SUBJECT	Orientation to Enterprise Risk Management
SUBMITTED TO	Board of Governors
MEETING DATE	September 27, 2023
SESSION CLASSIFICATION	Recommended session criteria from Board Meetings Policy: OPEN
REQUEST	For information only – No action requested
LEAD EXECUTIVE	Allen Amyotte, Interim Chief Assurance and Risk Officer
SUPPORTED BY	Omer Ahmed, Director, Enterprise Risk Management

PRIOR SUBMISSIONS

The subject matter of this submission has not previously been considered by the Board of Governors.

EXECUTIVE SUMMARY

The general mandate of the Board of Governors includes the responsibility to "*ensure adequate risk management procedures and associated internal controls are established and effectively maintained*". Enterprise Risk Management (ERM) is a coordinated and continuous process that enables management to holistically view key risks that impact the university. It also enables management to focus on the university's strategic priorities while making risk-informed decisions that best support these strategic goals and opportunities.

The Office of Enterprise Risk and Assurance (ERA) is responsible for delivering a progressive ERM framework and capabilities to management to identify, assess, and manage risks and seize opportunities related to the achievement of strategic and operational objectives. This presentation will provide an orientation on ERM, information on the risk management roles and responsibilities of the Board, Audit Committee, Executive Team and ERA, along with details of UBC's Major Risk Register.

The orientation will benefit new and existing Board members alike.

PRESENTATIONS

1. Enterprise Risk Management (ERM) Orientation for the Board of Governors

ENTERPRISE RISK MANAGEMENT (ERM) ORIENTATION FOR THE BOARD OF GOVERNORS

September 2023

OFFICE OF ENTERPRISE RISK & ASSURANCE (ERA)

Purpose

Familiarize you with UBC's Office of Enterprise Risk & Assurance (ERA)

Understand Enterprise Risk Management (ERM)

Provide information on the risk management role and responsibilities of the Board

OFFICE OF ENTERPRISE RISK AND ASSURANCE (ERA) PORTFOLIO AND SERVICE OFFERINGS

https://enterpriseriskassurance.ubc.ca/

Enterprise Risk Management

Build and maintain a progressive ERM framework and supporting capabilities to identify, assess, and manage key risks and opportunities

Internal Assurance

Provide independent and objective assurance to management and the Board that key risks are understood and managed appropriately

Fraud Risk Management

Investigate allegations of improper financial activity and promote ethical financial conduct in accordance with University Policy SC15

Advisory

Partner with management to provide insights and foresights in a variety of areas including strategic initiatives, opportunities and key risks

3

ERA - ENTERPRISE RISK MANAGEMENT SERVICES

ERM Transformation Project

- Comprehensive review of existing ERM program to ensure it is progressive and best-in-class.

Strategic & Operational Risk Assessments

- Enable UBC to optimize outcomes related to the achievement of strategic objectives.
- Provide reasonable assurance to key stakeholders (Board, Audit Committee, Executive Team) that risks are being appropriately monitored and mitigated.

Training & Awareness

- Enable people with the skills and knowledge to manage risk effectively and promote risk culture.
- Improve UBC's ability to anticipate, respond, and make risk-informed decisions.

Risk Advisory

- Partner with management to provide risk insights and foresights on strategic initiative and operational activities, e.g. Hybrid Work Steering Committee, impact of the COVID-19 pandemic on UBC, impact of the Ukraine / Russia conflict on UBC and related risk considerations

Emerging Risks & Trends

- Assess emerging risks and trends for potential impact on achievement of strategic objectives.
- Accelerate ability to respond to change and potential opportunities.

WHAT IS ENTERPRISE RISK MANAGEMENT?

ERM IS:	ERM IS NOT A:
A continuous process led by senior leadership	Means to prevent all risks
Built into routine business processes	Program to avoid all risks
Designed to identify and manage current and emerging risks	Prescriptive method for managing individual risks
Tied to the organization's strategic goals and objectives	One-time process
A means to hold leadership accountable for managing risks	Tool, system or software
Applied across the organization	'One size fits all' framework

RISK ASSESSMENT FRAMEWORK[1]

Monitoring and Review

Step 1	Step 2	Step 3	Step 4	Step 5
Establish the Context	Risk Identification	Risk Analysis	Risk Evaluation	Risk Treatment

Communication and Consultation

Recording & Reporting

1 – Based on ISO 31000, Risk Management - Guidelines

Benefits of ERM for UBC

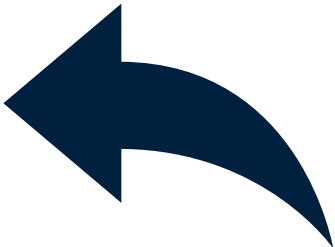Identification of risks preventing the achievement of UBC's strategic goals

Safeguards UBC to be resilient and achieve its objectives

Risk visibility and improved transparency on interconnectedness of risks

Aids risk-informed decision-making

Avoids taking unnecessary risks

7

RISK RESPONSIBILITIES

Board of Governors
- Established the Audit Committee to address risk and audit-related matters, with the authority to approve the annual ERA Plan and instruct the Chief Assurance and Risk Officer (CARO).

Audit Committee
- Considers matters relating to the ERM Program and processes and controls with respect to risks that may affect the reputation, financial position, resources or ability of UBC to carry out its objectives.

Executive Team
- Owners of the Major Risk Register (MRR), and accountable for mitigating the risks.
- Determines which risks should be incorporated or removed from the MRR.

Office of Enterprise Risk & Assurance (ERA)
- Facilitates the management of the MRR and provides analytical insights.
- The CARO is responsible for implementing, maintaining and integrating the ERM Program.
- Report to the Board of Governors at least annually on the ERM Program, strategic risks, and the management thereof, and to the Audit Committee on a quarterly basis.

ERA REPORTING CYCLES ON ERM

#	Subject	Audit Committee		Board	
		Frequency	**Meeting Month**	**Frequency**	**Meeting Month**
1	Major Risk Register – Annual Update	Annual	Nov[1]	Annual	Dec[2]
2	Major Risk Targeted Update	Quarterly	Mar, Jun, Sep[1]	n/a	n/a
3	ERM Transformation Program	Ad-hoc[3]	Ad-hoc[3]	n/a	n/a

[1] Source: UBC Board Secretariat Office. Standing agenda items for FY23/24.
[2] The Major Risk Register (MRR) was last presented to the board in April 2019.
[3] Ad-hoc reporting is based on key ERM Transformation project milestones.

What is the Major Risk Register (MRR)?

A repository of UBC's significant organization-wide risks to monitor and manage.

- A risk oversight tool for the Executive Team, Audit Committee & Board of Governors.

- Track potential key risks and opportunities that can impact UBC's strategic plan and objectives.

- Details risk ratings, a summary of the key controls in place and planned mitigation activities to be taken in response to the risk.

Key Contents of the Major Risk Register			
	Risk statement		Ownership
	Risk Rating (Probability of Occurrence & Severity of Impact)		Risk Response
	Key Controls		Control Rating
	Planned Mitigation Actions		

Format of Risk Reporting to the Board in December 2023

Potential information the Board could receive:

i. Details of risk movements since last update with rationale for changes

ii. Risk heat map

iii. Detailed Major Risk Register – includes full risk entry

iv. Dashboards for key risks – including risk trending information

QUESTIONS ?

APPENDIX

FREQUENTLY ASKED QUESTIONS

What is a risk?	Effect of uncertainty on objectives. *Source: ISO 31000 Risk Management - Guidelines*
What is the difference between a risk and an issue?	Risk is what could **potentially** happen in the **future**. An issue is an event that has **already occurred**.
Who owns the risks?	Each risk is owned by members of the Executive Management Team ("Executive Leads").
Why do we do ERM?	ERM enhances institutional reputation and credibility. It ensures key risks are communicated to management and the Board to make risk-informed decisions.
What is in it for me?	Provides assurance to Board members that management has created processes and is responding to risks effectively and efficiently.
What types of risk does UBC manage?	Information technology, safety & emergency management, financial, people & work-place, government / compliance, research, enrolment, teaching & learning, infrastructure and key relationships.

14

ERA RISK & OPPORTUNITY UNIVERSE

UBC Core Areas: *People and Places, Research Excellence, Transformative Learning, Local and Global Engagement*

UBC Strategic Focus Areas

Student Experience & Learning
- Student Mental Health & Wellness
- Student Experience
- Student Integrity
- Student Recruitment & Retention
- Student Services
- International Students
- Alumni Engagement
- Campus Living
- Program Quality Assurance
- International Programs

Research Excellence
- Research Funding
- Project Management
- Student Experiential Learning
- Research Data
- Intellectual Property
- Scholarly Integrity
- Research Partnerships

Local & Global
- External & Government Relations
- Industry Partnerships
- Community Relationships
- Indigenous Engagements
- Strategic Partnerships
- Marketing & Communications
- Licencing Partnerships

External Conditions

Global Landscape
- Geo-Political
- Competition
- Community Population & Demographics
- Pandemic
- Activism Activities

Regulatory & Compliance
- Regulatory
- Contract Management
- Legal Risk
- Privacy

Key Enablers

Faculty & Staff
- Attraction & Retention
- Training & Development
- Knowledge Management
- Succession Planning
- Performance Management
- Mental Health & Wellness
- Employee Engagement
- Faculty & Labour Relations

Financial
- Financial Management
- Liquidity & Debt Management
- Recording, Reporting, Monitoring
- Investment
- Fraud Risk Management
- Capital Management & Reserves Management
- Enrolment
- Procurement & Commitments
- Advancement & Donations

Facilities & Infrastructure
- Safety & Security
- Continuity Planning
- Operational Resiliency
- Project Management
- Capital Asset Strategy, Planning & Management
- Capital Projects

Technology
- IT Strategy
- IT Security
- IT Infrastructure
- Information Access
- Disaster Recovery Planning

## Internal Conditions

Governance
- Strategic Planning
- Organizational Performance
- Organizational Structure
- Policies & Procedures
- Records Management
- Reputation
- Transparency
- Leadership
- Accountability

Culture
- Environmental Social Governance
- Equity, Diversity & Inclusion
- Brand
- Change Management
- Empowerment
- Ethics & Values
- Collaboration & Coordination
- Innovation

15
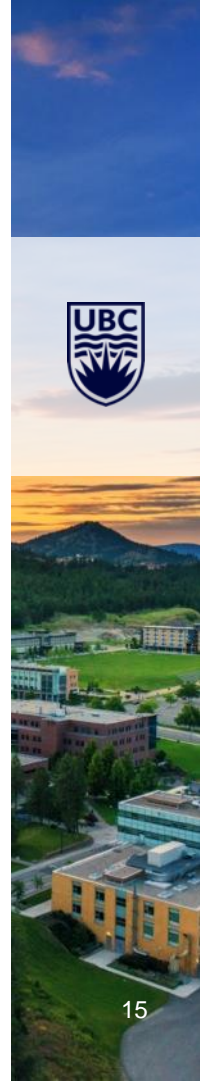
ERM Strategic & Operational Risk Assessment Process

Context

1. Preliminary planning meeting
   - Establish context (strategic, campus, portfolio, faculty/unit).
   - Facilitate identification of appropriate participants for workshops
2. ★ Connect with Internal Assurance to identify similar engagements that have taken place or will take place
3. Issue engagement letter
   - Details background, scope, timeline, responsibilities, deliverables

Risk Identification

1. Internal & External Risk Analysis
2. Distribute risk identification pre-workshop materials to participants:
   - Engagement timeline
   - Roles and responsibilities
   - Risk areas to consider
3. Facilitate risk identification workshop
4. Create draft risk register
5. Validate risk register and identify risk owners with sponsor
6. ★ Conduct internal ERA quality assurance review

Risk Assessment & Treatment

1. Share draft risk register and guidance on identification of key controls
2. Update risk register with key controls and planned mitigation activities
3. Distribute updated risk register and Risk Assessment pre-workshop materials to participants
4. Facilitate risk assessment workshop:
   - Rating and prioritization of identified risks
5. Update risk register with workshop results and feedback
6. ★ Conduct internal ERA quality

Reporting

1. Share results of workshop with sponsor; validate and obtain sign-off
2. Conduct completion meeting with sponsor
   - Share finalized deliverables and hand-off risk register
   - Obtain feedback on process
   - Send out ERA engagement survey
3. ★ Update ERA team on engagement and share lessons learned
4. ★ Management and Internal Assurance to determine if testing is required on key controls

RACI Chart

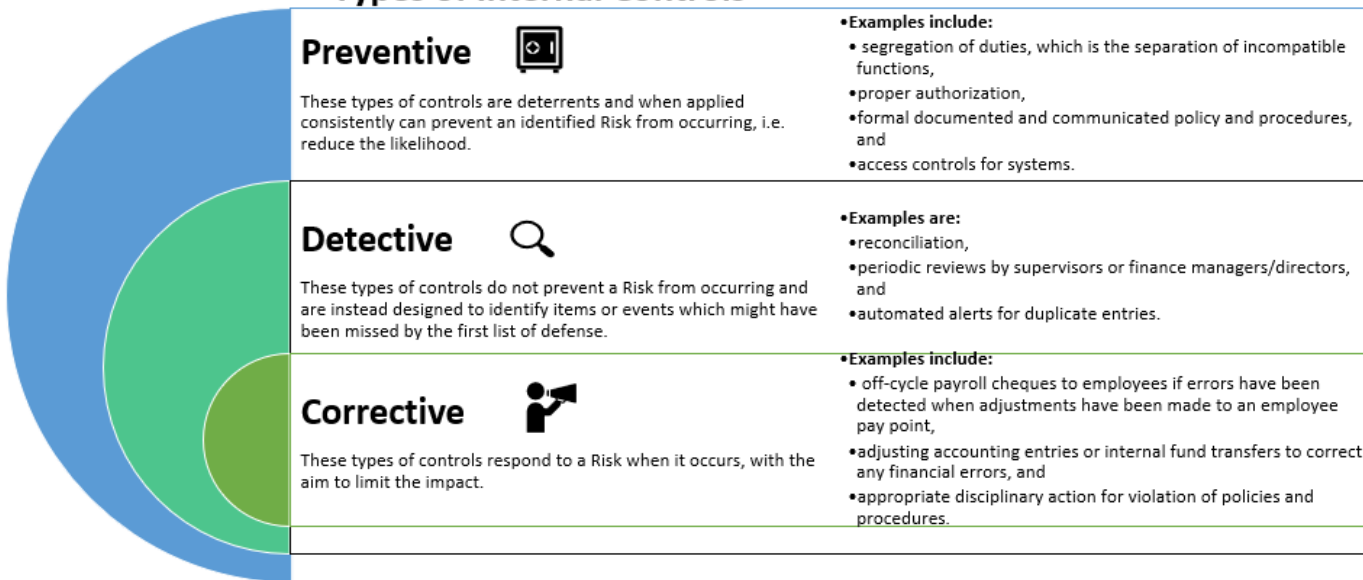|	Risk Identification	Risk Assessment & Treatment	Reporting
Engagement Sponsor	Accountable & Responsible	Accountable & Responsible	Accountable & Responsible
ERA (Facilitator)	Responsible	Responsible	Responsible
Other Stakeholders	Consulted	Consulted	Informed if applicable
Audit Committee	Informed if applicable	Informed if applicable	Informed if applicable

★ **Integration with Internal Assurance**

Definition & Purpose of Internal Controls

- Under the Committee of Sponsoring Organizations of the Treadway Commission (COSO) Internal Control-Integrated Framework, an internal control is broadly defined as a *"process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives"* of an entity.

- An internal control may exist as an activity within a business process, or within a program or service area.

- An effective system of **internal controls** reduces the Risk to an acceptable level. If the existing internal controls are not adequate or effective to reduce the Risk to an acceptable level, further **mitigation activities** are required to reduce either or both the likelihood and/or impact of the Risk.

Types of Internal Controls

Preventive

These types of controls are deterrents and when applied consistently can prevent an identified Risk from occurring, i.e. reduce the likelihood.

- Examples include:
  - segregation of duties, which is the separation of incompatible functions,
  - proper authorization,
  - formal documented and communicated policy and procedures, and
  - access controls for systems.

Detective

These types of controls do not prevent a Risk from occurring and are instead designed to identify items or events which might have been missed by the first list of defense.

- Examples are:
  - reconciliation,
  - periodic reviews by supervisors or finance managers/directors, and
  - automated alerts for duplicate entries.

Corrective

These types of controls respond to a Risk when it occurs, with the aim to limit the impact.

- Examples include:
  - off-cycle payroll cheques to employees if errors have been detected when adjustments have been made to an employee pay point,
  - adjusting accounting entries or internal fund transfers to correct any financial errors, and
  - appropriate disciplinary action for violation of policies and procedures.

THE UNIVERSITY OF BRITISH COLUMBIA