Office of the Auditor General of British Columbia

# Audit at a glance

## Why we did this audit

- Information technology is critical to post-secondary programs and the storage of the personal records of faculty, staff, and students. Cybersecurity attacks can lead to unauthorized access to sensitive information and damage to an institution's reputation.
- The Vancouver Island University (VIU) Board of Governors, like other university boards, is responsible for overseeing cybersecurity risk management and holding management accountable for its delivery.
- We selected VIU because it is a similar size to many other universities in British Columbia.

## Objective

To determine whether VIU's Board of Governors provided oversight of the university's cybersecurity risk management practices.

## Audit period

April 1, 2022, to March 31, 2023

## Conclusion

We concluded that VIU's Board of Governors has not provided oversight of the university's cybersecurity risk management practices.

VIU has accepted our four recommendations on updating policies, board training and development, and cybersecurity risk mitigation and responses.

## What we found

**The board established oversight roles and responsibilities, but policies are out of date**

- VIU policies and terms of reference define cybersecurity risk management roles and responsibilities.
- The university hasn't updated its risk management policy and it's not in compliance with its own timeline for review.
- The board of governors approved the president's goals for managing cybersecurity risk and receives the president's assessment of management's progress.

**Recommendation 1**

**Board training on how to oversee cybersecurity risk management isn't adequate**

- An orientation program provided to all new board members includes general information about enterprise risk management, but not oversight responsibilities for cybersecurity risk management.
- The board of governors doesn't have an annual development (training) program which would provide updates on areas of significant risk, such as cybersecurity, or any changes to its role in providing oversight of cybersecurity risk management.

**Recommendations 2 and 3**

# Audit at a glance *(continued)*

**A risk management framework was developed, but the board did not review the mitigation strategies until the end of the last fiscal year**

- The university has developed an enterprise risk management framework, including processes to identify and rank cybersecurity risks and provide mitigation strategies.
- Using this framework, the university has identified cybersecurity risk as a top priority.
- For most of the 2022/23 fiscal year, the board of governors had not reviewed management's evaluation and response to cybersecurity risks, including its compliance with legal and regulatory requirements.

**Recommendation 4**

## After reading the report, you may wish to ask the following questions of government:

1. What are government's expectations regarding board oversight of cybersecurity risk management at post-secondary institutions?
2. What are post-secondary boards doing to ensure they effectively oversee cybersecurity risk management?
3. How are post-secondary boards evaluating whether cybersecurity risk is adequately managed?