Scottish Government
Riaghaltas na h-Alba
gov.scot

Public Sector Action Plan

Cyber Resilience Framework

Self-Assessment Tool User Guide

Version 1.0 (Publication)
October 2019

Contact email:
CyberResilience@gov.scot

Revision History:
v. 1.0 Release Document

Contents

1. Introduction

1.1 Purpose

This annex introduces the Cyber Resilience Framework Concept Self-Assessment tool and provides guidance on its use.

1.2 Background

The tool is based upon a weighted security model matrix created utilising Common Categories across key standards and frameworks (see: Scottish Public Sector Cyber Resilience Framework 2019-20, Annex A: Standards Mapping Matrix).

2. Features of the Tool

2.1 Dashboard Tab

2.1.1 Statement of Applicability

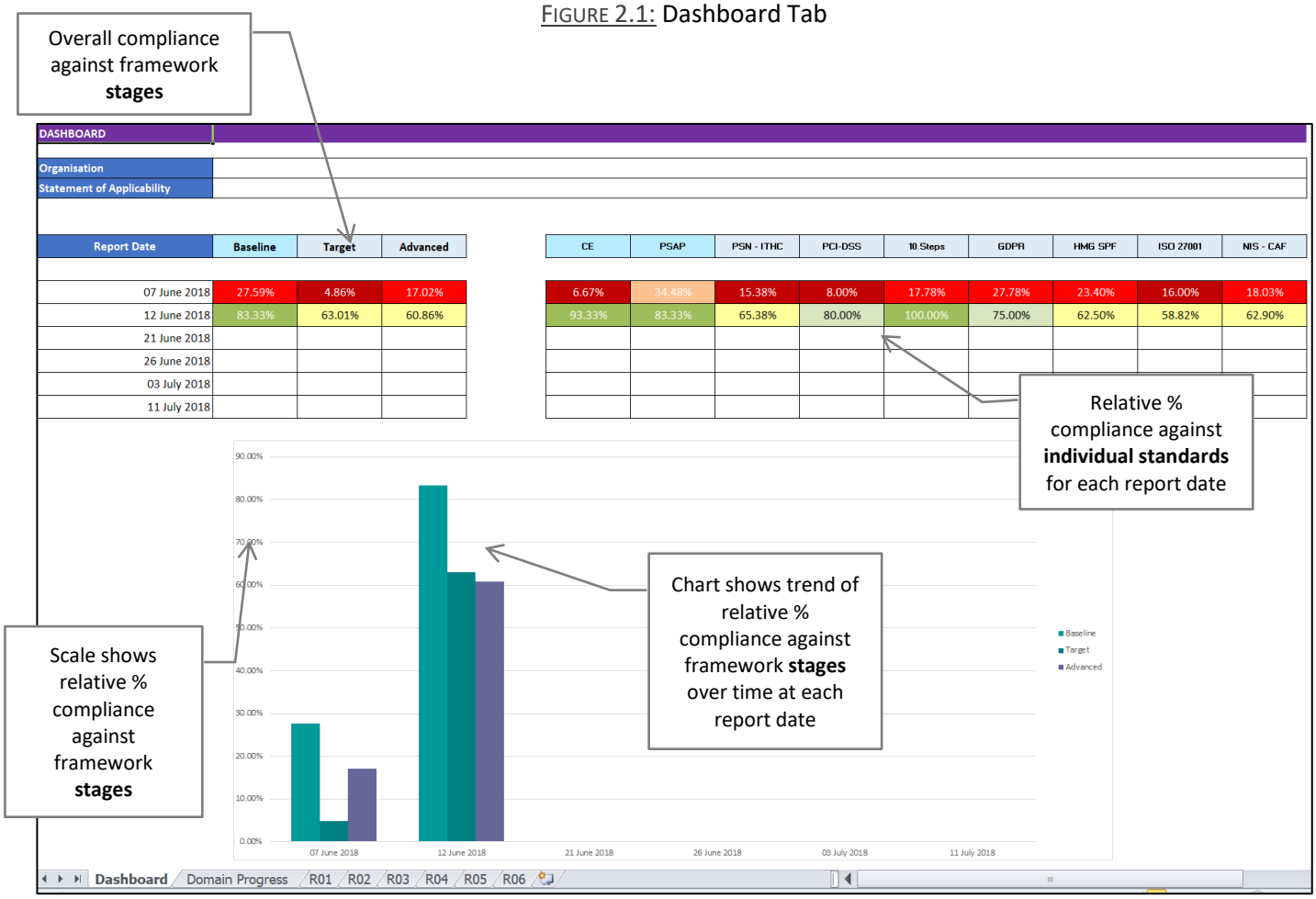
This is a free-text field to allow visibility and easy reporting on the Scope of the assessment. This will be particularly helpful if organisations are segmenting their assessments across the information and systems estates.

2.1.2 Status & Trend Analysis

As each report table is completed, the overall summary results are shown on the dashboard. This permits a ready assessment of progress against each of the standards or frameworks, alongside an overall percentage progress against all the stages (Baseline, Target and Advanced) of the Scottish Public Sector Cyber Resilience Framework.

Note that this table also allows recognition of achievements in delivery and readily demonstrates when organisations have gone "beyond compliance" and exceeded the requirements of a particular standard.

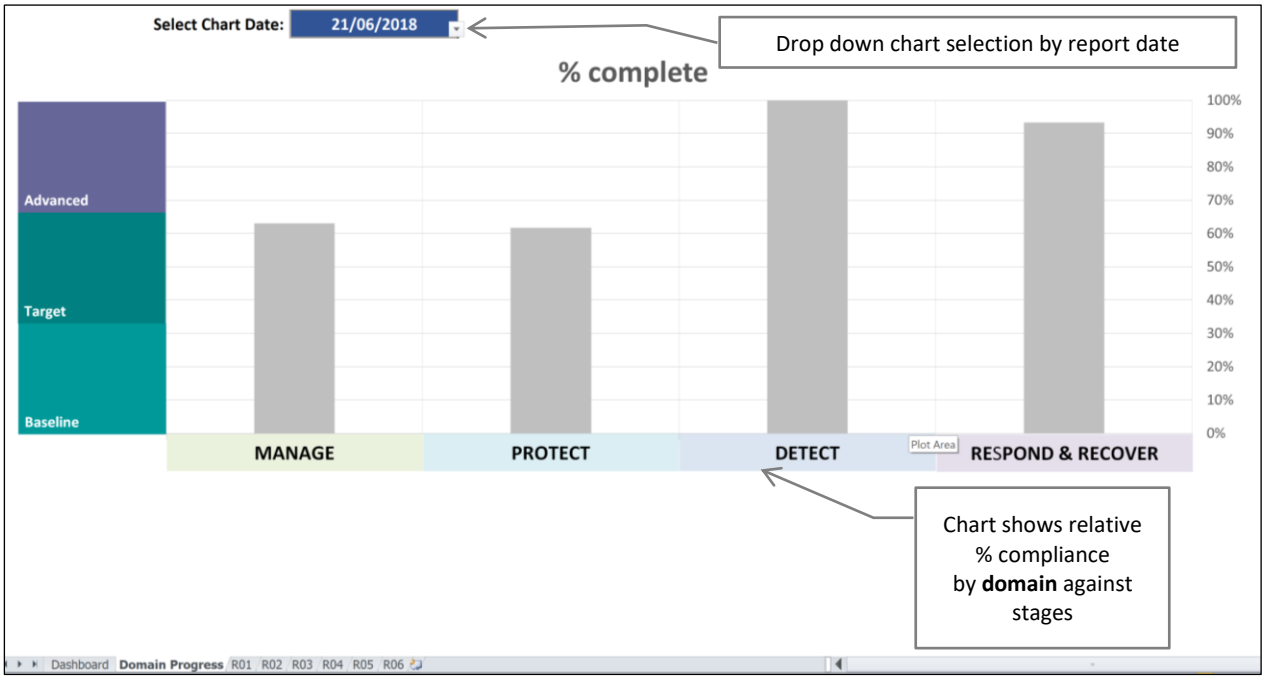
FIGURE 2.1: Dashboard Tab



2.2 Domain Progress Tab

This chart complements that of the Dashboard by presenting progress against the Baseline, Target and Advanced stages of the Cyber Resilience Framework for the selected date.

FIGURE 2.2: Domain-Stage Summary Chart



2.3 Report Tabs

The report tabs (R01, R02 etc.) represent the key activity areas of the tool. The features of these are shown in Figure 2.3.

Assessments of organisational compliance against each sub-category's requirements are made utilising the 6-tier radio button scale described at Table 2.1.

The tool calculates relative proportional compliance against each standard based upon this, as well as calculating overall compliance against all categories.

For convenience, the ticks column shows which sub-categories apply to each of the stages.

TABLE 2.1: Radio-Button Scale-Stage Summary Chart

Score	**0**	**1**	**2**	**3**	**4**	**5**
Stage	**BASELINE**		**TARGET**		**ADVANCED**	
Status	**Partial Baseline**	**Full Baseline**	**Partial Target**	**Full Target**	**Partial Advanced**	**Full Advanced**
Details	Over half of the Baseline Stage sub-category requirements are complete.	All of the Baseline Stage sub-category requirements are complete.	Over half of the Target Stage sub-category requirements are complete.	All of the Target Stage sub-category requirements are complete.	Over half of the Advanced Stage sub-category requirements are complete.	All of the Advanced Stage sub-category requirements are complete.

2.3.1 Categories; Sub-Categories

The list of categories has been aggregated from across all the standards and frameworks cited.

2.3.2 Radio Buttons

Use the radio buttons to show the current assessment of organisational compliance against the requirements in each of the sub-categories utilising the 6-tier scale (Table 2.1). The Not Applicable button may be employed where a sub-category is not relevant with an explanation provided in the **Comments box.** Utilising this button removes the sub-category from the organisation's compliance calculation.

2.3.3 Status Text

This is a summary of the level of compliance against the 6-tier scale as an aide memoir for convenience.

2.3.4 Stages RAG Status

This shows an aggregate of the relative compliance of the organisation across the three stages of the Cyber Resilience Framework using the colour scheme shown in Table 2.2.

2.3.5 Standards RAG Status

This shows the relative compliance of the organisation against categories within an individual standard using the colour scheme shown in Table 2.2.

TABLE 2.2: RAG colour scheme for Stages and Standards based upon levels of compliance

< 16.67%	Dark Red, White Text
16.67% - 33.33%	Bright Red, White Text
33.34% - 50.00%	Soft Orange, Black Text
50.01% - 66.67%	Yellow, Black Text
66.68% - 83.33%	Light Green, Black Text
83.34% - 100%	Dark Green, White text

2.3.6 Sub-categories RAG Status

This shows the relative compliance status for each sub-category within an individual standard. To make this visually more accessible a slightly different colour scheme has been adopted as shown in Table 2.3

TABLE 2.2: Sub-categories RAG colour scheme based upon levels of compliance

Not applicable	White
< 16.67%	Grey
16.67% - 33.33%	Light Red
33.34% - 50.00%	Soft Orange
50.01% - 66.67%	Yellow
66.68% - 83.33%	Light Green
83.34% - 100%	Dark Green

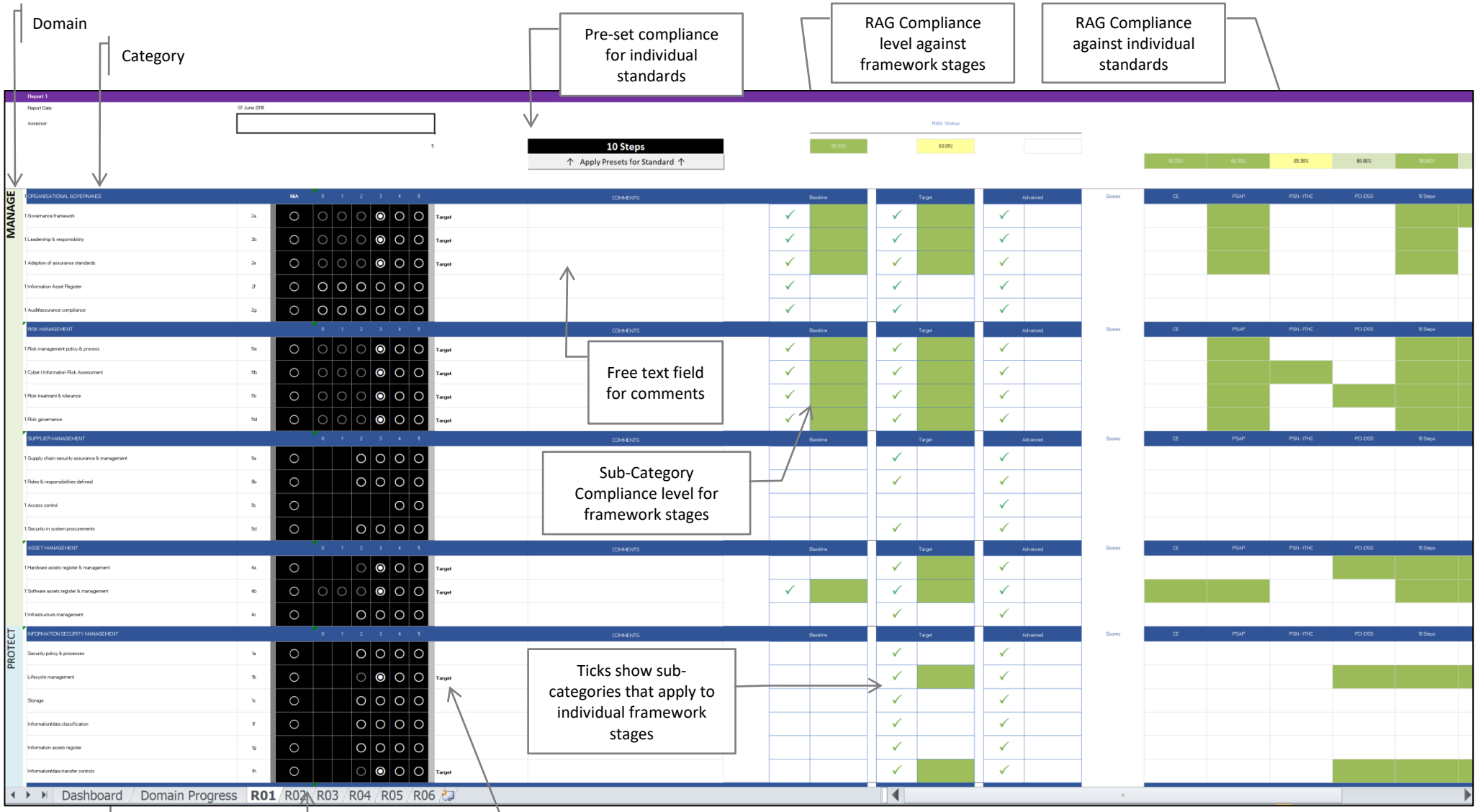
2.3.7 Standards Pre-set

The Pre-set drop down list can be used if an organisation has already attained compliance assurance against any of the standards. The pre-selection can be removed by holding down Shift and clicking on the pre-set button again.

2.3.8 Copy Previous

From Report 2 onwards, the "Copy Previous" button enables the result of the previous report to be auto-populated for convenience.

FIGURE 2.3: Report Tab



3. How to Use The Self-Assessment Tool

The tool should be used in conjunction with the requirements statements in the main Cyber Resilience Framework document to determine the compliance status of the organisation.

1. Start at the Report Tab

Using the Radio Buttons, evaluate the relative compliance of the organisation against each security sub-category on the six-tier grid utilising the criteria shown in Table 2.1

Note that where a sub-category is not relevant to the any of the three stages, this is reflected in a reduced number of radio buttons available for selection.

2. Review the Dashboard & Domain Progress

These aggregate the outcomes from the Report Tabs to capture and summarise the latest status of the organisation against individual standards and the three stages of the Cyber Resilience Framework (Fig 2.1) plus progress against the four domains against the three stages (Fig. 2.2).

These are intended to offer summary graphical reports for Senior Management and Board Members.

3. Status Review

From the initial report (R01) starting point, the gap between the Baseline, Target or Advanced Level of Cyber Resilience can be determined and a prioritised development plan established. This outcome can be deployed to highlight resources required and investment priorities.

4. Trend Analysis

Utilise successive Report tabs (R02, R03 etc.) to periodically re-assess the compliance status of the organisation. The “Copy Previous” button can be used if desired. The outcomes of these reports are aggregated into the Dashboard and Domain Progress chart presentations to show a trend analysis for reporting to senior management to demonstrate progress and RoI.