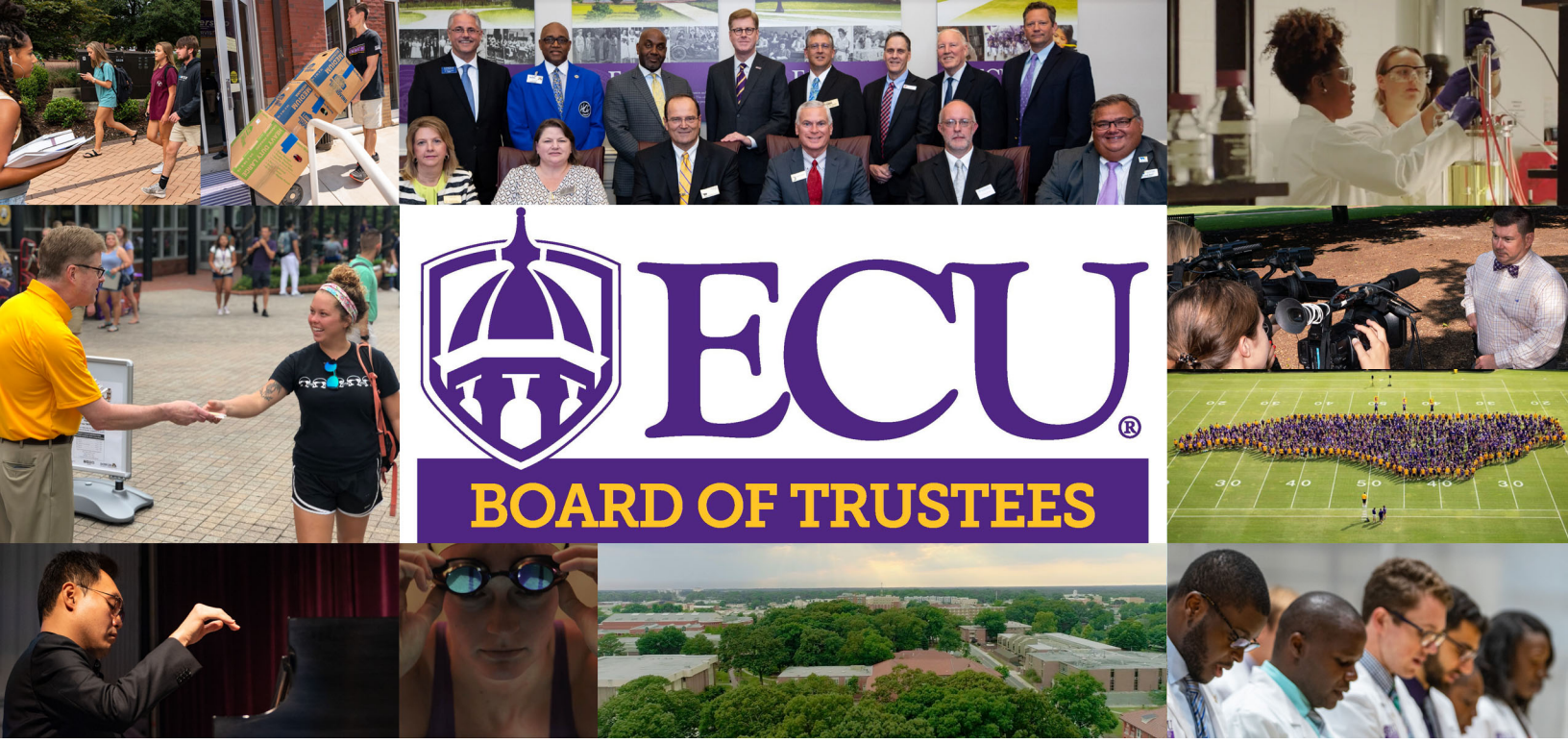


Audit, Risk Management, Compliance, and Ethics Committee Meeting
September 6, 2018
Agenda

I.	Approval of July12, 2018 Minutes	Action
II.	Office of Internal Audit - Mr. Wayne Poole	
A.	Internal Audit Annual Report - FY 2018	Information
B.	Internal Audit Operating Budget - FY 2019	Information
C.	Change to the Committee Charter	Action
III.	Enterprise Risk Management - Mr. Tim Wiseman	
A.	Update of ERM Activities	Information
IV.	Research Compliance - Dr. Mike Van Scott	
A.	Annual Employee COI Reporting	Information
V.	Financial Compliance	
A.	Update of PCI Compliance - Ms. Robin Mayo	Information
VI.	Office of Institutional Integrity - Ms. Michelle Evans	Information
VII.	Closed Session	
VIII.	Other Business	

Board of Trustees
Audit, Risk Management, Compliance, and Ethics Committee
September 6, 2018

Agenda Item: I.	Approval of July 12, 2018 Minutes
Responsible Person:	Kel Normann, Chair
Action Requested:	Approval
Notes:	N/A

Back To Agenda

Minutes from ECU BOT Audit, Risk Management, Compliance, and Ethics Committee
July 12, 2018
Murphy Center – ECU Campus

The Audit, Risk Management, Compliance, and Ethics Committee of the ECU Board of Trustees met in the Murphy Center on the campus of ECU on July 12, 2018.

Committee members present included Kel Normann (Chair), Bob Plybon (Vice Chair), Vince Smith, Max Joyner, Jason Poole, and Jordan Koontz.

Other board members present included Kieran Shanahan (Board Chair), Edwin Clark, Vern Davenport, and Fielding Miller

Others present included Chancellor Cecil Staton, James Hopf, Donna Payne, Paul Zigas, Tom Eppes, Chris Dyba, Nick Benson, Michelle Evans, Sara Thorndike, Dee Bowling, Mike Van Scott, Tony Rowe, Don Sweet, Alton Daniels, Megan Ayers, Tim Wiseman, Virginia Hardy, LaKesha Forbes, Lynn Roeder, Malorie Porter, Leila Faranesh, Mark Stacy, and Wayne Poole.

Kel Normann, Chair of the Committee, convened the meeting at 8:15AM. Mr. Normann read the conflict of interest provisions as required by the State Government Ethics Act. Mr. Normann asked if anyone would like to declare or report an actual or perceived conflict of interest. None were reported.

Mr. Normann asked for the approval of the minutes of the April 19, 2018 committee meeting.

Action Item: The minutes of the April 19, 2018 committee meeting were approved with no changes.

Mr. Tim Wiseman provided the **Enterprise Risk Management** (**ERM)** update.
Mr. Wiseman briefed the committee on the ERM office's recent activities and initiatives. Mr. Wiseman stated that the ERM office has spent considerable time sharing expertise with others in the UNC System and hosted an ERM conference at ECU yesterday. Mr. Wiseman stated that the upcoming year is a full ERM assessment cycle. The top risk survey and all corresponding activity will be launched again in the fall.

Mr. Wayne Poole provided the **Internal Audit** update.
Mr. Poole presented the Internal Audit dashboard as of June 30, 2018 (for the complete 2018 fiscal year). Internal Audit completed 86% of the annual audit plan (target is 80%) and achieved a 75% direct productivity rate (75% is the standard). Management completed 87% of the corrective actions which Internal Audit followed up on (95% is the standard). Mr. Poole stated that he is not alarmed about the latter number not meeting the standard since four of the five unresolved items were from one audit, and management is addressing that area. Mr. Poole also stated that Internal Audit will be using new tools and dashboards this year to track unresolved recommendations, and will be working with the Vice Chancellors more closely to ensure they have the timely information needed to monitor the action plans in their areas.

Mr. Poole presented the FY 2019 annual audit plan, which has already been approved by the Chancellor. The plan was included in the committee members' read-ahead materials.

Action Item: A motion was made and seconded to approve the FY 2019 annual audit plan as written. The motion was approved unanimously with no further discussion.

Mr. Poole stated that the annual certification letters that are required by the UNC System Office have been signed by the Chief Audit Officer and by Committee Chairman Kel Normann. The letters will be submitted to the System Office tomorrow.

Mr. Poole briefed the committee on Internal Audit's recent follow-up of the recommendations that were made in 2017 related to the University's Title IX complaint response processes. Mr. Poole stated that the University continues to make strong progress in this area and that the University's investigation and adjudication processes are significantly more mature than they were several years ago.

Closed Session

Back To Agenda

Minutes from ECU BOT Audit, Risk Management, Compliance, and Ethics Committee
July 12, 2018
Murphy Center – ECU Campus

At 8:35 AM, Mr. Plybon made a motion that the committee go into closed session in order to discuss items that are protected according to state statutes governing personnel information, internal audit working papers, student records, and/or otherwise not considered a public record within the meaning of Chapter 132 of the North Carolina General Statutes. The motion was seconded and unanimously approved.

Return to Open Session
The Committee returned to open session and continued work on the agenda at 8:50 AM.

Other Business
There was no other business.

There being no further business, the Audit Committee meeting was adjourned at 8:51 AM.

_____
Respectfully submitted,
Wayne Poole
ECU Office of Internal Audit and Management Advisory Services

Back To Agenda

Board of Trustees
Audit, Risk Management, Compliance, and Ethics Committee
September 6, 2018

Agenda Item: II.A.	Internal Audit Annual Report FY 2018
Responsible Person:	Wayne Poole
Action Requested:	None - Information
Notes:	N/A

Back To Agenda

Internal Audit Team

FY 2018 Year in Review

The Year in Numbers

- Audit Plan Completion: 86%
- Auditor Productivity: 75%
- Engagements Completed: 51
- Consultations: 124
- Hotline Triage: 30
- Committees/Workgroups: 14
- Search Committees: 4

Back To Agenda

We did it!!

- Managed a significant amount of change *("If you don't like change, you will like irrelevance even less")*
- Handled very high hotline and investigative audit volume
- Completed high-profile audits
- Implemented a new Audit Management System/e-workpapers

We did it!!

- Graduated our intern
- Added two phenomenal team members
- Maintained a fully certified auditor corps
- Served our state and our profession
- Served our community (food drive; pet supplies; service in schools…)

Back To Agenda

Yes, they really said it

"You guys are two for two. I never knew your office before yesterday, but two days in a row you guys were very knowledgeable and professional. I'm impressed."

Yes, they really said it

"You guys are really top-notch."

"If Internal Audit says it, then I believe it."

Back To Agenda

Yes, they really said it

"Our Office of Internal Audit is here to serve the University community and has done so with distinction for many years."

So…What Next?

- New year, new audit plan
- Increased public relations efforts
- Enhancing coordination with other assurance providers (IIA Standard 2050)
- Internal IIA Self-Assessment

Back To Agenda

So…What Next?

- Revamping follow-up tracking and reporting to Vice Chancellors and others
- Implement additional modules in the audit management system
- Continued growth in data analytics

So…What Next?

- Information sharing and team building
- Continuing soft skills development
- Additional team member certifications
- ACUA national conference presenters
- Co-sponsor Fall UNC Auditors Association conference
- Community Service

Back To Agenda

Board of Trustees
Audit, Risk Management, Compliance, and Ethics Committee
September 6, 2018

Agenda Item: II.B.	Internal Audit Operating Budget – FY 2019
Responsible Person:	Wayne Poole
Action Requested:	None - Information
Notes:	N/A

Back To Agenda

Board of Trustees
Audit, Risk Management, Compliance, and Ethics Committee
September 6, 2018

Agenda Item: II.C.	Change to the Committee Charter
Responsible Person:	Wayne Poole
Action Requested:	Action
Notes:	N/A

Back To Agenda

Audit, Enterprise Risk Management, Compliance, and Ethics Committee Charter

Purpose

The purpose of the Audit, Enterprise Risk Management, Compliance, and Ethics Committee (hereafter referred to as Committee) is to assist the East Carolina University Board of Trustees in fulfilling its oversight responsibilities for (1) the integrity of the University's financial statements, (2) the University's compliance with legal, regulatory, and ethical requirements, (3) the performance of the University's internal audit function, (4) the University's compliance with the Best Financial Practices Guidelines adopted by the UNC Board of Governors in November of 2005, and (5) the University's Information and IT Security programs. The Committee has jurisdiction over internal audit, enterprise risk management, compliance, information security, conflicts of interest, and ethics.

Organization

The Committee shall be a standing committee of the ECU Board of Trustees. Each Committee member must be independent of management and free of any relationship that would impair such independence.

If practicable, at least one member of the Committee should be a financial expert. A financial expert is someone who has an understanding of generally accepted accounting principles and financial statements; experience in applying such principles; experience in preparing, auditing, analyzing, or evaluating financial information; experience with internal controls and procedures for financial reporting; and an understanding of the audit committee function. If feasible, the role of financial expert will be rotated on an annual basis.

Meetings

The Committee shall meet at least four times a year and hold additional meetings as circumstances require. The Committee will invite representatives of management, auditors, legal counsel, and others to attend meetings and provide pertinent information as necessary. The Committee will receive reports regarding internal audit, enterprise risk management, compliance, conflicts of interest, and ethics. It will also hold private meetings with the Chief Audit Officer if deemed necessary. Meeting agendas will be prepared and provided in advance to members, along with appropriate briefing materials. Minutes of the meetings will be prepared.

Back To Agenda

Duties and Responsibilities

The following shall be the principal duties and responsibilities Committee as prescribed by the UNC BOG Best Financial Practices Guidelines:

- Meet at least quarterly during the year.
- Review the results of the annual financial audit with the North Carolina State Auditor or his designated representative.
- Discuss the results of any other audit performed and report/management letter (i.e. information system audits, investigative audits, etc.) issued by the North Carolina State Auditor with either the State Auditor or his staff, the Chief Audit Officer, or appropriate campus official.
- For any audit finding contained within a report or management letter issued by the State Auditor, review the institution's corrective action plan and receive a report once corrective action has taken place.
- Discuss the results of any audit performed by independent auditors and, if there were audit findings, review the institution's corrective action plan and receive a report once corrective action has taken place.
- Review all audits and management letters of University Associated Entities as defined in section 600.2.5.2[R] of the UNC Policy Manual.
- Receive quarterly reports from the Chief Audit Officer that, at a minimum, reports material (significant) reportable conditions, the corrective action plan for these conditions and a report once these conditions have been corrected.
- Ensure that the Chief Audit Officer reports to the Chancellor with a clear, recognized reporting relationship to the chair of the Committee.
- Receive, review, and approve the annual audit plan for the internal audit department.
- Ensure that all internal audits were conducted in accordance with professional standards.
- Receive and review an annual summary of audits performed by the internal audit department.
- Ensure the Chief Audit Officer forwards copies of both the approved audit plan and summary of internal audit results to UNC General Administration in the prescribed format.

Other:

- Review and concur in the appointment, replacement, or dismissal of the Chief Audit Officer and the compensation package.
- Review and assure the internal audit function has appropriate budget and staff resources.
- Review and accept internal audit reports when issued.
- Periodically review and revise the internal audit charter as needed.
- Resolve disagreements between internal audit and management concerning audit findings and recommendations.

Back To Agenda

The Committee, with the assistance of the Chief Audit Officer should periodically review and assess the adequacy of the Committee Charter.

Approved by the Committee by formal vote on September 6, 2018.

Back To Agenda

Board of Trustees
Audit, Risk Management, Compliance, and Ethics Committee
September 6, 2018

Agenda Item: III.A.	Update of ERM Activities
Responsible Person:	Tim Wiseman
Action Requested:	None - Information
Notes:	N/A

Back To Agenda

8/21/2018

INFORMATION PAPER

SUBJECT: Enterprise Risk Management (ERM) Update for the BOT-Audit, Risk Management, Compliance and Ethics Committee September 2018 Meeting

1. Purpose. To advise BOT-ARMCE committee members of significant ERM activities from the past two months and those planned or anticipated for the next two months.

2. Action Recapitulation:

a. Significant ERM Activities from the Past Two Months:

- ERM Consultation and Assistance to UNC-Support Office – Ongoing
  - System ERM Mini-Workshops Facilitation (ECU 7/11 & Winston-Salem 8/2)
  - ERM Framework Development & Consultation with Institutions
- Quarterly ERM Committee Meeting – (July)
- ERM Dialogue with Academic Deans and Directors and Student Government Association Leaders
- FEMA Training and Claim Portal Access
- ECU Included in Higher Ed Advanced Practice ERM Group (Formally Ivy Plus ERM Group) – Thought Leader/Recognized Mature Program Concept
- ERM Top Risks Pulse Check Survey
- University Admissions Safety and University Employee and Student Behavior Concern Teams Meetings and Actions
- ERM Consultations/Research/Inquiries – Various Departments

b. Significant ERM/CRO Activities Next Two Months:

- ERM Top Risks Survey Launch and Prioritization Exercise w/ Related Reporting
- Present ERM Session to University of North Carolina Auditors Association
- Quarterly ERM Committee Meeting – (October)
- Publish ERM "Five Things" Executive Newsletter/Tip Sheet – September
- One-on-One Risk Interviews with Key Campus Leaders
- ERM Consultation and Assistance to UNC-Support Office – Ongoing
- University Admissions Safety and University Employee and Student Behavior Concern Teams Meetings and Actions
- ERM Consultations/Research/Inquiries – Various Departments

3. Other: Attached are the Two Year ERM Activities Model chart, Top Risks Survey Timeline, NACD/Protiviti/NCSU white paper, "*Is Board Risk Oversight Addressing the Right Risks?*"

ACTION OFFICER: Tim Wiseman
Assistant Vice Chancellor for ERM & Military Programs
Spilman Bldg., Room 214, 252-737-2807

Back To Agenda

Two Year ERM Activities Model

Year	Primary Activities	Focus
Even Numbered "On" Year (Example '18-'19)	• Full ERM Risk Survey • Full Risk Prioritization Exercise • Reset • BOT & EC Presentations and Involvement • Risk Management Plans Creation (or Updates)	• Engaging Key Sensors • Assessment Process (Rigor and Detail) • Risk Register Update • Fresh Look at Current and Anticipated Risk Environment
Odd Numbered "Off" Year (Example '17-'18)	• Smaller Scale Re-Prioritization/ Re-Validation Exercise • Departmental Workshops • Interviews and Sensing Sessions • Presentations to Other Key Committees/Groups	• Risk Management Plans Update/ Adjustment • "By Exception" Reviews • Select Risk Management Project Work • ERM "Maturity" Assessment(s) • Education

ECU Enterprise Risk Management

Back To Agenda

Academic Year 2018-2019 ERM Top Risks Survey Action Timeline

(Draft as of 8/21/2018)

ERM Office	8/25/2018	Summarize Off Year "Pulse Check"
ERM Office	8/28/2018 or 9/25	Update to Academic Deans and Directors and Student Government Association Leadership on ERM and Upcoming Risk Survey
BOT-ARMCE	9/6/2018	Heads Up to BOT-ARMCE on Survey – Invitation
ERM Office	9/6/2018 (Tent.)	Launch Survey
EC	9/10/2018	Remind EC of Survey – Invite to Complete (VCAF)
ERM Office	10/6/2018	Close ERM Survey – Tabulate
ERMC	10/17/2018	Risk Prioritization Exercise (Register)
ERM Office	TBD	Make-Up Risk Prioritization Exercise (Absentees from 10/17)
EC	11/05/2018	Risk Survey and Top Ten Results to EC & RMPO Selection
ERMC	Nov - March 2019	Risk Mgmt Plans Worked (Working Groups)
ERM Office & Office of the Chancellor	NLT 12/31/2018	Coordinate ECU's Top Risks Response to UNC-SO
ERMC	Feb 2019	Review Draft Risk Mgmt Plans
EC	March 2019	Risk Mgmt Plan Summaries to EC
BOT-ARMCE	April 2019	Risk Mgmt Plan Summaries to BOT-ARMCE
ERM Office	April-	Follow-Up Actions

EC – Chancellor's Executive Council

BOT-ARMCE – Board of Trustees Audit, Risk Management, Compliance and Ethics Committee

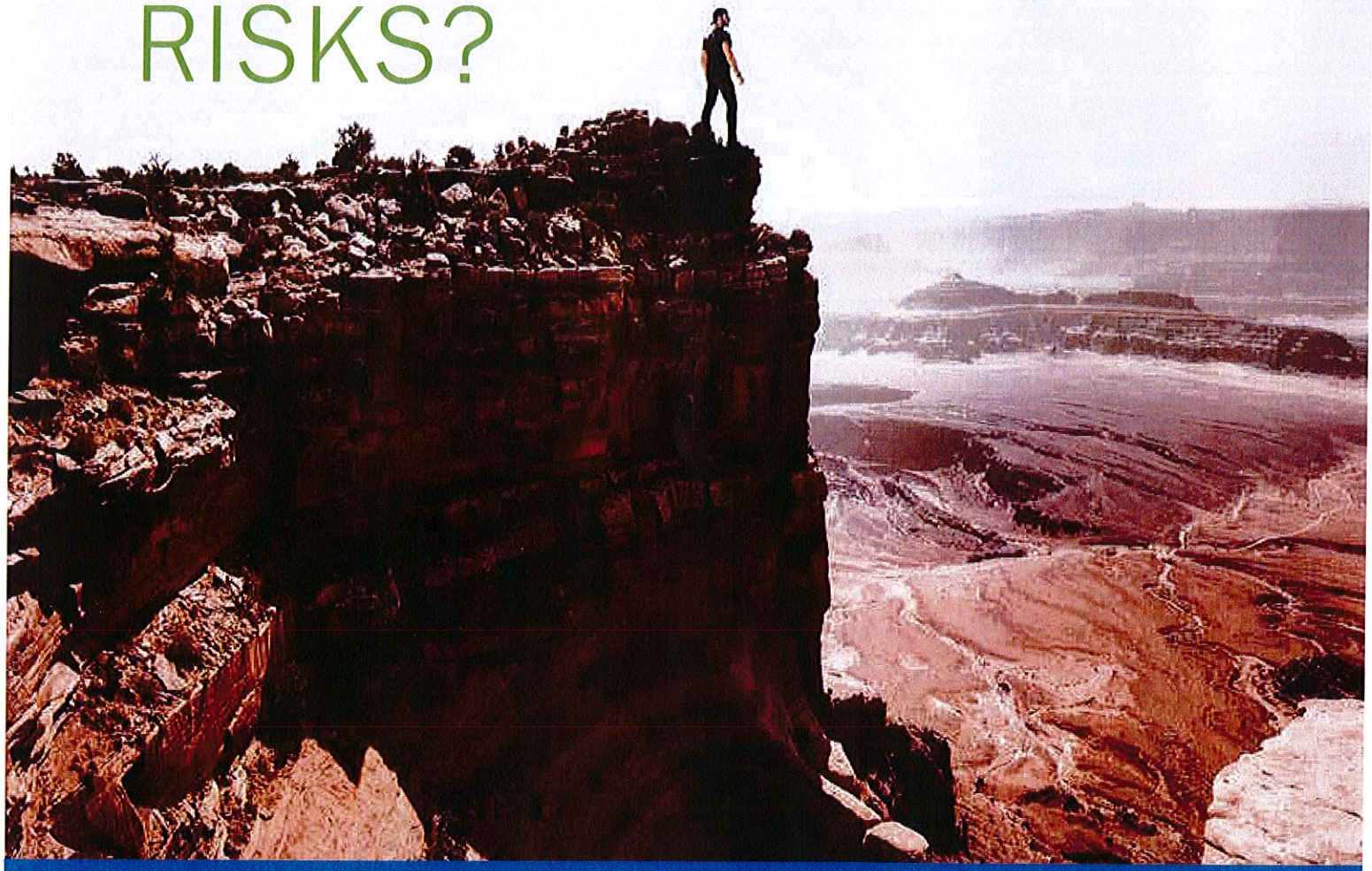
ERMC – Enterprise Risk Management Committee

ERM – Enterprise Risk Management

Back To Agenda

↳ PERMISSION RECEIVED FOR ECH BOT & ERM REFERENCE USE. NACD - JENNA 8-21-18

IS BOARD RISK OVERSIGHT ADDRESSING THE RIGHT RISKS?



Strategies for Addressing the New Risk Landscape

NACD protiviti® Face the Future with Confidence NC STATE UNIVERSITY

Back To Agenda

Back To Agenda

INTRODUCTION

Corporate directors and their management teams recognize that growing disruption and uncertainty in the marketplace are creating new, sometimes unforeseen risks, and altering the nature of existing risks. While overall global economic indicators are mostly positive and capital markets are relatively strong, tectonic shifts in how corporations create value demand a rethink of current risk management approaches and their board oversight. Rapid technological advancements, the introduction of new business models, and the disruption of entire industries pose new, often existential risks to companies.

Recent surveys of public company directors and C-suite executives separately conducted by the National Association of Corporate Directors (NACD) and by Protiviti in partnership with the ERM Initiative at North Carolina State University (NC State) highlight similar concerns that are top of mind for public company board members and executives. These two surveys, both conducted in mid-to-late 2017, indicate that public company directors and C-suite executives are now focused on new risks—ones that might undermine the fundamental drivers of value for their organizations.

This report, prepared by the parties responsible for these two surveys, discusses their joint findings, makes the case that current board risk-oversight practices may be inadequate to deal with today's evolving risk landscape, and suggests ways for boards to close the gap.

This report makes the case that current board risk-oversight practices may be inadequate to deal with today's evolving risk landscape, and suggests ways for boards to close the gap.

I. AN UNPRECEDENTED AND EVOLVING RISK LANDSCAPE

These are not yesterday's risks

The results from both surveys reveal that the focus on "yesterday's risks" that still preoccupy many boardroom discussions doesn't adequately address future business needs. Over the past five years, the top risk concerns have shifted from a focus on post-crisis financial discipline, regulatory compliance, and the challenges of growing organically to disruptive innovation, internal resistance to change, cybersecurity threats, and heightened political risk. Exhibit 1 summarizes the top 10 concerns highlighted in each survey, revealing a number of common issues on the minds of directors and executives.

Both surveys reveal that the focus on "yesterday's risks" that still preoccupy many boardroom discussions doesn't adequately address future business needs.

EXHIBIT 1

TOP 10 RISK CONCERNS

NACD SURVEY	PROTIVITI/NC STATE SURVEY
NACD TOP 10 TRENDS[1]	**PROTIVITI/NC STATE TOP 10 RISKS[2]**
1. Significant industry change	1. Rapid speed of disruptive innovations and new technologies
2. Business model disruption	2. Regulatory changes and scrutiny
3. Changing global economic conditions	3. Resistance to change
4. Cybersecurity threats	4. Cybersecurity threats
5. Competition for talent	5. Succession challenges and competition for talent
6. Political uncertainty in the United States	6. Operations not able to meet performance expectations
7. Technology disruption	7. Economic conditions
8. Corporate tax reform in the United States	8. Organization's culture may not escalate risk issues
9. Increased regulatory burden	9. Inability to use data analytics for market intelligence
10. Risk in M&A	10. Limited opportunities for organic growth

[1] These findings are based on responses from 587 public company corporate directors and executives which were obtained by NACD in June and July 2017, and are included in the full report, *2017–2018 NACD Public Company Governance Survey*.

[2] These findings are based on responses from 153 public company directors and C-suite executives serving on US corporate boards which were obtained September through October 2017, and are included in the Protiviti/NC State full report, *Executive Perspectives on Top Risks for 2018: Key Issues Being Discussed in the Boardroom and C-Suite*.

While there are some differences in the relative rankings of specific risks across the two surveys, collectively, the findings point to five overarching and interrelated risk themes that directors and senior executives perceive to have the potential to significantly impact their organizations' risk profiles.

Well over half of respondents identified "significant industry change" as a top risk.

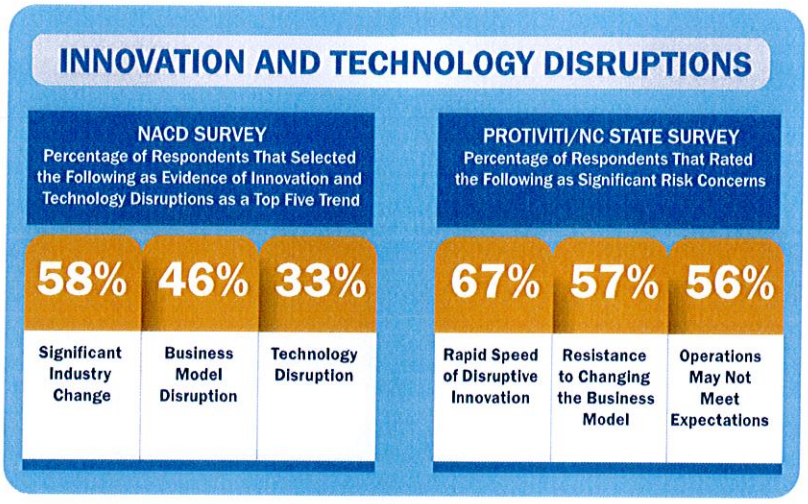
EXHIBIT 2

1. Innovation and Technology Disruptions — The speed of change in today's global marketplace is unprecedented, and only likely to accelerate over time. Directors and executives realize that the pace of innovation and the emergence of new technologies may have a disruptive effect on their organization's core business model, putting at risk future revenues.[3] No longer can business leaders assume that the status quo is sustainable for the long term.

Respondents to the NACD survey consistently identified concerns about

[3] The tools of the digital age are making it possible to reimagine core processes and functions and engage customers in ways that were unthinkable 5 to 10 years ago. Examples of these tools include exponential increases in computing power, cloud computing, robotic process automation, artificial intelligence, machine learning, the Internet of Things, mobile technologies, big data, speech recognition, advanced data analytics, social media, and visualization techniques. As demographics and customer preferences change, "born digital" market entrants are able to introduce innovative ways to enhance the customer experience and scale quickly in the face of rapid demand. Companies in many industries are focused on digitizing products and services, improving information for decision making, and achieving dramatic advances in productivity. As investing strategies and regulatory requirements place more emphasis on environmental, social, and governance themes, innovation takes on aspects of sustainability to achieve objectives other than acceptable financial performance. These and other factors are literally shrinking the half-life of business models, making innovation a strategic imperative.

EXHIBIT 3



Organizations need to be agile enough to respond to emerging developments.

significant industry changes, business model disruption, and technology disruptions. Well over half of respondents identified "significant industry change" as a top risk, while close to half rated "business model disruption" as a top risk concern. Similarly, two-thirds of the respondents to the Protiviti/NC State survey rated the rapid speed of disruptive innovation as a significant risk concern, while a majority indicated that resistance to change may restrict the organization from making necessary adjustments to the business model. Taken together, these findings indicate that companies may not only be struggling to respond to changes imposed by innovation, but may also be suffering from a cultural challenge that is making their organizations more resistant to change. More than half of respondents also highlighted their concerns that their companies' existing operations will be unable to meet performance expectations when confronted with "born digital" competitors.

Collectively, the NACD and Protiviti/NC State findings highlight director and executive concerns about advancements in digital technologies and the pressure they exert on established business models. Organizations need to be agile enough to respond to emerging developments that alter expectations about how products and services are delivered to customers and threaten their overall competitive position. Responses to new market innovations that are too slow, or an unwillingness within organizations to make necessary adjustments to the business model and to their core operations, may prove deadly to long-term corporate survivability.

2. Limitless Cyber Threats — To keep pace with rapidly evolving market innovations, organizations are constantly deploying new technologies to manage core operations, engage with key customers, and capture needed efficiencies for competiveness. While embracing technology is a recognized necessity, directors and senior executives are keenly aware that doing so increases their organization's exposure to cyber threats. They recognize that the probability is high that their organizations have already been breached. Given the extensive use of technology throughout a global organization and its data connectivity to key vendors, partners,

EXHIBIT 4

customers, and the online economy, pinpointing how a cybersecurity event might emerge can be an overwhelming task.

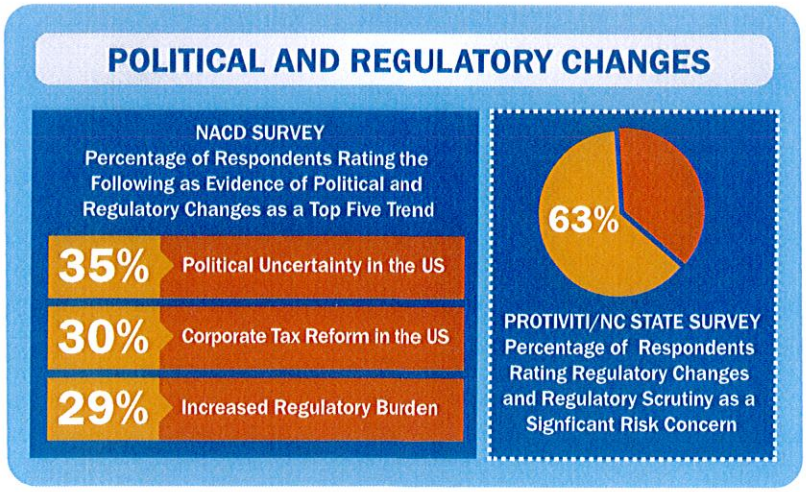
Increases in data breaches, ransomware attacks, and failures to patch known vulnerabilities, along with state-sponsored cyberterrorism, are driving urgency among directors and senior executives about the need for cyber resiliency and more advanced protection measures. The sophistication of perpetrators and the significant impact and headline visibility of cybersecurity events underscore the reality that an IT security issue creates an enterprise-level business risk.

Possible trade wars and increased protectionism could significantly disrupt global supply chains and ultimately increase production costs and consumer prices.

3. New Political Realities and Heightened Regulatory Risks — New political realities worldwide, driven by populist discontent, are challenging the merits of globalization, including free trade, unrestricted capital flows, and recruitment of overseas talent. Possible trade wars and increased protectionism could significantly disrupt global supply chains and ultimately increase production costs and consumer prices.

Political risk is exacerbated by a significant shift in how the United States exercises its global leadership role, affecting trade agreements, security alliances, and commitments to tackle global climate change. Moreover, we see regulation

EXHIBIT 5



around the globe strengthening in key areas, such as anticorruption and data privacy, with levels of enforcement increasing.

4. Competition for Talent — An organization's ability to respond creatively and resiliently to ever-changing risk conditions is contingent on their ability to attract and retain top talent. Respondents to both studies expressed concerns about their ability to attract and retain top talent, which will create significant leadership-succession challenges. Tightening labor markets combined with the need for a potentially different mix of talent in today's highly digital and data-intensive environment are breeding potentially fierce competition for the best and brightest.

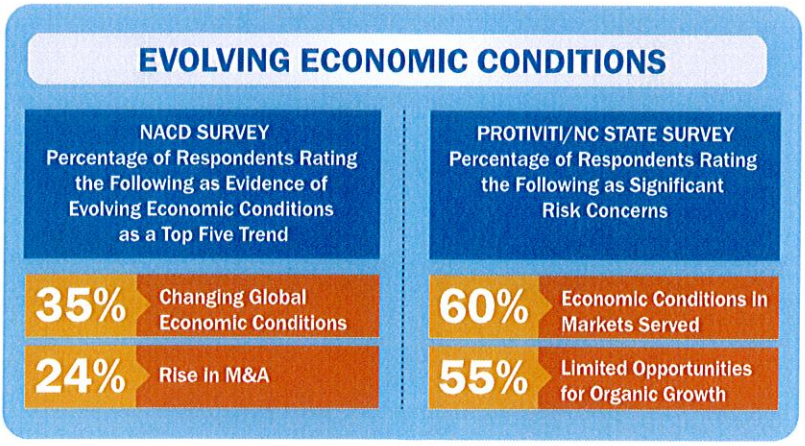
EXHIBIT 6

An organization's ability to respond creatively and resiliently to ever-changing risk conditions is contingent on their ability to attract and retain top talent.

Organizations that are in industries or sectors perceived to be slow-moving or "old-school" may face even greater challenges to assemble the workforce and leadership team needed to navigate this unprecedented environment.

5. Changing Global Economic Conditions — While overall economic conditions have improved significantly in recent years, respondents in both surveys included economic concerns in their list of top 10 concerns. Equity markets have hit all-time highs in recent months, yet some question whether

EXHIBIT 7



these gains are in fact market "bubbles" that might burst if some unexpected event emerges. For example, threats to free-trade policies have recently introduced volatility in the equity markets, triggering questions about whether market corrections might be near term. Moreover, the economic gains have not addressed fundamental concerns about growing income inequality in many countries. And there is a risk that these economic divisions, both within and between countries, may worsen when the technology revolution accelerates and more jobs are displaced through automation.

Evolving rate outlooks of central banks that suggest the end of the low-interest-rate and low-inflation era are fostering uncertainty among directors and executives as they evaluate how increased borrowing costs could affect planned investments as well as future growth opportunities, whether organic or through mergers or acquisitions. Directors also are mindful that the pace of economic growth could shift dramatically and suddenly, increasing the importance of being in the right markets at the right time.

Organizations can no longer manage today's risks if their operations are functioning inside fragmented, uncommunicative silos.

A Key Question for Directors: Does the organization's culture impede effective risk oversight?

These five themes do not manifest themselves in isolation; instead, they are interrelated. For example, the need to embrace disruptive technologies creates a demand for new talent. If that need is not successfully addressed, there may be operational missteps that open opportunities for massive security breaches that escalate regulatory scrutiny and critical questioning from top political leaders. Organizations can no longer manage today's risks if their operations are functioning inside fragmented, uncommunicative silos.

EXHIBIT 8

These interrelated themes highlight the importance of staying on top of the organization's emerging risk landscape. A majority of respondents to the NACD survey believe their boards must better understand the risks and opportunities that affect performance and drive strategic choices. In addition, three out of four participants in the NACD survey think that management's focus on long-term strategic goals has been compromised by pressure to deliver short-term results.

What's equally concerning is that a majority of respondents in the Protiviti/NC State survey believe the organization's culture may not sufficiently encourage the timely identification and escalation of risk issues that have the potential to significantly affect the company's core operations and strategic objectives. Ironically, 92 percent of directors in the NACD study rely on reporting from the CEO about the health of the organization's culture, and only 35 percent say they have a good understanding of the "mood in the middle" of their organization.

If an organization's processes for identifying and communicating emerging risks are immature, if the organization's culture doesn't encourage individuals to communicate risk concerns to senior management and the board, or if the organization is unduly constrained by myopic short-termism, any number of these five themes is likely to dramatically impact the organization's core business.

Three out of four participants in the NACD survey think that management's focus on long-term strategic goals has been compromised by pressure to deliver short-term results.

II. THE CASE FOR ACTION

Why current board risk-oversight practices fall short in today's business environment

The 2008 global financial crisis highlighted significant failures in how banks and other financial institutions managed risk. Regulators, directors, and executives have since taken action to guard against the recurrence of this calamity by introducing measures to improve risk management capabilities, including strengthening board oversight of risk. Enterprise risk management (ERM) emerged as a topic for consideration, and not just for banks. Nonfinancial institutions also made investments to safeguard their enterprises in response to prolonged uncertainty and increased regulatory scrutiny.

This renewed focus on corporate risk discipline certainly paid dividends in the first years of the postcrisis recovery. Establishment of formal ERM programs has helped companies to improve firm-wide visibility into risk exposures, establish stronger accountability for managing those exposures, and strengthen adherence to policies, laws, and regulations.

Important Progress Has Been Made

Board governance has been subject to significant reform as a result of the financial crisis, most prominently through the Dodd-Frank Wall Street Reform and Consumer Protection Act, which introduced new standards for board independence, shareholder proxy access, executive-pay disclosures, capital requirements, and the requirement for large banks to create board-level risk committees. The US Securities and Exchange Commission also adopted rules for enhancing risk disclosures for listed US public companies, requiring companies to provide more information about the board's role in risk oversight and stipulating that they evaluate the extent to which compensation structures could adversely impact the company's risk profile. Credit rating agencies are now assessing the board's role in risk oversight as part of the credit-evaluation process.

As a result, boards have been become more attuned to risk. According to the *2017–2018 NACD Public Company Governance Survey*, 84 percent of boards now receive, at least annually, reports on the ranking of top risks, while 80 percent get detailed updates about the effectiveness of mitigation of those top risks.[4]

They also have built more rigor into their oversight practices. In the aftermath of the crisis, NACD gathered a special Blue Ribbon Commission on risk governance in 2009 to offer boards a blueprint for effective risk oversight. The principles espoused by the Commission's report remain as applicable today as they were almost a decade ago, and it is encouraging to see that many of its recommendations have been adopted by a majority of boards, as evidenced in NACD's most recent board governance surveys. (See side bar.)

BOARD RISK-OVERSIGHT PROGRESS SINCE 2009

1. NACD RECOMMENDATION: Work with management to understand and agree on the types (and format) of risk information the board requires. **Adopted by 79 percent of boards**
2. NACD RECOMMENDATION: Assess the risk in the company's strategy. **Adopted by 64 percent of boards**
3. NACD RECOMMENDATION: Define the role of the full board and standing committees with regard to risk oversight. **Adopted by 60 percent of boards**
4. NACD RECOMMENDATION: Closely monitor potential risk in the company's incentive structure. **Adopted by 57 percent of boards**

Sources: *NACD Blue Ribbon Commission Report on Risk Governance: Balancing Risk and Reward (2009)* and *2017–2018 NACD Public Company Governance Survey*

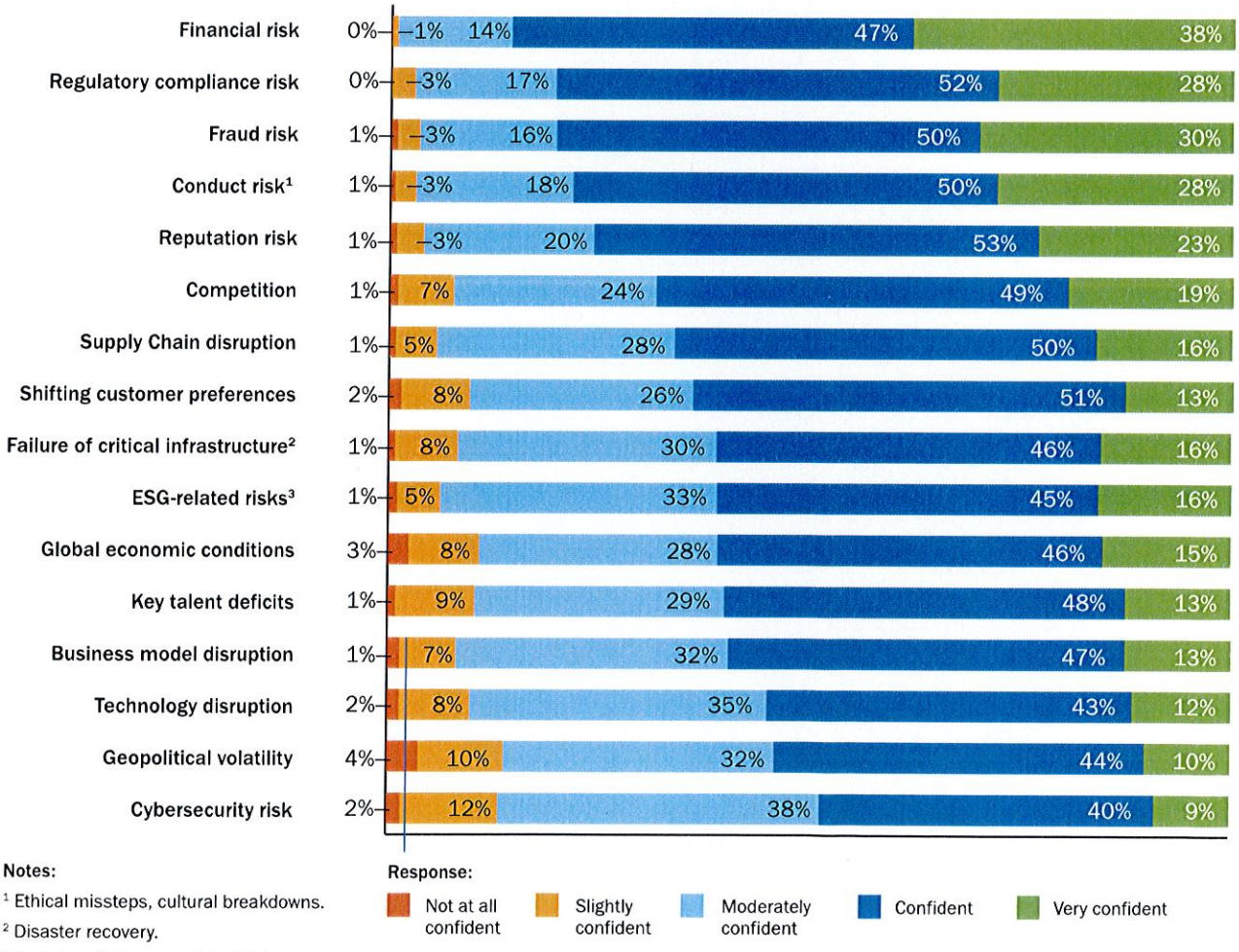
[4] These findings are based on unpublished survey responses from 587 public company corporate directors and executives which were obtained by NACD in June and July 2017.

But Is the Approach No Longer Fit for Purpose?

Board risk oversight practices have matured significantly over recent years. But many of these processes may not be designed to help boards and management focus optimally on today's most critical risk issues—issues that can disrupt their organization's business model and strategic objectives. Collectively, the results from the NACD and Protiviti/NC State studies suggest changes may be warranted to how organizations approach risk management and boards approach risk oversight. If these issues are left unaddressed, organizations may be less prepared to face new risk events that might ultimately undermine their fundamental business model and drivers of growth.

EXHIBIT 9

How confident are you in the ability of management to effectively manage the following risks?



Notes:

[1] Ethical missteps, cultural breakdowns.

[2] Disaster recovery.

[3] Including CSR and sustainability.

Note: +/- 100 due to rounding

Source: These findings are based on unpublished survey responses from 587 public company corporate directors and executives which were obtained by NACD in June and July 2017.

When assessing current levels of preparedness, it is striking to see that boards express the most confidence about management's ability to address those risks—financial and compliance—that were top of mind in the years following the financial crisis, but they are least confident about the management of risks that most significantly threaten the achievement of strategic objectives *today*—most notably, technology disruption, geopolitical volatility and cybersecurity threats.

Moreover, the *2017–2018 NACD Public Company Governance Survey* results suggest boards are spending either enough or too much meeting time on the review of compliance and financial reporting risk. In other words, these boards and companies may still be "fighting the last war"—fixating on "yesterday's" risks—that are well-understood and well-controlled in comparison to the more disruptive strategic risks.

This skewed and sometimes rigid focus on controlling financial and compliance risks may have also exacted a significant opportunity cost by reducing companies' confidence in taking risk. According to analysis published in the *Harvard Business Review*,[5] 60 percent of corporate strategy leaders believe "their company's decision-making process is too slow, in part because of an excessive focus on preventing risk," while only 20 percent of these leaders would describe their companies as "risk seeking." This degree of risk aversion may have slowed down corporate responses in recent years to disruptive threats in an environment where incumbents are exposed to "born digital" start-ups: companies that are focused on transforming customer experiences and enabled by the hyperscalability of digital business models and a lack of entry barriers. The irony of this risk-averse behavior is that it may in fact create even greater business-viability risks.

Institutional investors also are exerting pressure on boards to find a better balance between compliance-driven and strategy-focused risk oversight.

Institutional investors also are exerting pressure on boards to find a better balance between compliance-driven and strategy-focused risk oversight. They expect boards to be less focused on procedural matters, and they want boards to prioritize their proactive engagement with strategy and with the risks that could jeopardize the strategy in order to help drive long-term value creation. In 2017, Vanguard published guidance about four pillars of good governance, with board risk oversight being the fourth pillar, emphasizing that "directors are shareholders' eyes and ears on risk" and that "shareholders rely on a strong board to oversee the strategy for realizing opportunities and mitigating risks."[6]

A Key Question for Directors: Are we falling short and, if so, where?

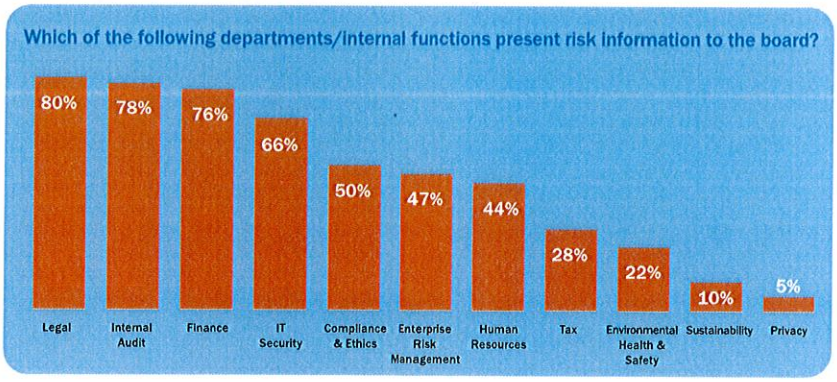
While the first-generation ERM programs adopted by companies created critical foundations for risk discipline, continued advancements of those programs are warranted to ensure that they are effective in helping the organization's leadership more proactively identify and manage the risk shocks of today's business environment. It's not just that boards and management teams are looking at risks retrospectively; the design and execution of pioneering ERM programs have also started to reveal several structural flaws:

[5] "How to Live with Risks," *Harvard Business Review*, July–August 2015.
[6] Vanguard, "An Open Letter to Directors of Public Companies Worldwide," August 31, 2017.

- ***After initial support from the top, ERM programs at many companies are now seen as peripheral.*** ERM is often perceived as an appendage by senior management and even as a distraction from doing business. These programs often lack sufficient authority to drive real change, have limited reach into their organizations, and rarely have a "seat at the table" to influence major strategic choices.
- ***ERM effectiveness is further weakened by internal governance structures where treatment of key risks is siloed across departments.*** Fragmentation across HR, legal, compliance, IT, procurement, and finance, for example, can inhibit discussions about how risks interact—a key point given the five interrelated themes cited earlier. Issues arise when risk ownership is migrated from the business line, where the risks manifest themselves, to functional specialists. A good illustration is the proliferation of risk reporting to the board among different management functions, which may complicate the board's understanding of enterprise risks if these departmental risk reports are not aligned. (See Exhibit 10).

Issues arise when risk ownership is migrated from the business line, where the risks manifest themselves, to functional specialists.

EXHIBIT 10



Source: These findings are based on unpublished survey responses from 587 public company corporate directors and executives which were obtained by NACD in June and July 2017.

- ***Many ERM programs are too reactive.*** They treat the symptoms of unnecessary risk-taking instead of attacking the disease. Risk professionals spend much of their time assessing and drafting mitigation plans for risks that should have been minimized or preempted at the line-manager level. For example, offering line managers better tools to make risk-informed decisions or to escalate risk concerns may reduce the need for additional internal controls and top-down policies.
- ***The assessment and the reporting of risk in many organizations are too static.*** For example, they offer little perspective about the future trajectory of risks and largely ignore projected changes in the company's overall risk profile in the medium and long terms. Simply stated, risk reporting does

not provide sufficient support to strategic decision-making processes. Similarly, information isn't always easy to interpret, and transparency about current vulnerabilities is lacking. In the *2017–2018 NACD Public Company Governance Survey*, 44 percent of directors who were dissatisfied with management's reporting about cyber risk indicated that the information didn't provide enough transparency about underlying problems.[7]

- ***Most risk assessments do not triangulate trends.*** Their analysis shows limited appreciation for interrelationships between, for example, technology, compliance, and reputational risks involving customer data that could inflict even more damage on the company. The growing interdependencies in today's global marketplace exacerbate the impact of this shortcoming.
- ***Although boards consider risks to the corporate strategy, deep-dive discussions about top risks and strategic choices at both the management and board levels happen separately and are rarely aligned.*** To illustrate, only 43 percent of corporate boards have developed or reviewed their company's risk-appetite framework to guide the strategy and determine which risks to take and which to avoid.[8]
- ***Traditional ERM approaches insufficiently recognize the importance of culture as the root of many risks.*** Fixated on policy and internal-control effectiveness, they don't assess whether the company is well-positioned through its conduct and culture to take the right risks while avoiding the wrong risks, from the perspective of the board and executive management.

Boards relying on risk management programs, that are limited by significant shortfalls, to inform their oversight may receive a false sense of security that key risks are well-managed, while in reality the level of risk exposure is growing.

The compound effect of these structural flaws is significant: boards relying on risk management programs, that are limited by significant shortfalls, to inform their oversight may receive a false sense of security that key risks are well-managed, while in reality the level of risk exposure is growing. A rapidly changing business environment compounds this challenge.

The bottom line is that boards need to review the quality of the risk-management process and the efficacy of their own risk-oversight practices through a new lens. Relevant questions include these:

1. Can we leverage risk management to thrive in an era of chaos and disruption, and not just hunker down?
2. Can we better anticipate future risks that can threaten long-term value creation?
3. Are we resilient and adaptive enough?
4. Does our culture enable us to identify and act on market opportunities and emerging risks as an early mover, or do we just follow the herd?

[7] NACD, *2017–2018 NACD Public Company Governance Survey* (Arlington, VA: NACD, 2017), p. 27.
[8] NACD, *2017–2018 NACD Public Company Governance Survey* (Arlington, VA: NACD, 2017), p. 24.

III. THE CALL TO ACTION

Four strategies for overcoming the risk-oversight gap

No process can be static in an ever-changing world driven by a myriad of external and internal factors. Every process requires improvement—continuously. The board risk-oversight process is no exception. In the case for action, we suggested that boards may be facing gaps in this process. The following strategies offer a roadmap to help close the risk-oversight gap.

A Key Question for Directors:
Are we well organized for risk oversight in the age of technological acceleration, and supported by the diverse expertise and experience we need in order to discharge our oversight role effectively?

1. Revisit the board's risk-governance model and director skill sets.
As noted in our case for action, risk profiles are changing. Depending on the mix of the enterprise's macroeconomic, strategic, and operational risks, the board should consider whether it has access to the diverse expertise and experience needed—either on the board or among external advisors—to provide the necessary oversight. In addition, the board should rethink how its various committees and the full board review and oversee risks. For example, given the risk of digital disruption affecting the organization, does the board have a sufficient understanding of digital business models, digital ecosystems, and the potential for hyperscaling digital platforms that facilitate rapid growth to disrupt the company's business model?

A Key Question for Directors:
Are we mindful of signs of organizational resistance to change? Are we encouraging management to embrace change and lead necessary transformations?

2. Focus on behavior: make culture an enterprise asset as well as an oversight priority.
Directors should consider engaging in open, transparent discussions with management about whether the organization's culture is impeding awareness of risk and communication about top risk exposures to the board for their oversight and review. Culture is almost always where reputation and financial performance outcomes start, as it is a potent source of strength or weakness for an organization. A strong culture is a critical asset for any brand and it is just as important as effective strategy and effective performance.

The board should expect management to understand the culture at the middle and at the bottom of the organization, and whether the mood in the middle is aligned with the tone at the top. Concerns that this topic may be "too soft" for objective assessment should not distract the board's focus on the real question:

> *Does the CEO really want to know the unvarnished truth about people's perceptions across the entity, and is he or she prepared to act on that knowledge?*

A "speak up" culture that encourages transparency and sharing of contrarian information and bad news entails convincing employees that it can be done without fear of repercussions to their careers or to their compensation. Candid, open, and constructive board and management interactions should consider tough questions:

- Are significant risk issues and market opportunities warranting attention by executive management and the board escalated to our attention on a timely basis?

- Does management apprise the board—in a timely manner—of significant risks or significant changes in the organization's risk profile?
- Is there a process for identifying emerging risks? Does the risk-identification process allow the board and management enough time to adequately consider response plans?
- Is adequate attention given to red flags which indicate a dysfunctional culture that suppresses the escalation of important risk and opportunity information, or that encourages unacceptable risk-taking?
- Are the risk management and internal audit functions giving sufficient emphasis to cultural matters, and reporting to us on a timely basis?
- Are we addressing the warning signs posted by risk management and internal audit on a timely basis?
- When there is evidence that one or more critical assumptions underlying the strategy are becoming, or have become, invalid, do we act on that knowledge in a timely way to revisit our strategy and undertake appropriate midcourse adjustments?

At a recent NACD directors' roundtable facilitated by Protiviti, the participating directors noted the importance of boards encouraging management to consider culture-related measures so that they can come forward with an approach that makes sense. The point is telling: what gets measured, matters.

3. Focus on the quality of the risk-management process.

A Key Question for Directors:
Does the risk-management process bring new value and insights to the dialogue and facilitate risk-informed decision making?

In addition to culture, directors may also want to discuss with management the organization's processes for managing enterprise-wide risks. Given the pace of change experienced in the industry and the nature and relative riskiness of the organization's operations, does the board understand the quality of the process informing its risk oversight? How much manual effort is required to generate the reports used in board meetings? How actionable is the entity's risk information for decision making? These and other questions focus on the robustness and maturity of the risk-management process.

As companies reimagine their core operating processes and key functions using the tools of the digital age—speech recognition, robotics, AI, machine learning, mobile technologies, advanced data analytics, and visualization techniques—boards should inquire as to whether risk management is being enhanced as well. Directors should ensure that the critical attributes of risk excellence are present:

- Critical enterprise risks are delineated from the day-to-day risks of managing the business so as to focus the dialogue on the risks that matter to the C-suite and the board.
- Accountability is established for risks that are embedded in the lines of business and core processes.
- Actionable risk information is not only reported up but also widely shared to enable more informed decision making.
- An open, positive dialogue for identifying and evaluating opportunities and risks is encouraged. Consideration should be given to reducing the risk of

undue bias and groupthink so that adequate attention is paid to differences in viewpoints that may exist among different executives and global jurisdictions.

- Risk reporting is dynamic and multidimensional, allowing decision makers to appreciate the impact of risk and opportunity on strategic goals and objectives, and allowing them to anticipate possible disruption of the business model.
- Decision makers have access to advanced data analytics and visualization techniques to assist them in reaching the best decisions.

Directors should request that management take a fresh look at the entity's risk management and the adequacy of risk information. To this end, the COSO ERM Framework[9] offers a summary of principles that enable companies to benchmark the quality of their risk-management process. The bottom line is that an annual listing of risks will not sustain board confidence in the digital age.

4. Ensure management integrates risk considerations into strategy, performance, and decision making.

A Key Question for Directors:
Are we satisfied that risk management is sufficiently integrated with strategy setting and execution, performance management and monitoring, and critical decision-making processes?

The rapid pace of change in the global marketplace provides a risky environment for entities of all types. The unique aspect regarding an exposure to disruptive change is that it presents a choice: on which side of the change curve do organizations want to be? For example, organizations need to make a conscious decision about whether they are going to be the disrupter and try to lead as a transformer of the industry or, alternatively, whether they are going to play a waiting game, monitor the competitive landscape, and react appropriately—and in a timely manner—to defend their market share.

It is important that the board ground its risk oversight with a solid understanding of the entity's key strategic drivers and of significant assumptions made by management that underpin the strategy. In addition, directors should have a mutual understanding with management of the enterprise's risk-appetite framework. Boards should ask management whether they:

- monitor significant risks related to the execution of the strategy and business model and consider the enterprise's risk appetite and risk tolerances in meeting key objectives;
- evaluate the risk-reward balance associated with different strategic alternatives to understand the risks the enterprise is taking on as a result of each alternative for creating enterprise value;
- track the external environment and macroeconomic trends for changes in significant assumptions underlying the strategy and continued relevance of the business model, and evaluate whether the trends exacerbate risk and/or create market opportunities;
- sustain a periodic board-level dialogue regarding the appetite for risk and whether the organization's risk profile is consistent with that appetite;

[9] *Enterprise Risk Management—Integrating with Strategy and Performance*, Committee of Sponsoring Organizations (COSO) of the Treadway Commission, June 2017, available at www.coso.org.

- integrate lead indicators and advanced data analytics into performance monitoring so that it becomes more anticipatory and forward-looking and supports risk-informed decision making and increased accountability; and
- involve the board in key decisions—e.g., acquisitions of new businesses, entry into new markets, introductions of innovative technologies, or alterations of key assumptions underlying the strategy—and invite challenge and open discussion regarding those decisions.

With the speed of change and constant advances in technology, the ability to respond rapidly to new market opportunities and emerging risks can be a major competitive advantage. Conversely, failure to remain abreast or ahead of the change curve can place an organization in the position of becoming captive to events rather than charting its own course. Therefore, directors need to ensure that risk and risk management are not appendages to strategy setting, performance management, and decision making.

In Closing . . .

We have presented a case for boards to take a fresh look at how they are approaching risk oversight, including how the entity's ERM is informing that oversight. We've noted that current risk-management practices for many industries are largely rooted in the prior century. Accordingly, the big question is this:

> *Are we prepared to improve our risk management and risk oversight or, alternatively, do we face the challenges of the next 10 years in the digital age with what we've been doing over the last 10 years?*

The nature, velocity, and persistence of risks have changed. Consequently, it's time for boards to revisit their governance model and skill sets and refresh the focus of their risk oversight. To that end, directors should expect management to enhance the quality of risk-management processes using new technologies. They should also expect management to better integrate risk considerations into their strategy setting and execution, their performance management, and their decision-making processes. In addition, closer attention must be given to sustaining a strong risk culture.

AVAILABLE RESOURCES FOR DIRECTORS

Report of the NACD Blue Ribbon Commission on Risk Governance: Balancing Risk and Reward (2009)
A guide for boards to improve their risk-oversight processes. Available at NACDonline.org.

Director Essentials: Strengthening Risk Oversight (2016)
A detailed overview of practices each director can adopt to strengthen risk oversight, including red flags, suggested approaches, and questions to ask. Available at NACDonline.org.

NACD Advisory Council on Risk Oversight: Board-Management Dialogue on Risk Appetite (2017)
This publication focuses on the board's role in the development and oversight of risk appetite, highlighting such matters as aligning the risk-appetite statement with company strategy and using the risk-appetite statement to inform critical processes and decisions. Available at NACDonline.org.

NACD Compensation Committee Chair Advisory Council and the Advisory Council on Risk Oversight: Incentives and Risk Taking (2017)
Discusses leading practices related to incentives and risk-taking, including reviewing whether the board has an appropriate balance of metrics and is calibrating goals and upside opportunity appropriately, considering the quality of performance. Available at NACDonline.org.

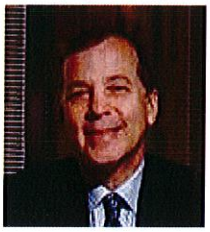
TBI Protiviti® Board Risk Oversight Meter™
This easy-to-use, web-based tool assists boards of directors with assessing, improving, and benchmarking the effectiveness of their risk-oversight processes. The tool was developed by The Board Institute Inc. (TBI) and Protiviti in collaboration with an advisory consortium of governance experts and active board members. For more information, see theboardinstitute.com.

Protiviti Board Perspectives: Risk Oversight
The longest-running monthly series of its kind devoted to board risk oversight, this resource offers insight into a wide variety of topics of interest to directors. Available at Protiviti.com/Board.

The ERM Initiative's ERM Library
This online portal provides access to abstracts of more than 500 articles, white papers, research studies, and videos on a variety of ERM topics. The library's table of contents and internal search engine can be used to pinpoint resources related to all components of an ERM process. Available at erm.ncsu.edu.

KEY CONTRIBUTORS

MARK S. BEASLEY, CPA, PhD, leads the ERM Initiative at North Carolina State University, which provides thought leadership on enterprise risk management practices. He served on COSO's ERM Framework Advisory Council, in addition to serving on the COSO board of directors for more than seven years. He consults with boards and senior executive teams on risk governance issues, and has published more than 90 articles, research monographs, books, and other thought-leadership pieces.



JIM DELOACH is a managing director of Protiviti, a global consulting firm. With more than 35 years of experience, he assists companies with integrating enterprise risk with strategy, business planning, and performance management. The author of several books, DeLoach is widely published and quoted in the press. With noted expertise in corporate governance and internal control systems, he has worked with hundreds of companies and groups in 30 countries and has served on the COSO Advisory Council for 10 years.

FRISO VAN DER OORD is director of Research, responsible for all NACD content development. He is an experienced governance advisor and business line manager, who has worked over the last 15 years with Fortune 500 and global executives on major risk, compliance, and integrity challenges, including serving in leadership roles at CEB and LRN. He holds a master of arts degree in International Relations from Johns Hopkins University's SAIS Program.

CONTRIBUTING PARTNERS

protiviti®
Face the Future with Confidence

PROTIVITI is a global consulting firm that delivers deep expertise, objective insights, a tailored approach, and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independently owned Member Firms provide consulting solutions in finance, technology, operations, data, analytics, governance, risk, and internal audit to our clients through our network of more than 70 offices in over 20 countries. We have served more than 60 percent of *Fortune* 1000® and 35 percent of *Fortune* Global 500® companies. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services.

NC STATE UNIVERSITY

ABOUT NORTH CAROLINA STATE UNIVERSITY'S ERM INITIATIVE

The Enterprise Risk Management (ERM) Initiative in the Poole College of Management at North Carolina State University provides thought leadership about ERM practices and their integration with strategy and corporate governance. Faculty in the ERM Initiative frequently work with boards of directors and senior management teams helping them link ERM to strategy and governance, host executive workshops and educational training sessions, and issue research and thought papers on practical approaches to implementing more effective risk oversight techniques (www.erm.ncsu.edu).

ABOUT NACD

NACD ELEVATE BOARD PERFORMANCE

THE NATIONAL ASSOCIATION OF CORPORATE DIRECTORS (NACD) empowers more than 19,000 directors to lead with confidence in the boardroom. As the recognized authority on leading boardroom practices, NACD helps boards strengthen investor trust and public confidence by ensuring that today's directors are well prepared for tomorrow's challenges. World-class boards join NACD to elevate performance, gain foresight, and instill confidence. Fostering collaboration among directors, investors, and corporate governance stakeholders, NACD has been setting the standard for responsible board leadership for 40 years. To learn more about NACD, visit www.NACDonline.org.

NACD | ELEVATE BOARD PERFORMANCE

Back To Agenda

Board of Trustees
Audit, Risk Management, Compliance, and Ethics Committee
September 6, 2018

Agenda Item: IV.A.	Annual Employee COI Reporting
Responsible Person:	Mike Van Scott
Action Requested:	None - Information
Notes:	N/A

Back To Agenda

EAST CAROLINA UNIVERSITY
Office of Research Integrity & Compliance
Brody Medical Sciences Building, 4N-64• 600 Moye Boulevard • Greenville, NC 27834
Office **252-744-2914** • Fax **252-744-2284** • **www.ecu.edu/irb**

MEMO: ECU Board of Trustees

DATE: August 17, 2018

FROM: Michael R. Van Scott, Ph.D.
Sr. Associate Vice Chancellor for Research
Division of Research, Economic Development, and Engagement

RE: 2017-2018 Conflict of Interest Disclosures

Federal regulation requires that all individuals paid from federal funds disclose potential conflicts of interest (42CFR50); and UNC policy and ECU regulations (UNC 3002.2.2, ECU REG10.45.02, REG 01.15.03, require all EHRA employees to disclose potential conflicts of interest annually.

For the 2017-2018 fiscal year:

1. 100% of all employees – faculty, staff, students, agents, and independent individuals - listed on a federal award issued to ECU completed the Annual Disclosure,
2. 99.74% of EHRA employees completed the Annual Disclosure, and
3. The 0.26% of EHRA employees that did not disclose consisted of non-tenure track faculty, and temporary and part-time employees.

The following changes to the annual disclosure process are anticipated for 2018-2019:

1. All new EHRA hires will be required to complete the Annual Disclosure within 30 days of their start date,
2. Conflicts of Interest training will be mandatory for all new employees, and
3. Quarterly reports or disclosures by non-tenure track, temporary, and part-time individuals will be developed to monitor compliance in this group of employees and facilitate intervention prior to the close of the reporting period.

Back To Agenda

Board of Trustees
Audit, Risk Management, Compliance, and Ethics Committee
September 6, 2018

Agenda Item: V.A.	Update on PCI Compliance
Responsible Person:	Robin Mayo
Action Requested:	None - Information
Notes:	N/A

Back To Agenda

COMPLIANCE MANAGEMENT
PCI COMPLIANCE UPDATE

Board of Trustee Meeting
Audit Committee
September 2018

Robin Mayo, MBA, PCIP

Back To Agenda

PCI Compliance

What does PCI-DSS compliance mean?

- In security terms, it means that your business adheres to the PCI DSS requirements for security management, policies, procedures, network architecture, software design and other critical protective measures.
- In operational terms, it means that you are playing your role to make sure that your customers' payment card data is being kept safely throughout every transaction, and that they – and you- can have confidence that they are protected against the pain and cost of data breaches.

Back To Agenda

ECU's Approach to PCI

- eCommerce Manager/PCI
- PCI Gap Analysis
- PCI Compliance Committee
- PCIP Certification (Payment Card Industry Professional)
- Educate/Train Campus
- Collaboration
  - ITCS
  - Materials Management (Purchasing)
  - Internal Auditor
  - Campus Merchants/departments

Back To Agenda

PCI Compliance

- Initial Gap Analysis completed Fall 2013 (PCI 2.0); repeated January 2015 (PCI 3.0)
- 65 items were identified (PCI 3.0)
- Remediation project established
- PCI 3.1 released April 2015
- PCI 3.2 released April 2016
- Compliance achieved and SAQ-D submitted in July 2018
  - 329 requirements that must be met

Back To Agenda

E-Commerce at a Glance

Item	Volume
Merchant Accounts	117
Transaction volume (#)*	552,297
Transaction volume ($)*	$42,798,951.80
U-stores	135
U-Pay Sites/TouchNet Integrations	12
Third party POS systems	6
POS Terminals/Card readers	162
Pay by Space Stations (meters)	9
Employees impacted/trained	834

*Values represent calendar year 2017, do not include online tuition payments or online payments received by ECU Physicians

Back To Agenda

The Future

- PCI Compliance is an on-going, day to day process
- Annual SAQ-D (compliance attestation)
- Migrating to P2PE (Point to Point Encryption)
- Education/Training
- Preparing for PCI DSS 4.0

Back To Agenda

Board of Trustees
Audit, Risk Management, Compliance, and Ethics Committee
September 6, 2018

Agenda Item: VI.	Office of Institutional Integrity
Responsible Person:	Michelle Evans
Action Requested:	None - Information
Notes:	N/A

Back To Agenda

Office of Institutional Integrity

East Carolina University

Back To Agenda

OII Focus and Guidance

- Office of Inspector General Work Plan and Updates
- Office of Civil Rights

  (HIPAA Privacy Rule & HIPAA Security Rule)
- State and Federal Statutes (e.g. CMS billing and documentation requirements)
- ECU Best Practices, Policies, Procedures, Regulations
- Industry Standards

Back To Agenda

Overview of OII

- Billing and Documentation Compliance
- HIPAA Privacy & HIPAA Security
- Other functions:
  - Clinical trials research billing reviews
  - Oversee Vendor management process
  - Oversee debarment review process
  - Oversee patient chart access and system logs
  - Pharmacy prescription reviews
  - Reviews ECU Physicians contracts for regulatory requirements
  - Reviews ECU HIPAA Business Associate Agreements for 3rd party relationships
  - Education (Cornerstone annual requirements, orientation, ad hoc)
- Monitoring 40%, Consultations 35%, Investigations 25%

Back To Agenda

High Risk Areas for OII

- Provider Billing and Documentation

  (CERT, OIG, DMA, TPE, Medicare post payment reviews, RAC audits, ZPIC Audits, internal reviews)
- Clinical Trial Documentation Reviews
- HIPAA Privacy Violations
- HIPAA Security Safeguards

Back To Agenda

ECUP Pharmacy Quarterly Prescription Reviews:

- Prescriptions written by ECU-P provider to another ECU-P provider and potential family members
- Random data using DHHS RAT-STATS statistical software for 10% of prescriptions identified during time period
- Completed one full year of reviews
- OII reviews documentation against the prescription written. ECUP Medical Director is involved in final clinical analysis and approval.

Back To Agenda

Billing Compliance 2017

- Random Annual Reviews (2017 – 2410 charts reviewed with an average score of 90%). This did not include a special project of 409 chart reviews.

Reviews CY 2017	Jan-17	Feb-17	Mar-17	Apr-17	May-17	Jun-17	Jul-17	Aug-17	Sep-17	Oct-17	Nov-17	Dec-17	Scoring Total
Number of Providers Reviewed	30	30	17	9	10	13	16	23	26	27	22	18	241
Average Score	92.43%	91.57%	90.00%	87.56%	95.00%	90.62%	94.25%	92.09%	91.23%	84.37%	84.55%	88.33%	90.17%
Number Passed	30	28	16	7	10	11	16	22	25	22	17	17	221
Number Failed	0	2	1	2	0	2	0	1	1	5	5	1	20

100% = No Errors
99% - 80% = Passed
79% or lower = Failed

Back To Agenda

Billing Compliance 2018

Reviews CY 2018	Jan-18	Feb-18	Mar-18	Apr-18	Apr-Bench	May-18	Jun-18	Jul-18	Aug-18	Sep-18	Oct-18	Nov-18	Dec-18	Scoring Total
Number of Providers Reviewed	30	15	20	15	27	22	22	23						174
Average Score	89.44%	91.08%	88.24%	82.50%	83.14%	88.18%	86.69%	92.82%						87.76%
Number Passed	26	14	15	10	22	17	17	18						139
Number Failed	4	1	5	5	5	5	5	5						35

Back To Agenda

Billing Compliance Benchmark Reviews

2018 CVS review complete. Internal Medicine pending.

Example:

CVS Jan 2017 – Dec 2017	Dr. A		Dr. B		Dr. C							
By Specialty												
New Out-Patient	# Billed	% Billed over total billed	# Billed	% Billed over total billed	# Billed	% Billed over total billed	Total # Billed	Departmental benchmark	FPSC National benchmark	Medicare NC benchmark	Medicare National benchmark	Medicare Average
99201	1	0.86%	0	0.00%	0	0.00%	143	3.12%	0.43%	0.10%	0.20%	0.15%
99202	24	20.69%	2	6.67%	10	16.39%	932	20.34%	2.41%	2.10%	1.70%	1.90%
99203	33	28.45%	2	6.67%	8	13.11%	1,878	40.98%	18.03%	14.50%	16.80%	15.65%
99204	57	49.14%	25	83.33%	41	67.21%	1,550	33.82%	53.32%	62.10%	61.70%	61.90%
99205	1	0.86%	1	3.33%	2	3.28%	80	1.75%	25.81%	21.20%	19.50%	20.35%
TOTAL	**116**		**30**		**61**		**4,583**					

Back To Agenda

Billing Compliance Benchmark Reviews

2018 CVS review complete. Internal Medicine pending.

Example:

CVS Jan 2017 – Dec 2017	Dr. A		Dr. B		Dr. C							
By Specialty												
New Out-Patient	# Billed	% Billed over total billed	# Billed	% Billed over total billed	# Billed	% Billed over total billed	Total # Billed	Departmental benchmark	FPSC National benchmark	Medicare NC benchmark	Medicare National benchmark	Medicare Average
99201	1	0.86%	0	0.00%	0	0.00%	143	3.12%	0.43%	0.10%	0.20%	0.15%
99202	24	20.69%	2	6.67%	10	16.39%	932	20.34%	2.41%	2.10%	1.70%	1.90%
99203	33	28.45%	2	6.67%	8	13.11%	1,878	40.98%	18.03%	14.30%	16.80%	15.65%
99204	57	49.14%	25	83.33%	41	67.21%	1,550	33.82%	53.32%	62.10%	61.70%	61.90%
99205	1	0.86%	1	3.33%	2	3.28%	80	1.75%	25.81%	21.20%	19.50%	20.35%
TOTAL	**116**		**30**		**61**		**4,583**					

Back To Agenda

Clinical Trials Billing Reviews

Medicare pays for significant amount of clinical research in “qualified studies.” OII reviews potential billing errors.

- Ensure that special modifiers are placed on charges for clinical trial participants.
- Ensure that Medicare is not charged when sponsor has agreed to pay for services.
- Review billing for services promised free by informed consent.
- Ensure that billing is consistent with contract and protocol.
- Ensure that Medicare Advantage is not charged for clinical research
- OII advises departments on errors and repayment requirements.

Back To Agenda

Clinical Trials Billing Reviews

Clinical Trial Reviews 2018	Totals
Front End Reviews	26
Back End Reviews	345
Errors Discovered	24

Front end reviews:

A Coverage Analysis is completed on the study before the study enrolls patients. All appropriate data is reviewed to verify that all services/procedures are deemed appropriate as either routine verses billed to the sponsor.

Back end reviews:

A billing review to ensure that the patient was billed appropriately either to the sponsor, insurance, or patient.

Back To Agenda

HIPAA Requirements Oversight

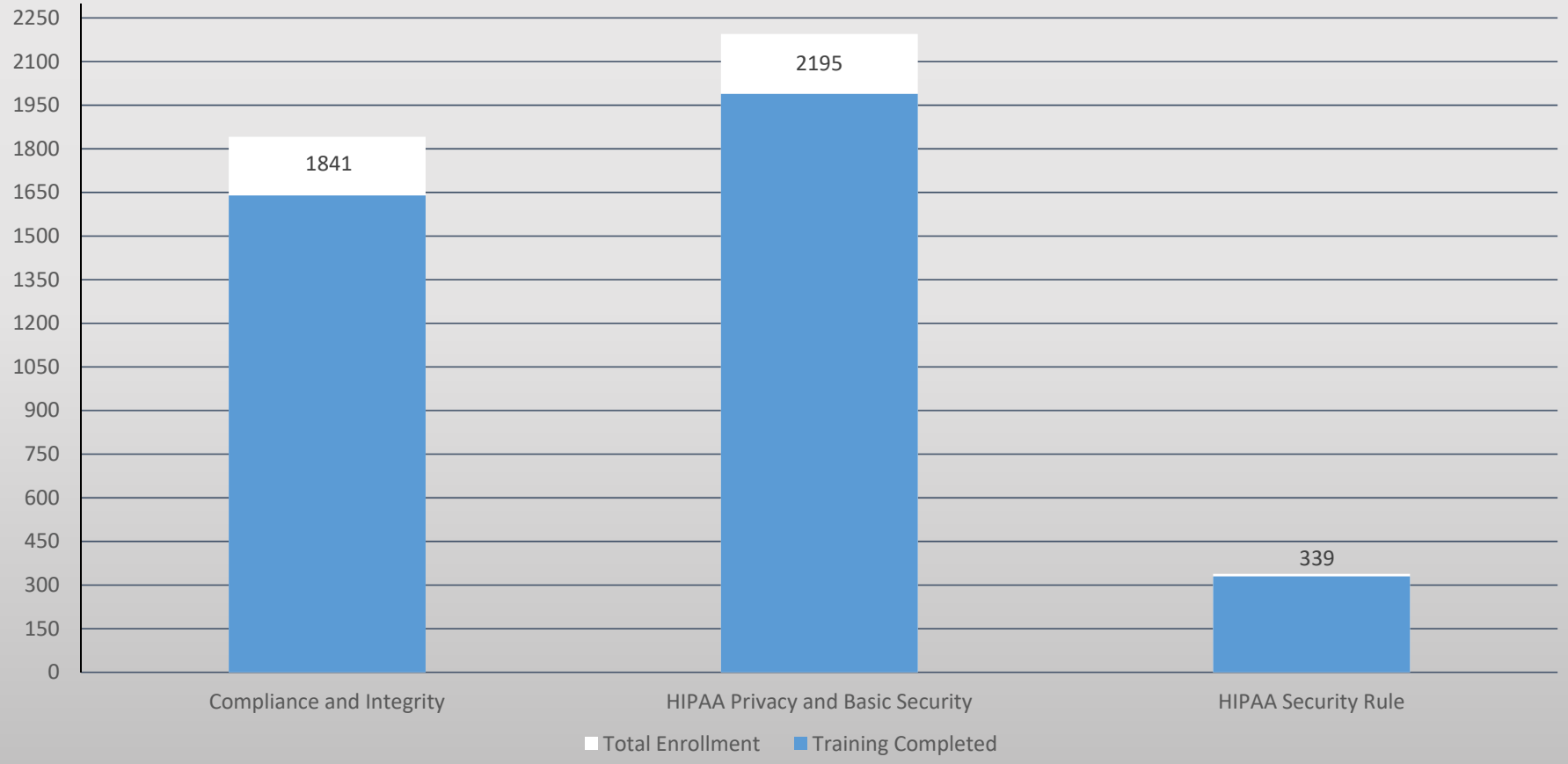
- Investigations, consultation & education
- Conduct and facilitate risk assessments for breach notification determinations and patient notifications
- HIPAA documents and agreements

Major initiatives this year:

- Implementation of system log reviews for HIPAA systems, across ECU
- Completion of the Risk Management Global Matrix for HIPAA
- Completion of the University Business Continuity Plan for HIPAA
- Consolidated and revised all HIPAA security ECU regulations and created a HIPAA Security manual (15 policies/34 standards to 15 total regulations)

Back To Agenda

Annual Training



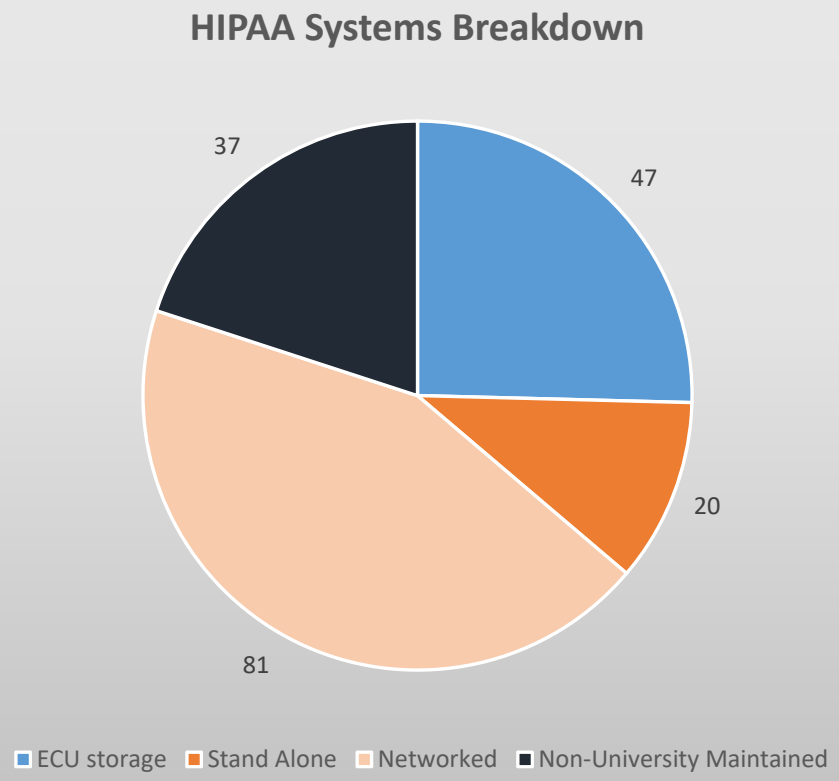
Back To Agenda

HIPAA Security Requirements Oversight

- Systems within ECU that contain electronic protected health information (ePHI)
- Works with ITCS to set guidelines for protection against threats/hazards of integrity and security of ePHI, and/or unauthorized use and disclosures.
- Maintain HIPAA system database for University
- Create and coordinate HIPAA annual regulatory risk assessments
- Assist the University in establishing administrative, physical, and technical compliance safeguards.

Back To Agenda

HIPAA Systems Inventory



ECU Network Storage

- Department/Clinic utilizes an ECU approved Network Storage location (Piratedrive or REDCap) to store ePHI.

Stand Alone

- This is a closed System (ex. EKG Machine). System is never connected to the network and operates as a stand-alone system.

Networked

- System is connected to the ECU network at any time (ex. Ultrasound Machine – images upload to EHR or Piratedrive).

Non-University Maintained

- This system uses a 3rd Party, cloud, or vender service to store ePHI (ex. Pharmacy repository). There must be a BAA in place to comply with all regulations.

Back To Agenda

HIPAA Privacy Investigations

Jan - Dec 2017: 101 investigations

Jan - August 2018 : 88 investigations

- These investigations resulted in 27 HIPAA violations (22 in 2017; 10 in 2018)
- Violations ranged from Level 1 to Level 3
- Communicated investigation ”trends” to HIPAA Steering Committee, Nursing Leadership group, individual clinics/departments, others as appropriate

Back To Agenda

HIPAA Breaches

2017 HIPAA Breaches - 59

2018 (Jan-August) HIPAA Breaches - 22

Breach to affected individuals, the Secretary (HHS),
and, in certain circumstances, to the media.

Business associates must notify covered entities if a breach occurs
at or by the business associate.

Back To Agenda

2018 Top Five HIPAA Investigation Topics

1) Emails containing PHI sent to the incorrect recipient
2) AVS documents given in error to an unintended recipient
3) Unintended mailed information received by an unintended recipient
4) Unintended written prescription errors
5) Unintentional demographic errors resulting in information sent to incorrect address

(Jan - July 2018)

Back To Agenda

Office of Institutional Integrity

Michelle C. Evans, MPA, CHC, CHPC
Interim Chief Institutional Integrity Officer
ECU HIPAA Privacy Officer
ECU HIPAA Security Officer

252.744.5200

evansmi@ecu.edu

Back To Agenda

Board of Trustees
Audit, Risk Management, Compliance, and Ethics Committee
September 6, 2018

Agenda Item: VII.	Closed Session
Responsible Person:	Kel Normann, Chair
Action Requested:	
Notes:	N/A

Back To Agenda

Board of Trustees
Audit, Risk Management, Compliance, and Ethics Committee
September 6, 2018

Agenda Item: VIII.	Other Business
Responsible Person:	Kel Normann, Chair
Action Requested:	
Notes:	N/A

Back To Agenda