The Institute of Internal Auditors

The IIA: North American Board Chairman Update

Benito Ybarra
CIA
Chairman – North American Board
The Institute of Internal Auditors

About The Institute of Internal Auditors

The internal audit profession's most widely recognized advocate, educator, and provider of standards, guidance, and certifications.

Established in 1941, The IIA today serves more than 200,000 members from more than 170 countries and territories.

Data as of Dec. 31, 2018

The Global IIA

200,000+ **Members**

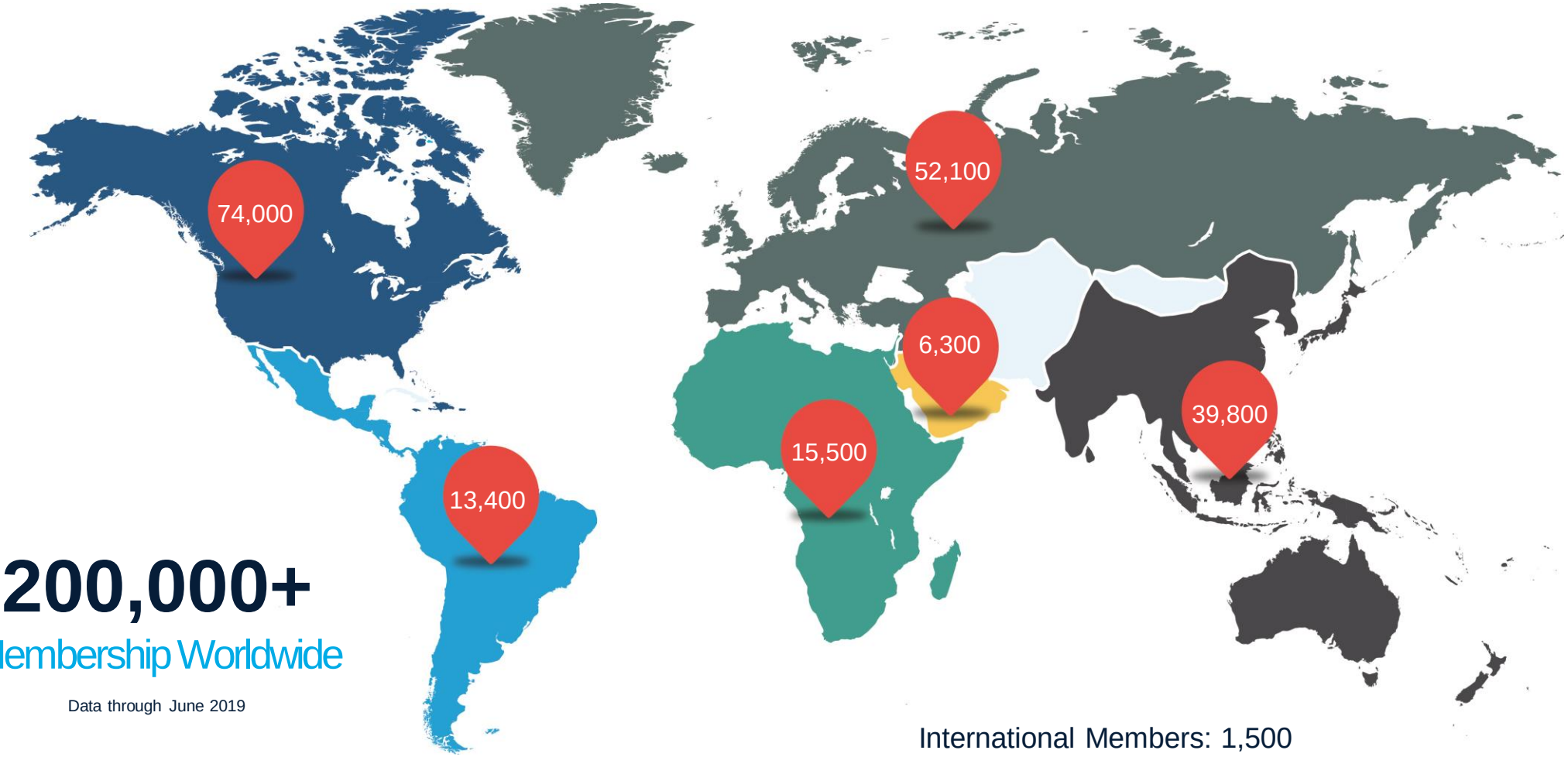
170+ **Countries & Territories**

110 **International Affiliates**

160+ **North American Chapters**

Data through June 2019

Membership by Region



200,000+

Membership Worldwide

Data through June 2019

International Members: 1,500

Certified Internal Auditor

IIA by the Numbers:

Overall Certified Internal Auditors

Certified Internal Auditor®

CIA certifications through August 2019

Chairman of the North American Board

CHAIR'S ROLE

Provide direction for The IIA's strategic plan in North America.

NORTH AMERICAN BOARD'S MISSION

To ensure that volunteer and staff activities of The IIA adequately address the needs of the North American membership through continuous monitoring of programs, services and budgets relating to North American members and chapters.

COMPOSITION

10 directors, including one member from Canada.
IIA President and CEO serves as ex-officio member.

IIA North America Strategic Goals 2019 - 2023

- **Stronger Profession:** The Internal audit profession is strengthened, through advocacy, by enabling IIA members to engage stakeholders and provide insight on risks impacting organizations.

- **Competent Professionals:** Members are competent, confident and courageous to deliver on stakeholder expectations and demonstrate the value of our profession.

- **Sustainable Value:** Value is delivered to IIA members through a sustainable operating model.

Agenda

- *OnRisk*
- Three Lines of Defense
- Board Duty of Oversight
- Step Forward – 2019/2020 NA Chairman Theme

OnRisk 2020

A guide to understanding, aligning, and optimizing risk

Methodology

Surveys and Interviews

- Unique approach brings together views from various perspectives
- 90 in-depth interviews divided equally among
  - Board
  - Executive Management
  - CAEs
- 600+ responses to a CAE survey

Overview

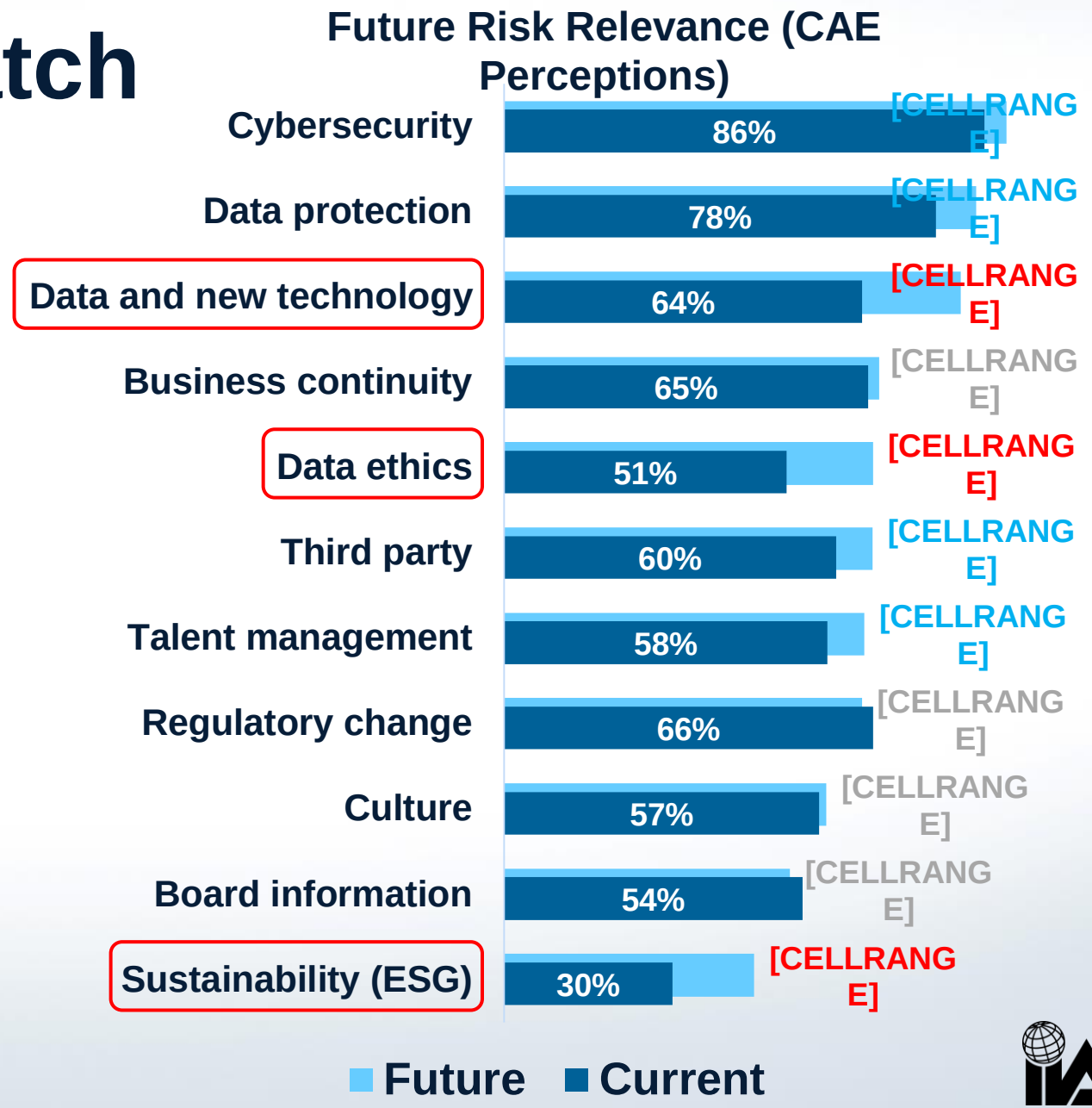
Top Risks for 2020 and Beyond

- Cybersecurity
- Data protection
- Regulatory change
- Business continuity/crisis response
- Data and new technology
- Third party
- Talent management
- Culture
- Board information
- Data ethics
- Sustainability (ESG)

Three Risks to Watch

Top 3 Future Risks

- Data and new technology
- Data ethics
- Sustainability (ESG)



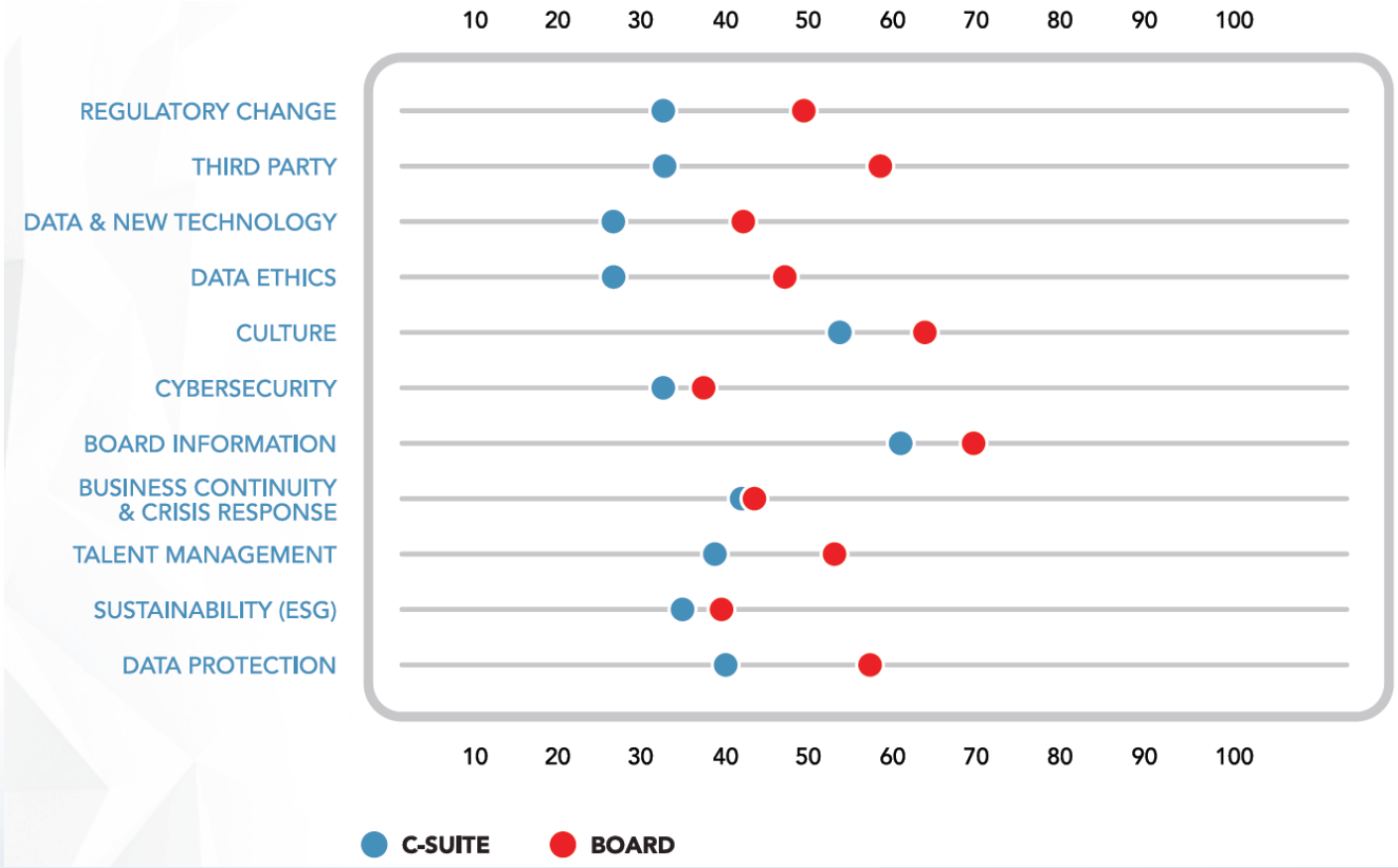
OnRisk 2020 CAE survey. Percentage of CAEs who rated the risk relevance at the top 2 levels on a 7-point scale. *n* = 630.

Board Overconfidence

Ability to Address Risk

- Board members consistently rate their organizations' capability to manage key risks higher than executive management does.

Organizational Risk Capability: C-suite and Board Perceptions



OnRisk 2020 qualitative interviews. How capable is your company when it comes to handling the following risks? Percentage who rated capability at the top 2 levels on a 7-point scale. *n* = 83.

The Risks

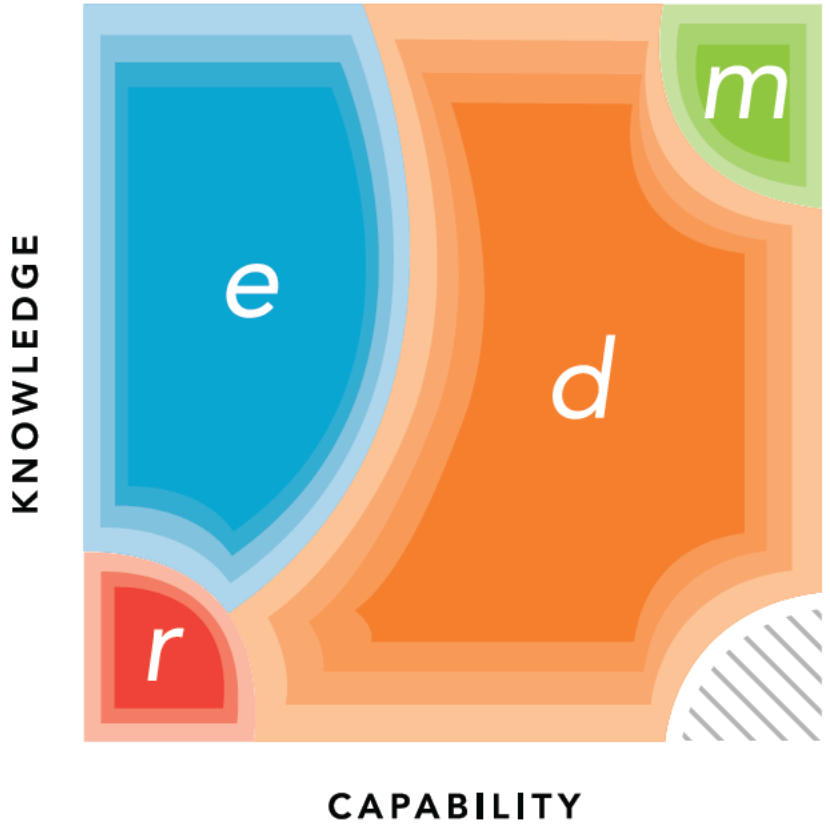
Top risks for 2020 and beyond

www.theiia.org/OnRisk

Risk Stages Model

Risk Stages

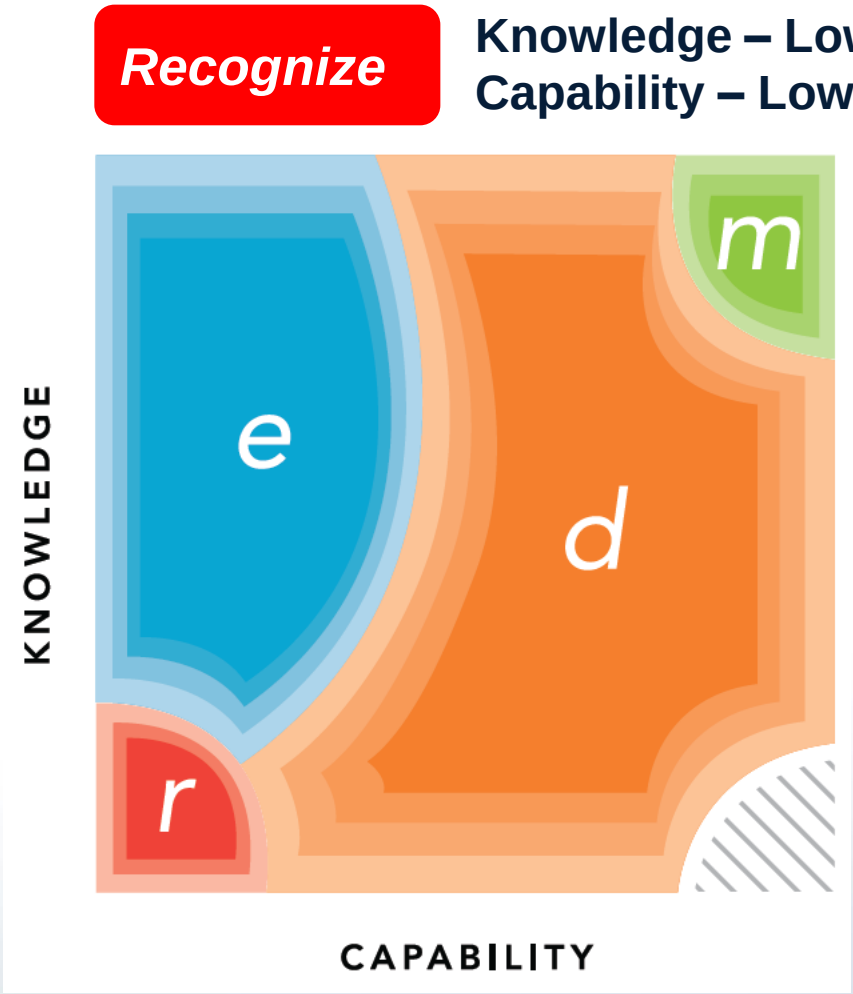
Recognize	**Knowledge – Low** **Capability – Low**
Explore	**Knowledge – Mid to High** **Capability – Low**
Develop	**Knowledge – Low to High** **Capability – Mid to High**
Maintain	**Knowledge – High** **Capability – High**



Recognize Stage

Emerging Risk

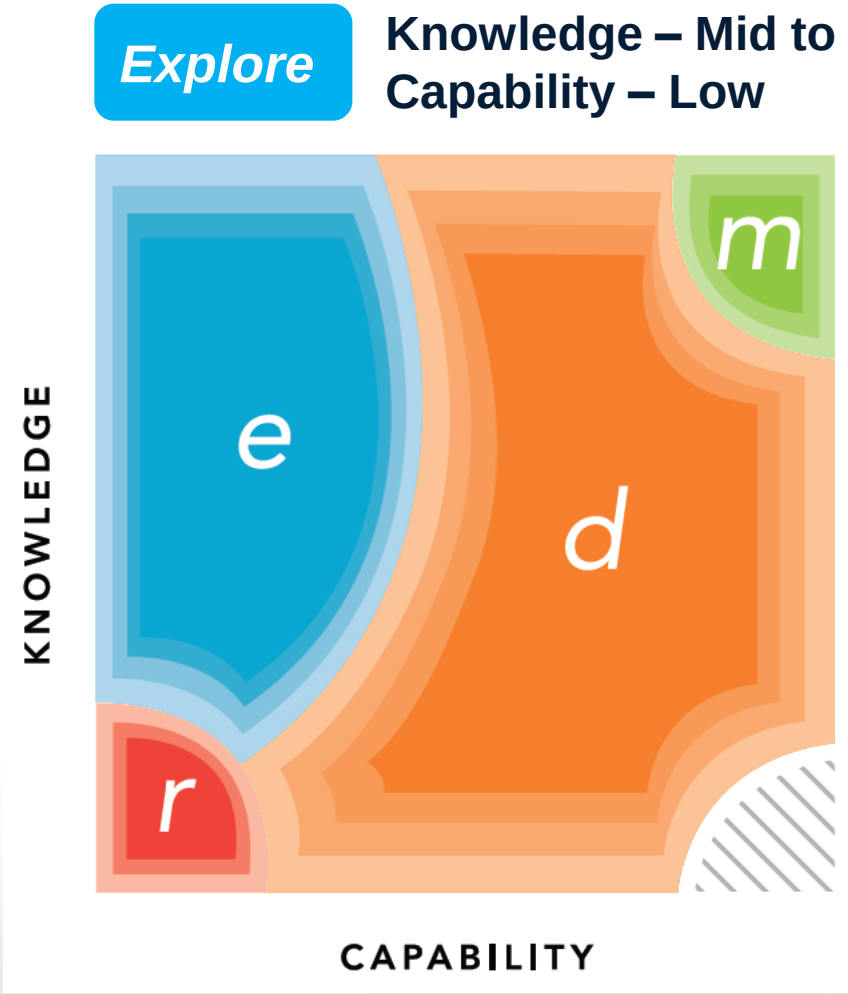
- A risk is perceived as emerging and knowledge of the risk among stakeholders is low.
- Risk response strategies are not implemented or are not assumed to be effectively designed given the low understanding of the underlying risk.
- Monitoring processes have not been contemplated. Inherent risk levels are not well understood.



Explore Stage

Growing Risk

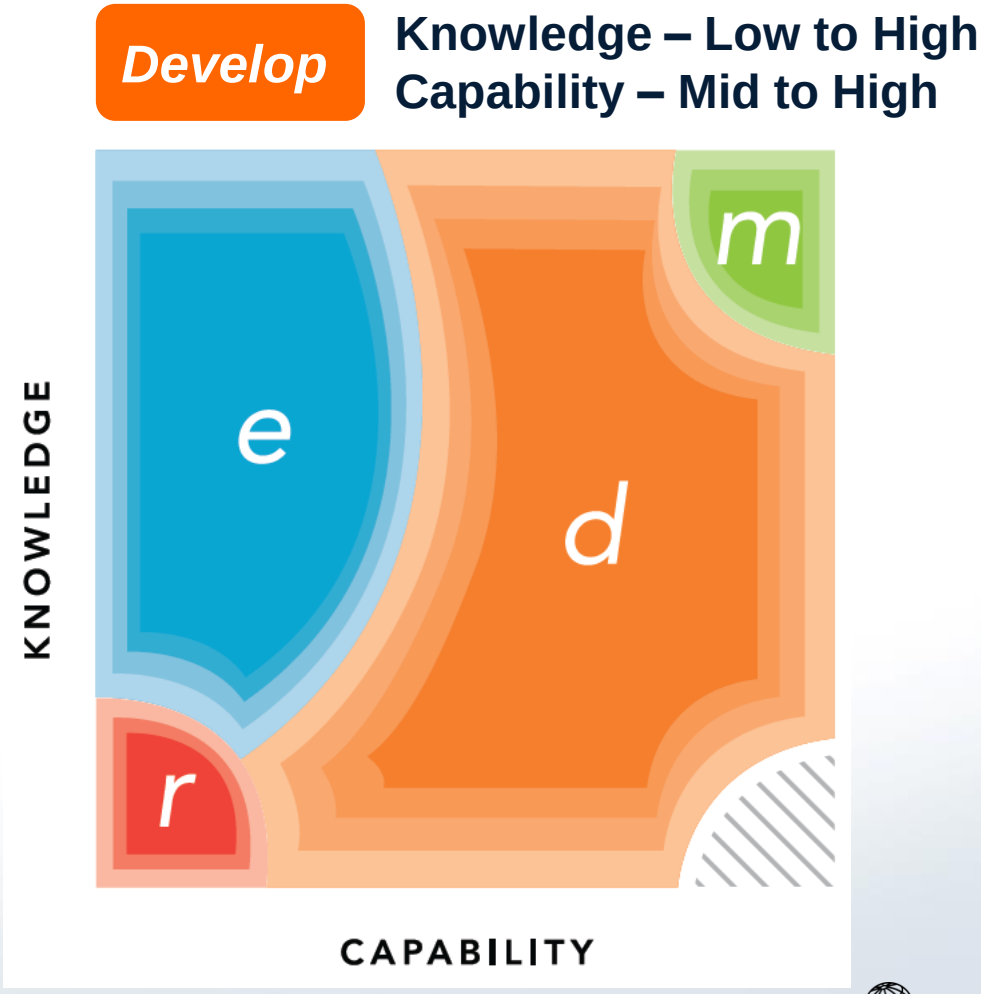
- Knowledge of the risk is growing among some but not all stakeholders. The risk may be perceived as emerging or dynamic.
- Risk response strategies have been contemplated but have not been fully implemented.
- Monitoring processes have not been contemplated or are not implemented. Inherent risk levels are generally understood.



Develop Stage

Active Risk

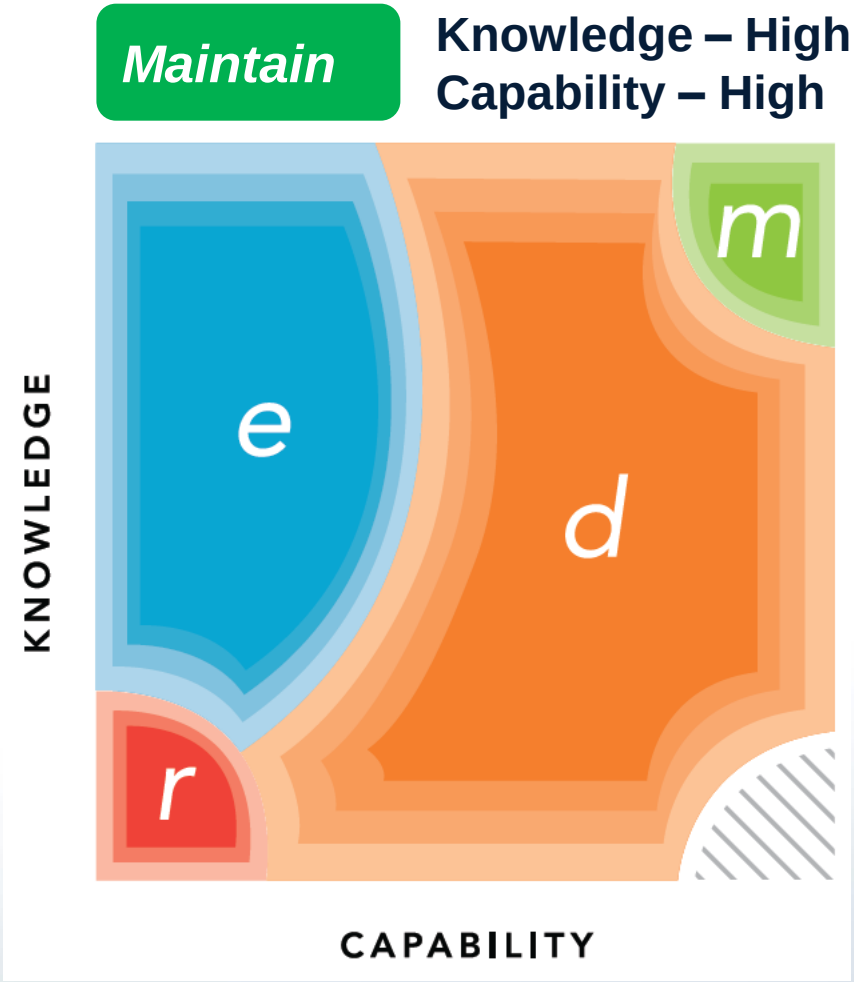
- Risk knowledge is high, at least with management teams.
- Risk response strategies may be developed or in process of being implemented.
- Monitoring processes may be in contemplation, but are not likely to have been fully implemented. Residual risk is generally understood.



Maintain Stage

Mature Risk

- Risk is well understood by all relevant stakeholders and is not perceived to be changing significantly.
- Risk response strategies, consistent with the perceived relevance of the risk, have been developed and implemented.
- Monitoring processes are utilized to ensure risk response strategies are operating effectively as designed. Residual risk levels are understood and believed to be at an acceptable level.



Cybersecurity

Description

- The growing sophistication and variety of cyberattacks continue to wreak havoc on organizations' brands and reputations, often resulting in disastrous financial impacts.
- This risk examines whether organizations are sufficiently prepared to manage cyber threats that could cause disruption and reputational harm.

Risk Relevance

Percentage of CAEs who rated the risk relevance at the 2 highest levels on a 7-point scale. Future was described as "five years from now." *n* = 630.

Risk Stage

Recognize

Data Protection

Description

- Beyond regulatory compliance, data privacy concerns are growing as investors and the general public demand greater control and increased security over personal data.
- This risk examines how organizations protect sensitive data in their care.

Risk Relevance

Percentage of CAEs who rated the risk relevance at the 2 highest levels on a 7-point scale. Future was described as “five years from now.” *n* = 630.

Risk Stage

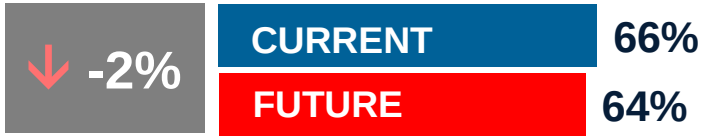
Recognize

Regulatory Change

Description

- A variety of regulatory issues, from tariffs to new data privacy laws, drive interest in this risk.
- This risk examines the challenges organizations face in a dynamic, and sometimes volatile, regulatory environment.

Risk Relevance



Percentage of CAEs who rated the risk relevance at the 2 highest levels on a 7-point scale. Future was described as “five years from now.” *n* = 630.

Risk Stage

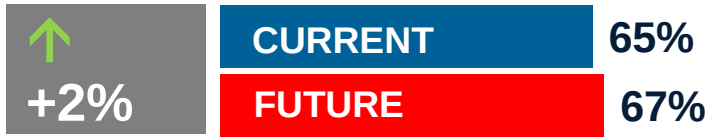
Develop

Business Continuity

Description

- Organizations face significant existential challenges, from cyber breaches and natural disasters to reputational scandals and succession planning.
- This risk examines organizations' abilities to prepare, react, respond, and recover.

Risk Relevance



Percentage of CAEs who rated the risk relevance at the 2 highest levels on a 7-point scale. Future was described as "five years from now." *n* = 630.

Risk Stage

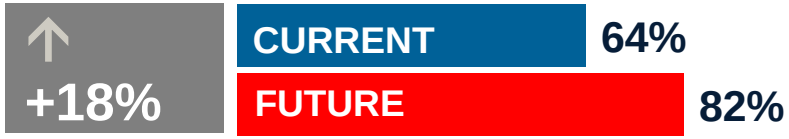
Explore

Data and New Technology

Description

- Organizations face significant disruption driven by the accelerating pace of technology and the growing ease of mass data collection. Consider traditional versus born-digital business models.
- This risk examines organizations' abilities to leverage data and new technology to thrive in the fourth industrial revolution.

Risk Relevance



Percentage of CAEs who rated the risk relevance at the 2 highest levels on a 7-point scale. Future was described as "five years from now." *n* = 630.

Risk Stage

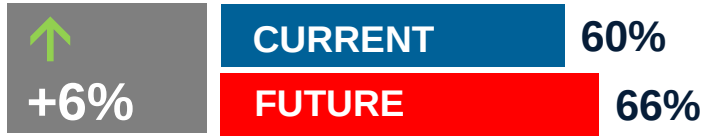
Recognize

Third Party

Description

- Increasing reliance on third parties for services, especially around IT, demands greater oversight and improved processes.
- This risk examines organizations' abilities to select and monitor third-party contracts.

Risk Relevance



Percentage of CAEs who rated the risk relevance at the 2 highest levels on a 7-point scale. Future was described as "five years from now." *n* = 630.

Risk Stage

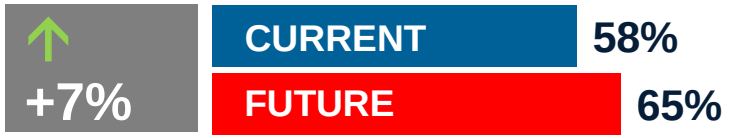
Explore

Talent Management

Description

- Historically low unemployment, a growing gig economy, and the continuing impact of digitalization are redefining how work gets done.
- This risk examines challenges organizations face in identifying, acquiring, and retaining the right talent to achieve their objectives.

Risk Relevance



Percentage of CAEs who rated the risk relevance at the 2 highest levels on a 7-point scale. Future was described as “five years from now.” *n* = 630.

Risk Stage

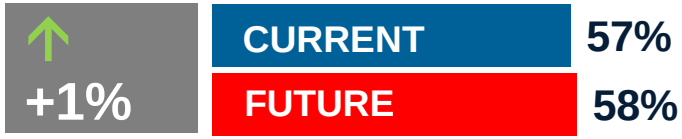
Develop

Culture

Description

- “The way things get done around here” has been at the core of a number of corporate scandals.
- This risk examines whether organizations understand, monitor, and manage the tone, incentives, and actions that drive behavior.

Risk Relevance



Percentage of CAEs who rated the risk relevance at the 2 highest levels on a 7-point scale. Future was described as “five years from now.” *n* = 630.

Risk Stage

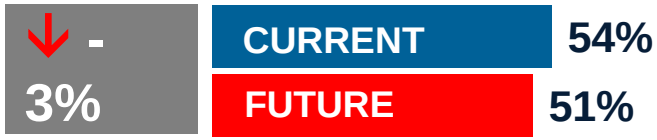
Maintain

Board Information

Description

- As regulators, investors, and the public demand stronger board oversight, boards place greater reliance on the information they are provided for decision making.
- This risk examines whether boards are receiving complete, timely, transparent, accurate, and relevant information.

Risk Relevance



Percentage of CAEs who rated the risk relevance at the 2 highest levels on a 7-point scale. Future was described as “five years from now.” *n* = 630.

Risk Stage

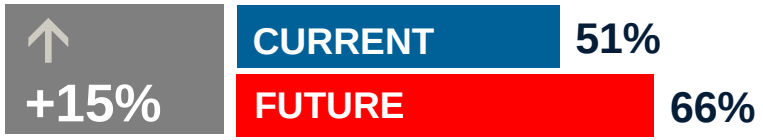
Develop

Data Ethics

Description

- Sophistication of the collection, analysis, and use of data is expanding exponentially, complicated by artificial intelligence.
- This risk examines organizational conduct and the potential associated reputational and financial damages for failure to establish proper data governance.

Risk Relevance



Percentage of CAEs who rated the risk relevance at the 2 highest levels on a 7-point scale. Future was described as “five years from now.” *n* = 630.

Risk Stage

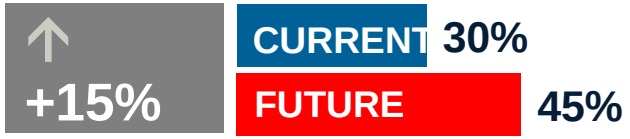
Recognize

Sustainability

Description

- The growth of environmental, social, and governance (ESG) awareness increasingly influences organizational decision making.
- This risk examines organizations' abilities to establish strategies to address long-term sustainability issues.

Risk Relevance



Percentage of CAEs who rated the risk relevance at the 2 highest levels on a 7-point scale. Future was described as "five years from now." *n* = 630.

Risk Stage

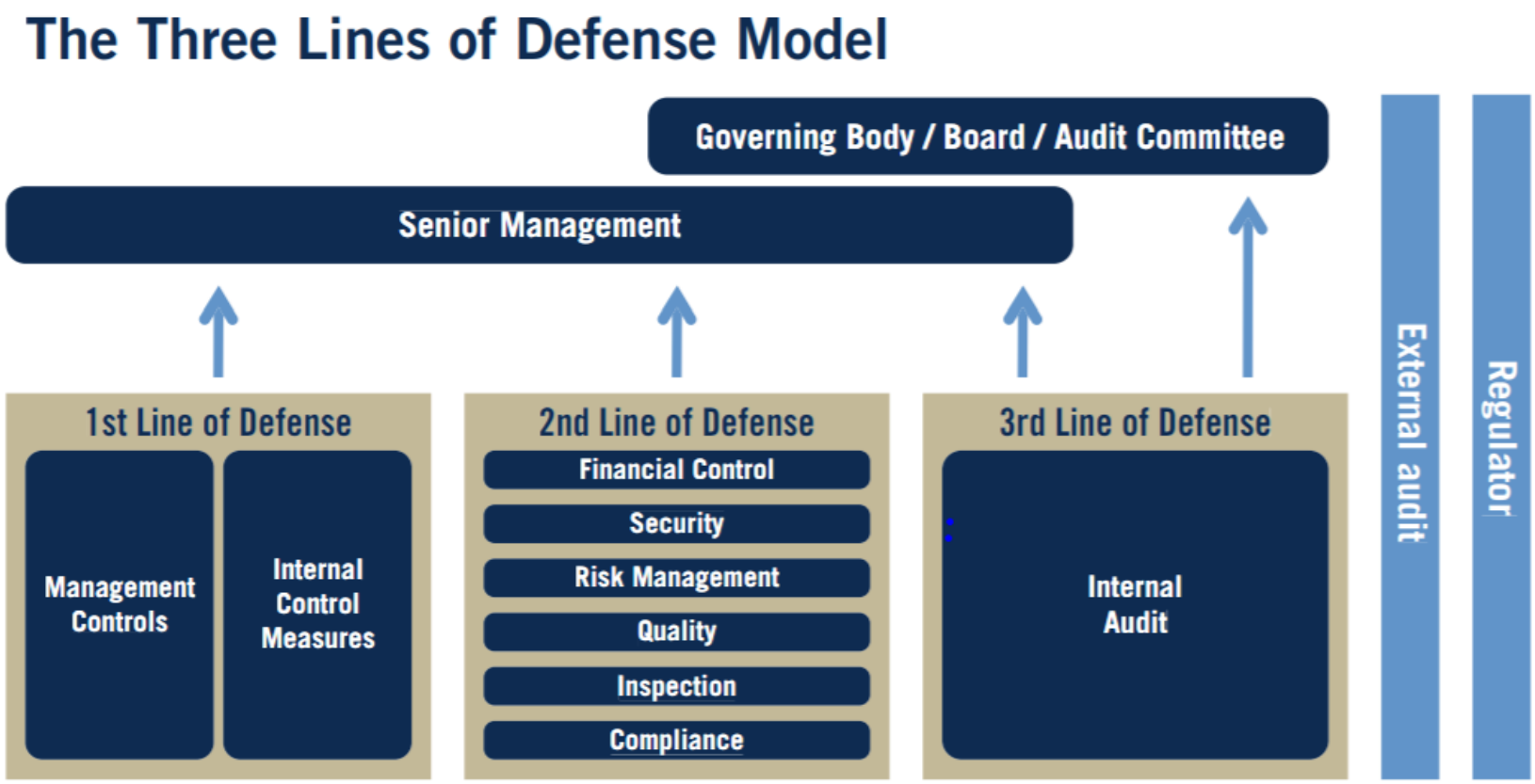
Explore

Three Lines of Defense

Background

- 20+ year-old governance model
- Designed to preserve and enhance organizational value
- Provides governing bodies:
  - Knowledge of the functions involved in identifying and managing risks
  - Knowledge of the functions involved in evaluating risk mitigation activities and their effectiveness

Three Lines of Defense



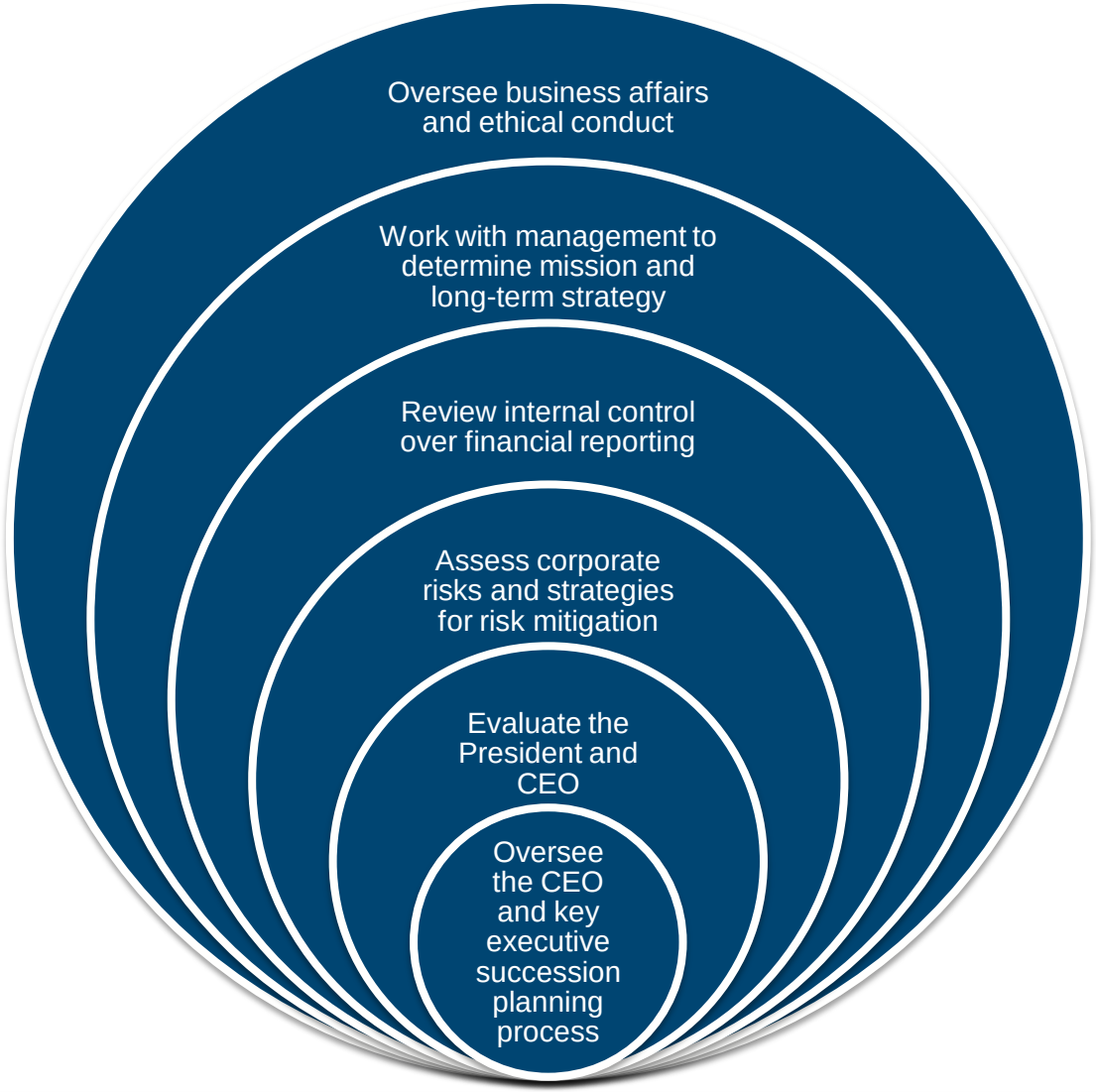
Adapted from ECIIA/FERMA *Guidance on the 8th EU Company Law Directive, article 41*

Establishes a risk and control framework

Board and Sr. Management serve as key stakeholders

Three lines are distinct but should coordinate to ensure enterprise-wide coverage for risk management

Board's Role



To Assure Long-term Shareholder Interests

First Line of Defense

Operational management reporting to Senior Management

Owns and manages risks

Establishes controls to mitigate risks

Supervise execution of the procedures, inclusive of controls

Implement corrective actions to address process and control deficiencies

Second Line of Defense

Risk management and compliance functions established by Senior Management

Facilitate and monitor risk management practices of 1st line

Assists 1st line in determining risk exposure

Reports risk information to organization

Monitors financial risks and potential financial reporting issues

Monitors compliance with specific laws/regulations

Third Line of Defense

Established and reports to the governing body

Consists of internal auditor and staff, where warranted

Provide objective and independent assurance regarding governance, risk management and internal controls

Provide assurance that 1st and 2nd lines of defense are operating effectively

Operate according to professional auditing standards

Definition of Internal Audit

Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.

Board Duty of Oversight

QUESTION

Does the internal audit function have a responsibility to keep the Board out of trouble?

Board Duty of Oversight

Caremark International Inc. Derivative Litigation (1996), **directors must make a good faith effort** to oversee the company's operations, including legal compliance and financial performance.

Caremark claims – may be brought by stockholders alleging that directors breach their **duty of oversight** by not making "a good faith effort to oversee the company's operations."

Case Study

- From 2009-2013, regulators identified compliance failures related to sanitation.
- 2015 – listeria contamination and limited recall of products.
- No evidence of reporting these issues to board until after the recall (meeting minutes).
- Plaintiff-stockholder claimed that BBC breached their fiduciary duty of loyalty by having failed to oversee and monitor the company's food safety operations.

Court dismissed suit stating that required inspections and reports by federal and state regulators constituted a reasonable system of oversight

Case Study (continued)

- Supreme Court overturned the dismissal, indicating that the board took no action to assure a system for board oversight of food safety.

- "The directors had "consciously failed" to attempt to assure that a reasonable information and reporting system existed with respect to the Company's "central issue" of food safety compliance."

Board Safeguards

- Determine your organization's key compliance risks
- Ensure there is a reasonable monitoring system in place
- Ensure compliance issues are reported and discussed at the board level

How Can Internal Audit Help?

- Define areas and issues central to the business/organization
- Work with General Counsel and Compliance to determine whether Board has established a reasonable system for oversight
- Ensure the board receives complete, relevant reporting from internal audit, external audit, compliance, and management (no cherry-picking)
- Develop a risk assessment and management plan that considers key compliance risks and engages the board
- Ensure board minutes are reflective of the oversight system/reporting

One more time…

Does the internal audit function have a responsibility to keep the Board out of trouble?

Step Forward

2019 – 2020 North American Board Chairman's Theme

Intangible Traits

Culture: Do What's Right

It Takes Courage

Embrace Conflict

Intangible Traits

Culture: Do What's Right

- Focus on the customer
- Exude integrity and accountability

It Takes Courage

- Know your board and executive team
- Take ownership in advancing the organization

Embrace Conflict

- Practice disciplined disruption
- Challenge those with whom you work

What I've Learned

Standards Are Critical, Integrity Is Crucial

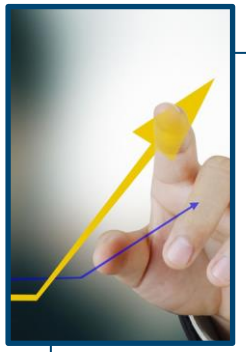
Bring Your Chair to the Table

Emulate Your Heroes

Support Your Visionaries

Make Things Better

My Challenge To You



Start With Your Stakeholders

Educate Your Board

Grow a Leader

Thank You

The Institute of Internal Auditors

Benito Ybarra, CIA

Chairman, IIA North American Board of Directors

benito.ybarra@txdot.gov