Office of the
Auditor General
of British Columbia

July 2023

# Board Oversight of Cybersecurity Risk Management at Vancouver Island University

An independent audit report

Office of the
**Auditor General**
of British Columbia

623 Fort Street
Victoria, British Columbia
V8W 1G1

P: 250.419.6100
F: 250.387.1230

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, *Board Oversight of Cybersecurity Risk Management at Vancouver Island University.*

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*.

Michael A. Pickup, FCPA, FCA
Auditor General of British Columbia
Victoria, B.C.

July 2023

# Contents

Vancouver Island University, Cowichan Campus
Source: Vancouver Island University

The Office of the Auditor General of British Columbia acknowledges with respect that we conduct our work on Coast Salish territories, primarily on the traditional lands of the Lekwungen people (Esquimalt and Songhees Nations).

# 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?

# Background

Post-secondary institutions increasingly rely on information technology (IT) for their operations and to protect the sensitive information of faculty, staff and students. They depend on IT for educational programs, student registration, enrollment, assignments, and grading. Students expect technology-enabled learning and universities must be able to provide it securely and reliably.

Protecting IT from cyberattacks, ransomware and other threats is a critical business issue. Vancouver Island University (VIU) ranks cybersecurity among its highest risks.

Management at VIU is responsible for conducting risk assessments and implementing and operating processes to mitigate risk. It is expected to report the status of risk management programs to the board of governors, which oversees management activities.

VIU's board of governors is expected to oversee cybersecurity risk management by evaluating whether the institution:

- Has current cybersecurity policies and procedures.
- Regularly assesses and monitors cybersecurity risks.
- Receives regular reports on the institution's cybersecurity posture.

## What's ERM?

Enterprise risk management (including cybersecurity risk management) protects systems and data. ERM uses technology, processes, and practices to:

- Identify assets and threats.
- Determine the likelihood of threats materializing.
- Determine the potential impacts.
- Document current mitigation strategies.
- Identify and implement mitigation strategies to manage residual risk (risk that remains after measures are in place).
- Monitor risk and mitigation strategies.

The board of governors is a line of defence to protect the university and improve its response to cyber threats. For example, the board of governors can evaluate whether management has implemented strategies to mitigate risks to its technology infrastructure.

The Crown Agencies and Board Resourcing Office recruits candidates for government appointments to public boards, including university boards of governors. The office recommends candidates to cabinet for approval prior to their formal appointment by the lieutenant governor. Board members, other than the president, receive no remuneration for being on the board of governors.

The *University Act* defines the membership of a university's board of governors. VIU has a 15-person board of governors:

- Eight members appointed by government (including two nominees from the institution's alumni association).
- Two elected by faculty.
- Two elected by members of student societies.
- One elected by staff.
- University chancellor.
- University president.

### Board powers

"The management, administration and control of the property, revenue, business and affairs of the university are vested in the board." – Section 27 (1), *University Act*

Source: Getty Images

# Objective

The audit objective was to determine whether Vancouver Island University's Board of Governors provided oversight of the university's cybersecurity risk management practices.

## Scope

We looked to determine if the board of governors provided oversight of the university's cybersecurity risk management practices, including:

- Defining roles and responsibilities for cybersecurity risk management.
- Training on oversight of cybersecurity risk management.
- Evaluating if a risk management framework and processes are in place and functioning.
- Evaluating if management assessed the university's legal and regulatory requirements regarding cybersecurity.

We audited the board of governors' oversight practices from April 1, 2022, to March 31, 2023.

This was not an audit of management's processes. We did not audit:

- The effectiveness of operational cybersecurity controls.
- Management's process for conducting risk assessments.

Learn more about the audit criteria on page 19.

Learn more about how we did this audit on page 17.

Source: Getty Images

# Conclusion

Vancouver Island University's Board of Governors has defined roles and responsibilities for overseeing risk management. It sets expectations for management to improve their enterprise risk management, which includes cybersecurity.

However, we concluded they haven't provided oversight of the university's cybersecurity risk management practices because:

- The board doesn't have a development (training) program to increase their subject matter knowledge in areas of risk, including cybersecurity risk, to assist them in their oversight responsibilities.
- The current risk management policy hasn't been updated since it was last approved by the board of governors in 2012. During the audit period, the board of governors reviewed, but didn't approve, an updated risk management policy.
- For most of the last fiscal year, the board of governors had not reviewed cybersecurity risk mitigation strategies which include compliance with legal and regulatory requirements.

Vancouver Island University, Parksville Qualicum Centre
Source: Vancouver Island University

# Findings and recommendations

## Cybersecurity risk management roles and responsibilities

In cybersecurity risk management, the different roles and responsibilities of the board of governors and management need to be defined and documented. Clearly documented roles and responsibilities establish:

- Clarity and consistency of expectations to prevent misunderstandings, conflicts and other issues between management and the board of governors and among board members.
- Clear accountability for board members and university management to meet expectations.

## The board established oversight roles and responsibilities, but there is a gap

### What we looked for

We examined whether the board of governors:

- Documented roles and responsibilities for overseeing cybersecurity risk management through governance and risk management policies.
- Established and evaluated whether the president met the expectations for managing cybersecurity risk.

Learn more about the audit criteria on page 19.

### What we found

#### Policy

The board of governors has documented its responsibilities for overseeing cybersecurity risk management, but the risk management policy is out of date.

They have approved policies and terms of reference that define their responsibilities for overseeing cybersecurity risk management. However, the risk management policy is past its last review date and is not current.

The Risk Management Policy was last reviewed and approved in 2012 (a scheduled 2017 review didn't occur). The board reviewed an updated risk management policy in March 2023, but it wasn't approved because the board didn't have a quorum to vote. The board of governors plans to conduct the vote at a future meeting.

## Why this matters

Not reviewing and updating risk management policies in a timely manner can lead to outdated and ineffective policies, resulting in confusion in roles and responsibilities and weakened accountability.

## Recommendation

We recommend that the Vancouver Island University's Board of Governors:

1. Ensure that governance and policy documents defining roles and responsibilities for cybersecurity risk management are reviewed and approved as scheduled.

See the response from the auditee on page 18.

### Board of governors' expectations of the president

The board of governors set expectations and reviewed the progress of the president in meeting goals for managing cybersecurity risk. Quarterly, the president updated the board on progress toward her goals. The board of governors discussed the president's assessment at the quarterly board meetings. However, the feedback wasn't documented.

## Why this matters

Setting expectations and reviewing progress are important because the president is the person responsible for directing the university's management. Management is responsible for completing the cybersecurity risk assessment and it operates processes for defending the university against cybersecurity threats. Therefore, the board's ability to oversee the implementation of cybersecurity risk management requires the evaluation of the president's progress in meeting expectations.

# Training

An individual appointed or elected to the university board of governors brings diverse and valuable experience. They will generally have areas where additional training would improve their ability to provide oversight of the university, for example cybersecurity risk management.

An orientation program for new board members that covers the governor's responsibilities for providing oversight of cybersecurity risk management is essential for board members to understand their responsibilities. An annual development program that includes training updates on areas of significant risk is important for board members to stay up to date on the latest trends and provide effective oversight by making informed decisions.

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

### What we looked for

VIU's governance policy states that the university should have an annual development program and orientation for board members. We looked to see if there is an orientation program for new board members that covers the board's responsibilities for oversight of cybersecurity risk management. We also examined whether the board of governors has an annual development program that includes training and updates on cybersecurity risk management.

Learn more about the audit criteria on page 19.

### What we found

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 orientation program for new board members provides a general overview of the university and its structure. However, a section on roles and responsibilities doesn't cover cybersecurity risk management oversight. It mentions cybersecurity (as an item in enterprise risk management reporting) but doesn't provide guidance on how the board of governors should provide oversight.

The board of governors doesn't have an annual development program to update areas of significant risk, such as cybersecurity, or on any changes to the board's role in providing oversight of cybersecurity risk management.

The university's governance policy states the board must have an annual development program that includes updates on areas of significant risk, such as cybersecurity risk management.

Because the university lists cybersecurity as one of their most significant risks, we inquired if any of the board members have a background in information technology. The board members' self-assessments showed they lack backgrounds in this area.

## Why this matters

Board members need to have up-to-date knowledge of cybersecurity risk management to be effective in their oversight role.

Robust orientation and board development programs can help board members to be effective in their oversight and decision making.

## Recommendations

We recommend that the Vancouver Island University's Board of Governors:

2. Create an annual development program and ensure board members receive annual training on cybersecurity risk management to support them in their oversight role.
3. Update the board orientation program to include information on the roles and responsibilities for oversight of cybersecurity risk management.

See the response from the auditee on page 18.

Vancouver Island University, Nanaimo Campus
Source: Vancouver Island University

# Cybersecurity risk management framework

An organization should have a documented cybersecurity risk management framework to evaluate risk in a structured way and provide:

- Clarity and consistency in assessing risk by providing clear procedures and guidelines.
- A way to identify risks by systematically assessing threat likelihood and impact.
- An approach to implementing appropriate measures to reduce the likelihood and impact of identified risks.
- A basis for continual improvement and identifying opportunities to enhance risk management practices.

The board of governors can provide oversight of the risk management framework by ensuring the framework and mitigation strategies are documented and communicated.

## The board reviewed the cybersecurity risk management framework and confirmed it was communicated to the university community

### What we looked for

We looked to see if the VIU Board of Governors reviewed the university's cybersecurity risk management framework and if they confirmed management communicated the risk management framework and policies to staff, students, and other key groups.

Learn more about the audit criteria on page 19.

### What we found

The board reviewed the cybersecurity risk management framework (a component of the enterprise risk management framework) and confirmed that the framework and policies were communicated to staff, students and other key groups.

Prior to fiscal year 2022, the board identified enterprise risk management as an area that needed improvement at VIU and the university created a staff position dedicated to the task. The university has now documented its risk management framework, which includes identifying and ranking risks and implementing mitigation measures.

In June 2022, the board of governors reviewed the enterprise risk management framework.

The board of governors has delegated communication of the risk management framework and policies to VIU management. They confirmed the risk management framework and policies were communicated to key parties by the university's management. The description of the integrated risk management framework and the policy documents relating to risk management are on the university's internal website.

### Why this matters

A documented risk management framework provides clarity and consistency for an organization's approach to risk management. By exercising its oversight, the board of governors helps ensure the risk management framework is documented and communicated, and that the university has processes to reduce unnecessary risk.

# Risk management processes

The board of governors' review of the university's cybersecurity risk assessment is important in fulfilling its responsibility to evaluate the university's cybersecurity management. The documented risk assessment and mitigation strategies help the board evaluate if the university is making informed decisions about cybersecurity investments and strategic priorities.

## For most of the fiscal year, the board had not reviewed cybersecurity risk mitigation strategies

### What we looked for

We examined if the board of governors regularly reviews the university's cybersecurity risk assessment and, if so, whether it looks at how management evaluates and mitigates cybersecurity risk, prioritizes risk areas, and documents its responses. We also looked to see if the board of governors confirmed that management had assessed its compliance with legal and regulatory requirements.

Learn more about the audit criteria on page 19.

### What we found

The board had not fulfilled its oversight responsibilities for confirming management had implemented mitigation strategies, including compliance with key requirements, until the end of the 2022/23 fiscal year.

The university has improved its risk management processes by hiring full-time staff to develop its enterprise risk management framework. VIU developed processes to identify and rank risks, including cybersecurity risks, and to provide mitigation strategies.

The board of governors reviewed the university's cybersecurity risk assessment to confirm management is evaluating and mitigating cybersecurity risk by prioritizing risk areas and documenting responses.

In June 2022, the board reviewed the framework VIU had implemented for identifying and rating risks. At that time, management placed cybersecurity risk as the third-highest risk to university operations. However, the risk assessment didn't include strategies for mitigating risk.

In March 2023, the board received a documented risk assessment from management that included mitigation strategies. The board of governors did not complete its oversight of the risk assessment process until March 30, 2023, when it reviewed the completed risk assessment that included the strategies to mitigate identified risks.

On that same date, the board of governors also confirmed management assessed the university's legal and regulatory requirements for cybersecurity risk management.

## Why this matters

Without documented risk mitigation strategies to review, the board can't fulfil its oversight responsibilities. It's unable to evaluate if management is adequately prepared to manage cybersecurity risks or if they are making informed decisions on investments and priorities, such as possible legal and regulatory requirements. The board has a responsibility to request management to provide this information throughout the year to help ensure an ongoing evaluation of management's response to cybersecurity risk.

## Recommendation

We recommend that the Vancouver Island University's Board of Governors:

4. Review cybersecurity risk mitigation strategies throughout the year.

See the response from the auditee on page 18.

# 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, inquiries with management, and corroboration and confirmation of evidence and findings with the board, primarily the board chair.

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 requirements of the code of ethics issued by the Chartered Professional Accountants of British Columbia that are relevant to this audit.

**Audit report date: July 13, 2023**

Michael A. Pickup, FCPA, FCA
Auditor General of British Columbia
Victoria, B.C.

# Appendix A: Recommendations and auditee response

**Recommendation 1:** Ensure that governance and policy documents defining roles and responsibilities for cybersecurity risk management are reviewed and approved as scheduled.

**Recommendation 1 response:** VIU accepts this recommendation and notes that updates to its Enterprise Risk Management Policy were approved by VIU's Board of Governors and is now in force. That policy can be found at: https://gov.viu.ca/policies-and-procedures/policy-index

**Recommendation 2:** Create an annual development program and ensure board members receive annual training on cybersecurity risk management to support them in their oversight role.

**Recommendation 2 response:** VIU accepts this recommendation. At the request of the Board Chair, the President has directed the University Secretary to develop and implement an annual development and training program for all VIU governors that includes risk management – with a specific focus on oversight of cybersecurity risk. This work has already commenced and will be in place for the 2023-24 Board year (September 2023-July 2024).

**Recommendation 3:** Update the board orientation program to include information on the roles and responsibilities for oversight of cybersecurity risk management.

**Recommendation 3 response:** VIU accepts this recommendation and will be updating its orientation for governors to include information on the roles and responsibilities for oversight of cybersecurity risk management. VIU anticipates having these updates in place for September 2023.

**Recommendation 4:** Review cybersecurity risk mitigation strategies annually.

**Recommendation 4 response:** VIU accepts this recommendation and will be adding regular updates on how VIU is managing and mitigating the risk of cybersecurity to its work plan for the 2023 (and all subsequent) Board year.

# Appendix B: Audit criteria

## Lines of Enquiry and Criteria:

### LOE 1: Cybersecurity Risk Management Roles and Responsibilities.

Criteria:

**1.1.** The board has documented terms of reference that define its responsibilities for overseeing cybersecurity risk management.

**1.2.** The board sets expectations for the president for managing cybersecurity risk.

**1.3.** The board assesses if the president is meeting stated expectations for managing cybersecurity risk.

### LOE 2: Training.

Criteria:

**2.1.** There is an orientation program provided to all new board members, covering the governors' responsibilities for providing oversight of cybersecurity risk management.

**2.2.** The board has an annual development program that includes updates on cybersecurity risk management.

### LOE 3: Cybersecurity Risk Management Framework.

Criteria:

**3.1.** The board reviews and approves the university's cybersecurity risk management framework.

**3.2.** The board confirms the cybersecurity risk management framework, and resulting policies, are communicated to applicable parties (staff, students, and third parties).

## LOE 4: Governance and Risk Management Processes.

### Criteria:

**4.1.** The board reviews the university's cybersecurity risk assessment to confirm management is evaluating and mitigating cybersecurity risk by prioritizing risk areas and documenting responses.

## LOE 5: Legal and Regulatory Requirements.

### Criteria:

**5.1.** The board confirms management has assessed the university's legal and regulatory requirements regarding cybersecurity risk management.

Office of the
**Auditor General**
of British Columbia

**Audit team**

Laura Hatt
*Assistant Auditor General*

René Pelletier
*Executive Director*

Greg Morhart
*Director, IT Audit*

Tommy Chung
*Performance Auditor*

Cover: Vancouver Island University, Powell River Campus
Source: Vancouver Island University

**Location**
623 Fort St.
Victoria, B.C.
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.

**Reproducing**

oagbc

@oag_bc

@oag_bc

/company/oagbc

oagbc

oag.bc.ca