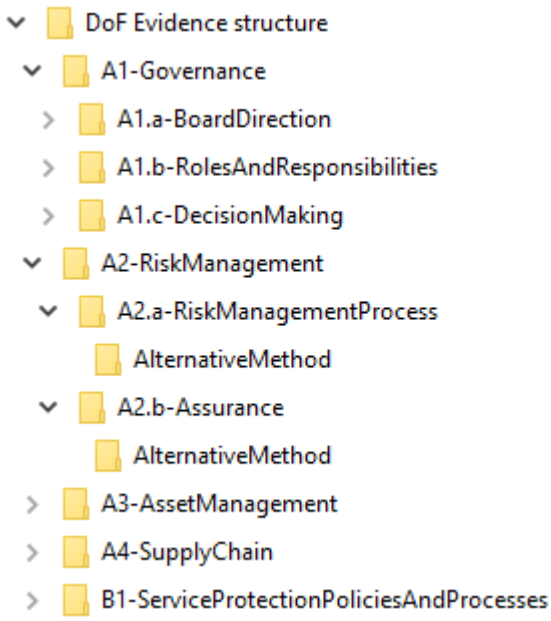


figure 12.2 – example sub-folder structure for CO evidence

12.3 A zip file can be provided to the OES on request to create this structure.

12.4 Evidence for each contributing outcome (CO) has a reference identifier e.g. the contributing outcome “Board Direction” has the reference identifier A1.a. Any supporting evidence for statement A1.a should be placed in the corresponding folder in the DoF NIS competent authority supplied evidence folder reference template.

12.5 Where an OES feels that they have achieved a contributing outcome in a manner different to that indicated by the associated CAF statements, each contributing outcome in the evidence template provides a folder called **“AlternativeMethod”,** as shown above, to store such evidence.

12.6 The evidence template also provides folders for evidence files that apply to multiple contributing outcomes e.g. security policies which would be better placed in the **“CommonFiles”** folder.

13 Evidence naming convention

13.1 When placing evidence files in a specific evidence folder, it is requested that OES use the prefix **“Filenn-“** at the start of each evidence filename where **nn** starts at 01 e.g. **File01-, File02-** etc. This will simplify the writing of evidence file names in the evidence part of the CAF, an example of which can be seen in figure 11.1.

13.2 If no supporting evidence is being provided for a particular CAF statement,

justification for this should be noted and explained in the "**evidence box"** on the CAF form.

13.3 If any supporting evidence for a particular CAF statement is found unsatisfactory, DoF NIS competent authority will request additional supporting evidence.

13.4 Whilst the nature and type of evidence referenced against each CO is the company's decision, the NCSC published a collection of guidance documents and reference links on their website which demonstrates how a CO may be evidenced.

13.5 Companies should also make use of the Justification comments or evidence boxes to include further information, where applicable, against the CO, this may include:

- Information around any of the individual indicators
- Internal or independent external audits
- If other controls (e.g. physical controls) are in place to justify the decisions
- If an individual indicator is not applicable to the company
- Any further information the company feel is relevant to the assessment.

14 Use of other frameworks

14.1 It is also acknowledged that companies have introduced cyber security management through other security frameworks e.g. ISO27001, NIST 800 53. It is not the aim of the competent authority to ask an OES to redo this work but we would ask that the outputs from these are mapped onto the CAF principles and contributing outcomes.

14.2 Where other frameworks have been used NCSC have developed mapping from common frameworks onto the CAF that can be forwarded upon request from the OES.

14.3 Any further questions around the CAF can be sent to NIS.CA@Finance-ni.gov.uk

15 REPORTING REQUIREMENTS TO DoF

15.1 A CAF return will be formally requested by DoF NIS competent authority in writing. Company submissions to DoF NIS competent authority should consist of the following artefacts:

- A completed DoF CAF (v3.1) Reporting Tool
- The company Essential Service NIS Scope included in the Reporting Tool
- An improvement plan (see detail in paragraph 15.3) addressing how the contributing outcomes below the relevant basic or Advanced CAF profile indicators are going to be met.
- CAF Evidence Template folder structure with appropriate information and evidence to corroborate the contributing outcome assessments on the CAF return.

15.2 Each submission should be accompanied by a signed declaration from the Board level contact (See Annex 4: NIS Board-Level Contact Declaration).

15.3 An improvement plan should detail how companies are addressing any COs below the relevant basic or advanced CAF profile and must include a Gaant chart with key milestones and timelines for these COs to meet or exceeded.

15.4 The Improvement Plan should include a narrative to aid the understanding, to the DOF competent authority, of the scale and prioritisation of any remaining activity of projects/actions, and how they tie back to the contributing outcomes. This should include dependencies on other teams or other projects where applicable.

15.5 When ready to submit the organisation should notify the competent authority via the email address NIS.CA@Finance-ni.gov.uk to receive secure handling instructions to submit the CAF returns.

16 DoF ASSESSMENT REPORTS

16.1 DoF will review each CAF submitted and where required may ask for clarification or additional information to fully understand the returns.

16.2 A report on the CAF self-assessment will be submitted to the main contact and lead with any recommendations and observations.

Annex 1: NCSC Basic CAF profile

Principle	Contributing Outcome	NCSC
A1. Governance	A1.a Board Direction	
	A1.b Roles & Responsibilities	
	A1.c Decision-making	
A2. Risk Management	A2.a Risk Management Process	
	A2.b Assurance	
A3. Asset Management	A3.a Asset Management	
A4. Supply Chain	A4.a Supply Chain	
B1. Policies & Processes	B1.a Policy & Process Development	
	B1.b Policy & Process Implementation	
B2. Identity & Access Control (IDAC)	B2.a Identity Verification, Authentication and Authorisation	
	B2.b Device Management	
	B2.c Privileged User Management	
	B2.d IDAC Management & Maintenance	
B3. Data Security	B3.a Understanding Data	
	B3.b Data in Transit	
	B3.c Stored Data	
	B3.d Mobile Data	
	B3.e Media/Equipment Sanitisation	
B4. System Security	B4.a Secure By Design	
	B4.b Secure Configuration	
	B4.c Secure Management	
	B4.d Vulnerability Management	
B5. Resilient Networks & Systems	B5.a Resilience Preparation	
	B5.b Design for Resilience	
	B5.c Backups	
B6. Staff Awareness & Training	B6.a Cyber Security Culture	
	B6.b Cyber Security Training	
C1. Security Monitoring	C1.a Monitoring Coverage	
	C1.b Securing Logs	
	C1.c Generating Alerts	
	C1.d Identifying Security Incidents	
	C1.e Monitoring Tools & Skills	
C2. Proactive Security Event Discovery	C2.a System Abnormalities for Attack Detection	
	C2.b Proactive Attack Discovery	
D1. Response & Recovery Planning	D1.a Response Plan	
	D1.b Response & Recovery Capability	
	D1.c Testing & Exercising	
D2. Lessons Learned	D2.a Incident Root Cause Analysis	
	D2.b Using Incidents to Drive Improvements	

Annex 2: Guidelines for the CAF Reporting Tool

i. Complete the Essential Service scope summary tab to set reference for other sections

ii. The CAF Summary Tab will auto update as you work through the document

iii. The Comments Box will expand to accommodate additional text

iv. Text in blue are hyperlinks

v. Please read the Indicator tables as outlined in Annex 3: Guidance for Reading Indicator Tables

vi. If submitting two CAFs please ensure they are clearly named to reflect the assessment

Annex 3: Guidance for Reading Indicator Tables

B4.a Secure by Design

You design security into the network and information systems that support the operation of essential functions. You minimise their attack surface and ensure that the operation of the essential function should not be impacted by the exploitation of any single vulnerability.

Not Achieved	Partially Achieved	Achieved
At least one of the following statements is true	All the following statements are true	All the following statements are true
Systems essential to the operation of the essential function are not appropriately segregated from other systems. Internet access is available from operational systems. Data flows between the essential function's operational systems and other systems are complex, making it hard	You employ appropriate expertise to design network and information systems. You design strong boundary defences where your networks and information systems interface with other organisations or the world at large. You design simple data flows	You employ appropriate expertise to design network and information systems. Your networks and information systems are segregated into appropriate security zones, e.g. operational systems for the essential function are segregated in a highly trusted, more secure zone.

B4.a Secure by Design

You design security into the network and information systems that support the operation of essential functions. You minimise their attack surface and ensure that the operation of the essential function should not be impacted by the exploitation of any single vulnerability.

Not Achieved	Partially Achieved	Achieved
At least one of the following statements is true	All the following statements are true	All the following statements are true
Systems essential to the operation of the essential function are not appropriately segregated from other systems. Internet access is available from operational systems. Data flows between the essential function's operational systems and other systems are complex, making it hard to discriminate between legitimate and illegitimate/malicious traffic. Remote or third party accesses circumvent some network controls to gain more direct access to operational systems of the essential function.	You employ appropriate expertise to design network and information systems. You design strong boundary defences where your networks and information systems interface with other organisations or the world at large. You design simple data flows between your networks and information systems and any external interface to enable effective monitoring. You design to make network and information system recovery simple. All inputs to operational systems are checked and validated at the network boundary where possible, or additional monitoring is in place for content-based attacks.	You employ appropriate expertise to design network and information systems. Your networks and information systems are segregated into appropriate security zones, e.g. operational systems for the essential function are segregated in a highly trusted, more secure zone. The networks and information systems supporting your essential function are designed to have simple data flows between components to support effective security monitoring. The networks and information systems supporting your essential function are designed to be easy to recover. Content-based attacks are mitigated for all inputs to operational systems that affect the essential function (e.g. via transformation and inspection).

Annex 4: NIS Board-Level Contact Declaration

[Company] CAF Submission			
Name:		**Role Title:**	
[Text]			
Signed:		**Date:**	