Office of the
Auditor General
of British Columbia

March 2026

Governance of Cybersecurity Risk Management at the BC Institute of Technology

An independent audit report

Office of the
Auditor General
of British Columbia

623 Fort Street
Victoria, British Columbia
V8W 1G1

250.419.6100

oag.bc.ca

The Honourable Raj Chouhan
Speaker of the Legislative Assembly
Province of British Columbia
Parliament Buildings
Victoria, British Columbia
V8V 1X4

Dear Mr. Speaker:

I have the honour to transmit to the Speaker of the Legislative Assembly of British Columbia the report, *Governance of Cybersecurity Risk Management at the BC Institute of Technology*.

We conducted this audit under the authority of Section 11(8) of the *Auditor General Act*. All work in this audit was performed to a reasonable level of assurance in accordance with the Canadian Standard on Assurance Engagements (CSAE) 3001 – Direct Engagements, set out by the Chartered Professional Accountants of Canada (CPA Canada) in the *CPA Canada Handbook – Assurance*.

Bridget Parrish, CPA, CA
Auditor General of British Columbia
Victoria, B.C.

March 2026

Contents

Audit at a glance 4

Background 6

Objective 9

Conclusion 9

Findings 10

About the audit 19

Appendix A: Audit criteria 20

Student Plaza, BCIT Burnaby Campus
Source: BCIT

The Office of the Auditor General acknowledges that we are living and working with gratitude and respect on the traditional territories of the First Nations peoples of British Columbia. We specifically acknowledge that our office is located on the traditional territories of the lək̓ʷəŋən people of the Songhees and Esquimalt Nations (Victoria).

Governance of Cybersecurity Risk Management at the BC Institute of Technology

Audit at a glance

Why we did this audit

- Cybersecurity incidents have increased in number and severity in recent years, and post-secondary institutions have been targets of cyberattacks. Cybersecurity breaches can lead to privacy violations, reputational damage, and financial loss.
- The BC Institute of Technology (BCIT), one of the province's largest post-secondary institutions, stores sensitive student records and research data. BCIT is responsible for managing cybersecurity risks to protect sensitive information.
- A governance framework, as the foundation of effective cybersecurity risk management, helps ensure cybersecurity practices align with an organization's goals.

Objective

To determine whether BCIT established a comprehensive governance framework to manage cybersecurity risks.

Audit period:

January 1, 2024 – September 30, 2025

Conclusion

We concluded that BCIT established a comprehensive governance framework to manage cybersecurity risks.

We made no recommendations.

What we found

BCIT established policies to manage cybersecurity risks and it was finalizing a suite of cybersecurity standards	▪ An enterprise risk management policy was in place to manage institutional risks, including cybersecurity risks. ▪ BCIT had policies to guide cybersecurity across the organization and was finalizing a suite of technical cybersecurity standards for staff. ▪ BCIT had a documented process for reviewing and updating its cybersecurity policies and procedures.
BCIT defined roles and responsibilities for cybersecurity risk management	▪ Roles and responsibilities were defined at all levels of the organization, from operational cybersecurity staff to the board of governors. ▪ Roles and responsibilities were defined in policies and internal guidance documents, terms of reference, and job descriptions.

March 2026

Audit at a glance *(continued)*

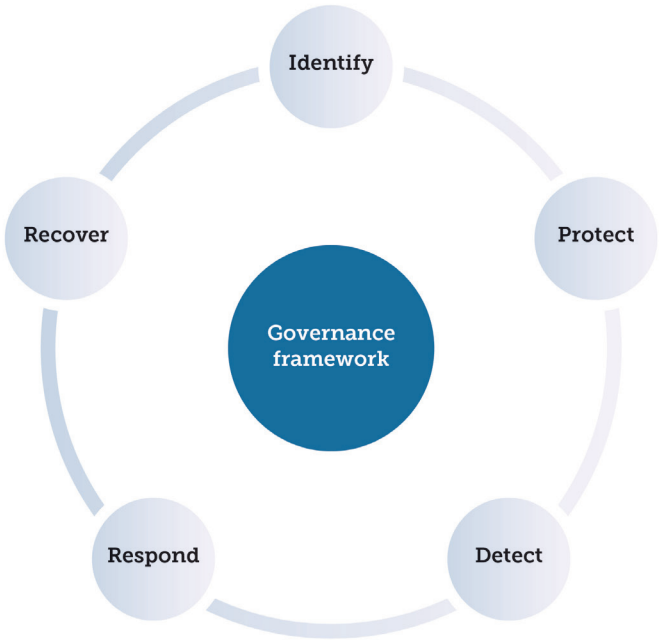
BCIT used its organizational context to inform cybersecurity risk management	▪ BCIT had various processes for consulting its different business areas about cybersecurity risks. ▪ It proactively assessed cybersecurity legal requirements by establishing policy and processes to meet privacy and security obligations. It also engaged external cybersecurity legal counsel as an advisor. ▪ BCIT used its strategic priorities to inform its cybersecurity risk management processes.
BCIT established key processes to support operational decisions about cybersecurity risks	▪ Objectives for cybersecurity risk management were set. ▪ BCIT documented its risk appetite. ▪ BCIT maintained an IT risk register to document, categorize, calculate and prioritize cybersecurity risks. ▪ There was a process to communicate cybersecurity risk information to senior leadership.
BCIT established and monitored cybersecurity metrics	▪ BCIT monitored the performance of its cybersecurity risk management activities by using a dashboard that reported on cybersecurity metrics. ▪ Dashboard reports supported the board's audit and finance committee with its oversight of cybersecurity.

Background

Cybersecurity threats like phishing and malware can lead to financial loss, reputational damage, and privacy violations. In response, organizations often rely on cybersecurity technologies, processes, and practices to protect their networks, devices, and data. The number and severity of cybersecurity incidents in Canada has increased in recent years, according to a 2025 report by the Canadian Centre for Cyber Security.

Organizations use cybersecurity risk management to identify, protect against, detect, respond to, and recover from potential threats to their data and IT systems. Governance frameworks form the foundation of cybersecurity risk management by setting out the related structures and processes.

Cybersecurity risk management



Source: Prepared by the Office of the Auditor General of B.C. based on the NIST Cybersecurity Framework 2.0

The National Institute of Standards and Technology (NIST) Cybersecurity Framework is a widely used best-practice source for industry, government, and other organizations to manage cybersecurity risks. The NIST Cybersecurity Framework identifies governance as a critical element of a cybersecurity risk management framework.

Cybersecurity attacks

Cyber attacks are malicious attempts to access, disrupt, damage, or steal information from computer systems, networks or devices.

Common examples of cyber attacks include:

- **Phishing** attacks target individuals with an email or other message that appears to be from a legitimate source. The email will try to trick the user to share sensitive information, gain access to their network, or download malware.
- **Malware** attacks occur when malicious software is covertly inserted into an organization's IT system to compromise the confidentiality, integrity, or availability of the data, applications, or operating system.
- **Ransomware** attackers encrypt an organization's data and demand payment to restore access. Attackers may also steal an organization's information and demand an additional payment in return for not disclosing the information.

Like many organizations, post-secondary institutions have been the targets of cyber attacks in recent years. These attacks often target students' personal data including social insurance numbers and banking information, or proprietary research. Cyber attacks can also disrupt programs and services.

Managing cybersecurity risks is important to maintain the security and reliability of services, and to protect personal information and data. This not only includes implementing technical controls, but also ensuring that leadership, faculty, staff, and students are aware of their cybersecurity responsibilities.

Source: Getty Images

Cybersecurity at BCIT

The BC Institute of Technology (BCIT) is one of the largest post-secondary institutions in the province, enrolling about 45,000 students each year. BCIT specializes in applied learning, with programs designed to offer workplace skills for B.C.'s economy.

BCIT rates cybersecurity as one of its top institutional risks and has adopted the NIST Cybersecurity Framework to guide its cybersecurity practice. BCIT has a dedicated Cybersecurity Office overseen by a chief information security officer (CISO) and staffed by a manager and four security analysts. The CISO is responsible for developing and leading BCIT's cybersecurity strategy and reports directly to the executive leadership. The CISO also has oversight of key IT operations.

BCIT established its Cybersecurity Office in 2019, and the CISO position was created in 2024. The CISO and Cybersecurity Office are independent from the IT Services department. This division supports the Cybersecurity Office's role in overseeing the security of IT systems and data.

While the risk of a cybersecurity attack can't be eliminated, a governance framework provides a foundation for BCIT to manage cybersecurity risks consistently and in line with its strategic priorities and goals.

BCIT Aerospace Technology Campus
Source: BCIT

Objective

The objective of the audit was to determine whether BCIT established a comprehensive governance framework to manage cybersecurity risks.

Scope

We audited BCIT to see if it had established a comprehensive governance framework to manage cybersecurity risks, specifically whether it:

- established policies to manage cybersecurity risks;
- defined roles and responsibilities for cybersecurity risk management;
- understood and used its organizational context to inform cybersecurity risk management;
- set direction and established processes to support operational decisions about cybersecurity risks; and
- monitored the performance of its cybersecurity risk management activities.

The audit focused on BCIT's governance structure for managing cybersecurity risks.

The audit period was from Jan. 1, 2024, to Sept. 30, 2025.

Learn more about the audit criteria on page 20.

Learn more about how we did this audit on page 19.

Conclusion

We concluded that BCIT established a comprehensive governance framework to manage cybersecurity risks, including: defined roles and responsibilities; relevant policies for managing cybersecurity risks; metrics to monitor performance; and processes to understand its organizational context and support operational decisions about cybersecurity risks.

Findings

Establishing policies

Policies, procedures, and standards establish guidance to ensure cybersecurity risks are managed consistently and are key elements of a cybersecurity governance framework. They help to communicate cybersecurity requirements, spell out roles and responsibilities, and set expectations for managing cybersecurity risks.

BCIT established policies to manage cybersecurity risks and was finalizing a suite of cybersecurity standards

What we looked for

We looked to see whether BCIT had established policies to manage cybersecurity risks, and whether BCIT had a process to periodically review and update those policies.

Learn more about the audit criteria on page 20.

What we found

We found that BCIT had policies for managing cybersecurity risks and was in the process of finalizing a suite of cybersecurity standards and procedures as of September 2025. Additionally, we found that BCIT had a documented process for reviewing and updating its policies and procedures but had not implemented an ongoing review of cybersecurity standards.

BCIT's ERM policy guides all risk functions including cybersecurity

BCIT's Enterprise Risk Management (ERM) policy sets out the principles and general requirements for managing institutional risks, including cybersecurity risks. ERM is a strategic, organization-wide approach to managing material risks. It involves identifying key risks, determining their likelihood and potential impacts, and implementing mitigation strategies. The policy establishes BCIT's governance model as well as roles and responsibilities for ERM across the organization.

BCIT's ERM team collaborates with the other risk and control functions, including the Cybersecurity Office, to align methodologies and collect risk information.

BCIT also developed a draft ERM standard in 2023 with detailed guidance on how to implement its broader ERM policy. The Cybersecurity Office relies on elements of the ERM standard for its cybersecurity risk assessments, such as the standard's risk rating scale. BCIT informed us that it intended to revisit the ERM standard in fall 2025 to consider whether revisions were needed prior to finalizing for approval.

BCIT established cybersecurity policies and was finalizing new cybersecurity standards

BCIT established two policies with guidance on cybersecurity: an information security policy and acceptable use of IT policy. The policies provide direction for information security across the organization and set roles and responsibilities for those involved in cybersecurity.

The cybersecurity policies were supported by more detailed, operational guidance for staff set out in technical cybersecurity standards and procedures. For example, the standards set requirements for securely transmitting electronic information. They also establish guidance for cybersecurity risk management, such as risk identification and risk response strategies.

During the audit period, BCIT was developing a new suite of technical cybersecurity standards. Eight technical standards had been finalized and were posted on BCIT's internal website. Twelve standards were in draft form as of September 2025, which BCIT indicated were going through the approval process.

BCIT had a process for reviewing cybersecurity policies, but hadn't implemented an ongoing review of standards

We found that BCIT had a documented process for reviewing and updating its cybersecurity policies and procedures, set out in its policy development and maintenance procedure document. The policy development and maintenance procedure requires that policies go through a standard review process every five years, at a minimum.

We also found that the Cybersecurity Office had developed a process for approving cybersecurity standards, but had not yet developed a process for routinely reviewing and updating them.

Why this matters

By establishing cybersecurity policies and standards, BCIT ensures that staff are aware of procedures, expectations, and roles and responsibilities for cybersecurity risk management. BCIT's process to routinely review and update its cybersecurity policies helps ensure the policies stay relevant and effective.

Recommendation

We made no recommendations in this area.

Defining roles and responsibilities

Defined roles and responsibilities are key parts of a governance framework because they ensure clear accountability, effective decision making, and coordinated action across an organization.

BCIT defined roles and responsibilities for cybersecurity risk management

What we looked for

We looked to see whether BCIT had defined roles and responsibilities for managing cybersecurity risks.

Learn more about the audit criteria on page 20.

What we found

We found that BCIT defined roles and responsibilities for managing cybersecurity risks at all levels of the organization – from operational cybersecurity staff to the board of governors – within policies and internal guidance documents, terms of reference, and job descriptions.

BCIT's cybersecurity incident response plan includes specific roles and responsibilities for responding to cybersecurity incidents. To practice its response to a cybersecurity incident using the plan, BCIT held two tabletop exercises in 2024 involving board and executive members. Based on the outcomes, BCIT identified areas to improve the clarity and understanding of staff roles and responsibilities and updated the plan accordingly.

Why this matters

Defined roles and responsibilities helped BCIT ensure that leadership and staff understand respective responsibilities for cybersecurity across the institution, supporting operational efficiency and accountability.

Recommendation

We made no recommendations in this area.

Understanding organizational context

Organizations should examine and understand their external and internal context when they design their framework for cybersecurity risk management. This understanding helps ensure that the framework aligns with the organization's mission, meets applicable legal and regulatory obligations, and meets the expectations of different business areas.

BCIT used its organizational context to inform cybersecurity risk management

What we looked for

We looked to see whether BCIT documented its organizational context and used it to inform its cybersecurity risk management. Specifically, we examined whether BCIT had:

- considered the expectations of different business areas on cybersecurity risk management;
- assessed its legal and regulatory requirements for cybersecurity; and
- documented and used its organizational mission to inform cybersecurity risk management.

Learn more about the audit criteria on page 20.

What we found

We found that BCIT acted to understand its organizational context and used the information to inform cybersecurity risk management.

BCIT consulted different business areas on cybersecurity risks

BCIT used a variety of processes and committees to consult faculty and staff from different business areas about cybersecurity risk management and to consider their expectations. For example, its risk advisory committee was responsible for discussing and analyzing emerging institutional risks, including those related to cybersecurity.

Also, as part of BCIT's security risk assessments for new technology, staff from the Cybersecurity Office met with people from different areas of BCIT to discuss their business needs and to understand the purpose of the new technology being adopted.

BCIT was proactive in assessing legal requirements for cybersecurity risk management

We found that BCIT proactively identified and assessed its legal and regulatory requirements for cybersecurity. BCIT had a policy and processes to meet its privacy and security obligations under the *Freedom of Information and Protection of Privacy Act*, which regulates the use and protection of personal information by public bodies in B.C. BCIT also retained external legal counsel, specializing in cybersecurity, to advise on cybersecurity issues and to assist with planning for responding to cybersecurity incidents.

BCIT used its strategic plan to inform cybersecurity risk management

We found that BCIT documented its organizational mission in its five-year strategic plan. The plan's priorities were used to develop BCIT's risk appetite statement, a tool to inform decisions about institutional risks, including cybersecurity risks.

Why this matters

By documenting and understanding its organizational context, including assessing its cybersecurity legal obligations and consulting different business areas, BCIT helped ensure cybersecurity risks were managed in alignment with its strategic priorities. These actions also enabled BCIT to tailor its cybersecurity framework to its specific needs.

Recommendation

We made no recommendations in this area.

Source: Getty Images

Processes to support operational decisions

Clear direction and an informed, structured approach to cybersecurity risk management can help ensure cybersecurity risks are identified, assessed, and managed in alignment with the organization's objectives. This involves setting high-level direction to guide decisions, developing consistent processes to analyze risks, and ensuring information is communicated to senior leaders who have oversight responsibilities. These elements are important components of a cybersecurity governance framework.

BCIT established key processes to support operational decisions about cybersecurity risks

What we looked for

We looked at whether BCIT set direction and established key processes to support operational decisions about cybersecurity risks by:

- setting objectives for cybersecurity risk management;
- documenting risk appetite;
- developing a standard method for calculating, documenting, categorizing, and prioritizing cybersecurity risks; and
- establishing a process to communicate cybersecurity risk information to senior leadership.

Learn more about the audit criteria on page 20.

What we found

We found that BCIT set direction and established key processes to support operational decisions about cybersecurity risks, including setting objectives; documenting its risk appetite; establishing a standard method for calculating, documenting, categorizing, and prioritizing cybersecurity risks; and establishing a process to communicate cybersecurity risk information to senior leadership.

BCIT set objectives for cybersecurity risk management

BCIT set objectives for cybersecurity risk management in its cybersecurity strategy, developed in 2019 when the Cybersecurity Office was established. BCIT also developed cybersecurity "roadmaps" to support the strategy, which were timelines with specific milestones and tasks to build BCIT's cybersecurity practice. The most recent roadmap was for 2025.

BCIT's 2025-2030 Strategic Plan included an initiative to continue developing a robust cybersecurity framework. It prioritized the privacy and protection of data and aimed to establish a community of cyber awareness.

BCIT documented its risk appetite

BCIT documented its risk appetite in a risk appetite statement, which stated the amount and type of risk it was willing to accept in pursuit of its objectives. The statement includes BCIT's overall risk appetite and detailed risk appetite statements for specific areas, including cybersecurity.

The board of governors approved BCIT's risk appetite statement, in accordance with its ERM policy, in December 2023. We found that BCIT had not conducted an annual review and update of its risk appetite statement as required by the ERM policy. BCIT informed us that after discussions with senior management and a consultant, they determined annual reviews would not be beneficial and decided to wait to conduct a formal review after two to three years.

BCIT maintained a risk register to calculate, categorize, and prioritize cybersecurity risks

BCIT maintained an IT risk register to document, calculate, categorize, and prioritize IT risks. BCIT's IT risk register is a spreadsheet used to log information about IT and cybersecurity risks. Cybersecurity Office staff explained that the IT risk register is updated on an ongoing basis when new risks are identified.

Staff in the Cybersecurity Office used the IT risk register to rate risks based on their likelihood and impact. A risk matrix included guidance on how to rate impact and likelihood on a scale. Staff also used the register to categorize risks by using pre-defined categories of IT risks, as well as broader organizational categories aligned with BCIT's ERM risk assessments.

BCIT prioritized cybersecurity risks based on their risk rating scores. It had also designed a method to create and monitor mitigation plans to ensure timely action on priority risks. This process was being implemented.

BCIT established a process to communicate cybersecurity risks to senior leadership

We found that BCIT established a process for its chief information security officer (CISO) to communicate cybersecurity risk information to the board of governors' audit and finance committee, responsible for overseeing cybersecurity risk management.

The CISO regularly provided cybersecurity updates at the board's audit and finance committee meetings, including:

- cybersecurity controls implemented to mitigate cybersecurity risks;
- cybersecurity training provided to executive;
- top cybersecurity risks at BCIT;
- general trends in cybersecurity threats; and
- the results of BCIT's cybersecurity metrics.

Why this matters

BCIT established direction to guide operational decisions about cybersecurity risks. This helped ensure that cybersecurity risk management aligned with BCIT's objectives, and that those responsible for overseeing cybersecurity received information they needed to fulfil their roles.

Recommendation

We made no recommendations in this area.

Source: Getty Images

Monitoring performance of cybersecurity framework

An organization can evaluate the performance of its cybersecurity framework and activities – and see whether it's achieving its objectives – by establishing and monitoring performance metrics. The results can also be used to adapt and improve cybersecurity practices.

BCIT established and monitored cybersecurity metrics

What we looked for

We looked at whether BCIT established and reviewed cybersecurity metrics.

Learn more about the audit criteria on page 20.

What we found

We found that BCIT established a process to monitor the performance of its cybersecurity risk management activities through cybersecurity metrics.

BCIT identified a series of cybersecurity metrics that provide insights about BCIT's cybersecurity posture, cybersecurity awareness program participation, exposure to cybersecurity threats, and responses to security vulnerabilities.

BCIT periodically compiled the metrics into a cybersecurity dashboard. BCIT started the cybersecurity dashboard in early 2024 to assist the audit and finance committee's oversight of cybersecurity. Most of the dashboard metrics were derived from BCIT's operational cybersecurity tools, which the Cybersecurity Office also monitors for day-to-day work.

Four of BCIT's seven cybersecurity metrics were pulled from cybersecurity tools that don't store historical data. BCIT hadn't established a system for logging historical performance against the cybersecurity metrics, other than what was captured periodically in each cybersecurity dashboard report.

Although full historic data wasn't available, staff manually added indicators to the cybersecurity dashboard reports to show how the metrics changed compared to the previous cybersecurity dashboard report, which enabled short-term comparisons.

Why this matters

BCIT's cybersecurity metrics support its ability to monitor the performance of its cybersecurity risk management framework. The metrics also support BCIT leadership with their oversight of cybersecurity.

Recommendation

We made no recommendations in this area.

About the audit

We conducted this audit under the authority of Section 11(8) of the *Auditor General Act* and in accordance with the Canadian Standard on Assurance Engagements (CSAE) 3001 – Direct Engagements, set out by the Chartered Professional Accountants of Canada (CPA Canada) in the *CPA Canada Handbook – Assurance*. These standards require that we comply with ethical requirements and conduct the audit to independently express a conclusion against the objective of the audit.

A direct audit involves understanding the subject matter to identify areas of significance and risk, and to identify relevant controls. This understanding is used as the basis for designing and performing audit procedures to obtain evidence on which to base the audit conclusion.

The audit procedures we conducted included document review, interviews with BCIT staff, and a review of controls to determine whether they were designed effectively.

We drew from the NIST Cybersecurity Framework and ISO 31000 Risk Management Guidelines to develop our audit objective and criteria.

We believe the audit evidence we have obtained is sufficient and appropriate to provide a basis for our conclusion.

Our office applies the Canadian Standard on Quality Management (CSQM 1), and we have complied with the independence and other ethical requirements of the code of professional conduct issued by the Chartered Professional Accountants of British Columbia that are relevant to this audit.

Audit report date: February 5, 2026

Bridget Parrish, CPA, CA
Auditor General of British Columbia
Victoria, B.C.

Appendix A: Audit criteria

Criterion 1: BCIT documented its organizational context to inform cybersecurity risk management.

Sub-Criteria:

1.1 BCIT documented its organizational mission and used it to inform cybersecurity risk management.

1.2 BCIT identified relevant stakeholders and considered their expectations regarding cybersecurity risk management.

1.3 BCIT assessed its legal and regulatory requirements regarding cybersecurity risk management.

Criterion 2: BCIT set direction to support operational decisions about cybersecurity risks.

Sub-Criteria:

2.1 BCIT set objectives for cybersecurity risk management.

2.2 BCIT documented its risk appetite.

2.3 BCIT established a standardized method for calculating, documenting, categorizing, and prioritizing cybersecurity risks.

2.4 BCIT established a process to communicate cybersecurity risk information to senior leadership.

2.5 BCIT integrated cybersecurity risk management in its enterprise risk management processes.

Criterion 3: BCIT defined roles and responsibilities for managing cybersecurity risks.

Criterion 4: BCIT established policy for managing cybersecurity risks.

Sub-Criteria:

4.1 BCIT established policy for managing cybersecurity risks which received approval from senior leadership.

4.2 BCIT established a process to periodically review and update its policy for managing cybersecurity risks.

Criterion 5: BCIT established a process to monitor the performance of its cybersecurity risk management activities.

Sub-Criteria:

5.1 BCIT established cybersecurity risk management performance indicators or metrics.

5.2 BCIT established a process to review the results of its cybersecurity risk management performance indicators or metrics.

This page left intentionally blank.

This page left intentionally blank.

This page left intentionally blank.

Office of the
Auditor General
of British Columbia

Report team

Laura Hatt
Assistant Auditor General

Amy Hart
Principal

Lisa Sevigny
Director

Emilie Benoit
Senior Auditor

Location
623 Fort Street
Victoria, British Columbia
Canada V8W 1G1

Office Hours
Monday to Friday
8:30 a.m. – 4:30 p.m.

Telephone: 250-419-6100
Toll-free through Enquiry BC: 1-800-663-7867
In Vancouver: 604-660-2421

Email: bcauditor@bcauditor.com

This report and others are available on our website, which also contains further information about the office.

Cover photo source: BCIT

oagbc
@oag_bc
@oag_bc
/company/oagbc
@oag_bc
oagbc

oag.bc.ca