



vmia

Self-Assessment Hub – Cyber Assessments

Client User Guide

- Victorian Government Cyber Maturity Benchmark
- Health Sector Cyber Security Assessments



Contents

Introduction to this guide	3
Victorian Government Cyber Maturity Benchmark (VGCMB)	4
Introduction.....	4
Completing an assessment (VGCMB).....	5
Health Sector Cyber Security Assessments	8
Introduction.....	8
Completing an assessment (Health Sector).....	9
Glossary.....	11
Generating reports (for all cyber assessments).....	12

**VMIA is the Victorian
Government's insurer
and risk adviser**

Level 10 South
161 Collins Street
Melbourne VIC 3000

P (03) 9270 6900
contact@vmia.vic.gov.au
ABN 39 682 497 841

vmia.vic.gov.au
© Victorian Managed
Insurance Authority



Victorian Managed Insurance Authority (VMIA) acknowledges the Traditional Custodians of the land on which we do business, and we pay our respects to Elders past, present, and emerging. We acknowledge the important contribution that Aboriginal and Torres Strait Islander peoples make in creating a thriving Victoria.

Introduction to this guide

The VMIA Self-Assessment Hub is an online tool operated by VMIA. Accessible only to authorised users, the Hub includes the following cyber self-assessment tools:

- Victorian Government Cyber Maturity Benchmark
- Health Sector Cyber Security Assessment
- Health Sector Medical Device Security Assessment.

About this guide

This reference guide will help Victorian Government departments and agencies to navigate and use any cyber assessment tools that are available to them on the VMIA Self-Assessment Hub effectively.

For general administrative tasks associated with the VMIA Self-Assessment Hub, please refer to the [Self-Assessment Hub – Client User Guide](#) for instructions:

- How to log in and log out
- Exploring the different user roles
- Maintaining users
- Self-Assessment Hub homepage.

Need assistance?

Contact us by email: cyberservice@vmia.vic.gov.au or phone: (03) 9270 6990.

Victorian Government Cyber Maturity Benchmark (VGCMB)

Introduction

The Victorian Government Cyber Maturity Benchmark is an annual self-assessment of baseline cyber security controls across the Victorian Government. Delivered in partnership with the Department of Government Services, Victoria, the Benchmark is based on the Australian Cyber Security Centre's Essential Eight Maturity Model and brings together risk, ICT and cyber professionals to assess baseline cyber controls and plan improvements that will protect government services and data.

The Victorian Government Chief Information Security Officer recommends organisations to implement the Essential Eight mitigation strategies as a baseline to prevent cyber incidents, mitigate the damage they cause, and recover from more efficiently and effectively.

Why take the assessment

The Benchmark self-assessment can help you to:

- review and understand the maturity of your organisation's baseline cyber controls
- produce reports that can be used to make decisions about investment in cyber security improvements
- support Victorian Protective Data Security Standard (VPDSS) attestation for Standard 11: ICT Security by providing information about technical controls
- compare your organisation's cyber maturity against a whole-of-government benchmark or selected sectors.

The Benchmark also helps the Department of Government Services and VMIA understand cyber maturity across the Victorian public sector and make informed decisions about how to improve the State's cyber security and recovery.

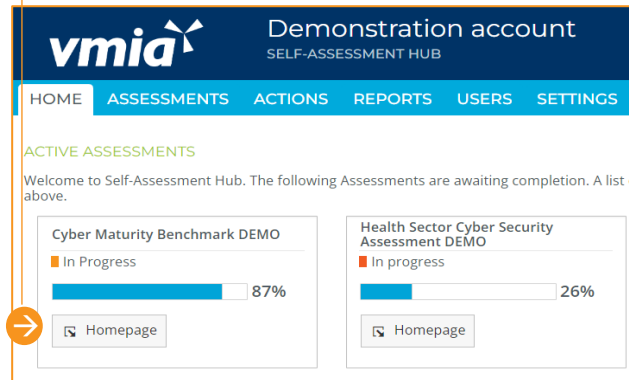
Completing an assessment (VGCMB)

Enter the assessment

From the Self-Assessment Hub homepage, navigate to 'Assessments'. There are two ways:

1. From the HOME tab, go to 'ACTIVE ASSESSMENTS'.
2. Click on the 'Homepage' button and the campaign page will appear.

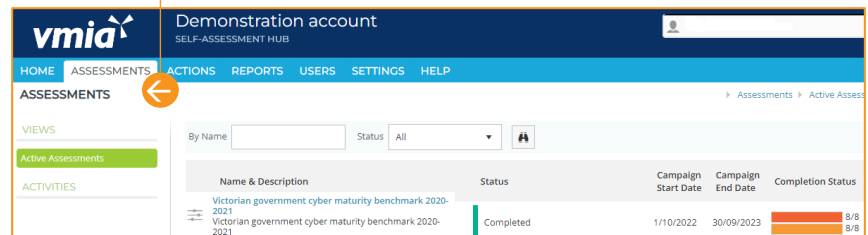
Click on Homepage



OR

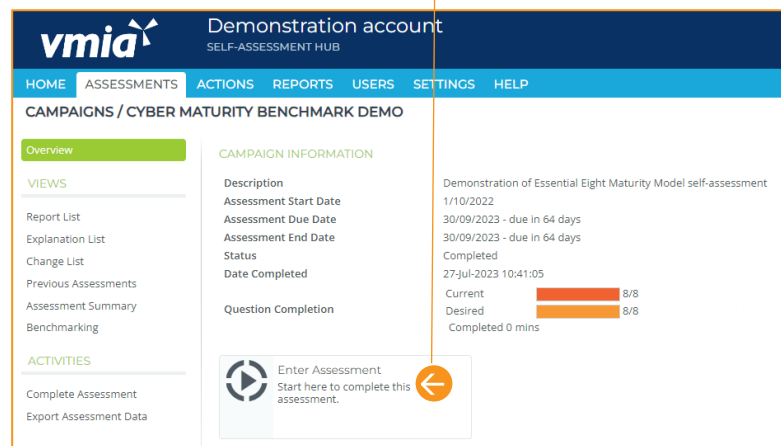
Assessments tab

1. From the tabs bar at the top of the window, click on the 'ASSESSMENTS' tab.
2. Click on the assessment name and the campaign page will appear.



3. Click on 'Enter Assessment' button.

Click to enter assessment



Answer the self-assessment questions.

To answer each of the eight self-assessment questions, select the appropriate level of maturity from the options provided. To help you select the right maturity level, there is a detailed description of the control at the top of the screen, and a description of the relevant control maturity for each of the levels under the Essential Eight (maturity levels zero, one, two and three).

Current maturity level

Desired maturity level

←

1.1. Application control

Application control is a security approach designed to protect against malicious code (also known as malware) executing on systems. When implemented robustly, it ensures only approved applications (e.g. executables, software libraries, scripts, installers, compiled HTML, HTML applications, control panel applets and drivers) can be executed.

While application control is primarily designed to prevent the execution and spread of malicious code, it can also prevent the installation or use of unapproved applications.

Prevent +

(2.1) →

Maturity Rating	Current	Desired
0	<p><input checked="" type="checkbox"/> Maturity Level Zero Not yet Maturity Level One, or not yet aligned to the intent of the mitigation strategy</p>	<input type="checkbox"/>
1	<p><input type="checkbox"/> Maturity Level One The execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets is prevented on workstations from within standard user profiles and temporary folders used by the operating system, web browsers and email clients.</p>	<input type="checkbox"/>
2	<p><input type="checkbox"/> Maturity Level Two Application control is implemented on workstations and internet-facing servers. Application control restricts the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets to an organisation-approved set. Allowed and blocked execution events on workstations and internet-facing servers are logged.</p>	<input type="checkbox"/>
3	<p><input type="checkbox"/> Maturity Level Three Application control is implemented on workstations and servers. Application control restricts the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications, control panel applets and drivers to an organisation-approved set. Microsoft's 'recommended block rules' are implemented. Microsoft's 'recommended driver block rules' are implemented. Application control rulesets are validated on an annual or more frequent basis. Allowed and blocked execution events on workstations and servers are centrally logged. Event logs are protected from unauthorised modification and deletion. Event logs are monitored for signs of compromise and actioned when any signs of compromise are detected.</p>	<input type="checkbox"/>

CONTROL EFFECTIVENESS

COVERAGE

■ Weak control coverage

Amount of compliant systems: Less than half ← Risk impact of the non-compliant systems: Moderate

ASSURANCE

■ Strong control coverage

Assurance over the controls: Internal Audit How old is that assurance: Less than 1 year old

EXPLANATORY NOTES

B *I* U abc </> :|: i|: ↶ es ↷

1. Choose current and desired maturity levels in the self-assessment.
2. Select your coverage and assurance ratings.
3. To help you assess the effectiveness of the controls in place, there are four additional questions for each of the eight control areas, in the form of drop-down menus. Simply select the option which most accurately represents the arrangements for each type of control.
4. Enter any explanatory notes.
5. You can add information about why the maturity level was chosen for each of the eight control areas, as well as notes about coverage and assurance.

Definition





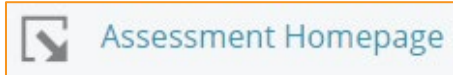
Current: Select the maturity level for your agency at this current point in time.

Desired: Select the option that best fits the maturity level your agency is working towards.

Coverage: The amount/percentage of systems in scope which have implemented the security control and the risk impact of systems in scope that are not covered.

Assurance: Who is responsible for maturity assessment of the control (e.g. self-assessed or audited) and how recently.

Navigate the questions

To:	Action:
Move to the next question or go back to a question	Click  or 
In the left-hand menu	red / orange tick  = answered question (current / future maturity rating) grey bar  = unanswered question.
Exit the assessment	Scroll down and click 

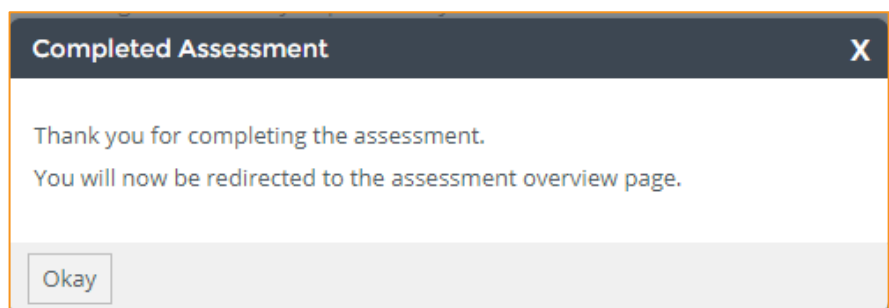
Save questions

The Benchmark self-assessment automatically saves as you work so you won't see any save buttons. Your answers and comments are saved as you progress through the assessment.

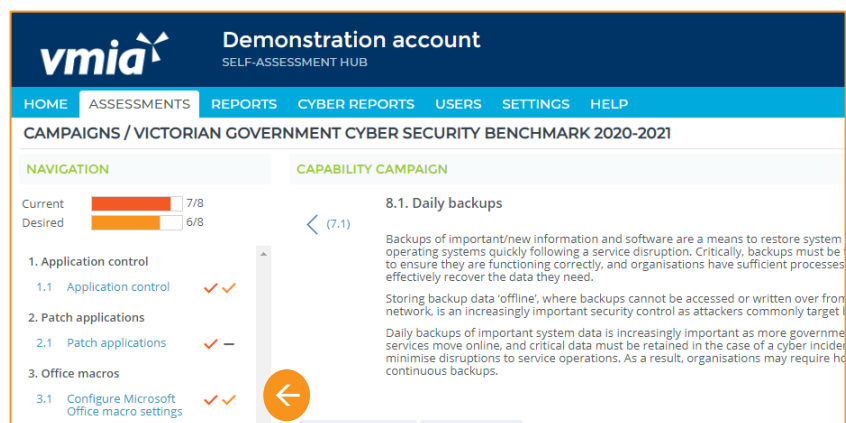
Completed assessment

Once the assessment has been completed, the following message will appear. Click the 'Okay' button to proceed to the overview screen, where you can review your assessment and access reporting.

If the 'Completed Assessment' message doesn't display, check the progress indicator – you may have missed a question.



Unanswered questions will have a grey dash next to them in the left-hand question menu.



A grey dash indicates a question is unanswered.

Health Sector Cyber Security Assessments

Introduction

The VMIA Self-Assessment Hub hosts two cyber assessments related to the Health Sector. The Department of Health operates a cyber security assurance program for the health sector, and started the cyber security uplift program in 2016. The first public health sector-wide assessment was completed in 2017 and extended to registered community health services in 2018.

The **Health Sector Cyber Security Assessment (CSA)** is an annual self-assessment of baseline controls across Victorian public health and community health services. Developed in partnership with eHealth (part of Department of Health), this cyber assessment brings together risk, ICT and cyber professionals to assess baseline cyber controls and plan improvements that will protect government services and data. The Health Sector CSA is the latest version of security controls to help health services detect, protect, and respond to the evolving cyber security environment.

The **Health Sector Medical Device Security Assessment (MDSA)** contains a subset of control strategies designed specifically for medical devices, mapped to the Health Sector Cyber Security Controls. It is a package of control strategies adapted from the Therapeutics Goods Administration's [Medical Device Cyber Security Guidance for large-scale service providers](#) and security best practices for industrial control systems. Maturity levels for each control strategy provide an indication of an organisation's cyber security maturity.

Why take the assessments

The Health Sector CSA is based on a package of controls drawn from complementary frameworks that focus on various cyber threats, including the following:

- Australian Signals Directorate's Essential Eight
- Centre for Internet Security
- Australian Cyber Security Centre's Information Security Manual
- National Institute of Standards and Technology.

Maturity levels for each control will provide an indication of an organisation's cyber security maturity and can help organisations to:

- review and understand cyber security maturity
- make informed decisions about cyber security improvements
- take focused steps to protect from cyber-attacks.

Completing an assessment (Health Sector)

Overview

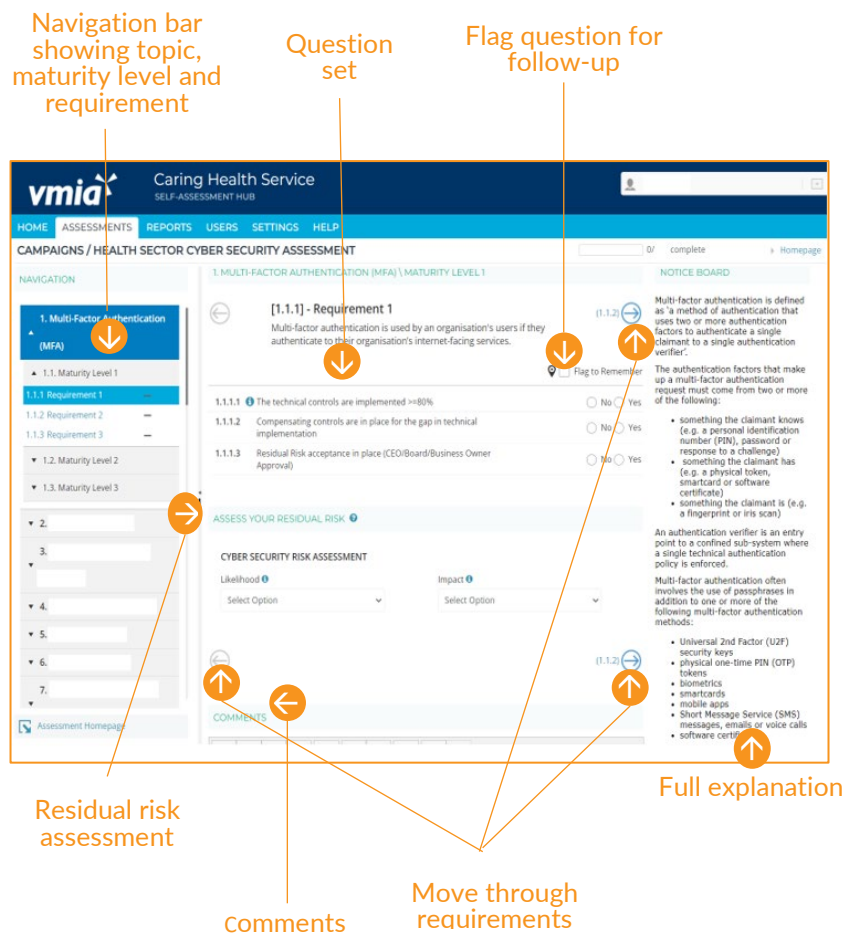
You'll be asked to respond to 'Topics' that relate to specific controls in each assessment framework.

Each topic contains a varying number of 'Requirements' divided into the three maturity levels: **Maturity Level 1 (ML1)**, **Maturity Level 2 (ML2)** and **Maturity Level 3 (ML3)**.



To complete the assessment, respond to questions in each of the requirements.

Let's step through one topic as an example.

1. Each requirement has descriptions and question sets.
2. The assessment navigation menu is on the left. Scroll through to see the list of topics.
3. The notice board on the right contains topic explanations. Scroll down to read all information including measurements and documentation.
4. Each requirement has three sections:
 - a. Question set – select most appropriate answer.
 - b. Assessment of residual risk – click dropdown box to see options.
 - c. Comments – free text section.
5. Move through requirements by clicking blue arrows or selecting on the navigation menu.



Notes:

- You don't need to attach evidence to this assessment. However, any evidence available to eHealth on request may be listed in comments section.
- If you need to answer a question later, use the 'Flag to remember' checkbox.
- Hover over info icons ( or ) for more information.

Topic summary page (Health Sector CSA only)

Data from the Health Sector CSA informs your completion of the Victorian Government Cyber Maturity Benchmark if it applies to your organisation. The topic summary page is an essential part of completing your Health Sector CSA.

The **topic summary page** can be accessed through your **assessment overview page**.

The screenshot shows the 'CAMPAIGNS / HEALTH SECTOR CYBER SECURITY ASSESSMENT DEMO' page. On the left sidebar, the 'Complete Topic Summaries' button is highlighted with a red box and an arrow. In the main content area, a card titled 'Complete Topic Summaries' is also highlighted with a red box and an arrow. Below this, the 'ASSESSMENT STRUCTURE' table is visible:

Topics	Topic Summary Completion	Completion
Topic 1. Multi-Factor Authentication (MFA)	✓	9/9
Topic 2. Application control	✓	8/8
Topic 3. Restrict administrative privileges	✓	18/18

Alternatively, **after you enter your assessment**, you can also access the topic summary page through the **navigation bar** situated on the **left had side** of your assessment page

The screenshot shows a 'NAVIGATION' sidebar with a tree view of assessment topics. The 'Topic Summaries' button at the bottom is highlighted with a red box and an arrow.

In the topic summary page (below), you can provide responses for your desired maturity level, coverage and assurance for Essential Eight. All other responses are automatically generated based on answers provided in your assessment.

Topic	Current	Desired	Coverage		Assurance		
			Amount of compliant systems	Risk impact of the non-compliant systems	Assurance over the controls	How old is that assurance	
1. Multi-Factor Authentication (MFA)	3 - Maturity Level Three	3 - Maturity Level Three	Most	Major	Select Option	Select Option	
2. Application control	2 - Maturity Level Two	2 - Maturity Level Two	Approx. half	Moderate	External Audit	Select Option	
3. Restrict administrative privileges	1 - Maturity Level One	2 - Maturity Level Two	Approx. half	Select Option	Self-Assessed	Select Option	
4. Patch operating systems	Select level	2 - Maturity Level Two	Select Option	Select Option	Select Option	Select Option	
5. Regular backups	Select level	2 - Maturity Level Two	Select Option	Select Option	Select Option	Select Option	
6. Patch Applications	3 - Maturity Level Three	2 - Maturity Level Two	Less than half	Select Option	Select Option	Select Option	
7. Microsoft Office macro settings	1 - Maturity Level One	2 - Maturity Level Two	Most	Select Option	Select Option	Select Option	
8. User application hardening	Select level	2 - Maturity Level Two	Select Option	Select Option	Select Option	Select Option	

Select from the dropdowns

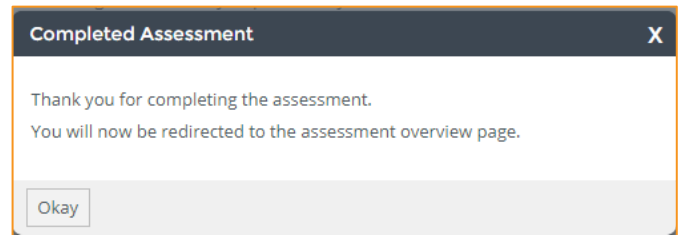
Save responses

The Hub automatically saves your work. Your answers and comments are saved as you progress through the assessment, and if you click on any page in the Hub before closing your browser.

Completed assessment

Once the assessment is complete, click 'Okay' to go to the overview screen to review your assessment and access reporting.

If the 'Completed Assessment' message doesn't display, check the progress indicator – you might have missed a question.



Glossary

Symbols (examples)	Meaning
	ML = Maturity Level of control
	% = Calculated based on requirements within each control
	Completed all questions and risk assessments
	Partially complete (e.g. completed all questions, incomplete risk assessment)
	Minimum requirement is not met
	Incomplete
	No responses recorded
	Additional information available
	Move to next requirement
	Move to previous requirement

Generating reports (for all cyber assessments)

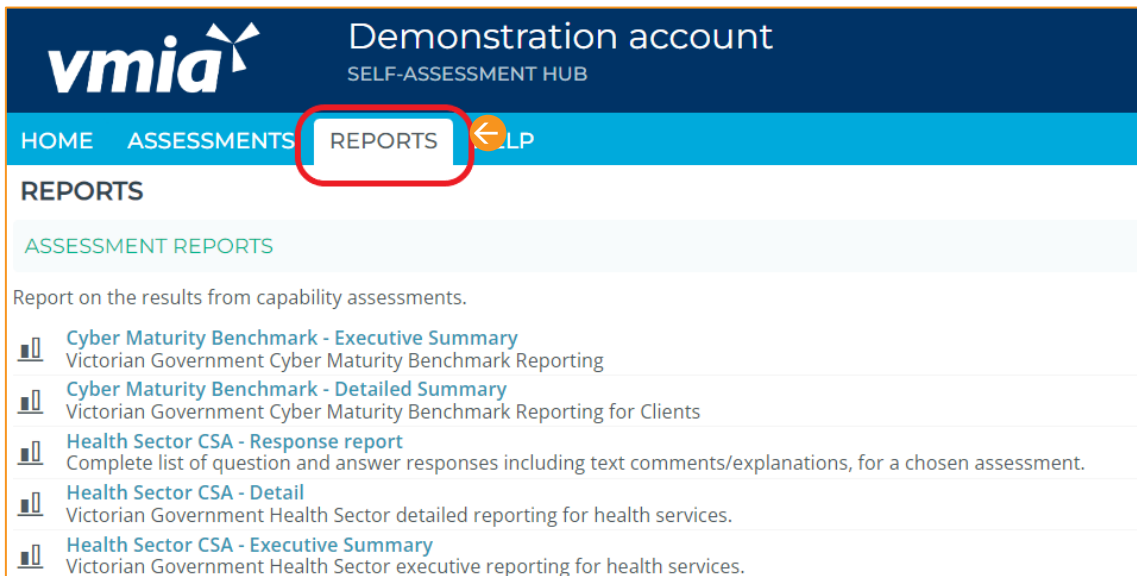
On any of your assessment overview pages, select “Report List” from the sub-menu to view reports specific to that assessment.

Report List



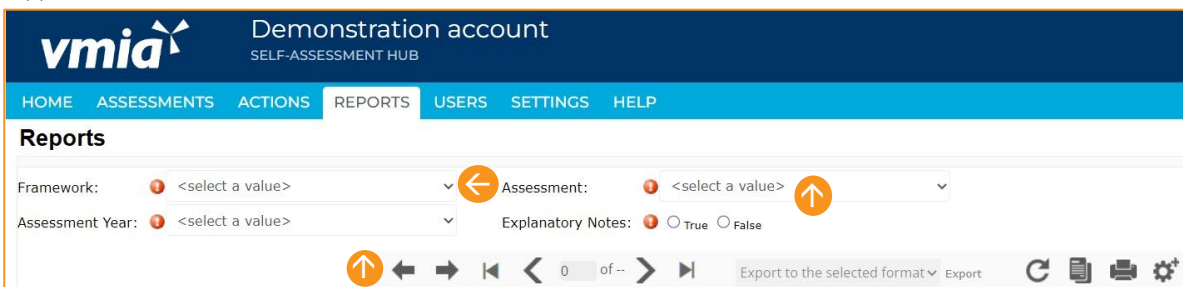
OR

You can view a list of all available reports for your organisation from the 'REPORTS' tab:



Select the report you wish to run

To generate the report, please select all options from the dropdown boxes available. You may also export to any formats supported.



Select from options available from dropdown boxes