

Three Lines of Defense



PRESENTED BY:

Trisha Burnett

WITH THE SUPPORT OF:

Amy Smith

Katie Bumgardner

Learning Objectives



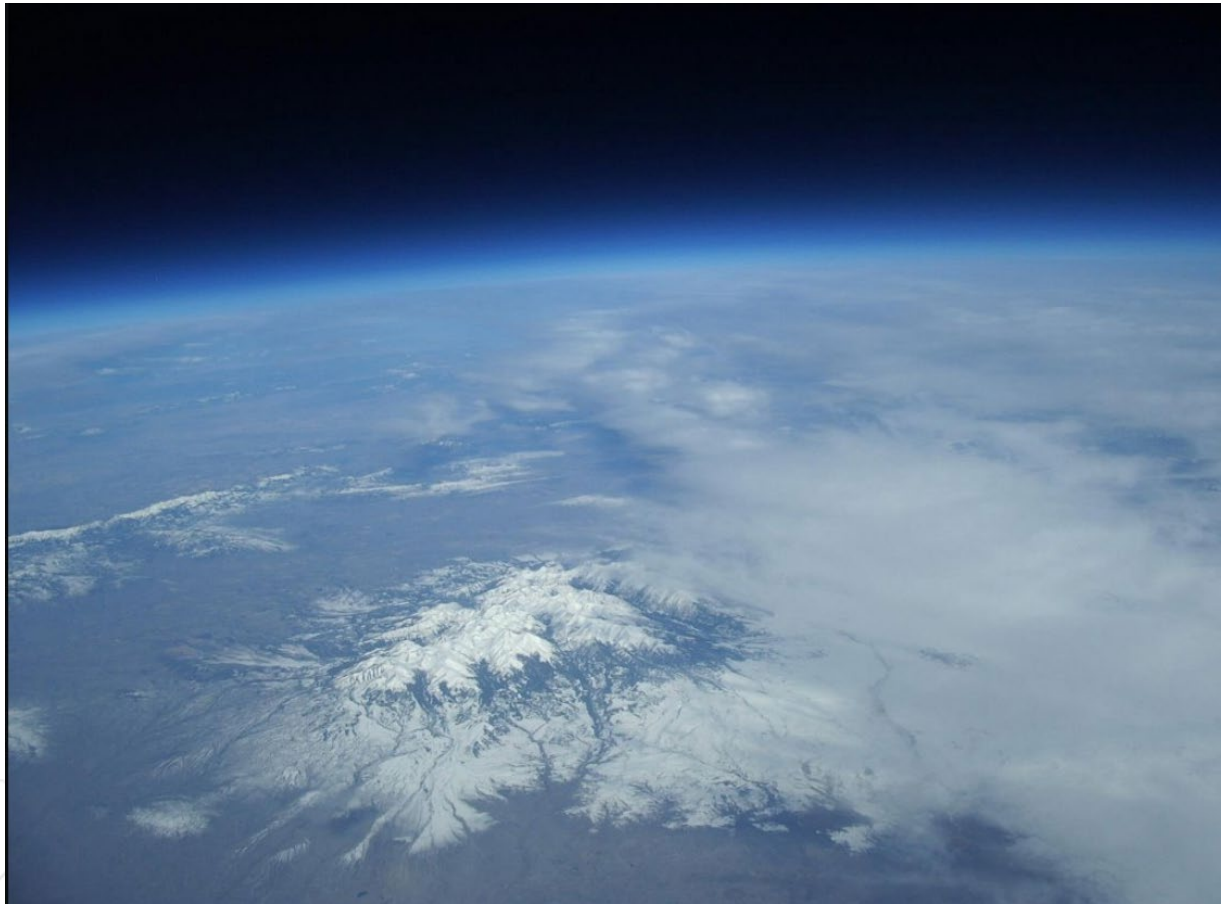
- Organizational Overview
- What is Risk, Really?
- What is Resiliency?
- Three Lines of Defense Model
- Internal Audit & Risk Management

Organizational Overview



UNIVERSITY OF
OREGON

Organizational Overview



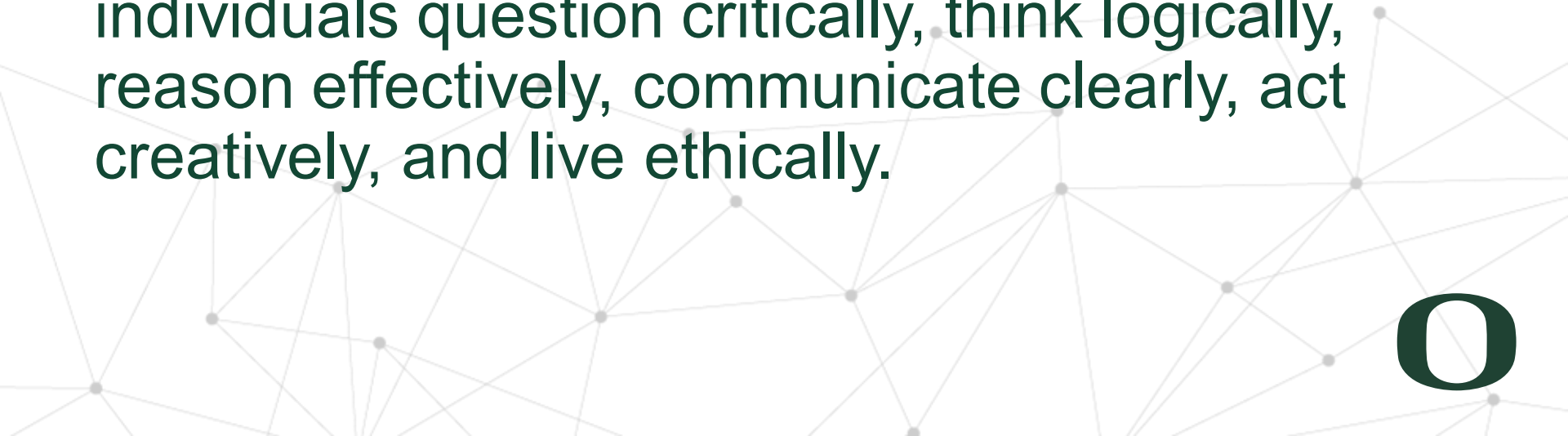
O

Organizational Overview



Mission

The University of Oregon is a comprehensive public research university committed to exceptional teaching, discovery, and service. We work at a human scale to generate big ideas. As a community of scholars, we help individuals question critically, think logically, reason effectively, communicate clearly, act creatively, and live ethically.



Organizational Overview



Purpose

We strive for excellence in teaching, research, artistic expression, and the generation, dissemination, preservation, and application of knowledge. We are devoted to educating the whole person, and to fostering the next generation of transformational leaders and informed participants in the global community. Through these pursuits, we enhance the social, cultural, physical, and economic wellbeing of our students, Oregon, the nation, and the world.



Organizational Overview



Vision

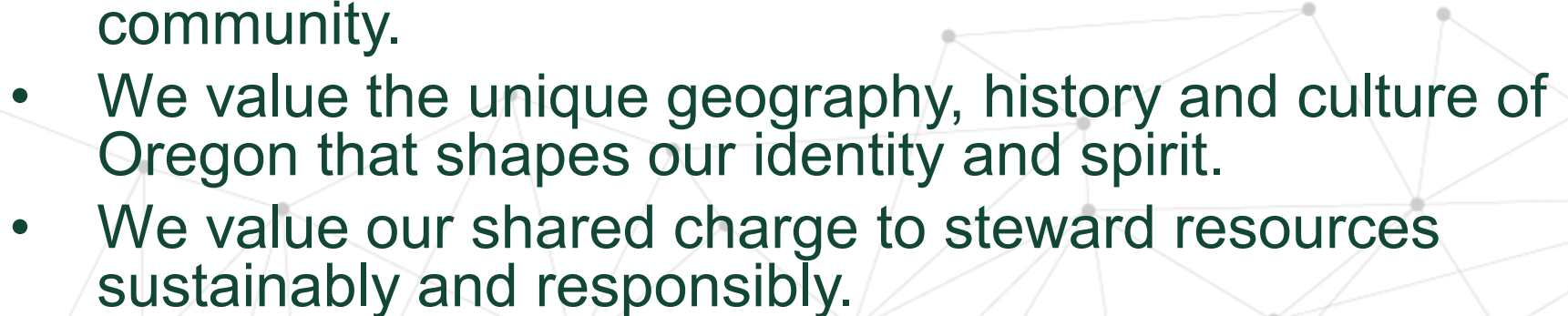
We aspire to be a preeminent and innovative public research university encompassing the humanities and arts, the natural and social sciences, and the professions. We seek to enrich the human condition through collaboration, teaching, mentoring, scholarship, experiential learning, creative inquiry, scientific discovery, outreach, and public service.



Organizational Overview



Values

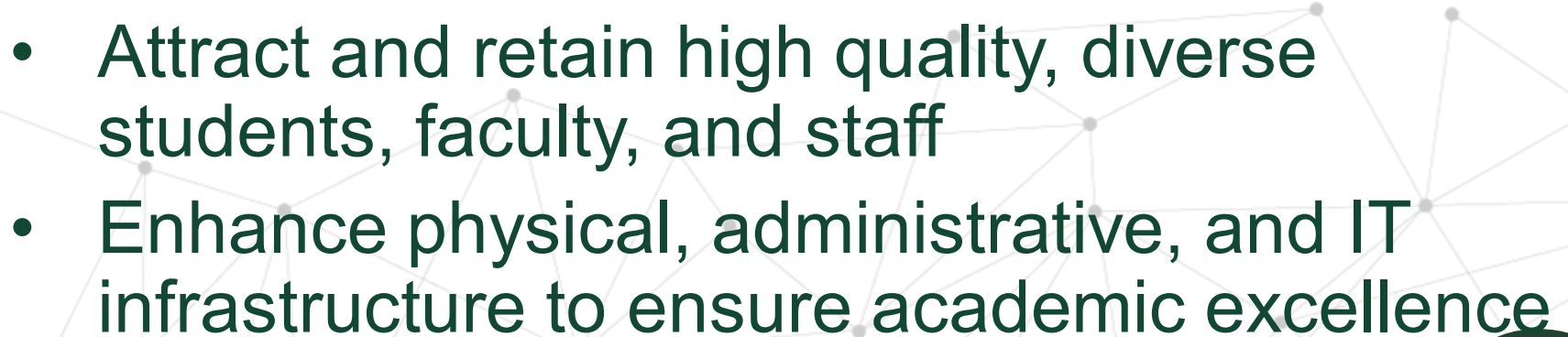
- We value the passions, aspirations, individuality, and success of the students, faculty, and staff who work and learn here.
 - We value academic freedom, creative expression, and intellectual discourse.
 - We value our diversity and seek to foster equity and inclusion in a welcoming, safe, and respectful community.
 - We value the unique geography, history and culture of Oregon that shapes our identity and spirit.
 - We value our shared charge to steward resources sustainably and responsibly.
- 



Organizational Overview



Objectives

- Promote and enhance student access, retention, and success
 - Enhance the impact of research, scholarship, creative inquiry, and graduate education
 - Attract and retain high quality, diverse students, faculty, and staff
 - Enhance physical, administrative, and IT infrastructure to ensure academic excellence
- 

O

Organizational Overview



Strategy

EXCELLENCE

2016-2021 strategic framework for the University of Oregon



O

Organizational Overview



Implementation

- Design operations to meet objectives
- Hire personnel to perform the operations
- Measure to ensure objectives are being met
- Re-evaluate objectives, operations, personnel, and metrics



O



Did We Leave Something Out?



O

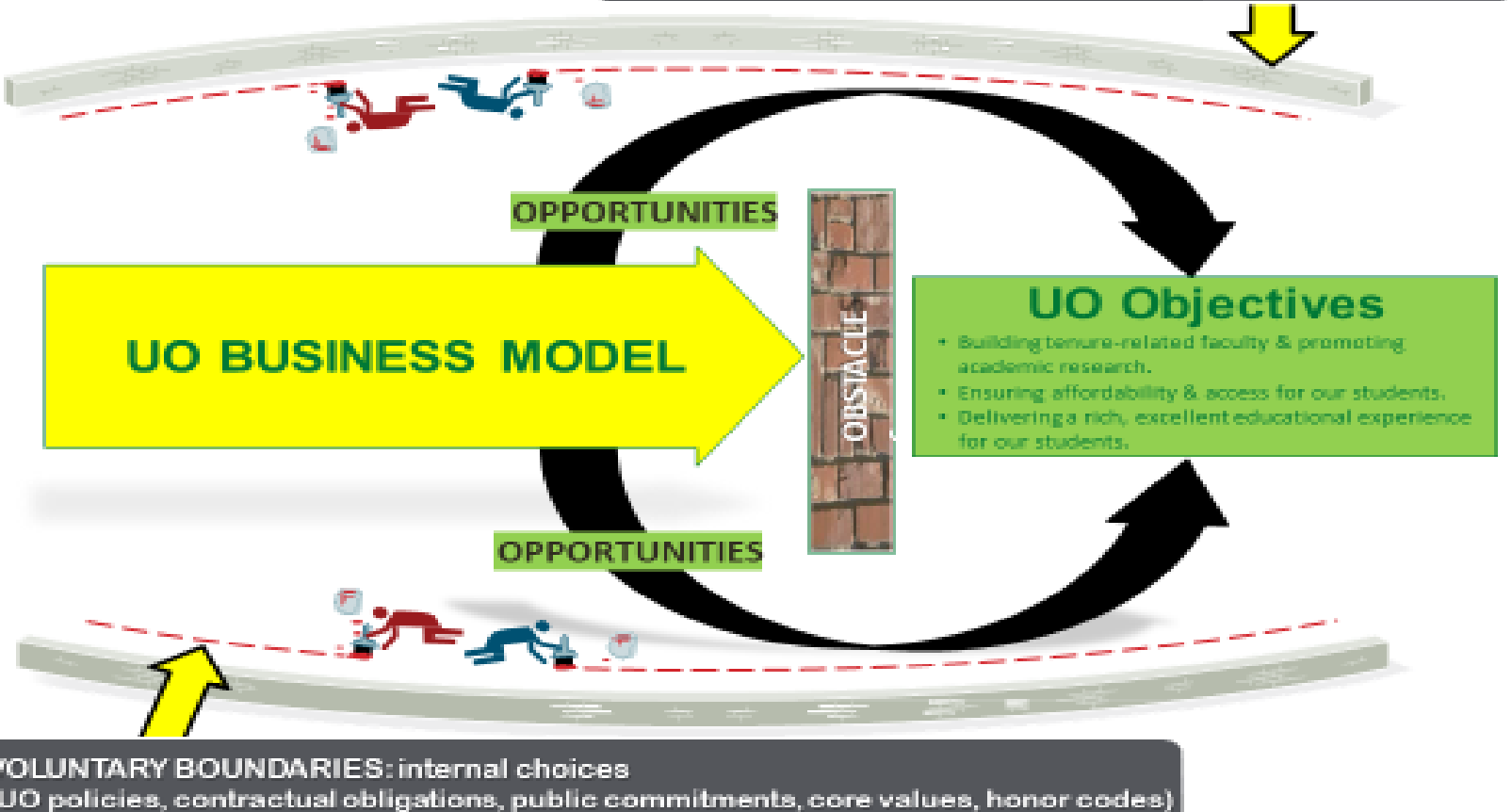
What is Risk, Really?



What is Risk, Really?

The BIG Picture

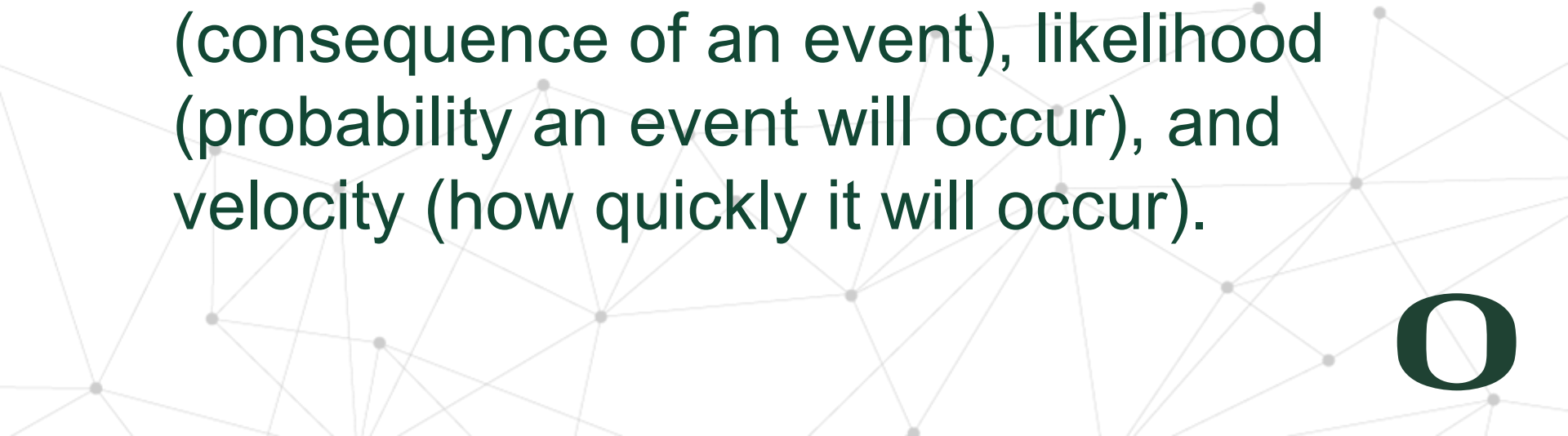
MANDATED BOUNDARIES: external forces
(federal, state, local laws and regulations)



What is Risk, Really?



Risk Definition

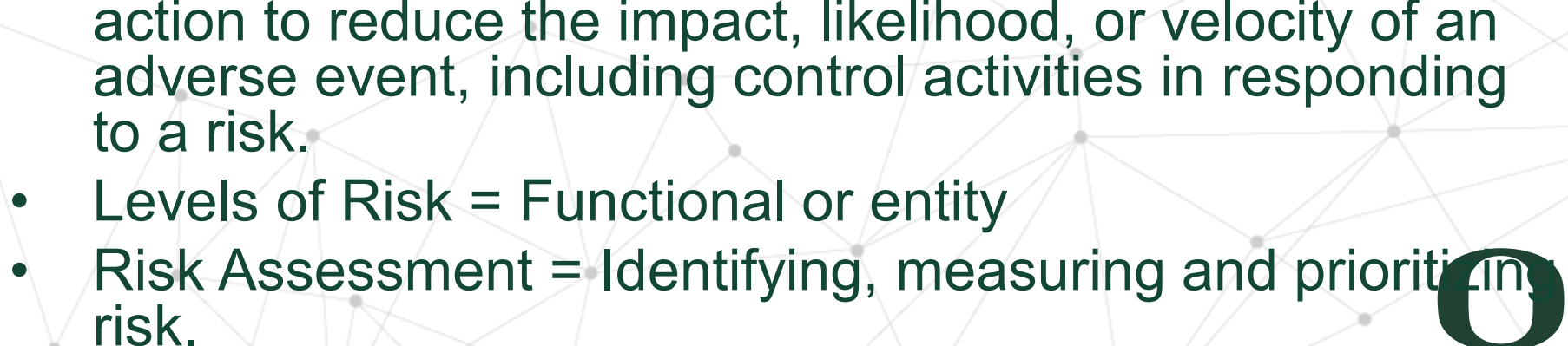
- Possibility of an event occurring that will have an impact on the achievement of objectives.
 - Measured in terms of impact (consequence of an event), likelihood (probability an event will occur), and velocity (how quickly it will occur).
- 

O

What is Risk, Really?



Risk Terms

- Risk Appetite = The desired risk the University is willing to accept in pursuit of its mission.
 - Risk Tolerance = Acceptable levels of variation relative to the achievement of specific objectives.
 - Inherent Risk = Derived from the nature of the risk
 - Risk Response = Actions taken to manage risk.
 - Residual Risk = Remaining risk after management takes action to reduce the impact, likelihood, or velocity of an adverse event, including control activities in responding to a risk.
 - Levels of Risk = Functional or entity
 - Risk Assessment = Identifying, measuring and prioritizing risk.
- 
- 

What is Risk, Really?

Risk Types

- Strategic - The possibility of an event or condition occurring that directly impacts the University's ability to fulfill key priorities, including its prosperity and existence in the long term.
- Financial - The possibility of an event or condition occurring that influences the University's ability to achieve its objectives related to financing operations, cash flows, and related transactions operations of the University, including the reliability of reporting.
- Compliance - The possibility of an event or condition occurring that influences the University's ability to achieve its objectives by conforming to value-adding internal policies, guidelines, commitments; or external requirements of governing bodies.



What is Risk, Really?



Risk Types

- Operational - The possibility of an event or condition occurring that influences the University's ability to achieve its objectives through the regular operations, such as failed internal processes, people and systems, or other events that impact the effective or efficient use of University resources.
- Reputational - The possibility of an event or condition occurring that influences the University's ability to achieve its objectives as a result of events that harm its reputation.
- Fraud - The possibility of an event or condition occurring that influences the University's ability to achieve its objectives as a result of fraud.

What is Risk, Really?



What is Resiliency, Really?



What is Resiliency, Really?



Striving for proficiency in three areas:

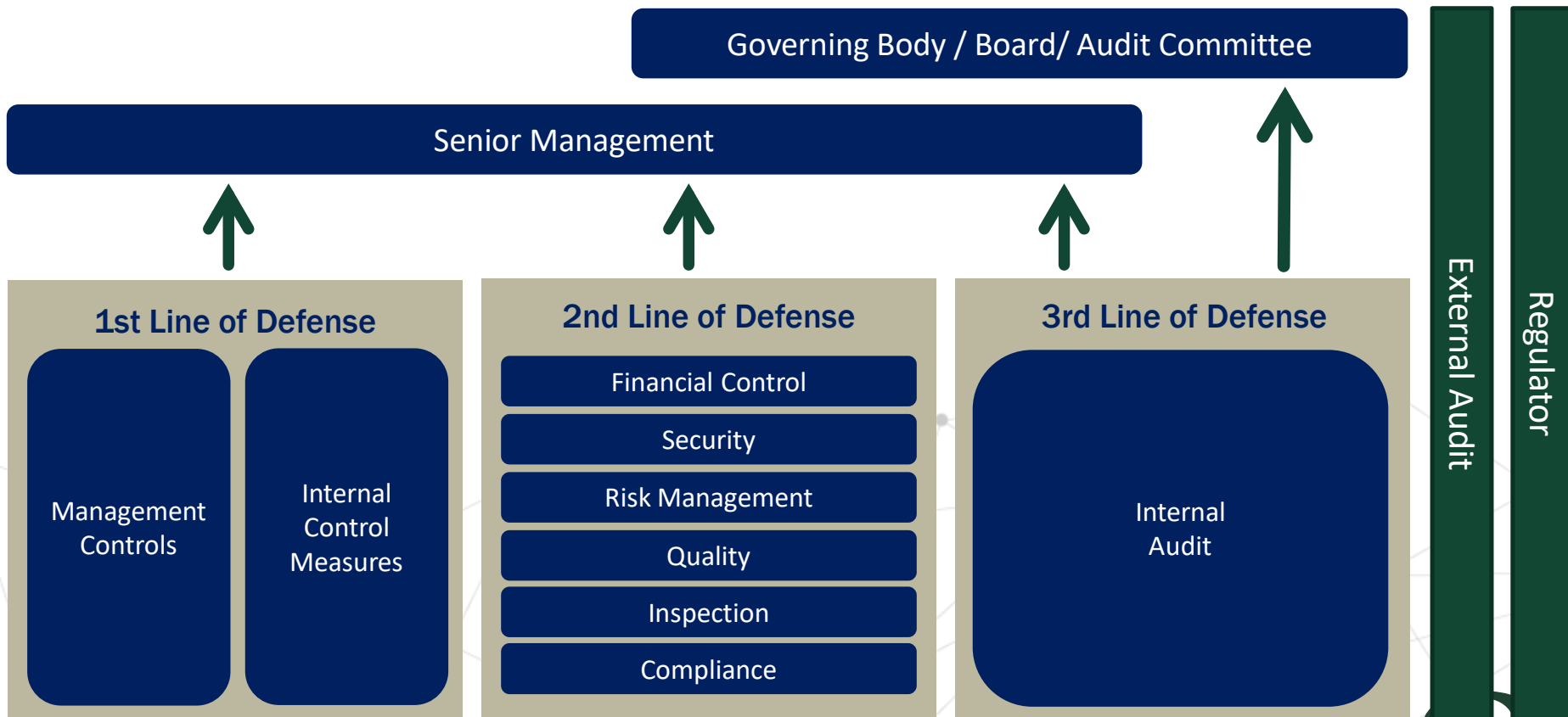
- **Leadership and culture** which stimulate the ability to stay aware, stay engaged, adapt, and make good decisions
- **Well-developed networks** which help us use partnerships to leverage assets efficiently
- **Change readiness** which requires active planning, proactive thinking, and innovative problem-solving



The Three Lines of Defense

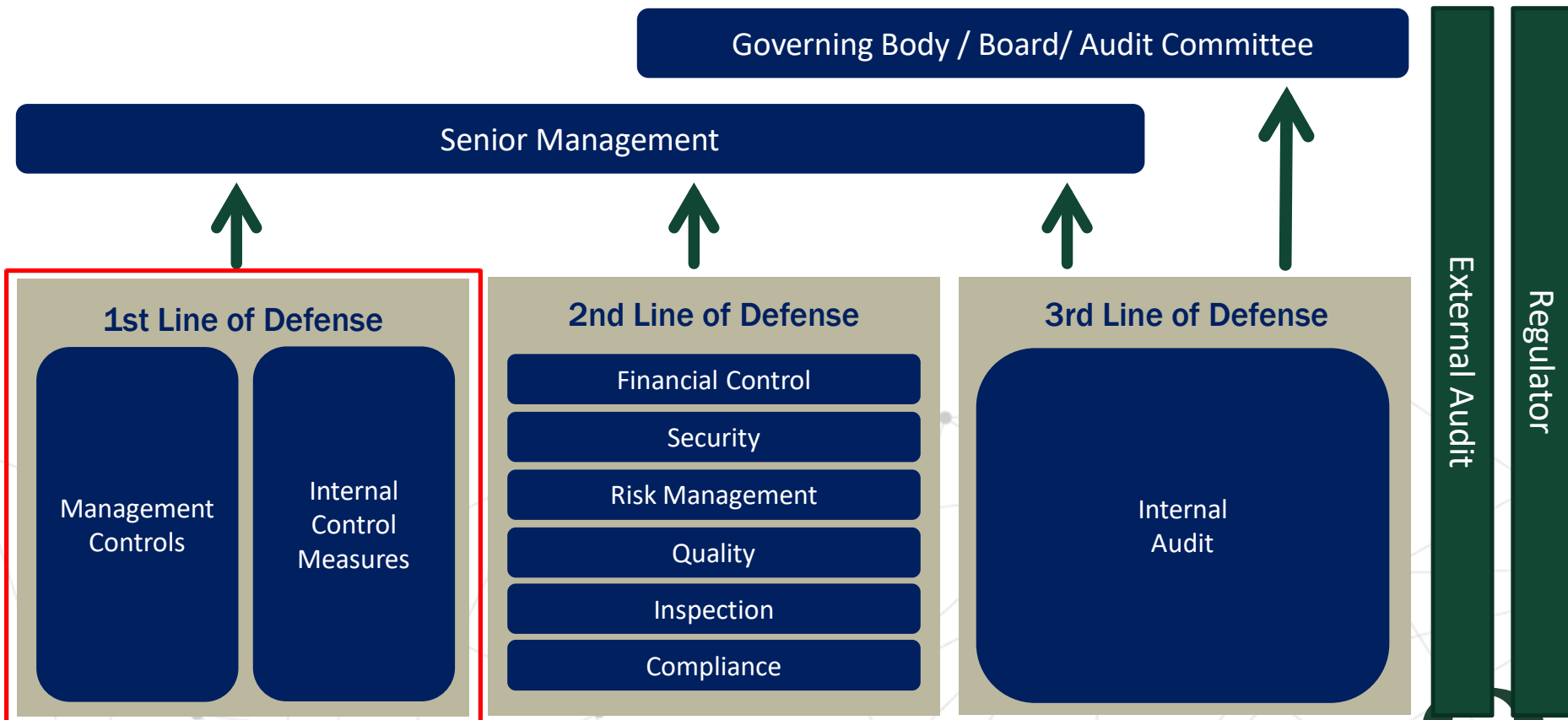


The Three Lines of Defense Model



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

The Three Lines of Defense Model



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

The Three Lines of Defense Model



1st Line

Operational management naturally serves as the first line of defense because controls are designed into systems and processes under the guidance of operational management.

There should be adequate oversight processes in place to ensure compliance and to highlight control breakdown, inadequate processes, and unexpected events

The majority of fraud is detected at the first line:

- Reported to or discovered by management
- Reported to Internal Audit
- Reported to fraud and ethics hotline
 - Website: www.uoregon.ethicspoint.com
 - Toll Free: 1-855-388-2710



The Three Lines of Defense Model



Operational Management Responsibilities

- Identifying, assessing, controlling, and mitigating risks.
- Guiding the development and implementation of university policies.
- Designing, implementing, and maintaining written internal procedures.
- Maintaining effective internal controls.
- Implementing corrective actions to address process and control deficiencies.
- Ensuring that activities are consistent with goals and objectives.

The Three Lines of Defense Model

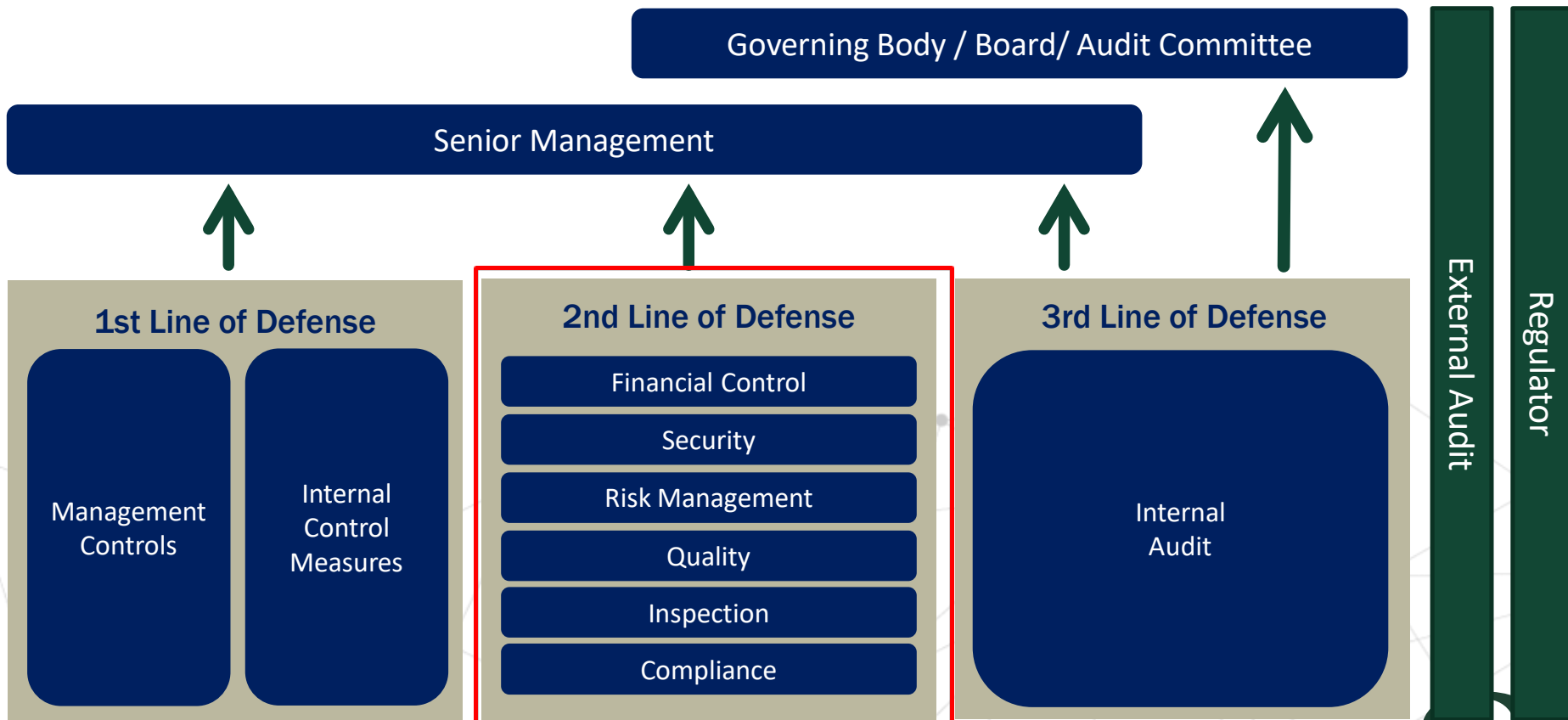


Implementation

- **Design operations to meet objectives**
 - **Hire personnel to perform the operations**
 - Measure to ensure objectives are being met
 - Re-evaluate objectives, operations, personnel, and metrics
- 

O

The Three Lines of Defense Model





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

The Three Lines of Defense Model



2nd Line

- Established by leadership to help build or monitor the first line-of-defense controls – but does not set the risk appetite
 - Also ensures the first line is properly designed, in place, and operating as intended
 - Second line typically includes:
 - A risk management function (e.g. Enterprise Risk Services, Strategic Enterprise Risk Management and Compliance Committee)
 - A compliance function (e.g. Athletics Compliance Office, Research Compliance Services, HIPAA Compliance Officer, IT Security Officer)
 - A controllership function (e.g. Business Affairs Office)
 - Certain functions operate at the university-wide level; others are only relevant on a departmental level
 - May intervene directly in modifying and developing internal control and risk systems; therefore cannot offer truly independent analyses to governing bodies regarding risk management and internal control
- 
- 

The Three Lines of Defense Model



Risk Management/Compliance Function Responsibilities


- Supporting management policies, defining who is responsible, and setting goals for implementing
- Providing risk management framework
- Identifying known and emerging issues
- Identifying shifts in the organization's chosen risk appetite
- Assisting management in developing processes and controls to manage the risks, issues, and shifts identified
- Identifying opportunities and areas for improving existing processes
- Provide guidance and training on risk management processes



The Three Lines of Defense Model

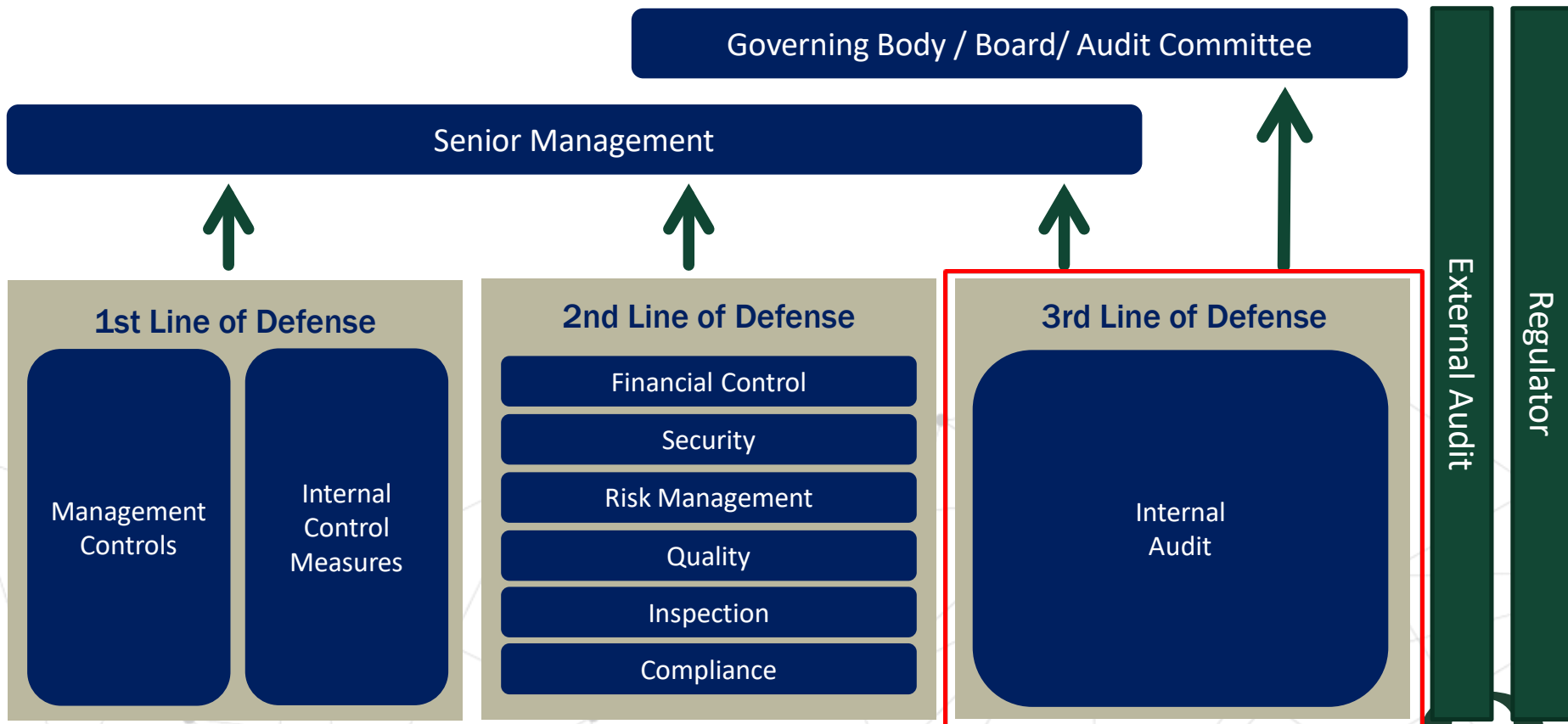


Implementation

- Design operations to meet objectives
 - Hire personnel to perform the operations
 - **Measure to ensure objectives are being met**
 - **Re-evaluate objectives, operations, personnel, and metrics**
- 

O

The Three Lines of Defense Model



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

The Three Lines of Defense Model



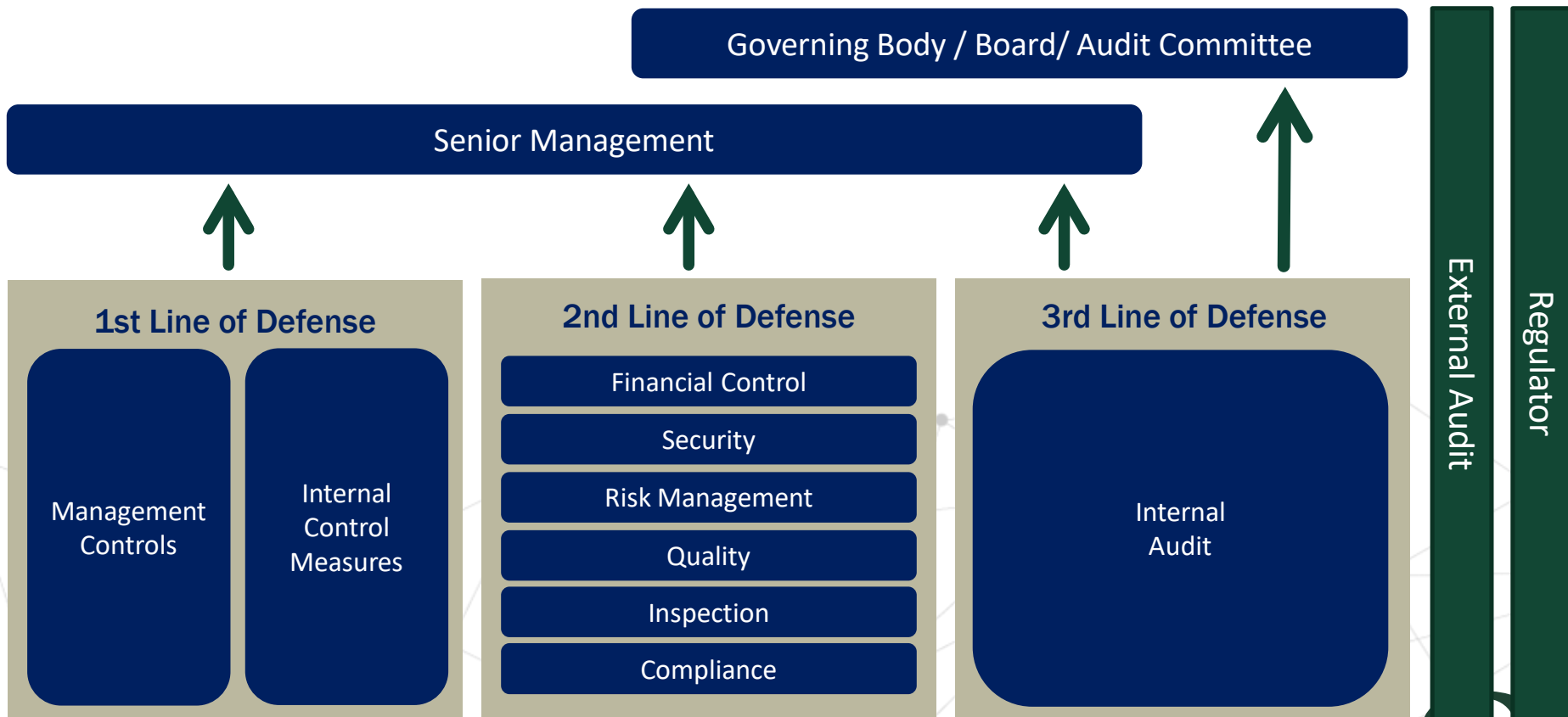
3rd Line

- Internal Audit provides the Board and Senior Management with comprehensive assurance based on the highest level of independence and objectivity within the organization not available in the second line of defense.
- Internal Audit provides assurance on the effectiveness of governance, risk management, and internal controls. This includes reporting on the performance of the first and second lines of defense in risk management and control objectives.

Internal Audit & Risk Management



The Three Lines of Defense Model



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

Questions?

