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

THE CYBER ASSESSMENT FRAMEWORK (CAF)

CONTENTS

1. INTRODUCTION AND PURPOSE

1.1 The purpose of this Guidance Document is to outline a framework to enable companies to create a NIS Scope and to provide guidelines to water companies, designated as an Operator of Essential Service (OES), on the completion of the Cyber Assessment Framework.

1.2 This Guidance has been issued by the Drinking Water Inspectorate (DWI), who undertake the operational responsibilities of the competent authority function, for the sector, under the NIS Regulations 2018 on behalf of the Secretary of State for Environment, Food and Rural Affairs and Welsh Ministers, and in compliance with regulation 3 of the NIS Regulations 2018.

1.3 Further Guidance Documents are available on the DWI website on the following topics:

- Roles and Responsibilities
- Incident Reporting
- Inspections (Audits)
- Enforcement

1.4 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 within another individual document if required.

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 production and delivery of wholesome water (the essential service).

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 the water sector 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 with regard to 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, in order 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. CREATING A NIS SCOPE

3.1 The creation of a NIS Scope will allow a company to identify the systems operating in either the IT or OT environments that impact on the production and delivery of wholesome water. The systems identified in the Scope are then included as part of the company's Cyber Assessment Framework (CAF).

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

3.3 The structure and reporting format of the Scope can be defined by the company however DWI recommends that companies should use an approach which best allows them to understand their systems.

3.4 In the first instance a company should identify the systems that underpin and support the production and delivery of wholesome water, understand their key functions and how these systems interact with other systems. This can include:

- A brief description of each system and its function
- A high level diagrammatic overview of the systems and their interconnectivity
- Identify the major dependencies between these systems
- Identify which systems are operated by third parties

3.5 For each of the systems identified in 3.4, 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 wholesome water.

3.6 Whilst it is appreciated that a NIS Scope will be dependent on the network and information systems in operation at each company, DWI expects, as a minimum that companies include any system that has a **direct impact** on the production and delivery of wholesome water, this should include, but not limited to:

- SCADA
- HMI
- PLCs
- RTUs
- IP Sensors
- IP Controllers
- Telemetry Master Stations

3.7 A NIS Scope will form part of the company's overall CAF submission and DWI will review and challenge the level and depth of the Scope where appropriate during the assessments of company's submission.

3.8 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. DWI 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.

4. OBJECTIVE OF THE CYBER ASSESSMENT FRAMEWORK

4.1 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.

4.2 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

4.3 These 4 objectives will be realised through the implementation of a set of 14 cyber security principles as outlined in Figure 4.1. These principles are designed to be outcome focused and therefore outline what needs to be achieved rather than exactly what needs to be completed.

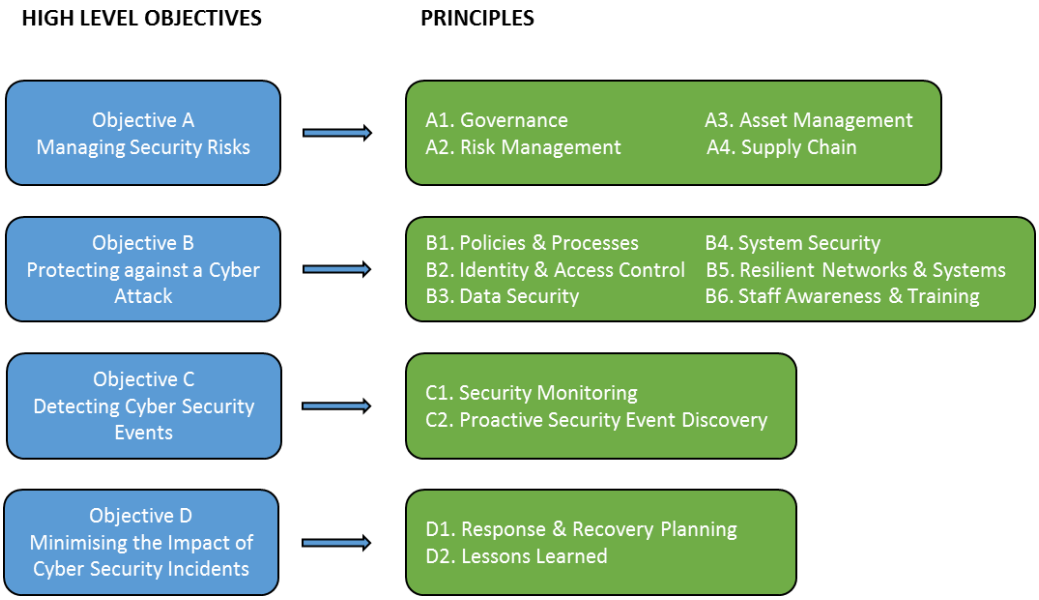


Figure 4.1: NIS Objectives and underlying Cyber Security Principles

4.4 The aim of the CAF therefore is to:

- Provides each company with a framework to assess how cyber security risks are being managed within their business in relation to the production and delivery of wholesome water.

- Allow the DWI to assess the extent to which each company is achieving the outcomes specified by the cyber security principles.

4.5 The results of the CAF will enable a company to identify a cyber security improvement package in line with the above objectives. This work package will be presented and discussed with DWI during the initial series of meetings. (See Section 10)

5. CAF STRUCTURE

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

5.2 The status of each contributing outcome is characterised as either being 'achieved' (Green), 'not achieved' (Red) and in some cases 'partially achieved' (Amber), dependent on the assessment of the indicators of good practice (IGPs).

5.3 These IGP's are considered the basis of the CAF profile, as outlined in Figure 5.1.

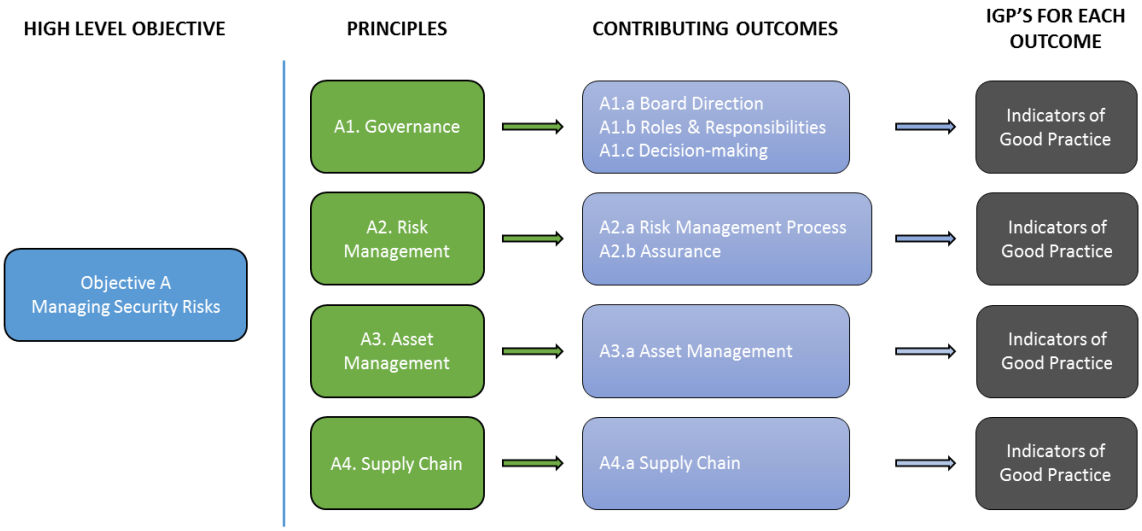


Figure 5.1: CAF Hierarchical Structure for Objective A

5.4 The results for all contributing outcomes will create a CAF profile. 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 level of cyber security some way beyond the bare minimum 'basic cyber hygiene' level. Ostensibly a CAF profile would consist of a mixture of some contributing outcomes to be met at 'achieved', some at 'partially achieved' and perhaps some (representing cyber security capabilities not appropriate at the level of the profile) identified as 'not applicable'.

5.5 DWI have created a CAF profile which is specific to the water sector. This profile outlines where DWI expects the sector to be working to achieve in the first years of the Regulations. This specific profile will be published to all water companies as part of DWI's assessment report following the first round of CAF submissions.

6. IT ENVIRONMENT AND OT ENVIRONMENTS

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

6.2 A single completed CAF covering both disciplines therefore may influence the status of the IGP's dependent on the strengths/weaknesses from either environment.

6.3 DWI acknowledges that companies may wish to complete separate CAF's for both the IT and OT disciplines on the basis that the information could be more beneficial to the company as it will provide a holistic assessment for each environment.

6.4 However DWI expects that a single completed CAF, combining the systems in scope for both IT and OT environments, is included as the primary CAF in the company's submission.

6.5 The 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.

6.6 If completed, a company may still include the individual IT and OT CAF's as part of the CAF submission and DWI are happy to reference these assessments during the discussions around future work planning.

7. CAF COMPLETION FOR AFFILIATED COMPANIES

7.1 The definition of an affiliated company is where two companies, operating in different geographical regions are operated by the same board of directors.

7.2 DWI appreciates that, dependent on the operational alignment of the two companies a single completed CAF may not reflect the true status of each company or it may be that the intention is to have the two companies operating separately, with no alignment.

7.3 Companies therefore, have the option to either submit a single CAF that combines the two affiliate companies or two individual CAF submissions. Companies should consider the benefits each option will provide as well as ensuring a consistent assessment is taken to any network and information systems common across both companies.

7.4 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.

7.5 DWI will discuss both profiles to ensure appropriate measures are being taken to achieve the sector specific profile for both companies and to understand the company's long term strategy with regards to system alignment.

8. COMPLETING THE CAF PROFILE

8.1 DWI would expect companies to complete the CAF using a number of staff to ensure the most accurate assessment is reflected. As with the NIS Scope, companies are best place to choose the relevant staff required and so DWI will not publish a prescriptive list however DWI would propose that the following roles should be represented as a minimum:

- IT staff and OT staff
- Resilience/Emergency Planners
- Security Managers
- Water Quality staff

8.2 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 water company may achieve the outcomes specified in the principles. It is recommended that companies refer to this guidance whilst completing the CAF.

8.3 In order for a consistent approach, companies should use the CAF Reporting Tool to complete their assessments, this can be obtain from the DWI's website and guidelines for using the tool are outlined in Annex 1.

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

8.5 Interpretation of each IGP column is standalone and therefore there is no direct correlation between each column for every contributing outcome. The IGP's should be read vertically and not applied horizontally (Annex 2).

8.6 The Green column of an IGP table defines the characteristics of fully achieving that contributing outcome. It is intended that all the indicators would need to be Green to support an assessment of 'achieved' as outlined in Figure 8.1

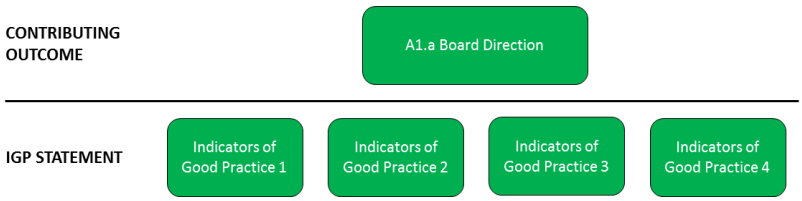


Figure 8.1: Characterisation of the Contributing Outcome following all IGP Statements being achieved

8.7 When present, the Amber column of an IGP table defines the characteristics of partially achieving that outcome. If at least one IGP is classified as Amber the contributing outcome will be assessed as 'partially achieved' as outlined in Figure 8.2. A 'partially achieved' status should be seen as still delivering worthwhile cyber security benefits.

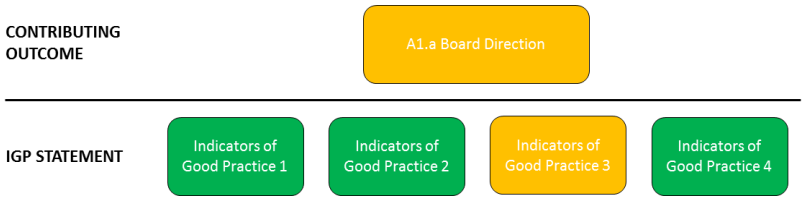


Figure 8.2: Characterisation of the Contributing Outcome following an IGP Statement being partially achieved

8.8 The Red column of an IGP table defines the characteristics of not achieving that contributing outcome. If a single indicator is characterised as Red then this would justify an assessment of 'not achieved' as outlined in Figure 8.3

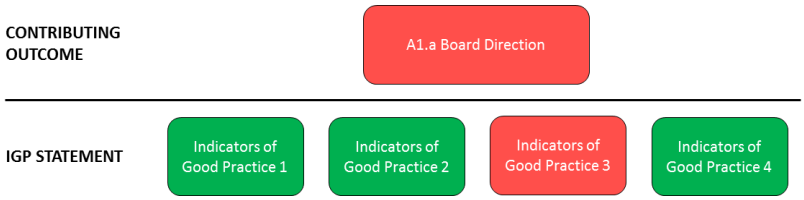


Figure 8.3: Characterisation of the Contributing Outcome following an IGP Statement being not achieved

8.9 A company may assess an IGP table as having individual statements that fall into each of the three characteristics. In this instance the Red column would be required to be selected as outlined Figure 8.4

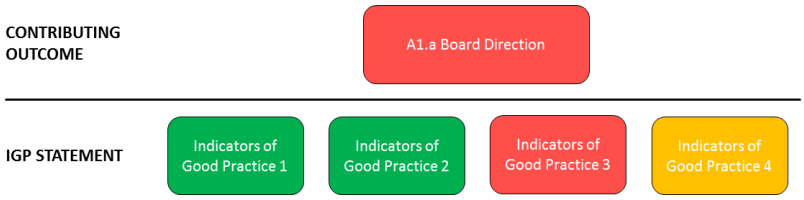
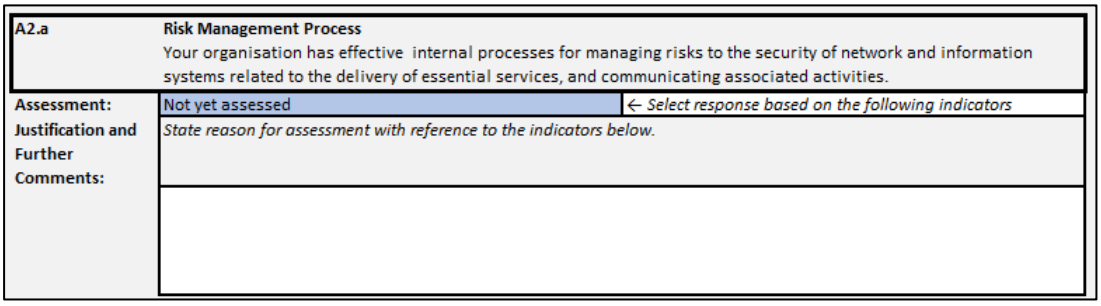


Figure 8.4: Characterisation of the Contributing Outcome following an IGP Statement being not achieved

8.10 Some contributing outcomes have the option to be characterised as 'not relevant'. Whilst DWI 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.

8.11 Companies should be able to justify the reasoning behind the assessment of each contributing outcome. This evidence should be referenced under the comments section in the CAF Reporting Tool (Figure 8.5), and should be able to be presented during discussions with DWI.



A2.a	Risk Management Process Your organisation has effective internal processes for managing risks to the security of network and information systems related to the delivery of essential services, and communicating associated activities.	
Assessment:	Not yet assessed	← *Select response based on the following indicators*
Justification and Further Comments:	*State reason for assessment with reference to the indicators below.*	

Figure 8.5: Comments Box for each Contributing Outcome

8.12 Whilst the nature and type of evidence referenced against each contributing outcome is the company's decision, the following could be included:

- Water UK: Cyber Security Principles for the Water Industry
- Defra: Water Sector Cyber Security Strategy
- Cyber Essentials
- Compliance to elements of security standards, ISO/IEC 27001, ISA/IEC 62443, NIST 800-53
- SCADA Self-Assessment Tool
- Company Business Continuity Plans (BCP's) and Emergency Plans (EP)
- Company Training for Cyber Security and general Staff Awareness Training

8.13 Companies should also make use of the comments box to include further information, where applicable, against the contributing outcome, this may include:

- Information around any of the individual IGP's
- if other controls (e.g. physical controls) are in place to justify the decisions
- if an individual IGP is not applicable to the company
- any further information the company feel is relevant to the assessment

8.14 It is recognised that companies have a number of sites which are either stand alone or are not connected to a wider company network. These sites are therefore protected by the physical barriers rather than the need to introduce cyber systems to those assets. DWI appreciates that companies have already invested in physical security measures as part of their SEMD programme and general security management, and that these measures already provide a level of cyber security.

8.15 It is also acknowledged that companies have introduced cyber security management prior to the Regulations coming into effect.

8.16 It is not the aim of the CAF therefore to replace or discard these measures and DWI will take a holistic view of a company's whole security practice when conducting its CAF assessments and subsequent discussions with the company.

8.17 Any questions around the CAF can be sent to dwi.NIS@defra.gov.uk

9. REPORTING REQUIREMENTS TO DWI

9.1 The timeline for companies to complete their Scope and CAF is outlined in Annex 3. Company's submissions to DWI should consist of the following documents:

- Company NIS Scope
- Completed CAF
- IT and OT profiles (optional)

9.2 Each submission should be accompanied by a signed declaration from the Board level contact (See Annex 4).

9.3 These submissions should be sent electronically to dwi.NIS@defra.gov.uk. It is recommended that companies send the email via a secure transfer alongside a separate email with the password. DWI will acknowledge receipt of the email.

9.4 Whilst companies should be able to justify their IGP scoring through suitable evidence, these documents **do not need** to be included as part of the CAF report. However companies may be asked to produce this evidence as part of any inspections conducted following the assessment process.

10. DWI ASSESSMENT REPORTS

10.1 DWI's approach to the CAF process is outlined below:

Create a NIS Scope ⇨ Undertake CAF Assessment ⇨ Identify Gaps ⇨ Outline Improvement Plan ⇨ Progress to achieve IGP Status

10.2 On receipt of submission, DWI will conduct analysis to produce an Assessment Report. This will be specific to each water company and will include:

i. An Executive Summary to the Board level contact
A high level summary outlining the results of the CAF assessment and the main areas of focus. This summary will not include any reference to the RAG status of each contributing outcome.

ii. CAF Profiles
There will be 3 CAF profiles included in the Assessment Report outlining the respective RAG status of each contributing outcomes.

1. the company profile;
2. the sector specific profile;
3. a profile overview of the industry

iii. Areas of Immediate Focus
The immediate focus will be to reach green status for the expected green contributing outcomes in the sector specific profile. As the sector profile will be issued within the Assessment Report, it should allow companies to consider how this could be achieved in advance of the initial meeting with DWI.

However, it should be noted that any red IGP's which give rise to concern will also be identified and these will be discussed in the post assessment meeting.

10.3 The Assessment Report will be sent to the NIS Day to Day contact. This correspondence will also include a range of dates which the company can choose in order for DWI to visit to discuss the CAF results, see evidence and outline a cyber security progress plan.

10.4 Companies are strongly encouraged to begin work on their cyber security progress plans in advance of this meeting to aid discussions. As a reference this work should include:

- Main areas the company feels should be the focus
- Areas of development against realistic timescales
- Justifications of where other evidence provides a level of protection to systems
- Long term strategy with regards system alignment (affiliated companies)

10.5 In general, DWI will not be considering enforcement action during the assessment of the initial CAF profiles. However, DWI have a statutory duty to ensure compliance with the NIS Regulations and in the unlikely eventuality that a company is significantly non-compliant with the Regulations, and that the company does not agree a timely resolution DWI will be minded to enforce.

Annex 1: Guidelines for the CAF Reporting Tool

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

ii. The Comments Box will expand to accommodate additional text

iii. Text in blue are hyperlinks

iv. Please read the IGP tables as outlined in Annex 2

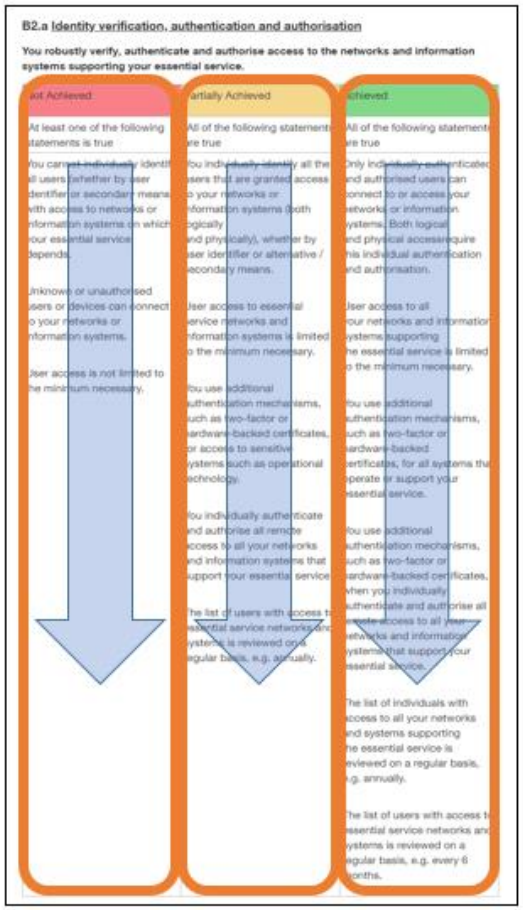
v. If submitting 2 CAF's please ensure they are clearly named to reflect the assessment

Annex 2: Guidance for Reading IGP Tables

B2.a Identity verification, authentication and authorisation

You robustly verify, authenticate and authorise access to the networks and information systems supporting your essential service.

Not Achieved	Partially Achieved	Achieved
At least one of the following statements is true	All of the following statements are true	All of the following statements are true
You cannot individually identify all users (whether by user identifier or secondary means) with access to networks or information systems on which your essential service depends.	You individually identify all the users that are granted access to your networks or information systems (both logically and physically), whether by user identifier or alternative / secondary means.	Only individually authenticated and authorised users can connect to or access your networks or information systems. Both logical and physical accessrequire this individual authentication and authorisation.
Unknown or unauthorised users or devices can connect to your networks or information systems. User access is not limited to	User access to essential service networks and information systems is limited to the minimum necessary.	User access to all your networks and information systems supporting the essential service is limited to the minimum necessary.



Annex 3: Timeline for Completion

Time Period	Actions	Designation
October 2018	Final, regulatory version of the CAF launched	NCSC
October 2018	Scope/CAF Guidance, CAF and Excel Reporting Tool circulated to sector	DWI
Nov - Dec 2018	NIS Scope completed	Water Company
Jan-Feb 2019	CAF completed	Water Company
March 2019	Water Company submit Scope and CAF to DWI	Water Company
March 2019	Analysis of CAF submissions	DWI
April 2019	Meeting with Water Company to discuss development plans	DWI/ Water Company

Annex 4: NIS Board Declaration

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