Guidance for Scottish Water on Network and Information Systems (NIS) Regulations 2018

Improvement Plans

Version 1.0

15/07/2021

Version	Date	Comment
0.1	24/06/2021	Draft for discussion with Scottish Water
1.0	15/07/2021	Final after Scottish Water's review

1. Background and purpose

1.1. The Network and Information Systems (NIS) Regulations 2018 came into effect on 10 May 2018. These Regulations designate drinking water supply and distribution as an essential service, and as such, Scottish Water has been designated as an Operator of Essential Services (OES).

1.2. These Regulations implement the NIS Directive which is designed to boost the overall level of security for network and information systems that support the delivery of essential services within the EU.

1.3. The Competent Authority (CA) for the water sector in Scotland is the Drinking Water Quality Regulator for Scotland (DWQR).

1.4. This guidance has been developed by the DWQR to set out the requirements regarding the submission of NIS Improvement Plans.

2. NIS self-assessment process

2.1. The DWQR uses the National Cyber Security Centre's (NCSC) Cyber Assessment Framework (CAF) to gain assurance that Scottish Water complies with the NIS Regulations. The CAF sets out 14 Principles that are further broken down in 39 Contributing Outcomes (COs)

2.2. Scottish Water undertakes a CAF self-assessment on DWQR's request. The first NIS CAF self-assessment was submitted to the DWQR in May 2019. A revised CAF self-assessment has been requested to cover Scottish Water's position up to March 2021.

2.3. Following a CAF self-assessment the submission is reviewed by the DWQR and discussed with Scottish Water. The discussion concludes with the agreement of:

- Scottish Waters CAF profile against each CO (based on a Red-Amber-Green scale)
- Scottish Water's target CAF profile and a timeline to achieve it
- Priority areas for improvement so that Scottish Water can transition to the agreed target CAF profile
- A date for the submission of an Improvement Plan (IP) that outlines Scottish Water's planned activities to deliver improvements in the agreed priority areas

2.4. The Improvement Plan for the 2019 CAF self-assessment was submitted in August 2019 and outlined Scottish Water's intended activities up to March 2021.

2.5. This guidance aims to outline the required structure and content of future improvement plans to ensure consistency across submissions and to facilitate the DWQR in fulfilling her role as a Competent Authority.

3. Improvement Plan purpose

3.1. The purpose of the submission of an Improvement Plan to the DWQR is:

- To assure the DWQR that the planned actions are targeting the agreed priority areas
- To assure the DWQR that actions are planned to progress at an appropriate pace
- To allow the DWQR to map the planned actions to the associated CAF COs they aim to improve and to assess the plan's adequacy to transitioning from the current to the target CAF profile.

3.2. While the CAF submission represents Scottish Water's status on the 39 COs at a point in time, the improvement plan is not intended to be a one-off static document. The timeline of an improvement plan may span a longer period but the plan itself will need to be regularly reviewed at a mutually agreed frequency to take on board new information and to update the DWQR on progress towards completing actions.

4. Improvement plan requirements

4.1. In order for an Improvement Plan to fulfil the purpose outlined in paragraph 3, the DWQR requires it to follow a set of principles that are outlined below.

4.2. Each action in the improvement plan must relate to the Essential Service and associated critical systems as defined by the scope agreed with the DWQR.

4.3. Each action in the improvement plan must be distinct and unique (i.e. there should not be multiple actions in the same entry and actions should not be duplicated)

4.4. Each action in the improvement plan must follow the SMART principle (specific, measurable, achievable, realistic, time-bound).

4.5. Each action must be assigned a theme area or project name. This is to allow the DWQR to filter for the specific theme area/ project and retrieve a list of all the actions associated with it, therefore gaining an overview of the scope of the theme area/ project.

4.6. Each action must clearly identify whether it relates to the IT estate, the OT estate, or both.

4.7. Each action must have an associated deadline.

4.8. Each action in the improvement plan must have a unique identifier. The identifier should have the format of the CAF CO code from which the action primarily originates, followed by a number uniquely identifying the action within this CO. For example. an action that primarily originates from improvement on the CO of asset management (that has the code A3a) should have a unique identifier in the format A3a-XX, where "XX" should be the number of the action within this CO (e.g. A3a-01, A3a-02 etc.)

4.9. Each action in the improvement plan must be mapped against ALL the COs that it contributes to improving. The CO that the action primarily originates from must be marked with a “P” (Primary). If there are other COs that the specific action delivers improvements on, they must be marked with a C (Contributing)

4.10. The improvement plan must clearly illustrate the current and the target CAF profile and allow the DWQR to filter for all the actions associated with a single CO (whether they are primary -“P”- or contributing -“C”- actions). This will allow the DWQR to inspect the planned actions to move SW from its current to its target profile on any CO.

4.11. The improvement plan must be submitted in an editable format (e.g. spreadsheet)

4.12. Some actions in the improvement plan will have necessary precedents. Scottish Water must list all necessary precedents against an action by referencing their unique identifiers against the action at hand. If there are multiple necessary precedents, their unique identifiers need to be separated by commas. For actions that have necessary precedents, the deadlines need to reflect their serial delivery.

5. Improvement plan template

5.1. The template to be used for the improvement plan has been separately provided to Scottish Water and can be accessed in this link (DWQR Guidance)

5.2. An example of the principles outlined in paragraph 4 is illustrated below.

NIS Improvement Plan Guidance

Each action must be assigned a single theme/ project

Each action must have a unique ID in the format "Primary CO code"-"Number"

Each action must be unique, distinct and SMART

The current and target CAF profiles against each CO must be listed (AC/PA/NA)

Each action must be identified as "IT"/ "OT" / "Both"

If an action has necessary pre-requisites, they need to be listed here using their unique IDs and separated by commas

					RELEVANT CAF CONTRIBUTING OUTCOME																																							
					Managing security risk							Preventing																				Minimising Impact							Detecting					
					Board Direction	Roles/ Responsibilities	Decision Making	Risk Management	Assurance	Asset Management	Supply Chain	Policy Process Dev	Policy Process Impl	Identity (V,A,A)	Device Management	PAM	IDAC (mng/ maint)	Understanding Data	Data in Transit	Stored Data	Mobile Data	Equipment Sanitisation	Secure by Design	Secure Configuration	Secure Management	Vulnerability Management	Resilience Preparation	Design for Resilience	Backups	Cyber Security Culture	Cyber Security Training	Monitoring Coverage	Securing Logs	Generating Alerts	Identifying Security Incidents	Monitoring Tools and Skills	Syst Abn Attach Detect	Proactive Attack Discovery	Response Plan	R&R Capability	Testing & Exercising	Incident Root Cause Analysis	Drive Improvement	
				Current	AC	AC	AC	PA	NA	NA	NA	PA	PA	NA	NA	NA	NA	NA	PA	NA	AC	NA	PA	NA	NA	PA	AC	PA	NA	AC	PA	AC	PA	AC	AC	AC	NA	NA	PA	AC	AC	AC	AC	
				Target	AC	AC	AC	AC	AC	NA	PA	PA	PA	PA	PA	PA	PA	PA	PA	PA	AC	AC	AC	PA	PA	PA	AC	AC	NA	AC	AC	AC	PA	AC	AC	AC	NA	NA	AC	AC	AC	AC	AC	
Theme/ Project	Action	Unique ID	IT/OT	Deadline	A1a	A1b	A1c	A2a	A2b	A3a	A4a	B1a	B1b	B2a	B2b	B2c	B2d	B3a	B3b	B3c	B3d	B3e	B4a	B4b	B4c	B4d	B5a	B5b	B5c	B6a	B6b	C1a	C1b	C1c	C1d	C1e	C2a	C2b	D1a	D1b	D1c	D2a	D2b	Necessary Prerequisites
NIS Audits	Complete 50 audits at prioritised WTWs	A3a-01	OT	Aug-22				C		P					C					C									C															
NIS Audits	Create OT asset register	A3a-02	OT	Dec-22		C				P																																		A3a-01, A3a-05
NIS Audits	Create process to update OT asset register	A3a-03	OT	Feb-23				C				P			C																													A3a-02

Each action must have an associated deadline. For actions that have necessary prerequisites, the deadlines needs to reflect the serial delivery.

Each action must have a single Primary CO associated with it (marked as "P") and can have multiple Contributing COs (marked as "C") to note the multiplicity of knock-on effects an action can have,