Strategic Enterprise Risk Management and Organizational Resilience Report

University of Oregon Board of Trustees

December 2021

Developed by:

UNIVERSITY OF OREGON | Safety and Risk Services

Table of Contents

Enterprise Risk Management and Organizational Resilience

What is Enterprise Risk Management?

Traditional risk management techniques include identifying and mitigating insurable risks or hazards, also known as risk transfer. Traditional risk management techniques are quickly becoming insufficient given the current trends in the insurance sector. Enterprise risk management (ERM) utilizes risk management techniques but takes the process further by holistically identifying, assessing and mitigating risks and exposures across the entire institution.

Source: Enterprise Risk Management Integrating with Strategy and Performance, Committee of Sponsoring Organizations of the Treadway Commission (COSO) June 2017

"ERM is a combination of strategic planning, traditional risk management and internal controls. A consensus definition, (…) is the following: [ERM] is a business process, led by senior leadership, that extends the concepts of risk management and includes:

- *Identifying risks across the entire enterprise;*
- *Assessing the impact of risks to the operations and mission;*
- *Developing and practicing response or mitigation plans; and*
- *Monitoring the identified risks, holding the risk owner accountable, and consistently scanning for emerging risks."*[1]

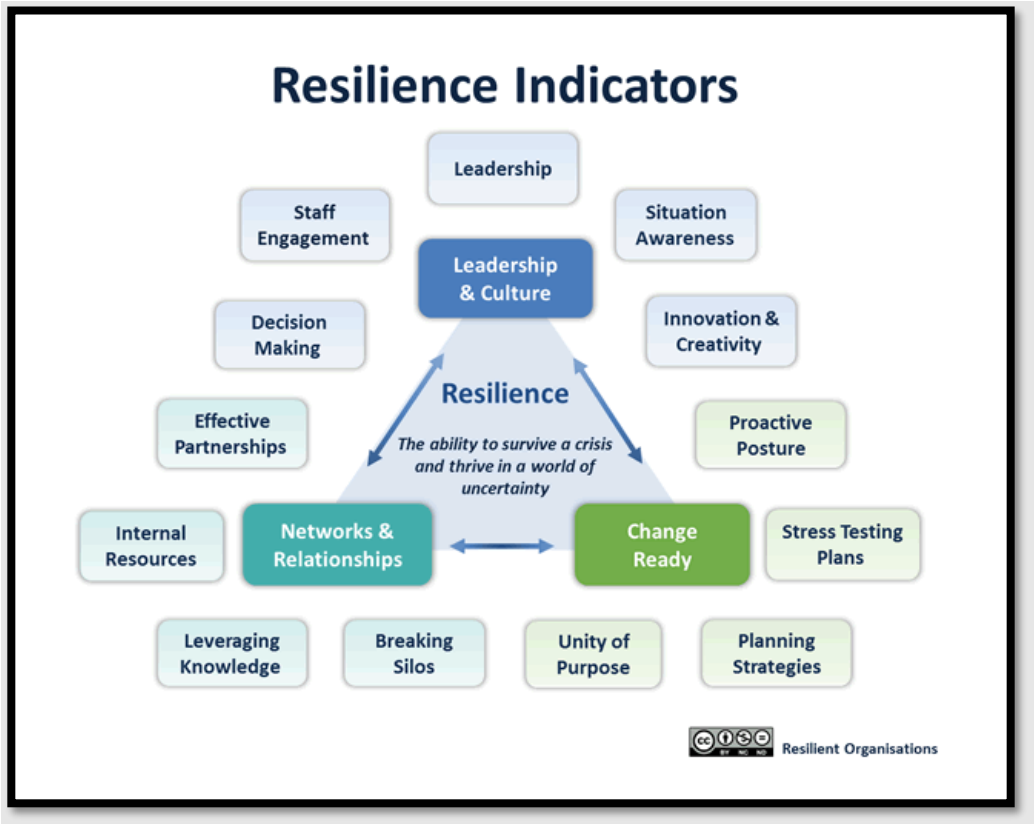
What is Organizational Resilience?

A resilient organization develops skills and resources to manage crises and adapt its systems and decision-making in the face of uncertainty. Organizational resilience is a capability that must be grown within the organization. Where the organization learns from every disruption and actively works to improve and evolve in a changing environment.

The University of Oregon partnered with Resilient Organizations in New Zealand to apply aspects of the model developed in New Zealand to advance operational and

[1] Janice M. Abraham, "Risk Management: An Accountability Guide for University and College Boards". AGB Press, the Association of Governing Boards of Universities and Colleges, and United Educators Insurance, 2013, page 6

strategic resilience on campus. The Resilient Organizations model is based on research looking at organizations of varied sizes, sectors, and ownership structures. They have discovered that "organizational resilience consists of three interdependent attributes and 13 indicators of resilience" [2]. The graphic below outlines the three attributes, leadership & Culture, Change Ready, and Networks & Partnerships in addition to the corresponding indicators.



Source: Resilient Organizations, https://www.resorgs.org.nz/ November 2021

Blending Enterprise Risk Management and Organizational Resilience

In today's decentralized, yet interconnected and rapidly evolving higher education environment, it is critical to embed the core concepts of enterprise risk management and operational and strategic resilience into our strategy-setting process at all levels within the university. Applying these tools cultivates a resilient world-class university that is future-ready, risk-aware, and not risk-averse.

Blending enterprise risk management and organizational resilience identifies and allows leadership to manage and monitor multiple cross-enterprise vulnerabilities, risk exposures, and capacities. These tools also increase situational awareness and reduce operational surprises and losses. This allows for improved decision-making, adaptive capacities and risk response. This process aligns strategy with operational capacity and

[2] Resilient Organizations, https://www.resorgs.org.nz/ November, 2021

risk appetite and improves deployment of limited resources – including human, financial, and asset/supply chain resources.

Strategic Enterprise Risk Management and Compliance Committee

Committee Charge and Membership

The Strategic Enterprise Risk Management and Compliance Committee (SERMC) is an advisory committee charged by, and providing recommendations to, the President of the University to oversee the University's Enterprise Risk Management and Organizational Resilience activities. The committee is chaired by Chief Resilience Officer and Associate Vice President for Safety and Risk Services and meets monthly.

The committee charge is to:

1. Develop tools and processes to actively identify, evaluate, and manage university risks
2. Ensure that systems and processes are in place to provide accountability for compliance with the University's legal and policy obligations
3. Encourage communication, problem-solving, and collaboration across divisions, units, and departments

Committee membership includes:

- Senior Vice President and Provost
- Vice President for Finance and Administration and Chief Financial Officer
- Vice President for Research and Innovation
- Vice President and General Counsel to the University
- Vice President for Equity and Inclusion
- Vice President for Student Life
- Vice President for Student Services and Enrollment Management
- Vice President for University Communications
- Vice President for University Advancement
- Vice Provost for Information Services and Chief Information Officer
- Associate Vice President for Safety and Risk Services and Chief Resilience Officer
- Associate Vice President for Human Resources and Chief Human Resources Officer
- Chief Internal Auditor
- Associate Vice President for Business Affairs and University Controller
- Director of Intercollegiate Athletics
- Assistant Vice President and Chief of Staff, Enrollment Management
- Associate Vice President, Director of Financial Aid, Enrollment Management

UO ERM Risk Owner – Roles and Responsibilities

A core element of the committee's charge is developing tools and processes to actively identify, evaluate, and manage university risks. The committee is accomplishing this through the Risk Exposure Matrix (REM), which serves as a register for tracking strategic, operational, and compliance risks and cataloging the mitigation and controls to manage the risk exposures as we advance the university's strategic plans. The REM is not intended to catalog all risk exposures but to focus on the exposures that could significantly impact the university's core mission or strategic objectives.

Committee members serve as risk area leads or "risk owners" over the potential risk exposure areas, conditions or events that exist in their portfolios. A risk owner (or their designee) is an accountable point of contact for an enterprise risk exposure at the senior leadership level, who coordinates efforts to mitigate and manage the risk with internal stakeholders who are responsible for parts of the risk.

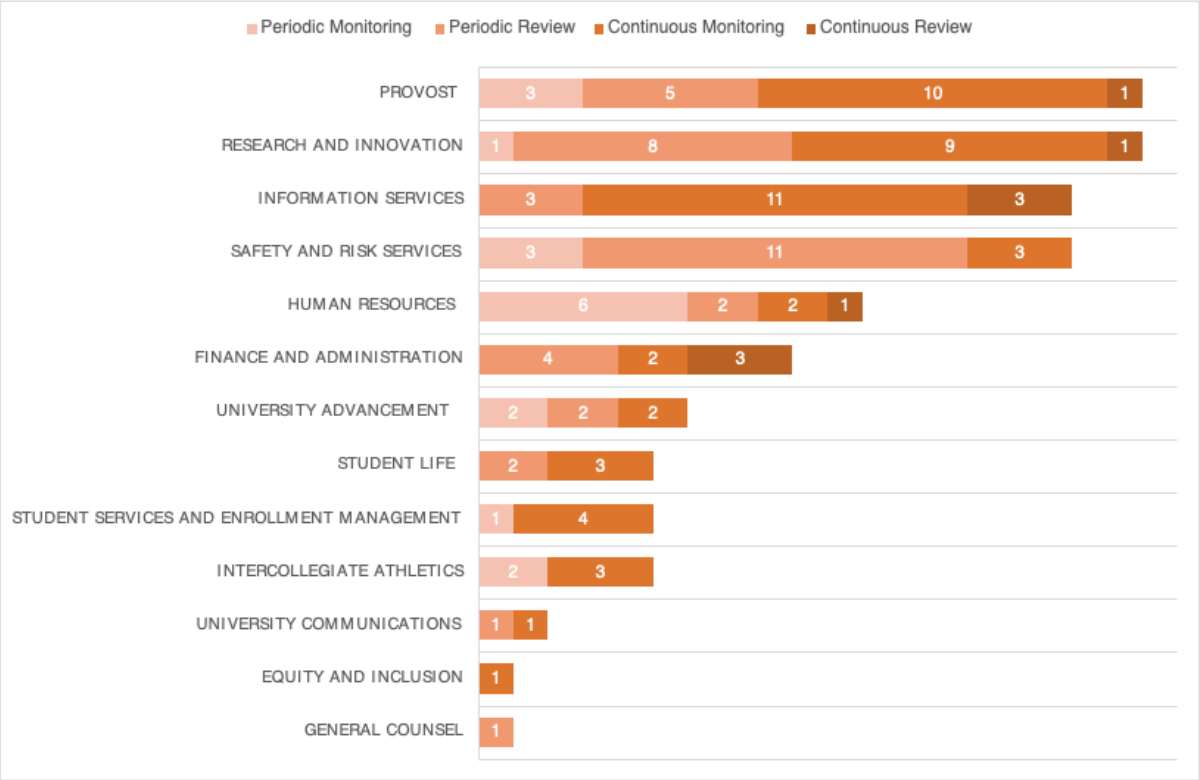
The responsibilities of the risk owner are to ensure that:

- Risks are identified, assessed, managed and monitored
- Risks are clearly articulated in risk statements
- Appropriate level of risk tolerance is determined
- Various internal stakeholders are assigned responsibility for each of the sub-risks identified within the university's risk exposure matrix.
- Risk management is integrated into operational activities
- Gaps in mitigation and monitoring activities are remediated
- The status of the mitigation and monitoring efforts are communicated to committee members
- The internal and external environments are scanned for emerging risks and opportunities

Risk Exposure Matrix (REM)

The REM is a dynamic document that is updated regularly. The following graph outlines the risks identified in the REM by the risk owner and the category of action assigned to the risk (e.g., continuous review, continuous monitoring, periodic review, or periodic monitoring). The REM is used as a tool to assist leadership in navigating risk exposures as they develop strategic and operational initiatives to advance the institution's mission.

Number of Risk Exposures by Area and Monitoring Type



Example of Risk Exposure Matrix Summary Card

The risk exposure cards summarize a potential exposure, condition, or event in the REM that could impact the University's mission or strategic objectives. In addition, the summary cards identify who is responsible for monitoring the potential exposure, who the internal management stakeholders are, any policies in place, and mitigation actions intended to reduce the University's exposure to the condition or event.

The risk owners are asked to review risk exposure cards at least annually and make appropriate updates. The goal is to keep the REM current to assist the University in navigating risk exposures. Members of the committee can also introduce new risk exposures by filling out a risk exposure card and presenting it to the committee for review, assessment and potential recommendations to the President.

The following page provides an example of one of the risk exposure cards.

UO REM

Row 25

Risk Exposure or Sub-Risks Exposure	**Export Controls**
Potential Exposures	Noncompliance with export control regulations can be costly for the university.
Description	United States export control laws regulate the release of goods and technologies that affect U.S. national security or foreign policy interests. As colleges and universities enroll international students, send professors abroad to research or study, hire international faculty, and develop advanced technologies on campus, compliance with U.S. export control laws is as crucial as ever. Importantly, export control laws do not just affect the physical shipment of an article or technology abroad - under the "deemed export" rule, an institution can export technology to a foreign country simply by disclosing information to a national of that country who may be working or visiting on campus. However, exceptions to these laws exist for fundamental research.
Risk Impact	**High**
Risk Likelihood	**High**
Risk Exposure Rating	Continuous Monitoring
UO Risk Owner	VP for Research and Innovation
Risk Owner Email	Cass Moseley
Risk Owner Delegate Email	Jim Slattery
Accountable Department / Position	Vice Provost International Affairs, Director, International Student & Scholar Services, Associate Vice Provost for International Affairs, Director, Printing and Mailing Services, Associate Vice President Business Affairs / Controller, Director of Purchasing and Contracting Services, Associate Vice President for Innovation
Internal Stakeholders	Enterprise Risk Management, General Counsel Information Services Business Affairs, Travel
Mitigation Summary	2021 - Implementation of RAP COI has been pushed to Spring 2022 due to changes in the vendor's software. 2020 - Coordinated disclosure process between RCS, SPS, Export Control, and OGC. RCR training being updated. The RAP COI module will be implemented in spring and summer 2021 to provide an electronic tool for managing COI-COC and FCOI disclosures and management plans. 2019 - unit within SPS working on this. obtained software tool to assist in Export Control functions. Began screening all foreign national courtesy appointments to determine if they were on denied entity/person list and notified effected units of what we would be required to offer such an appointment to provide such a person an appointment at UO. Thus far, all units have declined to pursue appointments in these instances. 2017 - Presented risks to SERMC resulting in SERMC sponsored work group on Export Control. Developed recommendations for moving forward; investing in temp staff to implement recommendations and stand up new system in 2018. SPS Contracts in the process of purchasing and implementing a software system for export control compliance and hope to have it implemented and operational by 11/1/2019.

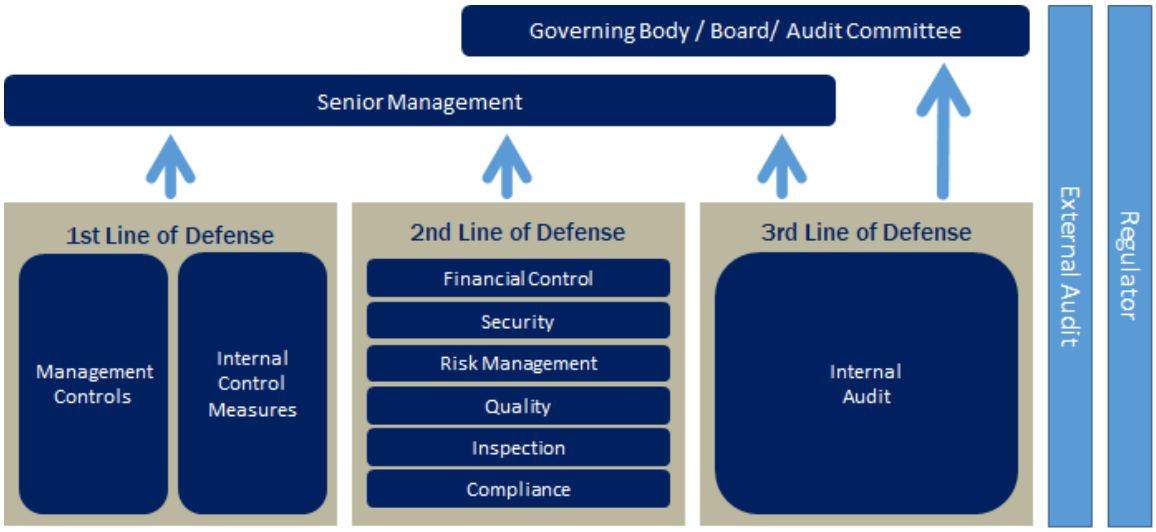
Risk Review Process

Risks included in the University's REM have three different types of review processes. All risks, regardless of risk rating go through the first type of review, which is annual review by senior leadership, or management review.

The second type of review risks are subject to is a Strategic Enterprise Risk and Resilience Committee Team review. The risks that typically fall under this type of review include periodic review and periodic monitoring. However, the risks that are rated as continuous review and continuous monitoring may also be included in a committee team review. The team review is conducted by a cross-departmental group of stakeholders and is typically conducted approximately every two or three years.

The third type of review risks are subject to is a comprehensive risk mitigation programmatic review, which is conducted by Internal Audit. Internal Audit is independent from implemented risk mitigation programs and serves in an objective consultative role.

This risk review process can further be described as an internal control system. The Federation of European Risk Management Association (FERMA) and the European Commission of Institutes of Internal Auditing (ECIIA) established a Three Lines of Defense Model that illustrates this internal control system.



Adapted from ECIIA/FERMA Guidance on 8th EU Company Law Directive, article 41

The first line of defense is "[o]perational management has ownership, responsibility and accountability for assessing, controlling and mitigating risks together with maintaining effective internal controls".

The second line of defense is "[t]he risk management function that facilitates and monitors the implementation of effective risk management practices by operational management and assists the risk owners in defining the target risk exposure and reporting adequate risk related information through the organization".

The third line of defense is "[t]he internal audit function (…), [which] through a risk based approach, provide assurance to the organization's board and senior management, on how effectively the organization assesses and manages its risk, including the manner in which the first and second lines of defense operate".[3]

SERMC Committee

Reporting Structure

To encourage communication, problem-solving, and collaboration across divisions, units, and departments, the committee risk owners and subject matter experts within their portfolios review and provide feedback on their risk exposure areas and document and update existing controls and mitigation strategies annually. In addition, risk owners present their risk areas to the committee annually to increase situational awareness among leadership and management.

The committee established a work group structure to address emerging risks. Additional information about the work groups will be discussed later in this report.

Standing committees and teams provide annual updates to the committee. Below is the tentative reporting calendar for 2022. Some standing committees or teams that report annually to the committee are regulatory and required by law. Other committees or teams are formed because of ongoing potential risk exposures in that given area. These committees and teams are charged with addressing risk and safety issues for the University.

[3] FERMA/ECIIA, "Monitoring the effectiveness of internal control, internal audit and risk management systems: Guidance for Boards and Audit Committees." Guidance on the 8th European Company Law Directive on Statutory Audit, September 21, 2010, pages 9-10

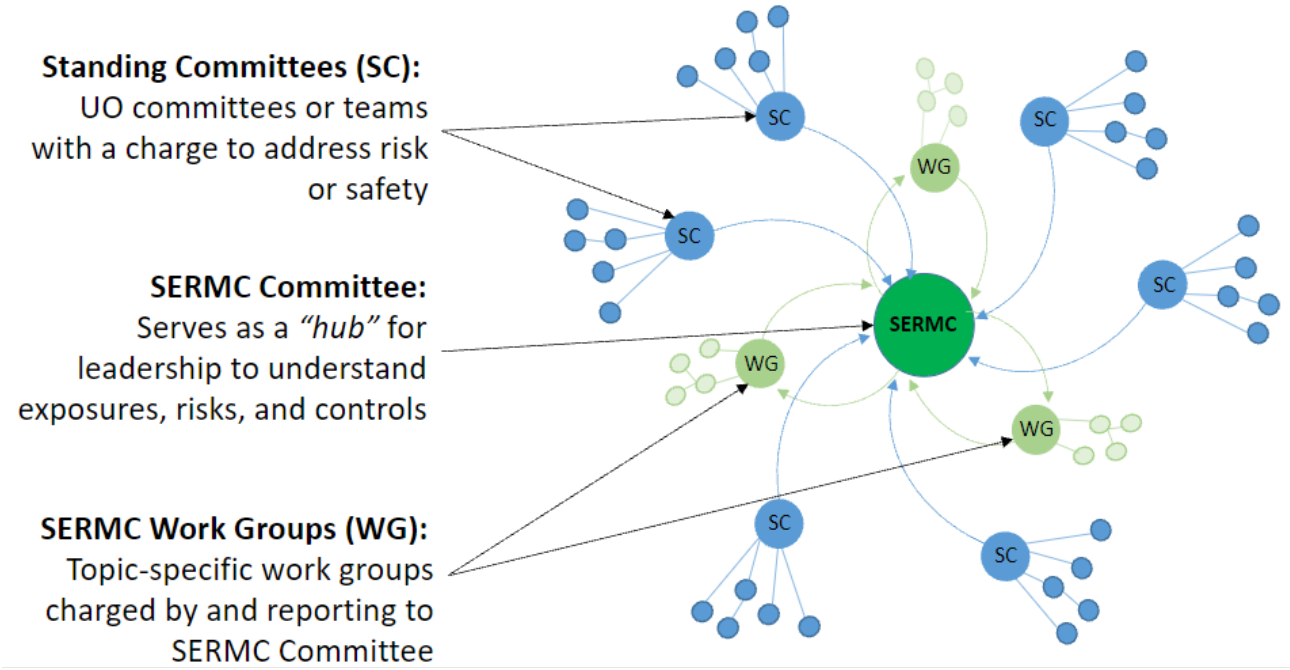
2022 Strategic Risk and Resilience Committee Calendar

Month	Standing committee, Operational or Team Presentations	University's Risk Exposure Matrix (REM) Updates
January	Campus Vulnerability Assessment Team / Behavioral Threat Assessment Team	Information Services / Research
February	Radiation Safety Committee	VPFA / Human Resources
March	Safety Advisory Committee	Chief Resilience Officer / SRS
April	*Meeting primarily for BAG strategic initiatives*	
May		Student Life / SSEM
June		Athletics / Advancement
July		Equity & Inclusion / Provost / Global Engagement
August		General Counsel / Communications
September	National Security & Research Committee	
October	Payment Card Industry Team / Red Flags Team / ICT Committee	
November	Data Security Incident Response Team / Incident Management Team	
December	Institutional Biosafety Committee / Laboratory Safety Committee	

SERMC Committee's Approach

Link, Leverage, and Align

The committee is the place where management and internal controls (e.g., standing committees, teams, processes, etc.) present the status and identify issues or concerns. When the committee members identify potential gaps or risk exposures that do not have a risk owner or that require additional in-depth analysis the committee establishes an inter-departmental and cross-disciplinary work group to explore the concern. The work groups focus primarily on topics that require special attention for purposes of compliance, planning response, or risk management. The committee provides the work group with a clearly defined charge, a set of expected outcomes, and a timeline for the work group to return to the committee with recommendations. Below is a list of the standing management committees.



SERMC Committee Standing Committees and Teams

- The **Campus Vulnerability Assessment Team** conducts coordinated, site-specific vulnerability assessments that evaluate safety, security, risk, emergency preparedness, and business continuity and oversees security policies and procedure.
- The **Institutional Biosafety Committee** was created as a requirement under the NIH Guidelines for Research Involving Recombinant or Synthetic Nucleic Acid Molecules and is responsible for ensuring that the research is conducted in full conformity with the provisions of the NIH Guidelines.

- The **Laboratory Safety Committee** is delegated primary responsibility for safety in laboratories, including instructional, research, and support workers in laboratories. The committee oversees the development and implementation of the university's Chemical Hygiene Plan.
- The **UO Incident Management Team** provides the command and control infrastructure that is required to manage the logistical, fiscal, planning, operational, safety and campus issues related to any and all incidents/emergencies.
- The **Data Security Incident Response Team** addresses data security issues and oversees the response to data security incidents by collaborating with the data stewards to ensure effective procedures for identifying suspected or actual breaches; overseeing or directly manage university response efforts to incidents involving data or security breaches.
- The **Behavioral Evaluation and Threat Assessment Team** exists to mitigate behavioral threats on campus through an integrated process of communication, education, prevention, problem identification, assessment, intervention, and response to incidents.
- The **Safety Advisory Committee** assists the university administration in providing a safe and healthy workplace for faculty, staff, and student workers by making recommendations on health and safety issues in accordance with OAR 437-001-0765.
- The **Radiation Safety Committee** is delegated primary responsibility for the safe use of ionizing radiation, including but not limited to instructional, research, and support functions. The committee serves as the administrative body required by state rules and under the conditions of the university's license for radioactive materials.
- The **Payment Card Industry Team** was created to reduce the risk of card data breach and to maintain compliance with Payment Card Industry data security standards. The team maintains the UO Payment Card Acceptance Policy and Procedures, oversees an annual PCI risk assessment process, engages a Qualified Security Assessor (QSA), partner with campus merchants, and business, IT and procurement professionals, and oversees the activities of the PCI program coordinator.
- The **National Security and Research Committee** was created to maintain an ongoing understanding of the regulatory landscape; educate the university community on national laws, policies, and regulations; and develop procedures that enable the advancement of the university mission while maintaining compliance with national laws, policies, and regulations.
- The **Information and Communication Technologies Accessibility Committee** provides oversight and support for policies and procedures related to access,

equity, and inclusion for information and communication technologies. This includes services employing information technology and telecommunications equipment used to support the university's mission. The committee helps to ensure equitable access to the university's increasing digital environment.

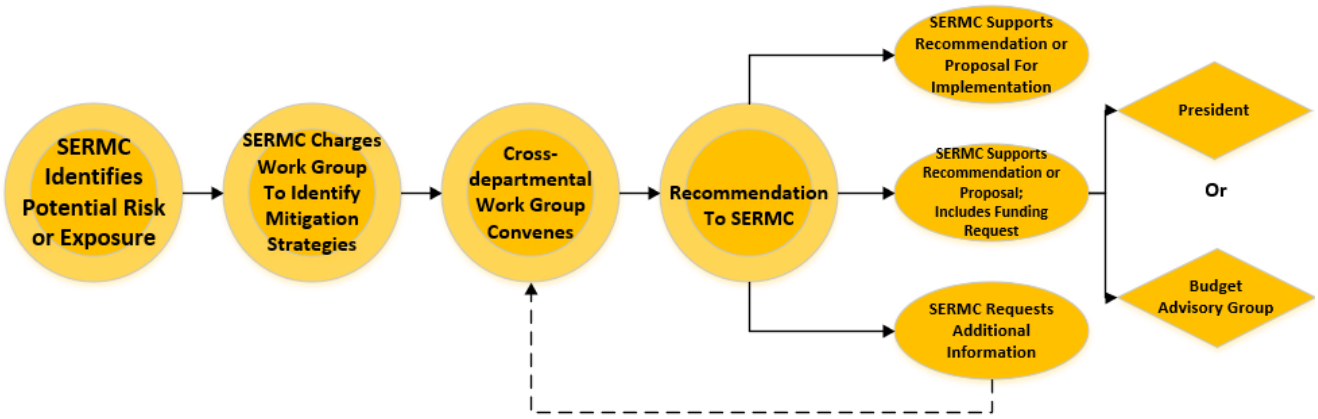
SERMC Committee's Work Groups

When the committee members identify potential gaps or risk exposures that do not have a risk owner or that require additional in-depth analysis the committee establishes an inter-departmental and cross-disciplinary work group to explore the concern. The work groups focus primarily on topics that require special attention for purposes of compliance, planning response, or risk management. The committee provides the work group with a clearly defined charge, a set of expected outcomes, and a timeline for the work group to return to the committee with recommendations.

Work Group Process

From risk identification to action

The work group approach allows the committee to bring campus partners to the table to better understand specific risk exposures, and to develop actionable recommendations to mitigate those risks. The work group structure also encourages information sharing, problem-solving, and collaboration across divisions, units and departments.



SERMC Current Work Groups
Completed and In-Progress

Information Communications Technology Accessibility Work Group

Complete

SERMC charged this work group to:

- Bring together stakeholders to develop strategies for removing barriers and improving accessibility of information and communication technologies (ICT) across campus (including UO websites, web pages, and web applications among others).
- Identify and review current policies/procedures/practices regarding accessible technologies at UO.
- Finalize an ICT Accessibility Policy and Procedures (including implementation guidelines) for submission to the Policy Advisory Council.
- Research methods to ensure information provided by or gathered from third-party vendors is accessible, including standards and language related to ICT procurement.

Membership:

- *Human Resources*
- *General Counsel*
- *Information Services*
- *Student Services and Enrollment Management*
- *University Communications*
- *Accessible Education Center*
- *Purchasing and Contracting Services*
- *UO Libraries*
- *Office of the Registrar*
- *Athletics*
- *Student Life*
- *Business Affairs*

Findings:

- *The work group recommended that the University dedicate more resources to ensure that all UO web pages and other active ICT be made accessible to the widest range of users, including those with disabilities.*

Actions:

- The work group created an accessibility link on the uoregon.edu home pages that directs individuals to a website where inquiries, requests, and complaints can be submitted. The website is https://www.uoregon.edu/accessibility.
- The work group drafted a policy and procedures to address ICT compliance at the University. The policy was reviewed and approved by the Policy Advisory Committee and went into effect July 9, 2019.
- The policy charged the CIO with forming an Information and Communications Technology Access Committee (ICT Access Committee). The ICT Access Committee was formed and began meeting in August 2020. This committee reports annually to the SERMC.
- The work group recommended the Budget Advisory Group fund a new position (ICT Accessibility Program Manager) who would specialize in ICT compliance. The Strategic Enterprise Risk and Resilience Committee supported the proposal. The work group developed a budget proposal for FY20 which was approved.

Clery Compliance Work Group

 *Complete*

SERMC charged this work group to:

1. Review all Clery-related workflows and systems at the university.
2. Document workflows and systems in clear procedures.
3. Identify potential opportunities to enhance or streamline systems to ease administrative burden and ensure compliance.
4. Review and compare our annual report structure to other universities' reports to see if there are opportunities to improve on the presentation of data.

Membership:

- *Human Resources*
- *University Communications*
- *General Counsel*
- *Internal Audit*
- *Safety and Risk Services*
- *Fire Marshal*
- *Title IX*
- *Dean of Students*
- *University Housing*
- *Office of Financial Aid*
- *Athletics*
- *UOPD*
- *BAO Travel*
- *International Affairs*
- *Asst. Director of Crisis & Intervention*

Findings:

- *The work group reviewed the university's Clery Act-related processes considering the requirements set forth in the Clery Act, federal rulemaking, federal guidance and other summaries of best practices.*
- *The work group concluded that the university is in compliance with all Clery-related obligations.*
- *The work group conducted an assessment and made certain changes, although not legally required, to comport with best practices.*

Actions:

- The work group recommended that Safety and Risk Services adopt the following procedures: Procedures for Collecting, Classifying, Counting and Publishing Clery Act data, Procedures for Fire Safety Disclosures and the Fire Log, and Campus Crime Alert Protocol. These were adopted by Safety and Risk Services.
- The work group recommended that all Campus Security Authorities (CSAs) receive ongoing training. The General Counsel's office and Safety and Risk Services worked together to create training for CSAs. CSAs will be required to take the training within one year of their CSA notification.
- The work group created and developed a Clery Act website where resources are available to the campus community. Clery.uoregon.edu.
- A process was put in place for notifications when student travel takes place for Clery reporting.
- Safety and Risk Services hired a Clery Compliance Officer in December 2021 that reports to the Director of Risk Management and Insurance.

Enterprise Training Coordination and Systems Work Group

In Progress

The University of Oregon has multiple platforms for training. Trainings institution-wide are becoming a critical component for students, faculty, staff and volunteers in mitigating exposures which necessitates a training system with the capability to track compliance. It is unclear what the cost is to the University to maintain these various training systems. The intent for this work group is to identify the various training systems currently in place and to explore a more holistic training system that could be used by the entire institution. In March 2018, SERMC charged this work group to:

1. Identify and catalog all training systems currently used on campus by cost, system owner, target audience, etc.
2. Explore strategic cost savings (both operational and direct costs) of moving to a comprehensive and managed enterprise training system.
3. Develop recommendations for SERMC.

Membership:

- *Human Resources*
- *University Communications*
- *General Counsel*
- *Purchasing and Contracting Services*
- *Safety and Risk Services*
- *Environmental Health and Safety*
- *HIPAA Privacy Officer*
- *Research and Innovation*
- *Title IX*
- *Student Life*
- *Business Affairs*
- *Office of the Provost*
- *Information Services*
- *Office of the Registrar*

Findings:

- *There are four intended audiences for all mandatory and activity-based trainings: Students, student employees, faculty and staff, and volunteers.*
- *MyTrack is the current training system on campus for employees. MyTrack tracks employees by job codes which immediately rules out students and volunteers.*
- *There currently is not a system on campus for delivering and tracking trainings for students and volunteers.*
- *The Dean of Students contracts out with a third party for their mandatory trainings.*
- *Activity-based trainings for students, e.g. lab safety training, is being delivered and tracked by faculty members or department.*
- *Volunteer training is also delivered and tracked similar to the process used for activity-based trainings for students.*

Actions:

- On February 13, 2019, the work group recommended that the university continue to use MyTrack for delivering training and tracking compliance for all employees and to keep student employees in MyTrack for recruitment and assessment.
- The work group recommended looking into software for delivering and tracking student and volunteer training. This process is still ongoing.

University Reporting Systems and Responsibilities

In Progress

In December 2019, SERMC charged this work group to take a closer look at the existing reporting software platforms used to ensure we are meeting the needs of the university. The two primary software systems platforms are EthicsPoint and Maxient. The risk to the university around reporting can be significant if the reports are not addressed and handled expeditiously. The committee has determined that this risk is significant enough a group should be formed to identify the various reporting systems, work flows and responsibilities and make recommendations. We anticipate a recommendation of findings will be brought to SERMC by the end of the calendar year.

Membership:

- *Human Resources*
- *Internal Audit*
- *University Communications*
- *General Counsel*
- *Safety and Risk Services*
- *Office of Investigations and Civil Rights Compliance*
- *Student Life*
- *Information Services*
- *Purchasing and Contracting Services*
- *University Housing*
- *Research and Innovation*
- *Athletics*

SERMC Charge:

- *Identify potential opportunities for efficiency in work flows and reporting systems for reporting channels.*
- *Identify potential opportunities to streamline reporting systems, including a review of existing software programs and identify whether or not reporting can be streamlined for efficiency.*
- *Identify the needs to support the systems.*
- *Ensuring system compliance with appropriate regulatory requirements and compatibility with the current university technology environment.*
- *Identify potential opportunities to restructure the report a concern website to align reporting categories with work flows, processes and responsibilities.*

Building Systems, Safety and Security Work Group

In Progress

In December 2019, SERMC charged this work group. The University relies on critical systems for building environmental control, safety and security on a daily basis in order to provide excellent teaching, research and service. Various aspects of these building systems are managed by different departments across campus and there are no consistent procedures applied. Additionally, it is difficult to know what infrastructure is in place for these systems, their security and resilience to failure and how they impact other systems upstream and downstream. Examples of these systems include, but are not limited to: building security (e.g., alarms, access, etc.), campus cameras (buildings and outdoor spaces), fire systems, UOPD and SOC data systems and security, power plant operation systems, building automation (heating and cooling), and cybersecurity for all systems. This work group was convened in the summer of 2021. The work group is currently identifying all systems on campus.

Membership:

- *Information Services*
    - *Network Team*
    - *Information Security Team*
- *Campus Planning and Facilities Management*
    - *Building Automation*
    - *Design and Construction*
    - *Utilities and Energy*
- *University Housing*
- *FASS IT*
- *Safety and Risk Services*
- *UOPD*
- *Fire Marshal*
- *Office of the Provost*
- *Research and Innovation*
- *Internal Audit*

SERMC Charge:

- *Catalog all building security and safety systems in addition to those listed in the overview.*
- *Identify all committees, teams and charges for all systems identified.*
- *Document how each system is funded and supported.*
- *Explore ways to streamline the committees and teams to ensure efficiency and effectiveness to the extent possible.*