



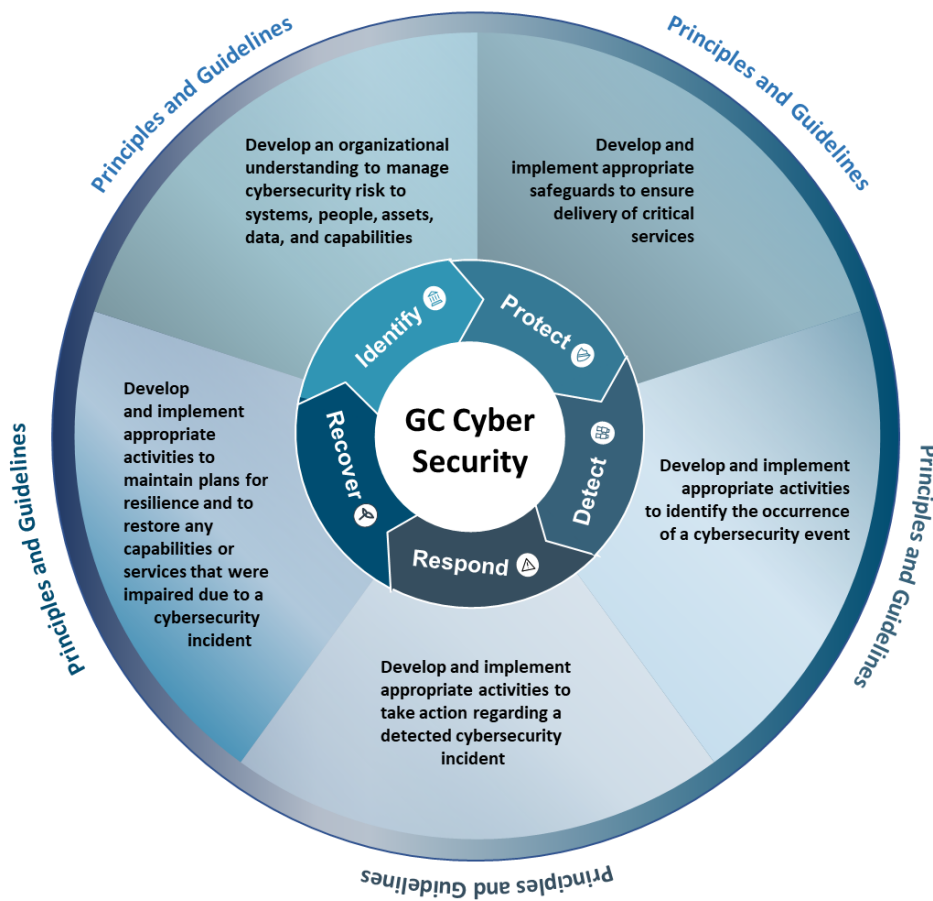
# Guide for Cyber Maturity Self-Assessment (CMSA) Tool



## Background

As per Section 4.4.4.1 of the [Directive on Service and Digital](#)<sup>1</sup>, the Designated Official for Cyber Security (DOCS) is responsible for “ensuring that cyber security requirements and appropriate risk-based measures are applied continuously in an **identify, protect, detect, respond, and recover** approach to protect information systems and services.”

To that end, a set of [GC Cyber Security Management Guidelines](#) has been established to support the DOCS in meeting this requirement.



It is expected that the DOCS work collaboratively<sup>2</sup> with the Departmental Chief Information Officer and Departmental Chief Security Officer in applying these principles and guidelines, with the aim of improving cyber security posture within a department or agency.

<sup>1</sup> As per the update to the Directive on Service and Digital targeting publication in early 2022.

<sup>2</sup> As per Section 4.4.4 of the Directive on Service and Digital.

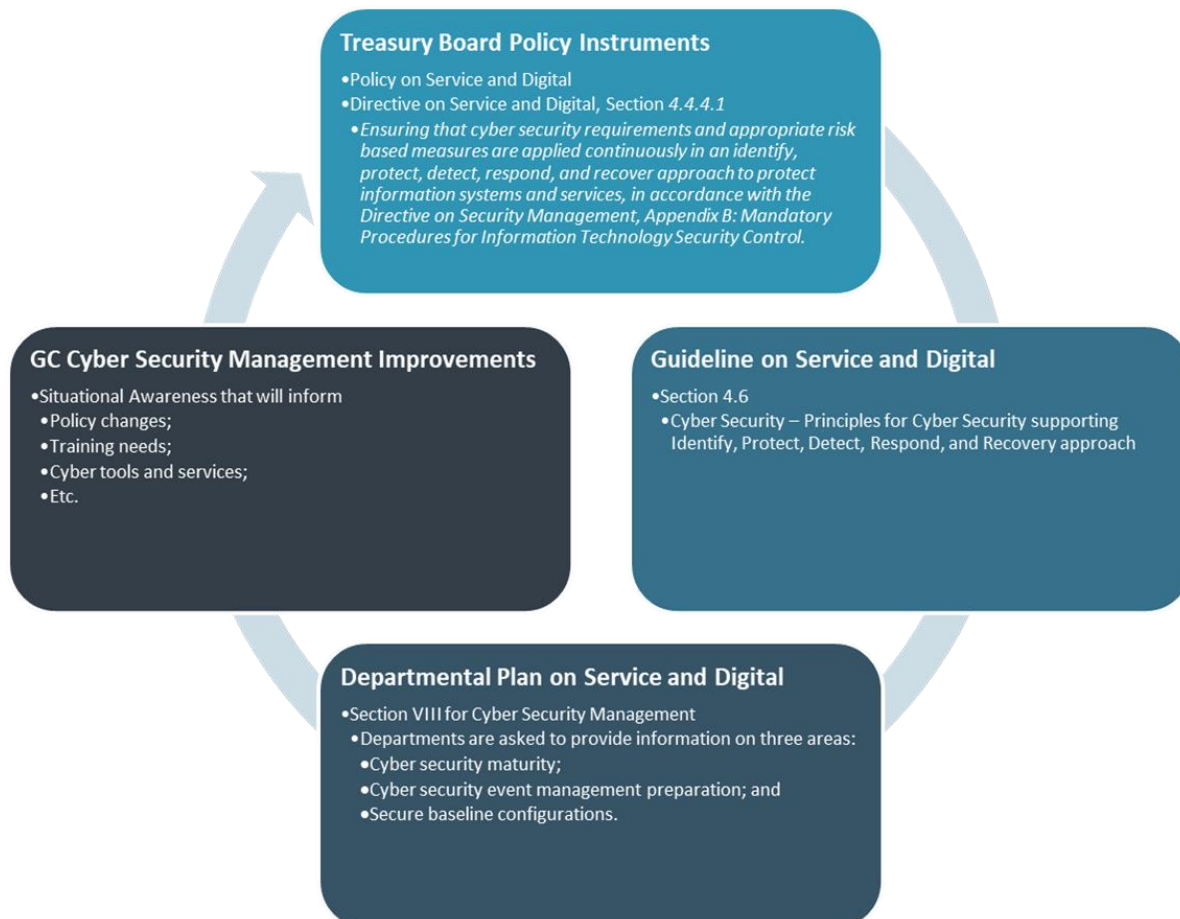


## Assessing Cyber Maturity

To understand the cyber security maturity posture across the Government of Canada (GC), a methodology to facilitate all GC institutions in assessing their cyber security maturity against recognized best practices has been established.

The GC [Cyber Maturity Self-Assessment Tool](#) (CMSA) aligns with the [GC Cyber Security Management Guidelines](#), as depicted below. The goals of the tool are to:

- ensure that enterprise cyber risks are being adequately managed and to identify areas of improvement;
- increase response time to potential risks by ensuring a secure and resilient enterprise infrastructure that enables the trusted delivery of programs and services; and
- reduce the cost and time spent in assessing cyber security maturity through other means (e.g., third party assessors).





## How to Access the CMSA Tool

The [CMSA](#) tool is hosted in the **Cyber Security Application Portal** of the **TBS Application Portal (TAP)**. Only users who are authenticated via GCpass (MyKey Login) and have been assigned a role within the Cyber Security Application Portal are granted access to the tool.

### Roles

There are two roles that are assigned within the CMSA tool:

1. **Designated Official for Cyber Security (DOCS)**, and
2. **Departmental Responder**.

The DOCS and Departmental Responder have equal access to the tool where they can: access, create and edit the CMSA report for their organization.

While the Departmental Responder will largely be responsible for responding to the CMSA, the DOCS will have access to the response information in order to review and approve of the GC organization's assessment.

Only TBS has the authority to assign users to a role in the **Cyber Security Application Portal**. Please contact TBS-Cyber Security's [DOCS Mailbox](#) to identify and/or modify the DOCS or Departmental Responder roles to ensure representatives have access to the tool.



## Steps to Accessing and Completing the Cyber Maturity Self-Assessment

### Step 1:

Access the TBS Application Portal at <https://portal-portail.tbs-sct.gc.ca/home-eng.aspx>.

Select the **Cyber Security Applications Portal** to access the CMSA tool.

The screenshot shows the TBS Applications Portal Home page. The page title is "TBS Applications Portal (TAP)". The navigation bar includes "TAP Home", "Applications", and "Help". There are links for "Sign In", "myEmployees", and "My TAP Profile". A yellow banner at the top of the main content area reads: "Oops, we're having some trouble. We appreciate your patience as we work quickly to get GC-VATS back up and running." Below this is a section titled "My Apps" with the instruction "To access an application, click on its image below." The page displays a grid of application tiles. The tile for "CSAP - BETA - Cyber Security Applications Portal" is circled in red. The tile contains the following text: "CSAP - BETA - Cyber Security Applications Portal" and "Provides federal departments access to an integrated set of digital cyber security tools". Other visible tiles include GC-VATS, PSPM, MAF, CORS, CALLIPERS, ETMS, PCIS, EEPR, GRI, HRDAV, and ERIS.



## Step 2:

Once on the homepage of the Cyber Security Applications Portal, select **'Access'** to access your organization's CMSA questionnaire.

The screenshot shows the Cyber Security Applications Portal homepage. At the top, there is a dark red navigation bar with the text "Cyber Security Applications Portal" on the left and "GCconnex GCpedia GCdirectory GCcollab" on the right, along with a "Français" link. Below this is a grey bar with "Cyber Maturity Self-Assessment" on the left. The main content area is white and features a "Home" link, a user login status "Signed in as [redacted] of TRS with role Department Responder" and an "Exit CSAP" button. The main heading is "Welcome to the Cyber Security Applications Portal" followed by a sub-heading "Cyber Maturity Self-Assessment (CMSA)". Below this, there is a paragraph: "Access the assessment questionnaire to measure your department's cyber maturity based on recognized best practices." A red box highlights the "Access" button. At the bottom left, it says "Version: 1.0.0".



### Step 3:

You will now land on your departmental CMSA page, which will identify assessments completed or in progress for your organization.

To begin a new assessment, select **'Start a new assessment'**.

It is not required that an assessment be completed in its entirety at once. You may save your work as you go and edit an existing assessment at any time.

The screenshot displays the 'Cyber Security Applications Portal' interface. At the top, there is a navigation bar with links for 'GCconnex', 'GCpedia', 'GCdirectory', and 'GCcollab', along with a 'Français' language option. Below this, the page title is 'Cyber Maturity Self-Assessment'. A user is signed in as 'TBS' with the role 'Department Responder'. The main content area features a 'Start a new assessment' button, which is highlighted with a red rectangular box. Below the button, there is a section titled 'Treasury Board of Canada Secretariat : Cyber Maturity Self-Assessments' with an 'Export to Excel' button. A table is present, but it is empty, displaying 'Showing 0 to 0 of 0 entries' and 'No data is available in the table'. The table headers include 'Last modified date (YYYY-MM-DD)', 'Last modified by', 'Status', 'Maturity score', and 'Actions'. The version number '1.0.0' is visible at the bottom left.



## Step 4:

Once a new assessment has been started (or you wish to modify an assessment in progress), you will be brought to a survey that is broken down into five tabs corresponding to the **Cyber Security Management Principles**: 1) **Identify**; 2) **Protect**; 3) **Detect**; 4) **Respond**; and 5) **Recover**.

- *If you would like more information and guidance on the GC Cyber Security Management Principles, we encourage you to check out the [GC Cyber Security Management guidelines](#) on GCpedia.*

Departmental Responders must complete the survey by responding to **all** the questions under each of the tabs corresponding to the Cyber Security Management Principles.

Departmental Responders may select '**Out of Departmental Scope**' if the responsibility outlined in the survey question is overseen by another organization. If selected, a comment box will appear requesting that you list the organization responsible.

Following the completion of the survey, select '**Save**' at the bottom of the webpage, followed by selecting the '**Results**' tab.

The screenshot displays the 'Cyber Security Applications Portal' interface. At the top, there are navigation links for 'GCconnex', 'GCpedia', 'GCdirectory', and 'GCcollab', along with a 'Français' language option. The main header reads 'Cyber Maturity Self-Assessment'. Below this, a breadcrumb trail shows 'Home > Cyber Maturity Self-Assessment'. A user is signed in as '██████████' of 'TBS' with the role 'Department Responder', and there is an 'Exit CSAP' button. The main content area is titled 'Cyber Maturity Self-Assessment' and includes a 'Help' link. A horizontal navigation bar contains five tabs: 'Identify', 'Protect', 'Detect', 'Respond', and 'Recover', with the 'Results' tab highlighted in red. Below the tabs, the 'Asset Management' section is visible, containing two questions: 'ID.AM-1 \* Physical devices and systems within the department are inventoried. How extensive is the process to inventory physical devices and systems? (required)' and 'ID.AM-2 \* Software platforms and applications within the department are inventoried. How extensive is the software and applications inventory process? (required)'. Each question has five radio button options ranging from '0 - No physical devices and systems inventory process exists' to '4 - The physical devices and systems are subject to a defined asset management life cycle (creation, processing, storage, transmission, deletion and destruction)', plus an 'Out of departmental scope' option.

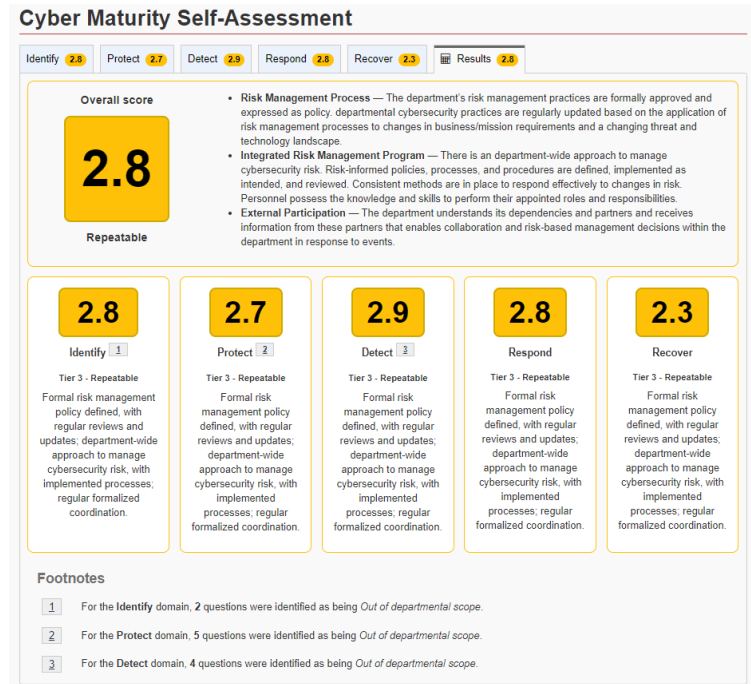




### Step 5:

Based on the responses to the survey, the ‘Results’ tab will summarize the organization’s cyber maturity level.

Your organization will be given an overall score between 0-4, as well as scores broken down by each of the five Cyber Security Management Principles (i.e., identify, protect, detect, respond, and recover).





Following the completion of the CMSA, the history of the assessment will populate within the CMSA page with the options to:

- **view an assessment** by selecting the **'eye' icon**;
- **modify or complete an assessment** by selecting the **'pen' icon**; and
- **export the assessment to excel format** by selecting **'Export to Excel'**.

Cyber Security Applications Portal

GCconnex GCpedia GCdirectory GCcollab Français

Cyber Maturity Self-Assessment

Home

Signed in as [redacted] .TRS with role Department Responder Exit CSAP

### Cyber Maturity Self-Assessment

► Help

#### Treasury Board of Canada Secretariat : Cyber Maturity Self-Assessments

Export to Excel

Filter items [input] Showing 1 to 1 of 1 entries | Show 10 entries

Last modified date (YYYY-MM-DD) ↑↓	Last modified by ↑↓	Status ↑↓	Maturity score ↑↓	Actions
2021-10-27	[redacted]	Draft (100% complete)	3.3	

1

Version: 1.0.0



## Contact Information

If you are having technical difficulties with the tool, please reach out to us at the following email address:

- DOCS / ADCS [DOCS-ADCS@tbs-sct.gc.ca](mailto:DOCS-ADCS@tbs-sct.gc.ca)

If you have any general questions or would like more information, please reach out to us at the following email address:

- TBS-Cyber [zbtscybers@tbs-sct.gc.ca](mailto:zbtscybers@tbs-sct.gc.ca)