University of Massachusetts
Amherst · Boston · Dartmouth · Lowell · Medical · Law · Online

UNIVERSITY OF MASSACHUSETTS - FY2022

ENTERPRISE RISK MANAGEMENT REPORT

JUNE 2022

Contents

Graphics and Tables

Executive Summary

The University of Massachusetts implements enterprise risk management to enhance our understanding of the University's systemwide exposure to enterprise risk, increase visibility and transparency of activities related to mitigating risk, enrich information sharing across the University, and support informed decision-making.

In Fiscal Years (FYs) 2021 and 2022, the University's Systemwide Enterprise Risk Management (ERM) Program continued to strengthen and achieve new milestones in maturing the ERM Program. These milestones include:

- Continuing implementation of mitigation and response actions to reduce the impacts of the coronavirus pandemic by leveraging the systemwide ERM program, its existing partnerships and governance structure
- Updating the ERM program's risk assessment tools to better align with a systemwide perspective on risk and the University's organizational structure
- Developing a framework and tool to document and measure the effectiveness of ongoing risk mitigation strategies
- Confirming alignment of the systemwide ERM Program with ISO risk management guidelines
- Receiving recognition from a national risk management association, and increasing visibility of the program to peers and other higher education institutions

The systemwide ERM Program continues to foster collaboration, enhance transparency across the system, and seek opportunities to improve and enhance the program to provide impact and value to the University.

I. Scope of the Report

This report details the activities of the University's systemwide ERM Program completed since the FY2020 ERM Report.

II. About the University's Systemwide Enterprise Risk Management Program

Enterprise Risk Management (ERM) is a framework that enables the University to anticipate, assess, and manage significant risks that may impact the University's ability to achieve its mission, strategic goals, or objectives. The systemwide ERM Program aligns with ISO 31000 risk management guidelines by creating and protecting value for the University through collaboration, transparency, integration, and continued improvement.

Among the key components of the University's Accountability Framework, the ERM Program is implemented to:

- Enhance our knowledge of the University's exposure to risk across the system
- Increase understanding of how effective the University is in mitigating risk
- Broaden information sharing across the university
- Better inform critical decision-making.

Graphic 1: Administration and Finance Accountability Framework

The systemwide ERM Program enlists a collaborative, cross-disciplinary approach to risk management and assessment to enhance transparency and provide value to the University.

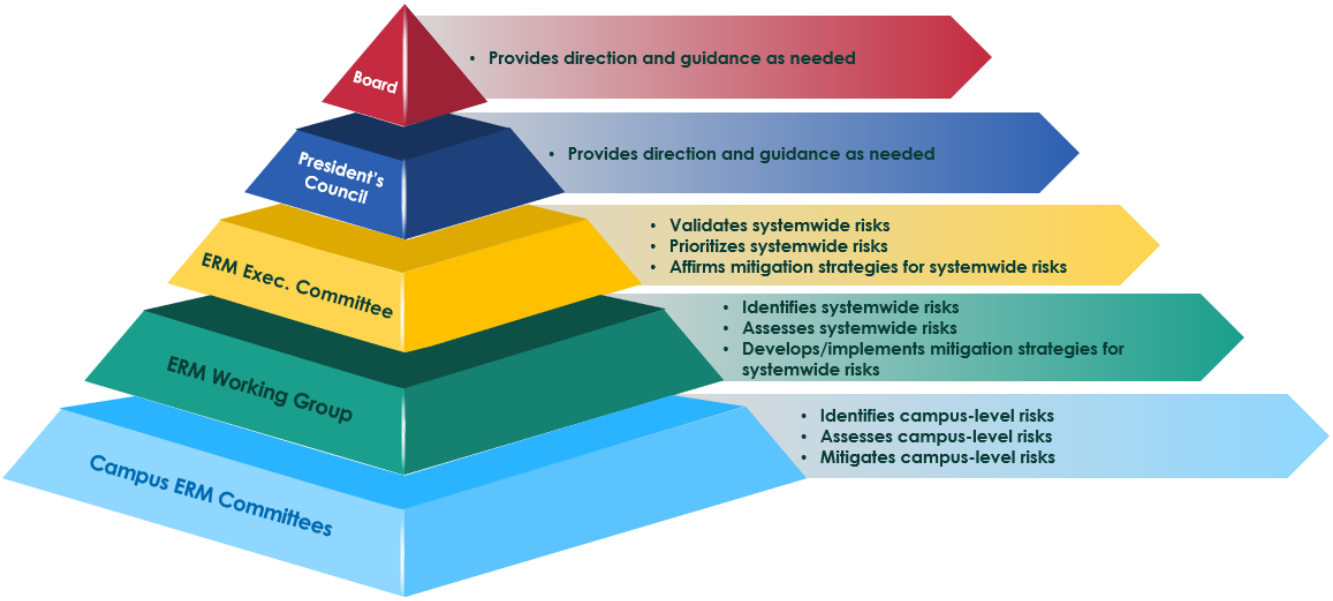
a. Governance Structure

The ERM Program governance structure defines roles and responsibilities across the ERM Program. This ensures diverse, systemwide representation in the ERM process from across disciplines and facilitates integration of strategies across the system. The governance structure is comprised of the following:

- Board of Trustees: The UMass Board of Trustees (BOT) fully supports the systemwide ERM Program and provides direction and guidance to the Program. The BOT Audit and Risk Committee receives an annual update on the Program at a regular meeting of the Committee; additional BOT committees are provided updates as needed.
- President's Council: Consisting of the President, the President's senior staff, and each Chancellor, President's Council actively supports the Program, providing direction and guidance as needed.

- ERM Executive Committee: Consisting of leadership representatives from the campuses and President's Office, the ERM Executive Committee validates and prioritizes risks and affirms risk mitigation strategies.
- ERM Working Group: Consisting of campus ERM representatives and seventeen discipline-specific subject matter experts from across the university system, the ERM Working Group identifies and assesses systemwide risks, and develops, implements, or monitors risk mitigation strategies.
- Campus ERM Committees: Membership may vary from campus to campus, but Campus ERM Committees are responsible for identifying, assessing, and mitigating campus-level risks.

Graphic 2: University Systemwide Enterprise Risk Management Program Governance Structure

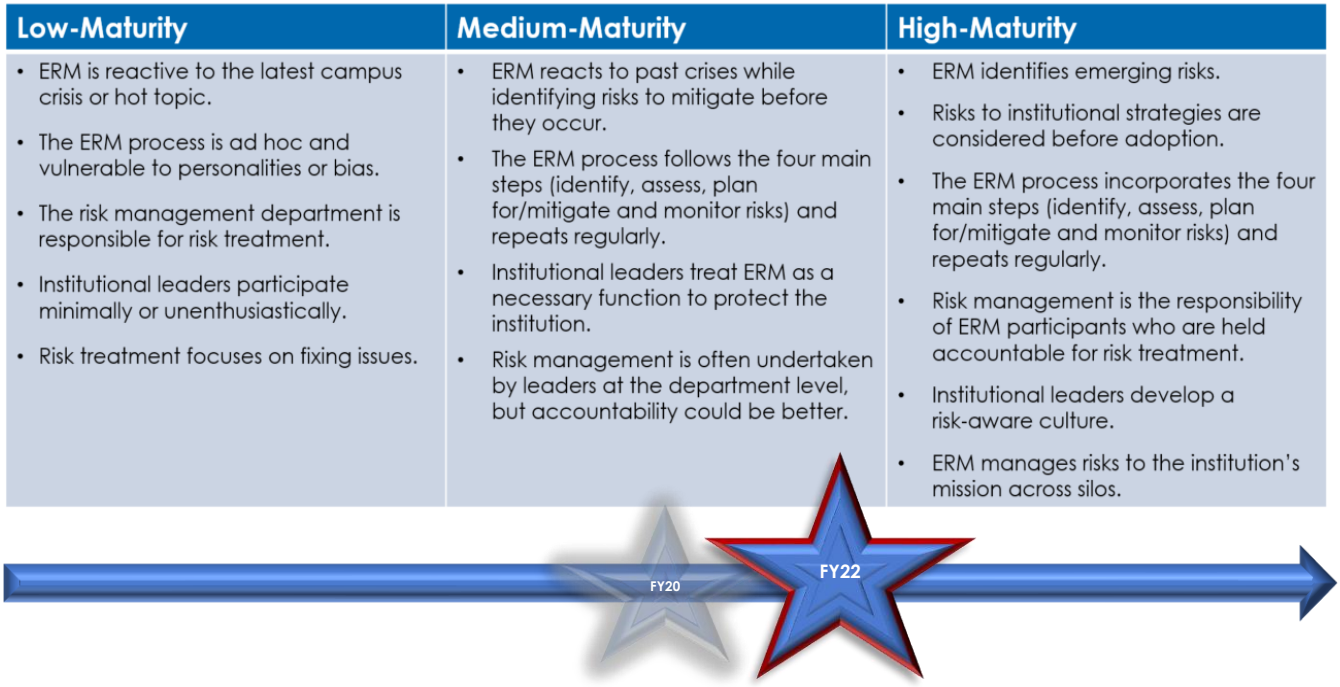


For more detailed information about the ERM Program governance structure, please see Appendix A.

b. Program Maturity

The University continues to mature its systemwide ERM program based on the Association of Governing Boards of Universities and Colleges (AGB)'s model for assessing program maturity. This model is based on criteria from United Educators *"Use a Maturity Tool to Advance the ERM Process – Higher Education."* Since FY 2020, the ERM Program has moved from mid-range to high-range of medium maturity.

Graphic 3: Program Maturity Model



In maturing the program, the University has shifted from a reactive to a proactive risk management strategy: implementing a regular cycle to identify, assess, mitigate and monitor risks; enhancing our ability to document and assess risk mitigation strategies; and conducting quarterly meetings with the ERM Executive Committee to inform leadership. The ERM Program is working toward increasing visibility of risk mitigation strategies across the University in an effort to increase familiarity of the ERM program and introduce risk management into everyday culture and activities.

III. Program Recognition

As the systemwide ERM Program continues to mature, the University has been working to achieve peer and national recognition through presentations, publications, and awards.

In June 2022, the ERM Program received the Public Risk Management Association (PRIMA) 2022 Outstanding Achievement for a Risk Management Product award for our new risk mitigation assessment framework. The award was presented at the June 2022 national conference in San Antonio, Texas.

In addition, the ERM program was invited to present at several conferences of various national associations, including both the regional and national conferences of the University Risk and Insurance Management Association (URMIA) and the Society of Corporate Compliance and Ethics (SCCE) higher education conference. The ERM Program was also asked to contribute content to PRIMA's education website by writing a blog on leveraging meaningful data through ERM and by recording a podcast about the successful use of ERM

in response to COVID-19. Finally, we have been invited to write an article for URMIA's monthly newsletter, which will be published in FY23.

IV. COVID-19 Response and Mitigation Coordination

The University systemwide ERM Program continued to coordinate across the system and with key external partners to facilitate coordination of response to and mitigation of the impacts related to COVID-19.

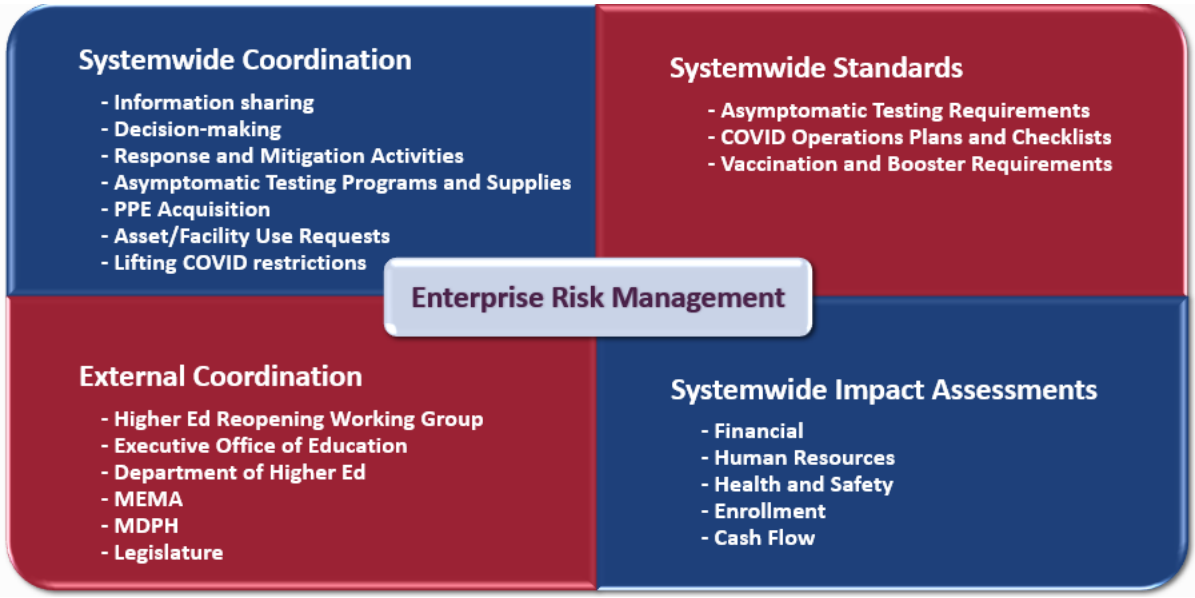
The ERM Program supported systemwide coordination to:

- Maintain a systemwide situational awareness model to enhance collaboration, coordination, and response across the system and to help ensure consistency in approach.
- Share information both at the leadership and operational levels related to local, state and federal guidance, best practices being implemented at our campuses and at other higher ed institutions, and the status of campus mitigation activities, including asymptomatic testing results, isolation and quarantine space usage, and masking requirements.
- Coordinate the acquisition of asymptomatic testing supplies and personal protective equipment during a timeframe when it was extraordinarily difficult to access these items.
- Coordinate requests the university received to support state response through use of our facilities as field hospitals, testing sites, and vaccination sites.
- Coordinate lifting of certain COVID-19 restrictions when state and federal guidance allowed for such reductions.

The ERM Program supported collaboration across the system to develop systemwide minimum standards on critical COVID-19 mitigation efforts, such as asymptomatic testing requirements; COVID-19 operational plans and checklists for each semester, and consistent vaccination and booster requirements for faculty, staff and students.

The ERM Program also served as the University's primary point of contact for key external partners, including the Executive Office of Education, the Department of Higher Education, and the other higher education segments to share information on COVID-19 activities across Massachusetts higher ed institutions and to assure the Administration that the University was meeting federal, state and local requirements. The Program also coordinated with other state partners like MEMA and MDPH on obtaining and providing resources, supporting state response, and understanding eligibility for federal disaster reimbursement.

Graphic 4: Leveraged ERM for Systemwide COVID-19 Response Coordination



In addition, the ERM Program supported University leadership serving on the Governor's higher education reopening working group, which set guidance for Massachusetts higher ed institutions as we collectively sought to reopen in Fall 2020. The Program also supported developing and providing updates to the Legislature and Administration on the University's COVID-19 activities.

Lastly, the ERM Program supported various assessments of Covid-related impacts to critical components of the University, including financial sustainability, cash flow and enrollment; impacts to employees such as remote work and family and medical leave; and impacts to the health and safety of faculty, staff, and students.

v. FY21 and FY22 Systemwide ERM Program Activities

Under the ERM Program's governance structure (see Appendix A), the University has continued to implement and enhance our program, following our two-year program cycle. This cycle incorporates risk assessment and prioritization, identification and development of risk mitigation strategies, assessment of risk mitigation strategies, and routine publication of information about ERM Program. Throughout this cycle, the University continuously implements risk mitigation strategies.

Graphic 5: Two-Year Enterprise Risk Management Program Cycle

The following sections provide updates on programmatic activities implements in each component of the cycle.

a. Identify and Assess Risks

The University's systemwide ERM Program focuses on *systemwide* risk, defined as risk that may result in university-wide impacts, impacts to multiple campuses, or significant impact on a single campus.

Under the University's systemwide ERM Program, the University contemplates several types of systemwide risks:

- **Operational** risk which may affect the University's ability to implement its operations.
- **Financial** risk which may cause financial instability or substantial loss of assets for the University.
- **Legal and/or Compliance** risk which may create or increase legal exposure and/or affect the University's ability to comply with internal and external regulations, policies, and procedures.
- **Workforce** risk which may impact the University's ability to recruit or retain faculty and staff and/or maintain a positive workplace culture.
- **Reputational** risk which may impact the University's brand and/or reputation
- **Life safety** risk which may impact the health and/or safety of students, faculty, or staff

When conducting risk assessments, the ERM Program assesses the system's ***inherent exposure*** to risks, meaning risks are assessed based on their potential impact to the University prior to implementation of risk mitigation strategies. Risks are assessed and rated using three risk assessment tools to answer questions related to specific risk factors:

- **Likelihood**: Could the University system experience this risk?
- **Consequence**: To what degree would the University system be impacted by this risk?
- **Urgency**: How soon does the University system need to prioritize this risk?

The ERM Working Group is responsible for assessing the likelihood and consequence of risks identified as having a systemwide impact. The ERM Executive Committee is responsible for assessing the urgency of systemwide risks, which in essence defines leadership's risk tolerance.

The ratings are then calculated to generate a risk's Inherent Risk Score (see Graphic 6).

Graphic 6: Inherent Risk Score Calculation

Enhance Risk Assessment Tools

At the beginning of FY 2022, the ERM Program engaged the ERM consulting practice of Arthur J. Gallagher to conduct a comprehensive review and enhancement of the program's risk assessment tools to ensure the tools reflect a systemwide perspective on risk and are aligned with the organization of the University.

The ERM Working Group and the ERM Executive Committee participated in the process of updating the tools. The updated tools are provided in Appendix D and a summary of changes to each tool is provided in Table 1.

Table 1: Summary of Changes to ERM Program Risk Assessment Tools

Tool	Changes
Likelihood	• Changed title from Probability to Likelihood • Decreased rating options from five levels to four levels to eliminate the possibility of neutral ratings • Created additional definitions for each rating level to ensure applicability of the tool to all types of risk
Consequence	• Changed title from Impact to Consequence • Decreased rating options from five levels to four levels to eliminate the possibility of neutral ratings • Added two new categories for assessment: Legal/Compliance and Workforce • Created new definitions of systemwide impact for each rating level and each consequence category
Urgency	• Clarified the definition • Updated the rating definitions/timeframes

The new tools were used to assess risks and generate the FY22 Systemwide Risk Registry. To develop the risk registry, the ERM Working Group assessed the likelihood and consequence of risks identified as having a systemwide impact. The ERM Working Group completed their role in the FY22 risk assessment process in December 2021.

The ERM Executive Committee assigned urgency ratings to each risk and completed this task in January 2022. An Inherent Risk Score for each risk was subsequently generated based on the risk assessments completed by the ERM Executive Committee and ERM Working Group.

b. Prioritize Risks

With Inherent Risk Scores calculated, the FY22 risks were then prioritized. Risks are prioritized based on the Inherent Risk Score, with the highest score ranked first. The ERM Executive Committee reviewed and affirmed the priority of FY22 risks.

The top ten FY 22 risks are detailed in Table 2 below. These risks align with priority risks identified by others in the higher education sector.

The full FY22 Risk Registry is detailed in Appendix A.

Table 2: Top 10 FY 2022 Systemwide Risks (Based on Inherent Risk Scores)

Rank	Name	Definition
1	Enrollment	Inability to sustain and/or increase enrollment of in-state, out-of-state, international, residential, commuter, undergraduate and/or graduate students.
2	Information Security	Inability to safeguard data and/or information systems to prevent unauthorized access - whether intentional or unintentional - by foreign or domestic actors or vendors with whom the University conducts business.
3	Financial Sustainability	Inability to adapt the University's business model to ensure financial sustainability, mitigate risk, and adjust to changing circumstances that influence funding or revenue.
4	Facilities and Deferred Maintenance	Inability to maintain facilities, including the prioritization of ongoing and deferred maintenance, and/or develop facilities and infrastructure to attract and retain students, staff and faculty, and to support critical research.
5	Student Health and Mental Health Support	Inability to maintain capabilities and resources to support students' physical and mental health, development and well-being.
6	Vendor Risk Management	Inability to verify that vendors, including subcontractors, comply with University requirements including but not limited to: undergoing appropriate screening such as restricted party lists, background and CORI checks, etc.; completing required training such as Title IX, harassment, etc., maintaining obligatory insurance coverage, and/or producing acceptable deliverables or providing acceptable services in accordance with the contract.
7-8	Attract, Recruit, Retain Faculty and Staff	Inability to attract, recruit, and retain qualified, skilled and reputable faculty and staff.
7-8	International Activities	Inability to effectively implement a consistent approach across to the University's international activities across the system, including but not limited to: management of student, faculty and staff travel; implementation of and compliance with export controls; research activities; protection of intellectual property; protection of data and data systems; and international tax compliance.

Rank	Name	Definition
9	Information Privacy	Inability to maintain compliance with state and federal information privacy standards, regulations and laws, including Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry (PCI) standards, Personally Identifiable Information (PII) requirements, Family Educational Rights and Privacy Act (FERPA) and General Data Protection Regulations (GDPR).
10	Diversity, Equity, Inclusion and Accessibility	Inability to sustain and/or enhance diversity, equity, inclusion and accessibility across all levels of the University, including leadership, faculty, staff, and students.

c. Identify, Assess and Implement Risk Mitigation Strategies

Risk mitigation is the core of any ERM Program. While it is impactful to understand risk and risk exposure, it is equally, if not more important to understand the strategies being implemented to address risk and provide transparency on the effectiveness of these strategies in reducing risk exposure.

The ERM Program has designed and is in the process of undertaking a more comprehensive approach not only to systematically document ongoing mitigation strategies, but also assess the effectiveness of mitigation strategies in reducing risk exposure. Because this framework is in the early stages of implementation, this report does not detail the multitude of ongoing mitigation strategies being employed across the University; rather, the results of the new framework and associated mitigation strategies will be detailed in future reports.

Under this new framework, the ERM Program has developed and is piloting a new tool that allows the University to document ongoing risk mitigation strategies for each of our FY22 risks and assess the effectiveness of those strategies in reducing risk exposure. This tool provides a platform to document ongoing risk mitigation strategies, assess those strategies, and evaluate their impact on reducing risk.

When considering a risk mitigation assessment tool, the ERM Program defined the following requirements:

- Documentation of risk mitigation strategies for transparency and common operating picture
- Demonstration of progress (or lack of progress) in reducing risk exposure

- Correlation of risk mitigation assessment to a risk's Inherent Risk Score
- Achieve all of this through a single, user-friendly process and tool.

The ERM Program researched publicly available tools and learned that, unlike risk assessment tools which were more widely available, there were few publicly available risk mitigation assessment tools. Tools that were publicly available required two processes to assess the impact of mitigation on risk: first, the tool required a stand-alone process to evaluate the risk mitigation strategy and often this assessment had little to no direct relevance to how risk is assessed; second, the risk had to be reassessed against the mitigation strategy to understand how impactful the strategy is on reducing risk exposure.

Given this, the ERM Program sought to develop our own tool, and enlisted a consultant to provide guidance on the development.

There are three components of the assessment which include:

- Evaluate the effectiveness of individual risk mitigation strategies on a risk
- Compare effectiveness of multiple risk mitigation strategies on a risk
- Evaluate the aggregate effectiveness of all risk mitigation strategies on a risk

Through this tool, the University can document risk mitigation strategies, provide transparency on risk mitigation strategies, demonstrate progress in mitigating risk as well as areas that may require additional attention, and enable more robust discussion on risk and risk mitigation priorities. The tool generates a Residual Risk Score for each risk, reflecting the effectiveness of risk mitigation strategies and demonstrating progress in reducing the University's risk exposure.

The tool does ***not*** track key performance indicators, define specific action items, or change the Inherent Risk Score of a risk.

The tool is currently being piloted with a subset of the ERM Working Group. The ERM Program intends to roll out the tool to the full ERM Working Group in FY2023.

d. Issue ERM Report

In accordance with the two-year program cycle, the ERM Program is issuing this report to detail activities of FY21 and FY22. The next ERM Report will be issued in FY24.

VI. Conclusion

FY 2021 to FY 2022 were active years for the University systemwide ERM Program. The Program continued to mature by enhancing the Program's risk assessment tools, conducting a new risk assessment to generate the FY22 Risk Registry, developing a tool to both document and assess the effectiveness of risk mitigation strategies, and increasing visibility of the Program to peers.

As we look forward, the ERM Program intends to continue to mature and make substantial progress in documenting and assessing risk mitigation strategies. These activities will further integrate risk management and the ERM Program into the culture and operations of the University.

Appendix A: University of Massachusetts FY22 Systemwide Risk Registry

Table A1: FY22 Systemwide Risk Registry

Rank	Risk Name	Risk Definition	Likelihood	Likelihood Rating	Consequence - Total Rating	Urgency Rating	Inherent Risk Score
1	Enrollment	Inability to sustain and/or increase enrollment of in-state, out-of-state, international, residential, commuter, undergraduate and/or graduate students.	Almost Certain	4	18	3	**216**
2	Information Security	Inability to safeguard data and/or information systems to prevent unauthorized access - whether intentional or unintentional - by foreign or domestic actors or vendors with whom the University conducts business.	Almost Certain	4	16	3	**192**
3	Financial Sustainability	Inability to adapt the University's business model to ensure financial sustainability, mitigate risk, and adjust to changing circumstances that influence funding or revenue.	Likely	3	16	3	**144**
4	Facilities and Deferred Maintenance	Inability to maintain facilities, including the prioritization of ongoing and deferred maintenance, and/or develop facilities and infrastructure to attract and retain students, staff and faculty, and to support critical research.	Almost Certain	4	16	2	**128**
5	Student Health and Mental Health Support	Inability to maintain capabilities and resources to support students' physical and mental health, development and well-being.	Likely	3	14	3	**126**
6	Vendor Risk Management	Inability to verify that vendors, including subcontractors, comply with University requirements including but not limited to: undergoing appropriate screening such as restricted party lists, background and CORI checks, etc.; completing required training such as Title IX, harassment, etc., maintaining obligatory insurance coverage, and/or producing acceptable deliverables or providing acceptable services in accordance with the contract.	Almost Certain	4	15	2	**120**

Rank	Risk Name	Risk Definition	Likelihood	Likelihood Rating	Consequence - Total Rating	Urgency Rating	Inherent Risk Score
7	Attract, Recruit, Retain Faculty and Staff	Inability to attract, recruit, and retain qualified, skilled and reputable faculty and staff.	Likely	3	15	2	**90**
7	International Activities	Inability to effectively implement a consistent approach across to the University's international activities across the system, including but not limited to management of student, faculty and staff travel; implementation of and compliance with export controls; research activities; protection of intellectual property; protection of data and data systems; and international tax compliance.	Likely	3	15	2	**90**
9	Information Privacy	Inability to maintain compliance with state and federal information privacy standards, regulations and laws, including Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry (PCI) standards, Personally Identifiable Information (PII) requirements, Family Educational Rights and Privacy Act (FERPA) and General Data Protection Regulations (GDPR).	Likely	3	14	2	**84**
10	Diversity, Equity, Inclusion and Accessibility	Inability to sustain and/or enhance diversity, equity, inclusion and accessibility across all levels of the University, including leadership, faculty, staff, and students.	Likely	3	13	2	**78**
11	All-hazards Planning and Response Capabilities	Inability to maintain all-hazards preparedness, response and mitigation plans and capabilities as part of an integrated emergency management program both at the system level, as well as on each campus. Hazards include but are not limited to hazardous weather, chemical/biological/radiological/nuclear/explosives (CBRNE) incidents, active shooter threats and incidents, infectious disease outbreaks, acts of civil disobedience, acts of bias and hate, and any additional threats that could impact the health and safety of the campus community or require the evacuation of a facility, a portion of a campus, or an entire campus.	Possible	2	19	2	**76**

Rank	Risk Name	Risk Definition	Likelihood	Likelihood Rating	Consequence - Total Rating	Urgency Rating	Inherent Risk Score
12	Multi-state Payroll Taxation	Inability to appropriately comply with other states' payroll tax withholding requirements.	Almost Certain	3	12	2	**72**
13	Labor Relations	Inability to maintain productive labor and employee relations.		3	12	2	**72**
14	Data Management	Inability to provide consistency in data across the system to support critical information sharing and strategic analytical analysis.	Likely	3	11	2	**66**
15	Research	Inability to develop and/or maintain transparent and consistent research protocols across the university system to ensure safety, accountability and compliance with applicable rules and regulations.	Possible	2	16	2	**64**
16	Multi-state Business Taxation	Inability to comply with other states' sales, excise and franchise tax requirements as the University expands its business model.	Likely	3	10	2	**60**
17	Sexual Assault Policies and Response Procedures	Inability to implement consistent protocols across the University to prevent, detect, prepare for, and respond to sexual assault, harassment, and other interpersonal violent acts (stalking, domestic violence, etc.) and maintain compliance with state and federal regulations.	Possible	2	14	2	**56**
17	IT Disaster Recovery	Inability to ensure access to systems and/or data in the event of a disruption in technology services.	Possible	2	13	2	**52**
17	Continuity Planning	Inability to develop, maintain and/or implement capabilities to maintain continued operations during incidents causing sustained disruption to key services or functions; capabilities include developing, maintaining, exercising and implementing continuity plans as part of an integrated emergency management program.	Possible	2	13	2	**52**
17	Environmental, Health, Public Health and Safety Regulations	Inability to comply with local, state and federal environmental, health, public health, and safety regulations and requirements.	Possible	2	13	2	**52**

Rank	Risk Name	Risk Definition	Likelihood	Likelihood Rating	Consequence - Total Rating	Urgency Rating	Inherent Risk Score
17	Alcohol and Substance Abuse	Inability to maintain capabilities and resources to prevent, detect and respond to, and support students impacted by alcohol and substance abuse on campuses, and maintain compliance with local, state and federal regulations.	Possible	2	13	2	**52**
22	Crisis Communications Coordination	Inability to develop, maintain and/or implement university-wide crisis communication coordination protocols and processes that address information-sharing and provide situational awareness among impacted campuses and the President's Office during an emergency and/or other impactful incident to support the University's response to an emergency.	Possible	2	12	2	**48**
23	Immigration Rules and Regulations	Inability to comply with federal immigration rules and regulations.	Possible	2	11	2	**44**
24	Fraud, Waste, Abuse	Inability to maintain capabilities to prevent, detect and respond to fraud, waste, and abuse.	Likely	3	14	1	**42**
25	Uninsured Loss	Inability to obtain legislative authority to obtain property insurance on state-owned facilities.	Almost Certain	4	9	1	**36**
26	Employment Law/Regulations	Inability to comply with local, state and federal employment laws and regulations.	Possible	2	14	1	**28**
26	NCAA Regulations	Inability to comply with NCAA regulations, including recruiting guidelines.	Possible	2	14	1	**28**
28	Policies/Procedures Regarding Minors on Campus	Inability to develop, maintain, and implement procedures to safeguard minors on campus.	Possible	2	10	1	**20**
28	Academic Quality and Standards	Inability to maintain academic quality and standards, including those required for accreditation.	Unlikely	1	20	1	**20**
30	Oversight of Student Organizations	Inability to maintain oversight of registered student organizations (finances, insurance, etc.)	Possible	2	8	1	**16**

Appendix B: ERM Governance Structure Roles and Responsibilities

The ERM Program has a formal governance structure which defines roles and responsibilities under the Program. The governance structure consists of campus ERM committees, the ERM Working Group, the ERM Executive Committee, the President's Council, and the Board of Trustees.

a. ERM Executive Committee

The ERM Executive Committee is responsible for validating the system-wide risks identified and assessed by the ERM Working Group and prioritizing those risks. The Executive Committee is also responsible for affirming mitigation strategies, approving the ERM annual report, ensuring the report is provided to the Board of Trustees.

The ERM Executive Committee is comprised of leadership from across the system:

- **Director of Enterprise Risk Management, Chair**
- **A representative from each campus as appointed by its leadership team**
- **Leadership from the President's Office:**
    - Senior Vice President, Administration and Finance
    - Associate Vice President, Administration and Finance
    - Senior Vice President, Academic Affairs
    - Associate Vice President, Academic Affairs
    - Chief Information Officer
    - General Counsel
    - Director, Internal Audit
    - A member representing research

See Appendix C for the current ERM Executive Committee Membership.

b. ERM Working Group

The ERM Working Group is truly the working body of the system-wide Enterprise Risk Management Program. The ERM Working Group is responsible for identifying and assessing risk across the system.

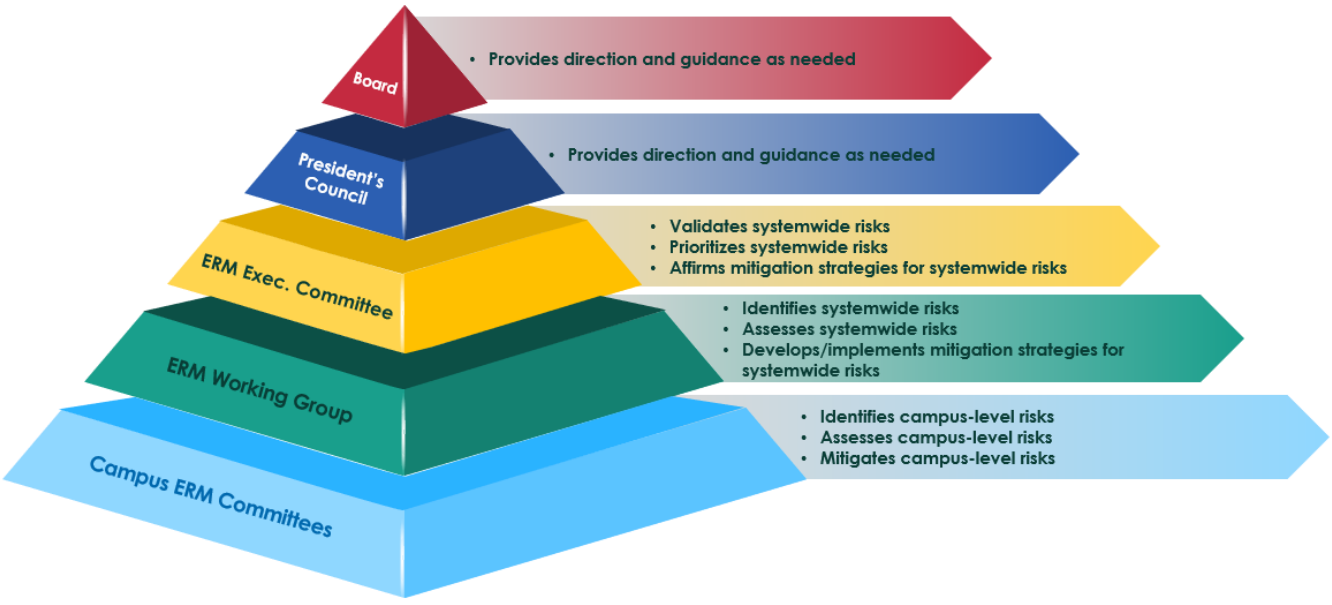
The ERM Working Group consists of:

- **Director of Enterprise Risk Management**: The Director of Enterprise Risk Management serves as the chair of the working group.
- **Two representatives from each campus**: The campus representatives are typically the leads on their respective campus for enterprise risk management.

- **A designated subject matter expert for seventeen identified focal areas**: The subject matter experts serve in lieu of the previous risk groups. These subject areas are as follows:
    - Academic affairs
    - Athletics
    - Communications
    - Controller
    - Facilities
    - Finance/Budget
    - Human resources
    - Information technology
    - Internal Audit
    - Insurance
    - International activities
    - Office of the General Counsel
    - Procurement
    - Research
    - Safety and security
    - Student affairs
    - Tax

See Appendix D for the current ERM Working Group Membership.

Graphic B1: University Systemwide Enterprise Risk Management Program Governance Structure



By bringing these voices together under the ERM Working Group, we ensure a multi-disciplinary approach to identifying risks, as well as enabling comparative risk assessments across the system and across critical subject areas.

The ERM Working Group also encompasses **risk-specific mitigation subcommittees**. Mitigation subcommittees are established to develop, implement, and monitor risk mitigation strategies for priority risks.

Each mitigation subcommittee will develop desired outcomes and milestones for mitigating the specific risk around which it was organized. It will capture ongoing work, identify any potential for new activity, facilitate implementation of strategies, and provide regular updates on the progress of mitigation strategies. Each risk will then be re-evaluated against its mitigation strategies.

Members of the mitigation subcommittee vary with each risk, but each relevant subject matter expert participates, and we can pull in stakeholders that may not formally be part of the ERM working group, who may be critical to mitigating the risk. This also brings mitigation activities under the formal ERM governance structure.

C. Campus ERM Committees

Campus ERM committees identify, assess and coordinate mitigation of campus-specific risks. Campuses have varying degrees of construct and formality to their ERM committees and campus-specific ERM programs.

Appendix C: ERM Executive Committee Membership

Table C1: ERM Executive Committee Membership

FY22 ERM Executive Committee Membership				
Last Name	**First Name**	**Campus**	**Title**	**Executive Committee Seat**
Calise	Lisa	UMPO	Senior Vice President and Treasurer, Administration & Finance	SVP, Administration & Finance
Culverwell	Marcy	UMass Chan	Associate Vice Chancellor, Administration & Finance	UMass Chan
David	Kyle	UMPO	Director, Internal Audit	Director, Internal Audit
Giuliani	Chris	Boston	Associate Vice Chancellor, Administration & Finance	Boston Campus
Gorzkowicz	Matt	UMPO	Associate Vice President, Administration & Finance	AVP, Administration and Finance
Hescock	Jeff	Amherst	Director, Environmental Health and Safety	Amherst Campus
Karberg	Andrew	UMPO	Associate Counsel, Compliance, Ethics, International Affairs	Research
LaGrassa	Michael	Dartmouth	Associate Vice Chancellor of Administrative Operations & Compliance	Dartmouth Campus
Leone	Gerry	UMPO	General Counsel	General Counsel
Miliano	Tom	Lowell	Executive Director, Administrative Services	Lowell Campus
Milligan	Michael	UITS	Chief Information Officer	Chief Information Officer
Newman	Katherine	UMPO	SVP and Chancellor, Academic Programs	SVP, Academic Affairs
Packard	Christine	UMPO	Director, Enterprise Risk Management	ERM Director/Chair

Appendix D: ERM Working Group Membership

Table D1: ERM Working Group Membership

FY22 ERM Working Group Membership						
Last Name	First Name	Campus	Title	ERM Working Group Member		
				Campus ERM Lead	SME	SME Topic
Britton	Kirsten	Amherst	Senior Associate Athletic Director		X	Athletics
Carragher	Candyce	UMPO	Senior Executive Associate to the Senior Vice President		X	Student Affairs
Cho	David	UPST	Chief Procurement Officer		X	Procurement
Coleman	Brian	UMass Chan	Associate CIO – Information Security	X		
Comeau	Justin	Boston	Manager, Emergency Planning & Business Continuity	X		
Conklin	Shane	Amherst	Associate Vice Chancellor for Facilities and Campus Services		X	Facilities
Culverwell	Marcy	UMass Chan	Associate Vice Chancellor, Administration and Finance	X		
Dunlap	John	UMPO	Chief Human Resources Officer		X	Human Resources
Martinez	Haydee	Dartmouth	Chief of Police	X		
Hescock	Jeff	Amherst	Executive Director of Environmental Health and Safety and Emergency Management	X	X	Safety and Security
Hitchcock	Patrick	UMPO	Controller		X	Controller
Karberg	Andrew	UMPO	Associate Counsel, Compliance, Ethics, International Affairs		X	Legal

FY22 ERM Working Group Membership						
Last Name	First Name	Campus	Title	ERM Working Group Member		
				Campus ERM Lead	SME	SME Topic
LaGrassa	Michael	Dartmouth	Associate Vice Chancellor of Administrative Operations & Compliance	X		
Mayers	Darryl	Boston	Assistant Vice Chancellor for Contracts and Compliance	X		
Murphy	Colin	UMPO	Director of Marketing and Communications		X	Communications
Packard	Christine	UMPO	Director, Enterprise Risk Management	X		
Pasquini	LeeAnn	UMPO	Assistant Vice President for Budget & Planning		X	Finance
Russell	Andrew	UMPO	Senior Assistant VP of Operations and Associate Treasurer		X	Tax
Scano	Derek	UMPO	Assistant Director, Internal Audit		X	Internal Audit
Smith	Bradford	UITS	Chief Information Security Officer		X	IT
Stockwell	Joshua	UMPO	Associate Counsel for IP and Research		X	Research
Sullivan	June	UMass Chan	Senior Director, Compliance and Policy	X		
Torres	Sandra	UMPO	Associate Counsel, Immigration & Int'l Services		X	International Activities
Tucker	Josh	UMPO	Insurance Analyst		X	Insurance
Wood	Rick	Lowell	Director, Office of Life Safety and Emergency Management	X		
Yanka	Ruth	Amherst	Executive Director A&F Operations, Vice Chancellor Administration and Finance	X		

Appendix E: Risk Assessment Tools

The ERM Program implements three risk assessment tools to evaluate risk and generate a risk registry: likelihood (Graphic D1), consequence (Graphic D2), and urgency (Graphic D3). Each tool guides assessors in identifying ratings for each risk. The ratings are then calculated to generate a risk's Inherent Risk Score (Graphic D4).

a. Likelihood Risk Assessment Tool

The Likelihood risk assessment tool assesses whether the University system could experience a risk, providing four rating options: unlikely (value of 1), possible (value of 2), likely (value of 3), certain or almost certain (value of 4).

Graphic E1: Risk Assessment Tool - Likelihood

Rating	Description	OR	Probability of Occurrence	OR	Rate of Occurrence
4 Certain or Almost Certain	HIGH - Almost certain to occur, expected in most circumstances	OR	>75%	OR	more than 2x per year
3 Likely	MEDIUM HIGH - Likely to occur or will probably occur		50 to 75%		1-2x per year
2 Possible	MEDIUM - Possible, this could occur		25 to 50%		once every 2-5 years
1 Unlikely	LOW - Unlikely, not expected to occur		Up to 25%		more than 5 years

b. Consequence Risk Assessment Tool

The Consequence assessment tool assesses how impactful a risk may be across six categories:

- Service disruption or impact to operations
- Financial impact
- Legal/compliance
- Workforce
- Reputation
- Life safety

The tool guides assessors in identifying ratings for the risk in each category: negligible (value of 1), low (value of 2), medium (value of 3) or high (value of 4). The ratings for the six categories are then added together to create a total consequence value for the risk.

Graphic E2: Risk Assessment Tool - Consequence

Rating	Service Disruption, Process Impact on Operations	Financial Impact	Legal/ Compliance	Workforce	Reputation	Life Safety
4 High	Serious disruption to or failure of service **AND/OR** Significant impacts to two or more campuses	State appropriation reduction of more than 15 percent **AND/OR** Loss of revenue or increase in expenses of greater than 15 percent or combination of both **AND/OR** Need to use stabilization fund **AND/OR** Impacts to all campuses	Increased state or federal regulatory scrutiny for additional campus(es) **AND/OR** External agency sanctions such as debarment or civil and/or criminal liability **AND/OR** Litigation exposure with significant financial ($10M+), reputational or precedent exposure **AND/OR** Substantial audit findings	Inability to recruit or retain employees with essential knowledge, skills and abilities **AND/OR** Work culture is defined by excessive internal conflict or widespread negativity **AND/OR** Inability to collaborate across the system or limited information sharing and cooperation **AND/OR** Low level of trust among colleagues	Negative national media coverage or negative social media activity (“viral”) for multiple days **AND/OR** Tangible, long-term impacts to enrollment (more than one cycle), philanthropy and public support **AND/OR** Significant personnel actions **AND/OR** Widespread internal reaction	Fatality or permanent disability to one or more people

Rating	Service Disruption, Process Impact on Operations	Financial Impact	Legal/ Compliance	Workforce	Reputation	Life Safety
3 Medium	Moderate disruption to service **AND/OR** Significant impact to one campus	State appropriation reduction of 10-15 percent **AND/OR** Loss of revenue or cost increase of 5-10 percent, or combination of both (est. $175M - $350M) **AND/OR** Impacts to BDL or UMA or UMass Chan	Restrictions or requirements placed on the University's operational activities **AND/OR** Substantial ($1M+) regulatory fines and/or response costs **AND/OR** Moderate audit findings **AND/OR** Litigation with substantial financial ($1M - $10M), reputational or precedent exposure	Difficulty recruiting or retaining employees with essential knowledge, skills and abilities **AND/OR** Work culture experiences frequent internal conflict or significant **AND/OR** Significant obstacles to systemwide collaboration **AND/OR** Decreased information sharing in many circumstances	Negative regional (northeast) media coverage or some negative social media activity **AND/OR** Tangible, short-term impacts to enrollment (one cycle), philanthropy and public support **AND/OR** Significant internal reaction	Serious injury of one or more people
2 Low	Minor impact to service **AND/OR** Some impact to more than one campus	Between $5M and 1 - 5 percent revenue loss or expense increase or combination of both (est. $5M to $175M impact) **AND/OR** Impacts to up to two campuses	Regulatory fines (less than $1M) **AND/OR** Minor audit findings **AND/OR** Litigation with financial (less than $1M), reputational or precedent exposure **AND/OR** Internally imposed consequences or requirement for formal corrective action	Minor impact to recruitment or retention **AND/OR** Work culture experiences some internal conflict or negativity **AND/OR** Challenges with systemwide collaboration **AND/OR** Decreased information sharing and cooperation in limited circumstances	Negative local media coverage or minimal social media activity **AND/OR** Moderate on-campus/internal reaction	Minor injury to more than one person

Rating	Service Disruption, Process Impact on Operations	Financial Impact	Legal/ Compliance	Workforce	Reputation	Life Safety
1 Negligible	Annoyance	Less than $5M impact	No to minimal impact	No to minimal impact to recruitment or retention **AND/OR** No to minimal impact to workplace culture **AND/OR** No to minimal impact to systemwide collaboration or information sharing	No to minor internal reaction	No impact or minor injury to individual

c. Urgency Risk Assessment Tool

The Urgency assessment tool assesses how soon the University needs to prioritize a risk. The tool guides the assessor in identifying a rating for the risk: low (more than 3 years), moderate (1-3 years) or high (within the next 12 months).

Graphic E3: Risk Assessment Tool - Urgency

Level		Timeframe
3	High	Within the next 12 months
2	Moderate	1-3 years
1	Low	More than 3 years

d. Inherent Risk Score Calculation

Once risks are assessed, the resulting ratings are then calculated to determine the risk's Inherent Risk Score.

Graphic E4: Inherent Risk Score Calculation