ERM Methodologies

Christine Packard

Assistant Vice President, Enterprise Risk Management

University of Massachusetts

Agenda

- Approach to Your ERM Program
- Risk Assessment Methodologies
- Mitigation Assessment Methodologies

Primary ERM Guidance Documents

COSO:
Committee of Sponsoring Organizations

- Organization consists of five (primarily financial) entities:
  - American Accounting Association
  - American Institute of CPAs
  - Financial Executives International
  - Association of Accountants and Financial Professionals in Business
  - Institute of Internal Auditors
- Guidance: Enterprise Risk Management—Integrated Framework
- The “Cube”

ISO:
International Organization for Standardization

Primary ERM Guidance Documents

COSO:
Committee of Sponsoring Organizations

Source: COSO Internal Control Framework ©2013

ISO:
International Organization for Standardization

Primary ERM Guidance Documents

COSO:
Committee of Sponsoring Organizations

Source: COSO Internal Control Framework ©2013

ISO:
International Organization for Standardization

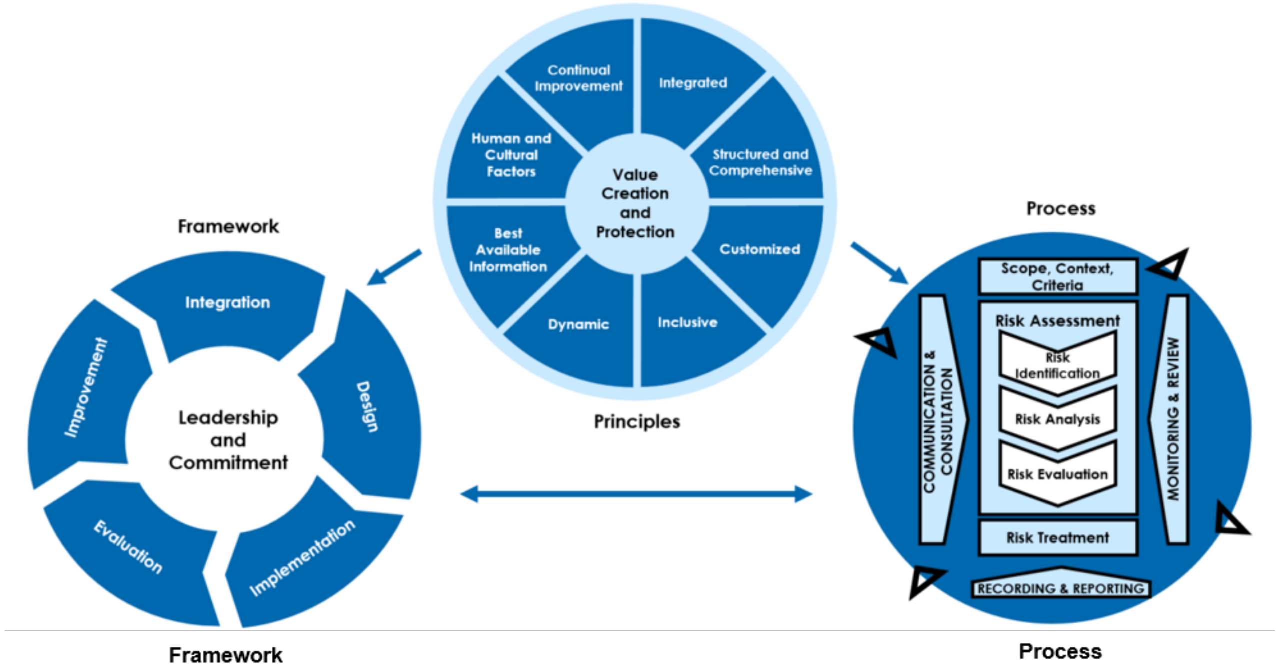
- Independent, non-governmental association with 167 national standards bodies as members
- Guidelines: Principles, framework, process for managing risk
- The "Wheels"

Primary ERM Guidance Documents

COSO:
Committee of Sponsoring Organizations

Source: COSO Internal Control Framework ©2013

ISO:
International Organization for Standardization



Primary ERM Guidance Documents

COSO:
Committee of Sponsoring Organizations

ISO:
International Organization for Standardization

Neither is specific to Higher Education

Best Approach to ERM: YOURO(wn)

- Your ERM Program has to work for your institution
- Only you know
  - What will get traction with your stakeholders
  - How to design your program to achieve your institution’s objectives
- ***Be advised by but not beholden to guidance documents***
- Blend best practices with your institution’s needs
- Don’t be pressured to “Keep Up with the Joneses”

Approach to Designing YOURO(wn) ERM Program

Key Components

- Governance structure
  - Roles and responsibilities
- Program Cycle
- Risk Assessment
- Mitigation Implementation and Assessment

> *Don't be afraid to iterate/adjust along the way*

It is critical to spend time designing and building this infrastructure – it will serve and support your ERM Program for a long time to come

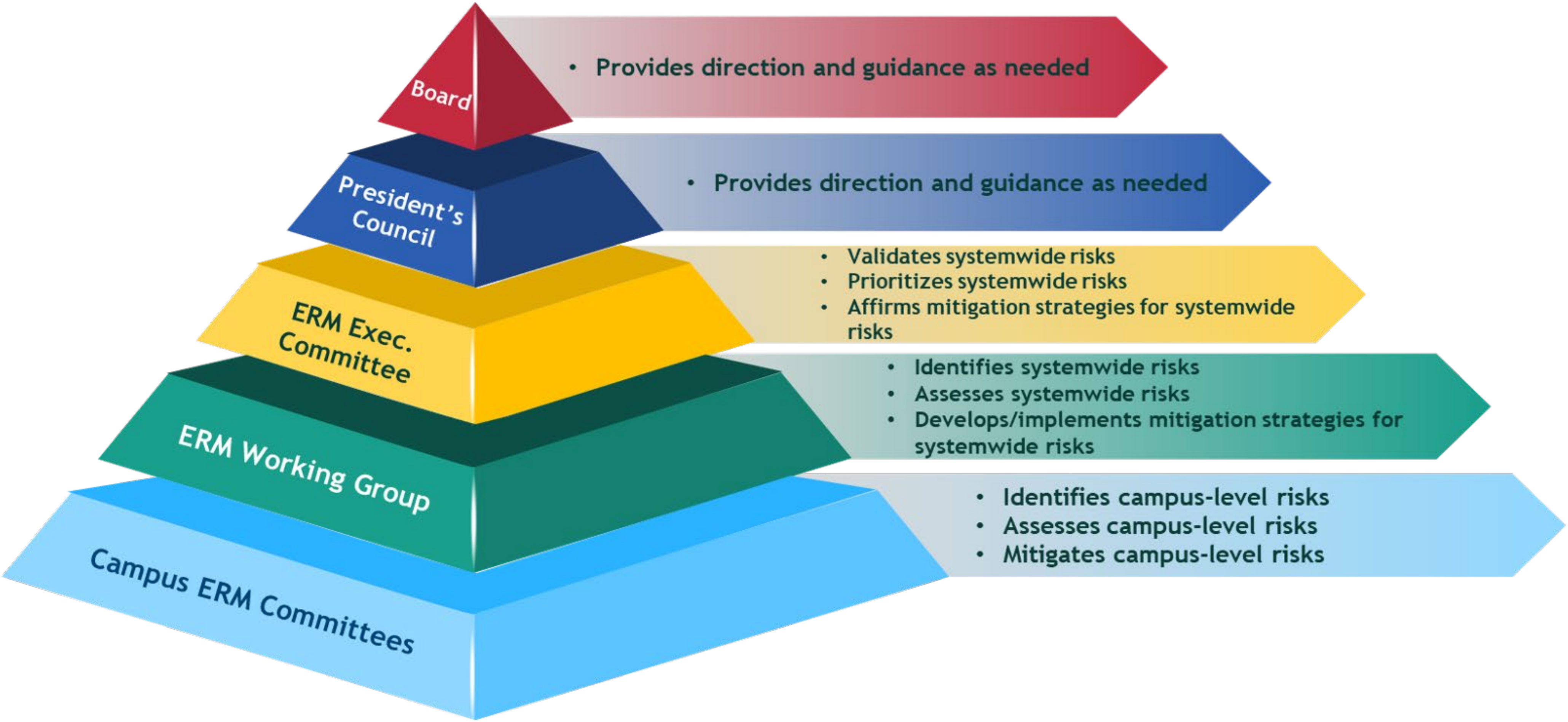
Governance Structure

- Varying approaches to governance structure
  - Committees, working groups, risk owners, etc.
  - Structure can consist of one or more of these
- Key component: Defining roles and responsibilities
  - Who is responsible (and not responsible) for doing what?
  - Who has (and does not have) authority for what?
- Cadence of meetings/discussions
  - Having regular touch points keeps your program stakeholders engaged

Governance Structure Considerations

- Who are your stakeholders?
- Who needs a consistent seat at the table?
  - Who can be brought to the table as needed?
- Who is the leadership voice?
- What do you want and need them to do?
  - Who conducts risk assessment?
  - Who prioritizes risk?

UMass Systemwide ERM Governance Structure



Program Cycle

- Program cycle
  - Risk identification and assessment
  - Mitigation identification and assessment
  - Monitoring and reporting
- Important to set cadence
  - Annually?
  - Biennially?
  - Other?

UMass ERM Program Two-Year Cycle

Risk Assessment Methodologies

Risk Assessment Methodology

- Risk Assessment is a key (and often the most cited) component of an ERM Program
- Purpose is to put risk into context for your institution
- Assesses risk exposure of the institution considering current environment, type of institution, geographic location of institution, etc.
- Key considerations for designing your risk assessment process:
  1. Mode
  2. Risk Exposure Factors
  3. Quantification/Calculation
  4. Risk Assessment Tools
  5. Use of Risk Assessment Data

Considerations for Designing and Conducting Your Risk Assessment

Choices for each consideration may influence other risk assessment considerations

1. Mode: *What mode of risk assessment do you want to use?*

Risk Assessment Mode	Pro	Con
Survey/Questionnaire	• Easy to manage • Reach large audience • Can be conducted at convenience of stakeholder	• Loss of context • Potential for lack of focus/engagement • Single perspective
Workshop/Meeting	• Cross-departmental/disciplinary conversation	• Viewed as a “special” program rather than something that is operational • Requires resources to coordinate and facilitate • Can’t ensure the right people are at the table (no shows, delegates, etc.)
Interview	• Opportunity for smaller conversations • Ability to build relationships	• Siloed discussion

Considerations for Designing and Conducting Your Risk Assessment

Choices for each consideration may influence other risk assessment considerations

2. Risk Exposure: *What aspects of your institution's risk exposure do you want to evaluate?*

A. Risk Exposure Type: Inherent or Controlled?

Risk Exposure Type	Pro	Con
Inherent Risk exposure ***without*** consideration of controls/mitigation strategies/risk treatments in place	• Do not need to have knowledge of controls to conduct assessment • Creates a baseline against which can measure mitigation strategies • Reduces likelihood of mitigation being inconsistently contemplated in risk assessment	• Sometimes difficult to contemplate (often requires facilitation of discussion) • Requires follow on assessment of mitigation strategies to understand residual risk
Controlled Risk exposure ***with*** consideration of controls/mitigation strategies/risk treatments in place	• Reflects residual risk • May not require follow on mitigation assessment	• Requires knowledge of controls and understanding of their effectiveness • May generate inconsistency in consideration of controls for all evaluated risks resulting in over- or under-assessment of risk exposure

Considerations for Designing and Conducting Your Risk Assessment

Choices for each consideration may influence other risk assessment considerations

2. **Risk Exposure:** ***What aspects of your institution's risk exposure do you want to evaluate?***

B. Risk Factors: Traditional

Risk Factor	Assessment
Likelihood	Will the risk impact your institution?
Consequence/Impact	Should the risk affect the institution, to what extent will the risk impact it?
Types of Impact *What types of impact are important to assess for your institution?*	– Operations – Financial – Legal – Compliance - Workforce - Reputation - Life Safety - Strategic - Other
Control Effectiveness	How well controlled is the risk?

Considerations for Designing and Conducting Your Risk Assessment

Choices for each consideration may influence other risk assessment considerations

2. Risk Exposure: ***What about your institution's risk exposure do you want to evaluate?***

B. Risk Factors: Non-Traditional

- Consider including additional risk factors in your risk assessment
  - Assessment of likelihood and consequence alone may result in many risks being calculated to have the same risk exposure/level
  - Additional risk factors enable you to amplify risks that may be of higher priority or greater concern
- Non-traditional factors may include:
  - Velocity: speed of onset of risk
  - Urgency: prioritization of risk
  - Other – something developed by you specifically for your institution

Considerations for Designing and Conducting Your Risk Assessment

Choices for each consideration may influence other risk assessment considerations

2. **Risk Exposure:** ***What about your institution's risk exposure do you want to evaluate?***

   C. Risk Assessment Responsibilities

   - Which components of your governance structure will assess which risk factors?
     - All assess all?
     - Certain subject matter experts assess certain factors?
     - Leadership vs management vs operational staff

Considerations for Designing and Conducting Your Risk Assessment

Choices for each consideration may influence other risk assessment considerations

3. Quantification/Calculation: *How will you calculate risk exposure?*

- Quantification
  - Each risk factor should have an associated quantification scale
  - Determine the range of the scale (1-3, 1-4, 1-5, etc.)
    - Recommend: Scale of 1 – 4
      - Forces assessors to lean one way or the other (rather than being neutral)
- Calculation
  - Risk assessment requires a calculation to quantify risk exposure
  - Calculation should include all assessed risk factors
  - Consider how risk factors should (or should not be) weighted

UMass ERM Program
Risk Factors and Quantification

Likelihood

- Scale of 1 – 4
- Assessed by ERM Working Group

Consequence

- 6 categories
  - Operations
  - Financial
  - Legal/Compliance
  - Workforce
  - Reputation
  - Life Safety
- Each category is a scale of 1 – 4
- Assessed by ERM Working Group

Urgency

- Scale of 1 – 3
- Assessed by ERM Executive Committee

UMass ERM Program
Risk Assessment Calculation

Likelihood Rating X **Sum of Consequence Category Ratings** X **Urgency Rating** = ***Inherent Risk Score***

Potential Risk Assessment with Controls Calculation

Likelihood X [Consequence* - Controls] = *Risk Score*

Likelihood X [Consequence* - Controls] X Urgency or Velocity or Other = *Risk Score*

*Some methodologies weight consequence categories

Considerations for Designing and Conducting Your Risk Assessment

Choices for each consideration may influence other risk assessment considerations

4. **Risk Assessment Tools:** ***How do you want to guide your risk assessment process?***

- Risk assessment tools (such as risk factor scales) are critical resources for the success of your risk assessment
- Tools like risk factor scales will:
  - Enable consistency in your risk assessment
  - Prevent risk assessors from "going too far down the rabbit hole"
  - Enable you to question an assessment that you believe may be too high/low
  - Support you in responding to any questions about a particular assessment rating

UMass ERM Program Likelihood Scale

What is the likelihood that the institution could experience this risk?
(select best option for risk/scenario)

Rating	Description		Probability of Occurrence		Rate of Occurrence
High	Certain or almost certain to occur **AND/OR** Expected in most circumstances	OR	More than 75%	OR	More than 2x per year
Medium	Likely to occur		50 to 75%		1 - 2 x per year
Low	Could possibly occur		25 to 50%		Once every 2 - 5 years
Negligible	Unlikely **AND/OR** Not expected to occur		Up to 25%		More than every 5+ years

UMass ERM Program Consequence Scale

How much would the University system be impacted by this risk in each of the categories?

Rating	Operations	Financial	Legal/ Compliance	Workforce	Reputation	Life Safety
High	Serious disruption to operations **AND/OR** Significant or complete service failure **AND/OR** Significant impacts to more than two campus	Loss of revenue (including state appropriation) or increase in expenses of greater than 5 percent or combination of both (est. greater than \$215M) **AND/OR** Need to use stabilization fund or line of credit **AND/OR** Impacts to all campuses	Substantial (\$5M+) regulatory fines and/or response costs **AND/OR** Increased state or federal regulatory scrutiny for additional campus(es) **AND/OR** Substantial audit findings **AND/OR** Litigation exposure with significant financial (\$10M+), reputational and/or precedent exposure **AND/OR** External agency sanctions such as debarment or civil and/or criminal liability	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	Negative national media coverage **AND/OR** Substantial ("viral") or long-term (mulituple days) negative social media activity **AND/OR** Tangible, long-term (more than one cycle) impacts to enrollment, philanthropy and/or public support **AND/OR** Widespread internal reaction	Fatality or permanent disability of one or more people
Medium	Moderate disruption to operations **AND/OR** Moderate disruption to service **AND/OR** Significant impact to one campus	Loss of revenue (including state appropriation) or cost increase of 2-5 percent, or combination of both (est. \$90M - \$215M) **AND/OR** Impacts to BDL or UMA or UMMS	Moderate (\$1M-\$5M) regulatory fines and/or response costs **AND/OR** Moderate audit findings **AND/OR** Litigation with moderate financial (\$5M - \$10M), reputational or precedent exposure **AND/OR** Externally-imposed restrictions or requirements placed on the University's operational activities	Difficulty recruiting or retaining employees with essential knowledge, skills and abilities **AND/OR** Work culture experiences frequent internal conflict or significant negativity	Negative regional (northeast) media coverage. **AND/OR** Moderate short-term negative social media activity **AND/OR** Tangible, short-term (one cycle) impacts to enrollment , philanthropy and/or public support **AND/OR** Significant internal reaction	Serious injury of one or more people
Low	Minor disruption to operations **AND/OR** Minor impact to service **AND/OR** Some impact to more than one campus	Between \$5M and up to a 2 percent revenue loss or expense increase or combination of both (est. \$5M to \$90M impact) **AND/OR** Impacts to up to two campuses	Regulatory fines (less than \$1M) and/or response costs **AND/OR** Minor audit findings **AND/OR** Litigation with minor financial (less than \$5M), reputational or precedent exposure **AND/OR** Internally-imposed consequences or requirements for formal corrective action	Minor impact to recruitment or retention **AND/OR** Work culture experiences some internal conflict or negativity	Negative local media coverage **AND/OR** Some short-term negative social media activity **AND/OR** Moderate on-campus/internal reaction	Minor injury to more than one person
Negligible	No Impact **OR** Annoyance	Less than \$5M impact	No to minimal impact	No to minimal impact to recruitment or retention **AND/OR** No to minimal impact on workplace culture	No to minor internal reaction	No impact or minor injury to individual

UMass ERM Program Consequence Scale

Detail on Operations and Reputation Consequence Categories

Rating	Operations	Reputation
High	Serious disruption to operations ***AND/OR*** Significant or complete service failure ***AND/OR*** Significant impacts to more than two campus	Negative national media coverage ***AND/OR*** Substantial ("viral") or long-term (multiple days) negative social media activity ***AND/OR*** Tangible, long-term (more than one cycle) impacts to enrollment, philanthropy and/or public support ***AND/OR*** Widespread internal reaction
Medium	Moderate disruption to operations ***AND/OR*** Moderate disruption to service ***AND/OR*** Significant impact to one campus	Negative regional (northeast) media coverage. **AND/OR** Moderate short-term negative social media activity **AND/OR** Tangible, short-term (one cycle) impacts to enrollment , philanthropy and/or public support **AND/OR** Significant internal reaction
Low	Minor disruption to operations ***AND/OR*** Minor impact to service ***AND/OR*** Some impact to more than one campus	Negative local media coverage **AND/OR** Some short-term negative social media activity **AND/OR** Moderate on-campus/internal reaction
Negligible	No Impact ***OR*** Annoyance	No to minor internal reaction

UMass ERM Program Consequence Scale

Detail on Operations and Reputation Consequence Categories

Rating	Operations	Reputation
High	Serious disruption to operations ***AND/OR*** Significant or complete service failure ***AND/OR*** Significant impacts to more than two campus	Negative national media coverage ***AND/OR*** Substantial ("viral") or long-term (multiple days) negative social media activity ***AND/OR*** Tangible, long-term (more than one cycle) impacts to enrollment, philanthropy and/or public support eaction
Medium	Moderate disruption to operati ***AND/OR*** Moderate disruption to servic ***AND/OR*** Significant impact to one camp	media coverage. ocial media activity nt , philanthropy and/or public support Significant internal reaction
Low	Minor disruption to operations ***AND/OR*** Minor impact to service ***AND/OR*** Some impact to more than one campus	Negative local media coverage **AND/OR** Some short-term negative social media activity **AND/OR** Moderate on-campus/internal reaction
Negligible	No Impact ***OR*** Annoyance	No to minor internal reaction

Defined Parameters

UMass ERM Program Consequence Scale

Detail on Operations and Reputation Consequence Categories

Rating	Operations	Reputation
High	Serious disruption to operations ***AND/OR*** Significant or complete [redacted] ***AND/OR*** Significant impacts to [redacted] campus [redacted]	Negative national media coverage ***AND/OR*** Substantial ("viral") or long-term (multiple days) negative social media activity [redacted]hilanthropy and/or public support
Medium	Moderate disruption [redacted] ***AND/OR*** Moderate disruption [redacted] ***AND/OR*** Significant impact to [redacted]	[redacted]erage. [redacted]ia activity [redacted]thropy and/or public support
Low	Minor disruption to [redacted] ***AND/OR*** Minor impact to service ***AND/OR*** Some impact to more than one campus	[redacted] **AND/OR** Some short-term negative social media activity **AND/OR** Moderate on-campus/internal reaction
Negligible	No Impact ***OR*** Annoyance	No to minor internal reaction

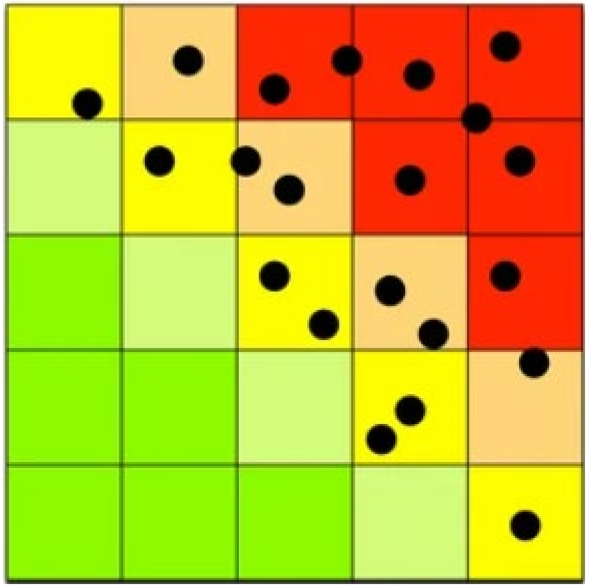
NO NUMBERS

Considerations for Designing and Conducting Your Risk Assessment

Choices for each consideration may influence other risk assessment considerations

5. **Using Risk Assessment Data:** ***How do you want to present your risk assessment results?***

- What is the story you want to tell?
- Options:
  - Heat Map
  - Risk Ranking
  - Other
- Risk Scores
  - To show or not to show?



Rank	Risk
1	Financial Sustainability
2	Enrollment
3	Research
4	Facilities and Deferred Maintenance
5	Diversity, Equity, Inclusion and Accessibility
6	Information Security
7	Student Health & Mental Health Support
8	Artificial Intelligence
9	Attract, Recruit, Retain Faculty and Staff
10	All-Hazards Planning and Response Capabilities

UMass FY2026 Systemwide Risk Registry

FY26 Rank	Risk
1	Financial Sustainability
2	Enrollment
3	Research
4	Facilities and Deferred Maintenance
5	Diversity, Equity, Inclusion and Accessibility
6	Information Security
7	Student Health & Mental Health Support
8	Artificial Intelligence
9	Attract, Recruit, Retain Faculty and Staff
10	All-Hazards Planning and Response Capabilities

FY26 Rank	Risk
11	International Activities
12	Data Privacy
13	Labor Relations
14	Athletic Regulations
15	Data Management
16	IT Disaster Recovery
17	Academic Quality and Standards
18	Vendor Risk Management
19	Title IX
20	Crisis Communication Coordination

FY26 Rank	Risk
21	Policies/Procedures Regarding Minors on Campus
22	Environmental and Public Health, & Safety Regulations
23	Sustainability
24	Fraud, Waste, Abuse
25	Continuity Planning
26	Multi-State Taxation
27	Employment Laws and Regulations
28	Alcohol and Substance Use Disorder
29	Oversight of Student Organizations

■ Priority Risks

Leverage ERM Data in Unique Ways

Leveraging data from the risk assessment on the Legal/Compliance risk factor, the UMass Systemwide ERM Program was able to provide information on the University's top compliance risks to the Executive Compliance Committee.

FY24 Risks* Ranked Based on Highest Legal/Compliance Exposure

**Top 10 FY24 systemwide risks are bolded/italicized*

High

- ***Information Security***
- ***Research***
- ***Diversity, Equity, Inclusion & Accessibility***
- Employment Laws & Regulations
- Academic Quality & Standards

Medium

- ***Facilities & Deferred Maintenance***
- ***Student Health & Mental Health Support***
- ***Artificial Intelligence***
- ***International Activities***
- Information Privacy
- All Hazards Plans & Response Cap.
- Vendor Risk Management
- Sexual Assault Policies & Response Procedures
- NCAA Regulations
- Env. Health, Pub. Health, & Safety Regs
- Alcohol and Substance Abuse
- Fraud, Waste, and Abuse
- Multi-State Payroll Tax
- Multi-State Business Tax
- Policies/Procedures Minors on Campus

Low/Negligible

- ***Enrollment***
- ***Financial Sustainability***
- ***Attract, Recruit, Retain Faculty/Staff***
- Labor Relations
- Data Management
- IT Disaster Recovery
- Continuity Planning
- Crisis Communications Coord.
- Uninsured Loss
- Oversight of Student Organizations

Resources

- URMIA
  - ERM Roundtable Community
  - Library
  - Webinars and Podcasts
  - Conferences
- Peers and Colleagues
  - Brainstorm
  - Talk through successes and challenges
  - Borrow ideas

Mitigation Assessment Methodologies

Mitigation Strategies

- A mitigation strategy is an activity, initiative or program that either happens to or is intentionally designed to reduce risk
- Those unfamiliar with ERM may think of mitigation as a brand new strategy developed in response to a specific risk
- However, mitigation strategies are being implemented all the time at your institution, such as:
  - Operational activities
  - Programs
  - Policies
  - EVERYONE at your institution is a risk manager!
- Sometimes these operational activities need a booster or focused initiative to supplement them (mitigation action plans)

Mitigation Assessment Methodologies

How to do you want to measure risk reduction?

A. Measure independent mitigation effectiveness factors

B. Measure mitigation factors aligned with risk assessment risk factors

Mitigation Assessment Methodologies

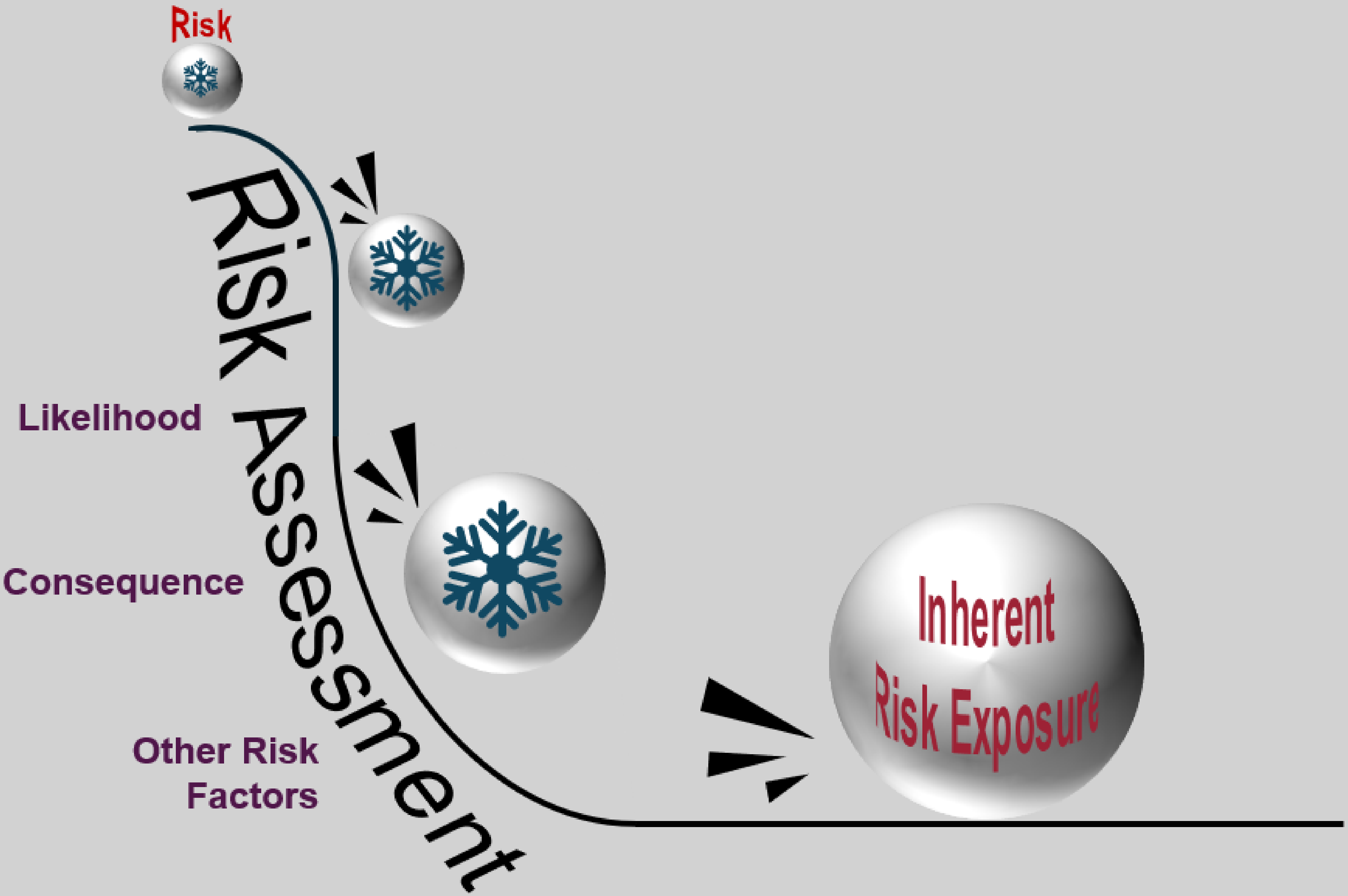
A. Measure independent mitigation effectiveness factors

1. Factors can include measures for
   - Resources needed
   - Cost savings
   - Efficiency
   - Resilience
   - Alignment with strategic goals/objectives
2. Creates an evaluation independent of your risk assessment

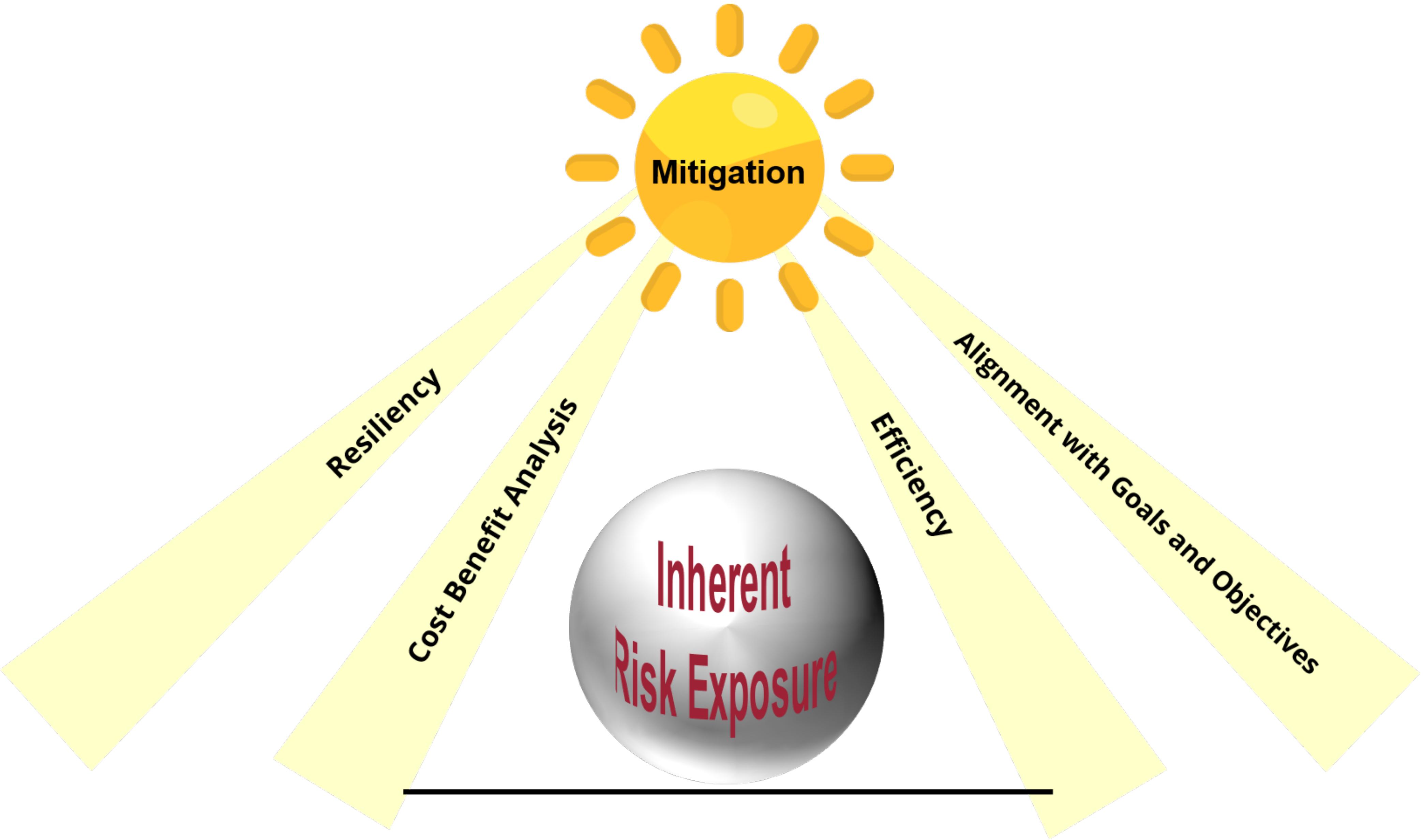
Mitigation Assessment Methodologies

B. Measure mitigation factors aligned with risk assessment risk factors
   1. Evaluate same factors as risk assessment
   2. Determine how much each risk factor is reduced as a result of the mitigation strategy

Assessment of Risk Exposure



Independent Mitigation Assessment



Correlation of Risk Assessment and Mitigation Assessment

Mitigation Assessment Considerations

- Degree of mitigation strategy implementation
  - Full or partial “credit” for impact
- Scope of mitigation strategy
  - Benefits a particular college, department, program or full institution
- Degree of effectiveness
  - Scale (significant, moderate, neutral, adverse)
- Impact of single strategy and/or all strategies

Mitigation Assessment Results: Facilities & Deferred Maintenance Risk (FY22)

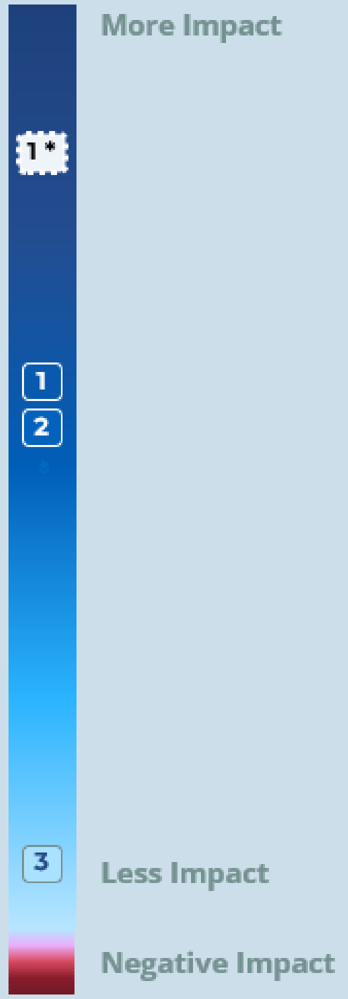
Rank	Mitigation Strategy as of June 30, 2023	Implementation Status
1	Reaching/Maintaining Keep Up Targets	Partially*
	Reaching/Maintaining Catch Up Targets	Partially*
2	Annual Update of Campus Deferred Maintenance (Gordian)	Fully
	Capital Policy & Standards	Fully
	Reporting – Biannual Capital Plan	Fully
	Reporting – Quarterly Capital Reporting Including Keep Up and Catch Up	Partially
3	Tracking Spending Against DCAMM Contracts	Partially

** The impact of these strategies would be significantly greater if these strategies were fully implemented. See scale.*

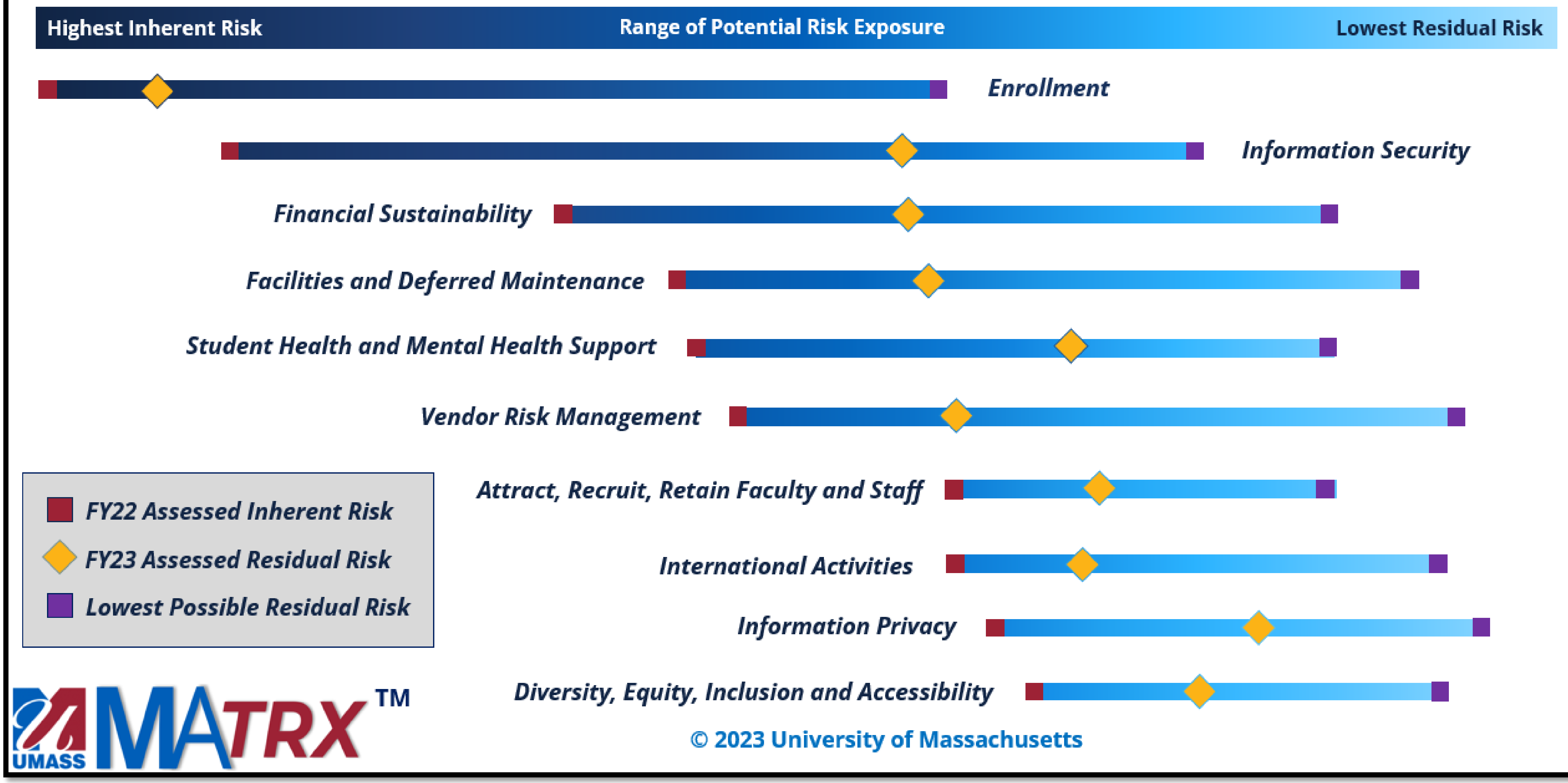
UMASS MATRX™

7 Strategies

Scale: Assessed Systemwide Impact of Mitigation Strategy by Rank



FY22 Risks: Movement in Reducing Risk Exposure



Key Take-Aways

- ERM Methodologies should be designed to serve your institution
  - Enables your ERM Program to be dynamic and tangible rather than a check the box exercise
- Leverage best practices/guidance documents, but adjust to meet the needs of your institution
- Make adjustments to your program as you learn
- You don’t necessarily need fancy/expensive platforms to be successful

Questions?

- **Christine Packard**
- Assistant Vice President, Enterprise Risk Management
- University of Massachusetts
- cpackard@umassp.edu