FAQs

Cybera Security Nexus

Provincial Cybersecurity Self-Assessment Program

What is a Cybersecurity Self-Assessment?

A cybersecurity self-assessment is a self-directed mechanism to determine an organization’s overall security posture. Cybera’s provincial cybersecurity assessment program, offered through the Cybera Security Nexus, leverages the globally recognized NIST Cybersecurity Framework (CSF), which is broken into five functions and 23 categories.

The assessment contains a series of control questions, with specially crafted multiple choice answers, to aid an organization in understanding the maturity of its cybersecurity program.

Why is this assessment based on the NIST CSF?

The NIST CSF was selected as the main framework for the service because it has already been adopted by several federal, provincial and private sector organizations, and because of its clean delineation across five functional areas:

- Identify
- Protect
- Detect
- Respond
- Recover

We recognize there are multiple other frameworks in use throughout the education and public sectors. But by utilizing one central framework, a common discussion with a common set of vernacular can begin to be had between all Cybera members. We will also be able to aggregate data from the assessments to illuminate areas for potential funding opportunities, new member services, or ShareIT opportunities.

The platform utilized to undertake the self-assessment has the ability to crosswalk between different frameworks which may allow for your organization completing the NIST CSF as a self-assessment, but then later perform a CIS self-assessment, with any overlapping questions already answered. This helps to eliminate assessment fatigue.

More information on the NIST CSF can be found here: https://www.nist.gov/cyberframework.

What specific questions will the self-assessment help me to answer?

Completing the self-assessment will assist you in answering the following questions.

What are the institution’s current cybersecurity strengths?

There is no doubt that Alberta institutions are doing some great things in the cybersecurity landscape. If they were not, they would be in the news all the time. Performing a self-assessment using an internationally recognized framework — which covers all the areas that should be in a cybersecurity program — allows the institution to see where they are doing well. It’s not always about finding the vulnerabilities, some of this is about celebrating the things that are being done right.

What are the institution’s current cybersecurity weaknesses?

If this was a Family Feud question, the survey would say this is the number one question in a cybersecurity self-assessment. You don’t know what you don’t know until somebody asks you all the questions. Emphasis on ALL the questions. In today's fast-paced environments, cybersecurity is most often implemented through external drivers, not because of a pre-planned set of controls the organization decides to implement. This often results in only the obvious things being implemented. Take, for instance, Multi-Factor Authentication. This has been around in cybersecurity frameworks for more than a decade, yet until cyber insurance providers started asking if it was present (and denying insurance coverage for clients — or at the very least, increasing their premiums — if it had not been implemented), the adoption levels were low. Understanding the gaps allows institutions to plan proactively to fill them in, before they are asked to do so by an internal or external party.

What are the institution’s current cybersecurity risks?

Risks are not the same as weaknesses. A series of weaknesses around a specific control area increases the likelihood of an event, culminating in an elevated risk for the institution. Although every institution has a slightly different risk appetite, it is challenging to understand how much risk the organization is being exposed to unless the areas of weakness are understood. Understanding the risk exposure is critical to knowing where to expend limited resources (another question that is answered – see below) to lower the risk to the organization.

What is the current maturity of the institution’s cybersecurity program?

The multiple-choice answers to the control questions in the Cybera Cybersecurity Assessment platform include a graduated maturity model mechanism. This allows the institution to identify a numeric level of maturity for that specific area. When the answers are viewed in related groups, it is possible to produce an average maturity for that specific group. The greater the maturity in an area, the higher the institution’s resilience if that control area is tested in some way. Organizations need to decide how high a maturity level they require to meet their risk tolerance. It is not always cost effective to strive for the highest level of maturity when a lower level will meet the organization's risk appetite. Understanding the organization's maturity for the different areas in the cybersecurity framework provides another means by which to help prioritize where resources should be focused.

How does the institution measure up against an established cybersecurity framework?

Many cybersecurity programs are driven by the tactical implementation of cybersecurity technology because these things are visible and readily available. After this, the whirlwind of institutional activities take over, and cybersecurity items fade into the background (unless an incident occurs). As important as tactical implementation of cybersecurity technologies is, it does not cover the full spectrum that a cybersecurity program should encompass. An honest self-assessment against a recognized cybersecurity framework gives the institution a more complete picture of the status of its cybersecurity program. Knowing where you are is the start of knowing where you need to be.

Where should the institution focus its cybersecurity spend?

With limited resources and increasing security threats, the most important insight provided by an honest self-assessment against an established cybersecurity framework is the information required to build a roadmap for the institution’s cybersecurity program. This can be based on the risks identified, gaps presented, or maturity calculated. Whichever criteria is leveraged, dollars spent can be focused on authentic needs and provide direct support to those areas.

Where does the institution rank amongst its peers?

It’s human nature to want to compare yourself against others to see where you rank. Being at the top provides bragging rights and may even make its way into marketing materials to draw in more prospective participants. Being in the middle may allow for management to indicate they are doing “enough” and not too much. Being at the bottom may provide leverage to seek funding for larger improvements. Regardless of their motivation, the assessment participants will receive information that shows how they compare to their peer organizations.

How would a cybersecurity self-assessment make my organization more secure?

On its own, completing a cybersecurity self-assessment will not move the needle forward on your cybersecurity program. However, the results from an honestly-answered cybersecurity self-assessment will reveal where your strengths, weaknesses, and corresponding latent risks exist. This can provide insight into developing or expanding upon your organization's cybersecurity roadmap. It can also provide information to support your existing efforts, or data that can be used to seek funding to address any identified risks.

Will the self-assessment help determine where organizations should focus cybersecurity spend?

With limited resources and increasing security threats, likely the most important insight provided from an honest self-assessment against an established cybersecurity framework is the information required to build a roadmap for the institution’s cybersecurity program.

This can be based on the risks identified, gaps presented, or maturity calculated. Whichever criteria is leveraged, dollars can then be focused on authentic needs to provide direct support to those areas.

How many questions are in the self-assessment questionnaire?

There are 240 control questions encompassing all five of the NIST CSF functional areas (Identify, Protect, Detect, Respond, Recover).

How long will it take to complete the self-assessment questionnaire?

If the identified responder to the assessment for your organization has all of the answers to all 240 self-assessment questions, it certainly would be possible to complete the entire assessment in less than half a day.

The assessment platform also allows questions to be delegated to members of your organization. Delegation of certain questions to subject matter experts across your organization is recommended, but it may lengthen the assessment process. On the other hand, depending on your organization, it may be easier to divide and conquer the assessment questions and delegate certain categories.

What data will I need to provide to get started?

We will need some information to be able to set up your account in the assessment platform(First Name, Last Name, email).

The assessment itself is multiple choice, and you will need to answer all 240 questions to complete the assessment.

What information will my organization receive after completing the Cybersecurity assessment?

Organizations will receive three items:

1. **Customized assessment results and recommendations report**
   Target audience: Security teams, CIOs and …..

   - A summary of the assessment results, including the assessed maturity level compared to the expected maturity levels overall, separated into the five NIST CSF functions. Organizations will also be able to quickly see their top three assessed risks and recommendations to address them.

2. **Aggregated comparative report**
   Target audience: Security teams, CIOs and ….

   - A report showing the aggregated regional results identifying common areas of strength and the most significant risks. (per the Global Complexity Index).

3. **Raw maturity data**
   Target Audience: Security teams

   - Raw data of your organization's maturity results directly from the assessment platform.
   - Security teams can use their organization's data to do their own analysis, or a deeper dive into their security gaps should they wish to.
   - CIOs can use these results to help prioritize security investments for their team and raise awareness of these issues at the executive level, and with other stakeholders.

When will our assessment reports be available to us?

The regional comparison report will be distributed within three months of the assessment deadline. The individual customized assessment results and recommendations report may be delivered to a participant in advance of this deadline, as the Cybera analysis teams will be authoring each of these reports individually.

This is dependent on the timeliness of the completion of the self-assessment.

What is the deadline for completing the Assessment?

Assessment period ends: Deadline will be announced soon.