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
Polling Question

How many people are employed by the Institute of Internal Auditors?

A. Less than 500
B. Between 500 - 1000
C. Greater than 1000

A: ~230
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
Polling Questions

How many of you are Certified Internal Auditors?

Why is certification important?
Certified Internal Auditor

Only globally-recognized certification for internal auditors

Committed to providing value

Competent

Help improve organizational culture

Inspire the highest level of ethical conduct

Can perform a quality internal audit anywhere in the world
IIA by the Numbers:
Overall Certified Internal Auditors

IIA CIA Certifications

Grand Total: 161,742

Europe: 17,725

North America: 54,455

Central/South America: 1,623

Africa: 3,955

Middle East: 3,974

Asia/Pacific: 74,888

Caribbean: 86

Other: 5,036

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.
Feedback

What do you want from the IIA?
Agenda

- OnRisk
- Board Duty of Oversight
- Privacy
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)

Future Risk Relevance (CAE Perceptions)

- Cybersecurity: 86% (Future), +4
- Data protection: 78% (Future), +7
- Data and new technology: 64% (Future), +18
- Business continuity: 65% (Future), +2
- Data ethics: 51% (Future), +15
- Third party: 60% (Future), +6
- Talent management: 58% (Future), +7
- Regulatory change: 66% (Future), +2
- Culture: 57% (Future), +1
- Board information: 54% (Future), -3
- Sustainability (ESG): 30% (Future), +15
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
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

<table>
<thead>
<tr>
<th></th>
<th>CURRENT</th>
<th>FUTURE</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.”</td>
<td>86%</td>
<td>90%</td>
</tr>
<tr>
<td>+4%</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Risk Stage

Recognize

www.theiia.org/OnRisk
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

CURRENT 78%  FUTURE 85%

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
Board Overconfidence

Ability to Address Risk

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

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.
Board Duty of Oversight
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)

• Delaware 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 risk management plan that considers key compliance risks and engages the board
- Ensure board minutes are reflective of the oversight system/reporting
Privacy
Regulatory Impacts

• California Consumer Privacy Act
  – Effective January 2020
  – Enforcement July 2020
• Gives consumer more control over their personal information
• Spans outside of California’s borders
• Giving rise to privacy laws in other states
• Potential to drive federal privacy laws
Businesses must inform consumers of their intent to collect personal information.

Consumers have the right to know what personal information a company has collected, where the data came from, how it will be used, and with whom it’s shared.

Consumers have the right to prevent businesses from selling their personal information to third parties.

Consumers can request businesses to remove the personal information that the business has on them.

Businesses are prohibited from charging consumers different prices or refusing service, based on consumers exercising their privacy rights.
Things to consider

• Does your organization currently identify and classify personal data?
• Is your organization ready to communicate the personal information your company has collected, where the data came from, how it will be used, and with whom it’s shared?
• Are your opt-out procedures flexible enough to accommodate CCPA?
• Can your organization monetize CCPA and other privacy regulations?
Step Forward
2019 – 2020 North American Board Chairman’s Theme
Opportunities

**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
Thank You

The Institute of Internal Auditors

Benito Ybarra, CIA
Chairman, IIA North American Board of Directors
benito.ybarra@txdot.gov