UMass System-wide Enterprise Risk Management Program Update

Audit and Risk Committee
April 6, 2022

Christine Packard, Director, Enterprise Risk Management

Agenda

- 2-Year ERM Program Cycle
- FY22 Risk Assessment and Prioritization
  - Top 10 FY22 Risks
- Ongoing Activities
  - COVID-19 Response Coordination
  - Insurance as A Mitigation Strategy
  - Additional ERM Programmatic Activities
- Looking Ahead
  - Increasing Focus on Risk Mitigation
  - ERM Report

Appendices

A. ERM Program Governance
B. Risk Assessment Tools and Risk Score Calculation
C. FY22 Risk Registry

A&F Accountability Framework

Independent and objective assurance that analyzes data, processes, policies and controls

Standard processes to provide reasonable assurance regarding achievement of objectives

Reliable, timely information that is accessible and understandable

Systematic approach to identifying, assessing and managing risks across the organization

2-Year ERM Program Cycle

FY22 Risk Assessment and Prioritization

- Engaged Arthur J. Gallagher
  - Conducted comprehensive review and update of the ERM program's risk assessment tools (Summer – Fall 2021)
- ERM Working Group identified and assessed FY22 risks with updated tools (December 2021)

- ERM Executive Committee reviewed and prioritized FY22 risks (January 2022)
- FY22 Risk Registry reflects the University's inherent exposure to risk
  - Does not account for implementation of risk mitigation strategies
  - Generates Inherent Risk Score

Top 10 FY22 Risks

Rank	Risk Name
1	Enrollment
2	Information Security
3	Financial Sustainability
4	Facilities and Deferred Maintenance
5	Student Health & Mental Health Support

Rank	Risk Name
6	Vendor Risk Management
7	Attract, Recruit, Retain Faculty and Staff
8	International Activities
9	Information Privacy
10	Diversity, Equity and Inclusion

Complete FY22 Risk Registry can be found in Appendix C

COVID-19 Response and Mitigation Coordination

- ERM Program continued to coordinate COVID-19 response and mitigation strategies
- With Campuses
  - Asymptomatic testing program
  - Vaccine and booster requirements
  - Information sharing
    - Best practices
    - Local, state and federal requirements
- With External Partners
  - Executive Office of Education
  - Department of Higher Education
  - MEMA/FEMA

Insurance as A Mitigation Strategy

- On track for May 1 insurance renewals
- Key takeaways:
  - Insurance market remains hard
  - Underwriters are increasing premiums by 10% on average across most lines of coverage
  - Significant increases in cyber coverage premium and retentions

Line of Coverage Marketed	Goal of Marketing	Status
International Travel Accident and Sickness	Identify available underwriters and enhance emergency services	Enhanced services
Cyber security	Maintain or increase current $10M limit	• Markets ranging from 60-300% increases in premiums and retentions • Limits being reduced
Fiduciary	Increase current $5M limit	Reduced appetite for increasing limits
Additional Excess Liability Limits	Increase current $10M limit	Evaluating $5M increments

Additional ERM Programmatic Activities

- Executed or expanded MSAs with three firms to provide ERM consulting services and external expertise as needed
  - Arthur J. Gallagher
  - Deloitte
  - KPMG
- Confirmed program alignment with ISO risk management guidelines (31000)
- Presenting at three conferences:
  - University Risk Management and Insurance Association (URMIA) regional conference (April 2022)
  - URMIA national conference (September 2022)
  - Society of Corporate Compliance and Ethics (SCCE) Higher Education Compliance Conference (June 2022)
- Public Risk Management Association (PRIMA) Recognition
  - Blog: *"Moving Risk Assessment Beyond Heat Maps: Obtaining Meaningful Risk Data to Inform Decision-Making"*
  - Podcast: "*Leveraging Enterprise Risk Management as a Crisis Response Tool: A COVID Story*"

Looking Ahead: Shifting Focus to Risk Mitigation

June 2022

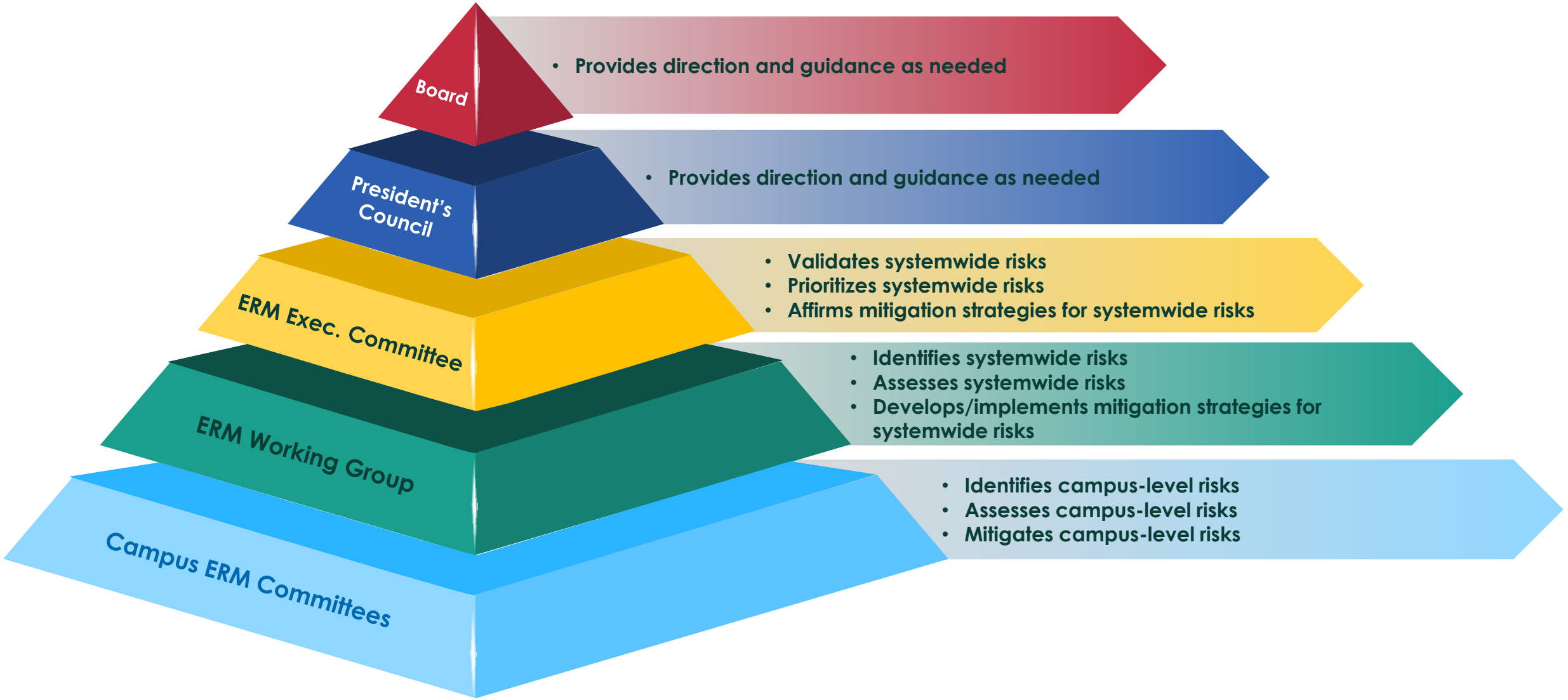
- Engage ERM Working Group to identify risk owners and risk mitigation contributors
- Identify and document risk mitigation strategies

- Finalize framework and new tool to assess risk mitigation strategies
  - Tool will generate a Residual Risk Score to demonstrate degree of progress in mitigating risk
- Assess risk mitigation strategies using new tool

Appendix A

ERM Program Governance

ERM Governance Structure



Appendix B

Risk Assessment Tools and Risk Score Calculation

Updated 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%		2-5x per year
1 Unlikely	LOW Unlikely, not expected to occur		Up to 25%		more than 5 years

Updated 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 more than two campus	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 ***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 of one or more people
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 UMMS	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 ***AND/OR*** Significant obstacles to system-wide 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

(continued on following page)

Updated Risk Assessment Tool – Consequence

(Continued from previous page)

Rating	Service Disruption, Process Impact on Operations	Financial Impact	Legal / Compliance	Workforce	Reputation	Life Safety
2 Low	Minor impact on 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	Minor impact to recruitment or retention ***AND/OR*** Work culture experiences some internal conflict ***AND/OR*** Challenges with system-wide collaboration ***AND/OR*** Decreased information sharing and cooperation in limited circumstances workplace culture	Negative local media coverage or minimal social media activity ***AND/OR*** Moderate on-campus/internal reaction	Minor injury to more than one person
1 Negligible	Annoyance	Less than $5M impact	Requirement for formal corrective action or none	No to minimal impact to recruitment or retention ***AND/OR*** No to minimal impact to workplace culture	No to minor internal reaction	No impact or minor injury to individual

Consequence Rating is calculated as the sum of all category ratings. For example:

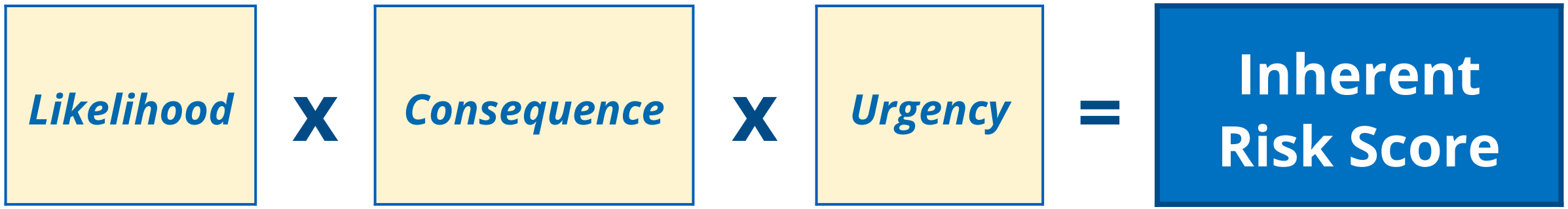
Risk Name	Service Disruption, Process Impact on Operations	Financial Impact	Legal / Compliance	Workforce	Reputation	Life Safety	Consequence Rating
Risk Example A	3	2	3	4	3	1	16

Risk Assessment Tool - Urgency

Urgency: How soon do we need to prioritize this risk?

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

Risk Score Calculation



Appendix C

FY22 Risk Registry

FY22 Risk Registry

FY22 Rank	Risk Name	Risk Definition	Likelihood Rating	Consequence 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.	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.	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.	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.	4	16	2	128
5	Student Health and Mental Health Support	Inability to maintain capabilities and resources to support the physical and mental health, development and well-being of students.	3	14	3	126

FY22 Risk Registry (continued)

FY22 Rank	Risk Name	Risk Definition	Likelihood Rating	Consequence Rating	Urgency Rating	Inherent Risk Score
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.	4	15	2	120
7	Attract, Recruit, Retain Faculty and Staff	Inability to attract, recruit, and retain qualified, skilled and reputable faculty and staff.	3	15	2	90
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.	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).	3	14	2	84
10	Diversity, Equity and Inclusion	Inability to sustain and/or enhance diversity, equity and inclusion across all levels of the University, including leadership, faculty, staff, and students.	3	13	2	78

FY22 Risk Registry (continued)

FY22 Rank	Risk Name	Risk Definition	Likelihood Rating	Consequence Rating	Urgency Rating	Inherent Risk Score
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.	2	19	2	76
12	Multi-state Payroll Taxation	Inability to appropriately comply with other states' payroll tax withholding requirements.	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.	3	11	2	66
15	Research	Inability to develop and/or maintain transparent and consistent research protocols across University System to ensure safety, accountability and compliance with applicable rules and regulations.	2	16	2	64

FY22 Risk Registry (continued)

FY22 Rank	Risk Name	Risk Definition	Likelihood Rating	Consequence Rating	Urgency Rating	Inherent Risk Score
16	Multi-state Business Taxation	Inability to comply with other states' sales, excise and franchise tax requirements as the University expands its business model.	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.	2	14	2	56
18	IT Disaster Recovery	Inability to ensure access to systems and/or data in the event of a disruption in technology services.	2	13	2	52
19	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.	2	13	2	52
20	Environmental, Health, Public Health and Safety Regulations	Inability to comply with local, state and federal environmental, health, public health, and safety regulations and requirements.	2	13	2	52

FY22 Risk Registry (continued)

FY22 Rank	Risk Name	Risk Definition	Likelihood Rating	Consequence Rating	Urgency Rating	Inherent Risk Score
21	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.	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.	2	12	2	48
23	Immigration Rules and Regulations	Inability to comply with federal immigration rules and regulations.	2	11	2	44
24	Fraud, Waste, Abuse	Inability to maintain capabilities to prevent, detect and respond to fraud, waste, and abuse.	3	14	1	42
25	Uninsured Loss	Inability to obtain legislative authority to obtain property insurance on state-owned facilities.	4	9	1	36

FY22 Risk Registry (continued)

FY22 Rank	Risk Name	Risk Definition	Likelihood Rating	Consequence Rating	Urgency Rating	Inherent Risk Score
26	Employment Law/Regulations	Inability to comply with local, state and federal employment laws and regulations.	2	14	1	52
27	NCAA Regulations	Inability to comply with NCAA regulations, including recruiting guidelines.	2	14	1	48
28	Policies/Procedures Regarding Minors on Campus	Inability to develop, maintain, and implement procedures to safeguard minors on campus.	2	10	1	44
29	Academic Quality and Standards	Inability to maintain academic quality and standards, including those required for accreditation.	1	20	1	42
30	Oversight of Student Organizations	Inability to maintain oversight of registered student organizations. (finances, insurance, etc.)	2	8	1	36