Office of the Auditor General of British Columbia

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.

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.