East Carolina University | Board of Trustees Meeting

Audit Committee Meeting | July 14, 2016

Agenda

I. Approval of April 7, 2016 Minutes — Action

II. Office of Internal Audit – Ms. Stacie Tronto

- A. Annual Engagement Plan 2016 - 2017 — Action
- B. Internal Audit Charter — Action
- C. Audit Committee Charter — Action
- D. Certification Letters — Action

III. Research Compliance - Ms. Norma Epley

- A. Results of FDA Review — Information

IV. Enterprise Risk Management - Mr. Tim Wiseman

- A. ERM Update — Information
- B. COSO Update — Information
- C. Article — Information

V. Other Business

VI. Closed Session

East Carolina University
Board of Trustees
Audit, ERM, Compliance and Ethics Committee
July 14, 2016

Session	Audit, ERM, Compliance and Ethics Committee
Responsible Person	Kel Normann, Chair
Agenda Item	I.
Item Description	Approval of Minutes – April 8, 2016
Comments	
Action Requested	Approval
Disposition	
Notes	

Back To Agenda

DRAFT

Minutes from ECU BOT Audit Committee
April 7, 2016
East Carolina Heart Institute

The Audit Committee of the ECU Board of Trustees met in regular session on April 7, 2016 at 10:00am in the East Carolina Heart Institute on the campus of East Carolina University. Committee members present included Kel Normann (Chair), Vern Davenport, Mark Copeland, Bob Plybon, and Terry Yeargan

Other board members present included Leigh Fanning.

Others present included Chancellor Steve Ballard, Phyllis Horns, Rick Niswander, Nick Benson, Gary Vanderpool, Dee Bowling, Tim Wiseman, Ken DeVille, Michelle Evans, Norma Epley, Hiromi Sanders, Kate Scarabelli, Julius Norwood, Stacie Tronto, and Wayne Poole.

Kel Normann, Chair of the Audit Committee, convened the meeting at 10:00AM. 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 February 18, 2016 audit committee meeting.

Action Item: The minutes of the February 18, 2016 audit committee meeting were approved with no changes.

Mr. Tim Wiseman provided the **Enterprise Risk Management** (**ERM)** update.
Mr. Wiseman presented an update on the Enterprise Risk Management activity. Mr. Wiseman advised the committee that an Interim Regulation on University Youth Programs has been drafted and will be in place very soon. This will provide the backbone for the oversight of youth-related camps and programs throughout the University. Mr. Wiseman advised that the risk management/insurance function for the University will be moving from Campus Operations into the ERM office. This should provide several benefits and synergies. The ERM office will soon be launching an ERM awards program for the University and will seek nominations for individuals and departments that are progressive in incorporating risk considerations into their operations. Mr. Wiseman stated that the ERM top risk survey and review process will begin again in the fall of 2016.

Mr. Wiseman provided an article on *Executive Perspectives on Top Risks for 2016* for the committee members to review. The article was published by NCSU. Mr. Wiseman noted that a recent survey revealed that the top risks facing boards of directors and executives across the globe are similar to the University's top risks.

Mr. Davenport mentioned the recent hospital ransomware attacks that have been covered by the media. He stated that ECU and Vidant should discuss whether or not these risks are sufficiently mitigated and how the entities would operate if such an incident occurred here. Dr. Benson stated that ECU has had conversations with Vidant about this, and that last month the Epic system was down for two days. ECUP validated that it can operate without the electronic health record in emergency situations.

Mr. Wiseman updated the committee on a UNC General Administration policy change. The UNC BOG Audit Committee has been renamed to the "Committee on Audit, Risk Management, and Compliance", and has been formally assigned the responsibility of oversight for the system's Internal Audit, Enterprise Risk Management, and Compliance-related issues. Ms. Tronto stated that the Board may need to consider renaming our Audit Committee to formally encompass risk management and compliance as well. Ms. Tronto will coordinate with the Chancellor, Board, and others in the coming months to determine how to approach this.

Ms. Stacie Tronto provided the **Internal Audit update**.
Ms. Tronto presented the Internal Audit dashboard for the 2015-2016 fiscal year to date (as of March 19, 2016). The Internal Audit team has completed 58% of the annual audit plan for the year (the target for the year is 80%). Ms. Tronto stated that the team is on track to meet or exceed the goal this year. The team's utilization rate

Back To Agenda

("direct" productivity hours) for the year to date is 77% for the auditors (the target is 75%), and 73% for the office as a whole, including the University Program Specialist, who performs a number of administrative duties for the office and is not an auditor.

Ms. Tronto stated that IA has completed 87 consultations this year to date, accounting for 19% of the office's hours. The target is for consultations to account for approximately 20% of IA's hours.

Ms. Tronto stated that University management has made satisfactory progress on 93% of the corrective actions/recommendations for which Internal Audit has completed a follow-up this year (the target is 95%). The three recommendations that have not yet been satisfactorily addressed are all related to the Division of Health Sciences, and Dr. Horns and Mr. Vanderpool are engaged in seeing that these are resolved. IA will complete another follow-up on these specific recommendations prior to June 30.

Ms. Tronto presented one proposed change to the FY 2016 engagement plan. Ms. Tronto proposed that a planned audit of the ECU Physicians patient billing cycle be changed to a consultation due to new leadership in the ECUP Clinical Financial Services area and process changes that are being implemented. Ms. Tronto stated that IA can provide greater value to management by consulting on these process changes rather than performing an audit at this time.

Action Item: The committee approved a motion to accept this proposed change to the annual audit plan.

Ms. Tronto updated the Committee on the Internal Audit Quality Assessment Review. The external reviewers were on site last week to perform the assessment of Internal Audit. The final report is pending, but Ms. Tronto stated that ECU Internal Audit received the highest possible rating with regard to its conformance to the *Standards for the Professional Practice of Internal Auditing*. The reviewers had a few recommendations for IA and University management to consider. These included things such as adopting a University-wide code of ethics and an Internal Control Policy, and considering audits of the University's overall governance. Ms. Tronto stated that she will seek input from Chancellor Ballard and Mr. Normann on these items. Ms. Tronto stated that the external reviewers had never seen an IA shop that was so well supported by University management and the Board. Mr. Normann expressed appreciation for the hard work of IA and stated that the comments from the external reviewers and from State Auditor Beth Wood confirm his belief that we have a top-notch IA team.

Ms. Norma Epley presented the **Research Compliance Report**

Ms. Epley presented information on the University's Institutional Review Board (IRB) for research involving human subjects. The IRB reviews all human research at ECU and Vidant. Ms. Epley stated that effective February 1, 2016, the University entered into an agreement with one external IRB to provide the reviews for specific industry-sponsored research studies in which the company's research protocol has already been reviewed by that external IRB. The University could potentially contract with two other commercial IRBs in the future, but that would require a change in the existing research insurance coverage.

Ms. Epley updated the committee on the pros and cons of using external/commercial IRBs. The pros include more research exposure for the University and a potential increase in the number and complexity of trials, which could be beneficial to the University and the people of eastern NC. The cons include some degree of loss of control over the review process. However, the University would retain responsibility for a number of ancillary and compliance-related reviews on all studies before participants could be enrolled.

Back To Agenda

Ms. Epley stated that as of this date, the vast majority (99%) of research studies are still reviewed by the University’s internal IRB. Ms. Epley stated that she will keep the committee apprised if plans evolve or changes are proposed to the current IRB structure.

Other Business
Mr. Normann asked if anyone had other business for the committee. No other business was brought forward by anyone in attendance.

There being no further business, the Audit Committee meeting was adjourned at 10:54 AM.

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

Back To Agenda

East Carolina University
Board of Trustees
Audit, ERM, Compliance and Ethics Committee
July 14, 2016

Session	Audit, ERM, Compliance and Ethics Committee
Responsible Person	Stacie Tronto, Chief Audit Officer
Agenda Item	II.
Item Description	Office of Internal Audit
Comments	
Action Requested	Approval
Disposition	
Notes	a. Annual Engagement Plan 2016-17 b. Internal Audit Charter c. Audit Committee Charter d. Certification Letters

Back To Agenda

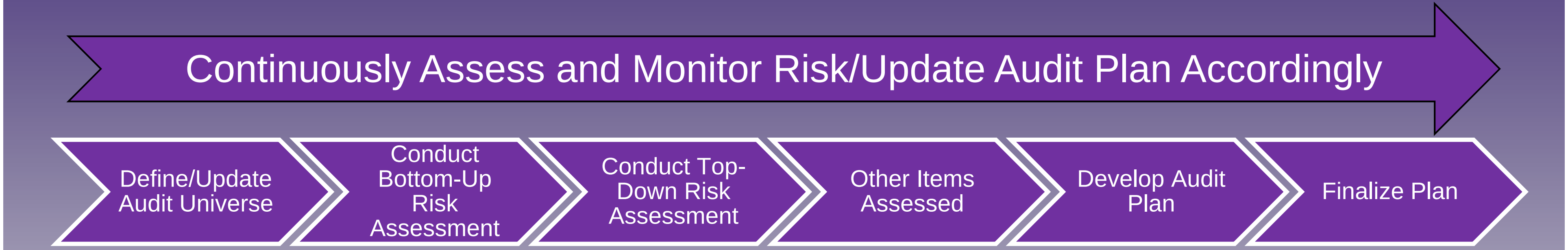
Risk Based Audit Plan - Objectives

- Compliance with IIA Standard 2010 – Planning
- Identify the priorities of Internal Audit based on the assessment of risk and potential exposures that may affect ECU's ability to accomplish its objectives
- To share and coordinate activities w/other internal and external providers of relevant assurance services to ensure proper coverage and minimize duplication of efforts
- To present the Internal Audit plan and resource requirements to the Audit Committee and Chancellor for review and approval

East Carolina
UNIVERSITY

Back To Agenda

Audit Planning Process



Continuously Assess and Monitor Risk/Update Audit Plan Accordingly

Define/Update Audit Universe

- Ensures completeness of risk coverage
- Vision, mission, and strategic plan
- Latest financial statement
- Financial balances
- Organization chart, chart of accounts
- Last audit completed and results of audit

Conduct Bottom-Up Risk Assessment

- Ratings based on objective guidance; judgment applied
- Criticality of unit
- Internal Control
- Public or political sensitivity
- Legal and Governance
- Change in management
- Financial Impact
- Fraud and Abuse

Conduct Top-Down Risk Assessment

- Facilitated by ERM
- Uncovers issues impacting University at an enterprise level
- Links to strategic objectives
- Identifies most critical risk (strategic, operational, compliance, reputational, financial)

Other Items Assessed

- Review other assurance providers plans and results of reviews
- Review latest findings from State Audit reports
- Review ECU BOT Minutes and ECU-P Board Minutes
- Review UNC FIT and Internal Control Assessment

Develop Audit Plan

- Based on prioritized audit universe, top-down assessment
- Management requested reviews
- Determine if pending audits from previous plan need to be brought forward
- Determine follow-up reviews
- Determine available auditor hours

Finalize Plan

- Present to Executive Council for Discussion
- Approval by Chancellor
- Approval by ECU BOT Audit Committee
- Remit to UNC GA
- Remit to Council of Internal Auditing

East Carolina UNIVERSITY

Back To Agenda

East Carolina University
Office of Internal Audit
Annual Engagement Plan
By Type
FY 2016-2017

Description	Budget Status	Budgeted Hours	%age of Total	Risk Ranking
Integrated/Operational Audits:				
Kronos/Payroll	WIP	500	3%	High
Organizational Continuity	WIP	260	2%	High
Telemedicine	WIP	300	2%	High
Comparative Medicine	CYP	400	2%	High
DHS Contract Revenue	CYP	400	2%	High
Governance/Ethics	CYP	600	4%	High
SoDM CSLC	CYP	400	2%	High
One Card Access	CYP	400	2%	High
Total Operational Audit Hours		**3260**	**20%**	
Compliance Audits:				
Conflict of Interest/Management Plans	CYP	300	2%	High
Academic Library Services Leave Time	CYP	300	2%	Med
Total Compliance Audit Hours		**600**	**4%**	
Information Technology Audits:				
2017 IT DR and COOP	CYP	100	1%	High
Incident Detection and Response Procedures	CYP	400	2%	High
User Account On-Boarding and Off-Boarding	CYP	400	2%	High
Total Information Technology Audit Hours		**900**	**5%**	
Special Reviews:				
Special Reviews - Pending	CYP	1100	7%	NA
Special Reviews in Progress	WIP	200	1%	NA
Total Special Review Audit Hours		**1300**	**8%**	
Follow-Up Reviews:				
2nd - IT Data Governance (A15017)	CYP	40	0%	High
2nd - Athletic Camps (A15039)	CYP	100	1%	High
2nd - Human Resources (A13023)	CYP	40	0%	High
2nd - Parking and Transportation Services (A15014)	CYP	100	1%	High
Occupational Therapy (A16027)	CYP	120	1%	Med
Biostatistics (A16011)	CYP	120	1%	Med
ERP Logical Access (A16010)	CYP	160	1%	High
Cloud Computing (A16003)	CYP	40	0%	High
Academic Integrity (A16019)	CYP	120	1%	High
Student Health Services (A16006)	CYP	100	1%	High
Total Follow-Up Review Audit Hours		**940**	**6%**	

Budget Status:
BF = Brought Forward From Previous Year's Plan
AYP = Added to Current Year Plan
CYP = Current Year Plan
CYP-B = Current Year Plan (Budgeted under Special Reviews - Pending)
WIP = Work-In-Progress

Back To Agenda

East Carolina University
Office of Internal Audit
Annual Engagement Plan
By Type
FY 2016-2017

Description	Budget Status	Budgeted Hours	%age of Total	Risk Ranking
Other/Special Projects:				
Consultations	CYP	3252	20%	NA
Committees/Other Routine Tasks (ie. SBI Reports, Assist State Auditor)	CYP	500	3%	NA
Pro-Card Analytics	CYP	600	4%	High
Travel Expenses Analytics	CYP	600	4%	High
Self-Assessment of Internal Audit	CYP	100	1%	NA
Risk Asessment/Audit Planning 2017-2018	CYP	100	1%	NA
Risk Assessment/Audit Planning 2016-2017	WIP	20	0%	NA
Total Other/Special Project Hours		**5172**	**31%**	
Total Direct Audit Hours		**12172**	**73%**	
Administration	CYP	1310	8%	NA
Leave	CYP	2496	15%	NA
Professional Development	CYP	662	4%	NA
Total Indirect Audit Hours:		**4468**	**27%**	
Grand Total Audit Hours		**16640**	**100%**	

Chancellor/Date

ECU BOT Audit Committee Chair/Date

Budget Status:
BF = Brought Forward From Previous Year's Plan
AYP = Added to Current Year Plan
CYP = Current Year Plan
CYP-B = Current Year Plan (Budgeted under Special Reviews - Pending)
WIP = Work-In-Progress

Back To Agenda

Internal Audit Charter

Mission and Scope of Work

The mission of the Office of Internal Audit and Management Advisory Services (OIAMAS) is to enhance and protect organizational value by providing risk-based and objective assurance, advice and insight.

The scope of work of the OIAMAS is to determine whether the organization's network of risk management, control, and governance processes, as designed and represented by management, is adequate and functioning in a manner to ensure:

- Risks are appropriately identified and managed.
- Interaction with the various governance groups occurs as needed.
- Significant financial, managerial, and operating information is accurate, reliable, and timely.
- Employees' actions are in compliance with policies, standards, procedures, and applicable laws and regulations.
- Resources are acquired economically, used efficiently, and adequately protected.
- Programs, plans, and objectives are achieved.
- Quality and continuous improvement are fostered in the organization's control process.
- Significant legislative or regulatory issues impacting the organization are recognized and addressed appropriately.

Opportunities for improving management control and the organization's image may be identified during audits. They will be communicated to the appropriate level of management.

Accountability

The Chief Audit Officer, in the discharge of his/her duties, shall be accountable to the East Carolina University Board of Trustees through the Audit, Enterprise Risk Management, Compliance, and Ethics Committee (hereafter referred to as Committee) and the Chancellor to:

- Provide annually an assessment on the adequacy and effectiveness of the organization's processes for controlling its activities and managing its risks in the areas set forth under the mission and scope of work.

Back To Agenda

- Report significant issues related to the processes for controlling the activities of the organization and its affiliates, including potential improvements to those processes, and provide information concerning such issues through resolution.
- Periodically provide information on the status and results of the annual audit plan and the sufficiency of the internal audit department resources.
- Coordinate internal activities with other monitoring functions such as risk management, compliance, security, legal, ethics, environmental, and external audits.

Independence and Objectivity

The internal audit activity should be free from interference in determining the scope of internal auditing, performing work, and communicating results. To provide for the independence of the OIAMAS, its personnel report to the Chief Audit Officer, who reports administratively to the Chancellor and functionally to the ~~East Carolina University Board of Trustees Audit~~ Committee. The Chief Audit Officer shall have full and independent access to the Chancellor and the ~~East Carolina University Board of Trustees Audit~~ Committee.

Functional oversight by the ~~East Carolina University Board of Trustees Audit~~ Committee includes:

- Approve the annual internal audit plan and monitor progress quarterly.
- Review and accept internal audit reports when issued.
- Periodically review and revise the internal audit charter as needed.
- Confirm and assure the independence of the internal audit function.
- 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.
- Meet privately with the Chief Audit Officer as deemed necessary.
- Review the effectiveness of the internal audit function, including compliance with The Institute of Internal Auditors' *Standards for the Professional Practice of Internal Auditing.*
- Resolve disagreements between internal audit and management concerning audit findings and recommendations.

Administrative oversight by the Chancellor includes day-to-day oversight such as approval of Chief Audit Officer annual leave and travel.

Back To Agenda

Responsibility

The Chief Audit Officer and staff of OIAMAS have responsibility to:

- Develop a flexible annual audit plan using an appropriate risk-based methodology, including any risks or control concerns identified by management, and submit that plan to the Chancellor and ~~East Carolina University Board of Trustees Audit~~ the Committee for review and approval as well as periodic updates.
- Implement the annual audit plan, as approved, including as appropriate any special tasks or projects requested by management, the Chancellor, the Vice President of Compliance and Audit Services of the UNC System, external auditors, and the ~~East Carolina University Board of Trustees Audit~~ Committee.
- Maintain a professional audit staff with sufficient knowledge, skills, experience, and professional certifications to meet the requirements of the Internal Audit Charter.
- Evaluate and assess significant functions and new or changing services, processes, operations, and control processes coincident with their development, implementation, and/or expansion.
- Issue periodic reports to management, the Chancellor and the ~~East Carolina University Board of Trustees Audit~~ Committee summarizing results of audit activities.
- Keep the Chancellor and the~~East Carolina University Board of Trustees Audit~~ Committee informed of emerging trends and successful practices in internal auditing.
- Provide a list of significant measurement goals and results to the Chancellor and the~~Audit East Carolina University Board of Trustees Audit~~ Committee.
- Conduct investigations of alleged misuse of University resources and assist with other investigations as requested by the Chancellor, University Attorney, and/or others as appropriate.
- Consider the scope of work of the external auditors and regulators, as appropriate, for the purpose of providing optimal audit coverage to the organization.
- Serve as a liaison between University management and external auditors.

Back To Agenda

- Provide assurance services[1] to the Chancellor and ~~and~~ the ~~East Carolina University Board of Trustees Audit~~ Committee. ~~by assessing the adequacy of entity internal control; adequacy of process or sub-entity internal control; adequacy of enterprise risk management; adequacy of governance processes; and compliance with laws or regulations.~~
- As appropriate, provide consulting and advisory services[2] to management that add value and improve the governance, risk management, and control processes without the internal auditor assuming management responsibility.
- Establish a quality assurance program by which the Chief Audit Officer assures the operation of internal audit activities.
- Ensure the requirements are met with regard to internal audit activities as set forth by UNC Board of Governors and the Council of Internal Auditing.

Authority

The Chief Audit Officer and the staff of OIAMAS are authorized to:

- Have unrestricted access to all functions, records, property, and personnel in accordance with North Carolina General Statutes.
- Allocate resources, set frequencies, select subjects, determine scope of work, and apply the techniques required to accomplish audit objectives.
- Provide consulting services to management as deemed appropriate.

The Chief Audit Officer and the staff of OIAMAS are not authorized to:

- Perform any operational duties for the organization or its affiliates.
- Initiate or approve accounting transactions external to OIAMAS.
- Direct the activities of any organization employee not employed by OIAMAS, except to the extent such employees have been appropriately assigned to auditing teams or to otherwise assist the internal auditors.

Standards of Internal Auditing

The internal audit profession is covered by the International Professional Practice Framework of The Institute of Internal Auditors. This framework includes

[1] Assurance services involves an objective assessment of evidence to provide an independent opinion or conclusions regarding an entity, operation, function, process, system, or other subject matter. The nature and scope of the assurance services are determined by the internal auditor.

[2] Consulting and advisory services are generally performed at the specific request of an engagement client. The nature and scope of the consulting engagement are subject to agreement with the engagement client.

Back To Agenda

mandatory elements consisting of Core Principles, the Definition of Internal Auditing, the Code of Ethics, and the *International Standards for the Professional Practice of Internal Auditing.* The OIAMAS will meet or exceed these mandatory requirements of the profession.

~~**Approved by the East Carolina University Board of Trustees Audit Committee on November 19, 2015.**~~

Approved by the Committee on July 14, 2016.

Back To Agenda

Procedure A-1
07/01/04
Revised 09/15/09
Revised 04/15/10
Revised 11/19/15
Revised 07/14/16
Page 1 of 3

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

Purpose

The purpose of the Audit, Enterprise Risk Management, Compliance, and Ethic Committee (hereafter referred to as Committee) is t~~T~~o 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, and (4) the University's compliance with the Best Financial Practices Guidelines adopted by the UNC Board of Governors in November of 2005. The ~~Audit~~ Committee has jurisdiction over internal audit, enterprise risk management, compliance, conflicts of interest, and ethics.

Organization

The ~~Audit~~ 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 ~~Audit~~ 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 ~~Audit~~ Committee shall meet at least four times a year and hold additional meetings as circumstances require. The ~~Audit~~ 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

Back To Agenda

provided in advance to members, along with appropriate briefing materials. Minutes of the meetings will be prepared.

Duties and Responsibilities

The following shall be the principal duties and responsibilities ~~of the Audit~~ 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.
- The Chief Audit Officer reports to the Chancellor with a clear, recognized reporting relationship to the chair of the ~~BOT Audit~~ 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.

Back To Agenda

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.

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

~~**Approved by ECU BOT Audit Committee on November 19, 2015**~~
Approved by the Committee on July 14, 2016.

Back To Agenda

Board of Trustees Audit Committee
Certification Letter
July 14, 2016

Ms. S. Lynne Sanders, CPA
Vice President for Compliance and Audit Services
The University of North Carolina
140 Friday Center Drive
Chapel Hill, North Carolina 27517

Dear Ms. Sanders:

In accordance with the Best Financial Practices Guidelines adopted by the Board of Governors in November 2005, I confirm that the Board of Trustees (BOT) Audit Committee of **East Carolina University** is in compliance with the following (any exceptions must be identified and explained in an accompanying statement). The Board of Trustees (BOT) Audit Committee:

1. Met at least four times this past fiscal year.

2. Reviewed the results of the annual financial audit with representatives of the North Carolina Office of the State Auditor (OSA) and discussed corrective actions, if needed.

3. Reviewed the results of any other audit performed and report/management letter (i.e. investigations, Statewide Federal Compliance Audit Reports, etc.) issued by the OSA with representatives of the State Auditor's Office, the Chief Audit Officer and/or appropriate campus official.

4. For any audit finding contained within a report or management letter issued by the OSA, reviewed the institution's corrective action plan and the report of the internal auditor on whether or not the institution has made satisfactory progress in resolving the deficiencies noted, in accordance with North Carolina General Statute 116-30.1 as amended.

5. Reviewed all audits and management letters of University Associated Entities as defined in Section 600.2.5.2 [R] of the UNC Policy Manual.

6. Received and reviewed quarterly reports from the institution's Chief Audit Officer that, at a minimum, reported material (significant) reportable conditions, the institution's corrective action plan for these conditions and a report once these conditions have been corrected.

Back To Agenda

7. Received, reviewed, and approved, at the beginning of the audit cycle, the annual audit plan for the internal audit department.

8. Received and reviewed, at the end of the audit cycle, a comparison of the annual audit plan with internal audits performed by the internal audit department.

I further attest the following:

1. The institution's Chief Audit Officer reports directly to the Chancellor with a clear and recognized reporting relationship to the chair of the BOT Audit Committee.

2. The Audit Committee charter defines appropriate roles and responsibilities. One of these responsibilities is the assurance that the institution is performing self-assessments of operating risks and evaluations of internal controls on a regular basis.

3. Internal audit functions are carried out in a way that meets professional standards.

4. The institution's Chief Audit Officer forwarded copies of both the approved audit plan and the summary of internal audit results, including any material reportable conditions and how they were addressed, to UNC General Administration in the prescribed format.

____

Chair of BOT Audit Committee

Note: A summary of these certifications from each campus will be provided annually to the current Board of Governors chair of the Committee on Audit, Risk Management and Compliance.

Back To Agenda

Chief Audit Officers
Certification Letter
July 14, 2016

Ms. S. Lynne Sanders, CPA
Vice President for Compliance and Audit Services
The University of North Carolina
140 Friday Center Drive
Chapel Hill, North Carolina 27517

Dear Ms. Sanders:

As Chief Audit Officer at **East Carolina University**, I confirm that we are in compliance with the following (any exceptions must be identified and explained in an accompanying statement):

1. Meeting with and updating the Board of Trustees (BOT) Audit Committee at least four times this past fiscal year.

2. Attending the financial audit exit conference conducted by the North Carolina Office of the State Auditor (OSA). **– Note: No exit conference conducted as ECU elected not to have one since there were no findings.**

3. Reviewing and discussing the results of any other audit performed and report/management letter (i.e. investigations, Statewide Federal Compliance Audit Reports, etc.) issued by the OSA with either representatives of the State Auditor and/or appropriate campus official.

4. Reporting directly to the Chancellor with a clear and recognized reporting relationship to the chair of the BOT Audit Committee.

5. Constructing the audit plan with the consideration of risk and potential internal control deficiencies and included any audits outlined by the UNC General Administration (UNC-GA).

6. Ensuring that all internal audits were planned, documented and executed in accordance with professional standards.

7. Forwarding copies of both the approved audit plan and the summary of internal audit results to UNC-GA in the prescribed format and updated the BOT Audit Committee for completion.

____
Chief Audit Officer

Back To Agenda

Note: A summary of these certifications from each campus will be provided annually to the current Board of Governors chair of the Committee on Audit, Risk Management and Compliance.

Back To Agenda

East Carolina University
Board of Trustees
Audit, ERM, Compliance and Ethics Committee
July 14, 2016

Session	Audit, ERM, Compliance and Ethics Committee
Responsible Person	Norma Epley
Agenda Item	III.
Item Description	Research Compliance
Comments	
Action Requested	Information
Disposition	
Notes	a. Results of FDA Review

Back To Agenda

East Carolina University
Board of Trustees
Audit, ERM, Compliance and Ethics Committee
July 14, 2016

Session	Audit, ERM, Compliance and Ethics Committee
Responsible Person	Tim Wiseman
Agenda Item	IV.
Item Description	Enterprise Risk Management
Comments	
Action Requested	Information
Disposition	
Notes	a. ERM Update b. COSO Update c. Article

Back To Agenda

3/23/2016

INFORMATION PAPER

SUBJECT: Enterprise Risk Management (ERM) Update for the BOT-A Committee April 2016 Meeting

1. Purpose. To advise BOT-A committee members of significant ERM and Chief Risk Officer (CRO) activities from the past two months and those planned or anticipated for the next two months.

2. Action Recapitulation:

a. Significant ERM/CRO Activities from the Past Two Months:

- Movement of Risk Management-Insurance Function from Campus Operations to ERM
- Hiring Action: Risk Management and Insurance Program Specialist - Complete
- Taught ISO 31000 ERM in Higher Ed Workshops (Parts I & II), Raleigh (Apr & May)
- Quarterly Enterprise Risk Management Committee Meeting and Actions (May)
- Presented Two Sessions [ERM Roundtable and the Return on Investment of ERM] at the Public Risk Mgmt and Insurance Association Conference, Atlanta, GA (June)
- Drones/UAS Interim Regulation Coordination – New FAA Guidelines
- Re-Admissions Risk Case Reviews and University Behavioral Concerns Team Actions
- ERM Consultations and Inquiries – Various Departments

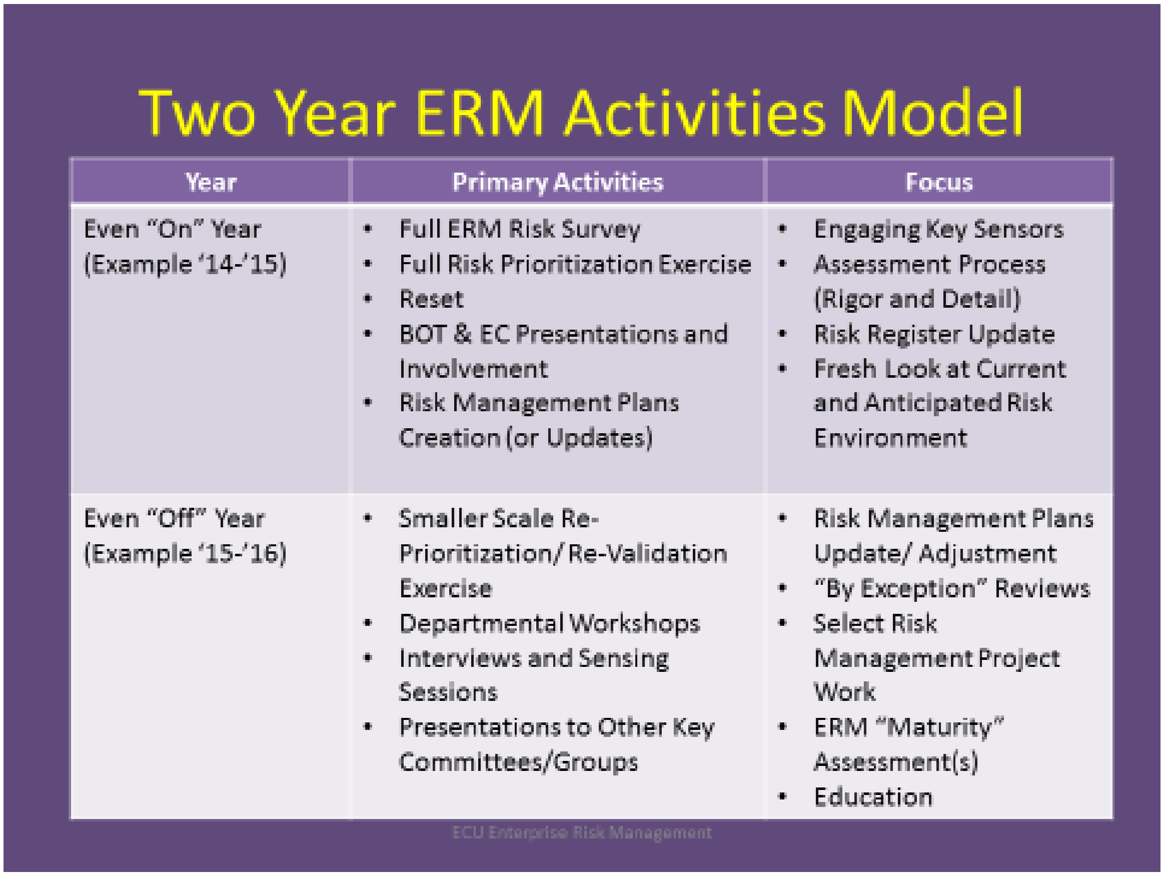
b. Significant ERM/CRO Activities Next Two Months:

- University Youth Programs Task Force – Conduct Refresher Workshop/Prepare for Full Implementation of Interim Regulation
- Initial ERM Orientation for Dr. Staton
- Quarterly Enterprise Risk Management Committee Meeting and Actions (July)
- Draft and Launch '16-'17 ERM Top Risk Survey
- Review of COSO *Enterprise Risk Management – Aligning Risk with Strategy and Performance* Exposure Draft (Executive Summary Attached)
- URMIA Annual Conference; RIMS Regional Conference; NC PRIMA Workshop (Sept)
- Re-Admissions Risk Case Reviews and University Behavioral Concerns Team Actions
- ERM Consultations/Research/Inquiries – Various Departments

3. Other: ECU was featured in a recent article in the magazine of the American Association of State Colleges and Universities. The article is on *managing reputational risk*. (Copy Attached)

ACTION OFFICER: Tim Wiseman
Assistant Vice Chancellor for ERM & Military Programs
Spilman Bldg, Room 214, 252-737-2803

Back To Agenda



Two Year ERM Activities Model

Year	Primary Activities	Focus
Even "On" Year (Example '14-'15)	• 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
Even "Off" Year (Example '15-'16)	• 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

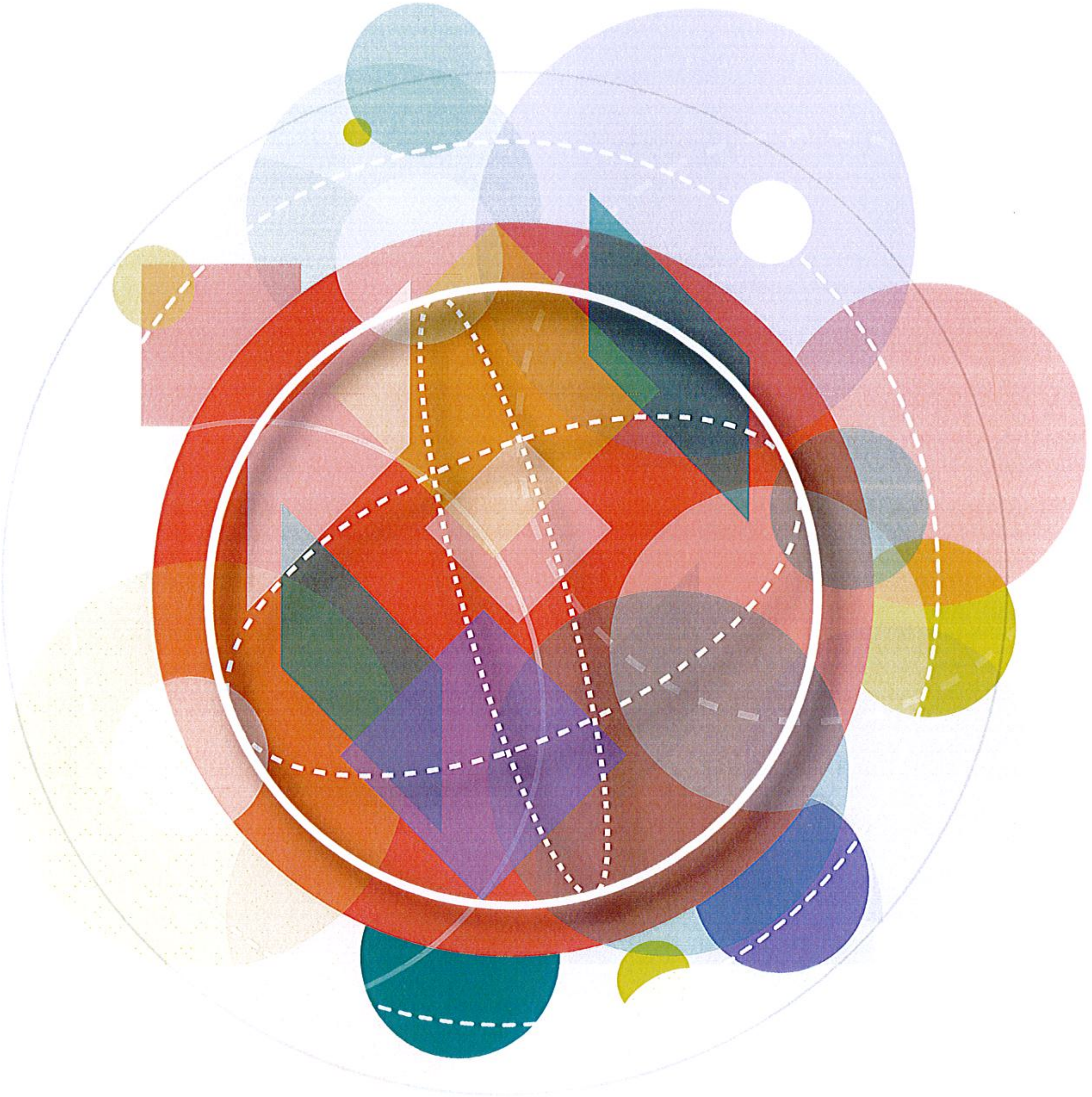
COSO

Committee of Sponsoring Organizations of the Treadway Commission

Enterprise Risk Management

Aligning Risk with Strategy and Performance

Executive Summary



June 2016 edition

To submit comments on this Public Exposure Draft, please visit www.erm.coso.org. Responses are due by **September 15, 2016**. Respondents will be asked a series of questions. Those questions may be found on-line at www.erm.coso.org and in a separate document provided at the time of download. Respondents may upload letters through this site. Please do not send responses by fax.

Written comments on the exposure draft will become part of the public record and will be available on-line until **December 31, 2016**.

Back To Agenda

This project was commissioned by the Committee of Sponsoring Organizations of the Treadway Commission (COSO), which is dedicated to providing thought leadership through the development of comprehensive frameworks and guidance on internal control, enterprise risk management, and fraud deterrence designed to improve organizational performance and oversight and to reduce the extent of fraud in organizations. COSO is a private sector initiative, jointly sponsored and funded by:

- American Accounting Association
- American Institute of Certified Public Accountants
- Financial Executives International
- Institute of Management Accountants
- The Institute of Internal Auditors

Back To Agenda

Foreword

In keeping with its overall mission, the COSO Board commissioned and published in 2004 *Enterprise Risk Management—Integrated Framework*. Over the past decade, that publication has gained broad acceptance by organizations in their efforts to manage risk. However, also through that period, the complexity of risk has changed, new risks have emerged, and boards have enhanced their awareness and oversight of enterprise risk management while asking for improved risk reporting. This update to the 2004 publication addresses the evolution of enterprise risk management and the need for organizations to improve their approach to managing risk in today's business environment.

The new title, *Enterprise Risk Management—Aligning Risk with Strategy and Performance*, recognizes the increasing importance of the connection between strategy and entity performance. The updated content offers a perspective on current and evolving concepts and applications of enterprise risk management. The second part of the publication, the Framework, accommodates different viewpoints and organizational structures, and enhances strategies and decision-making. In short, this update:

- Provides greater insight into the role of enterprise risk management when setting and executing strategy.
- Enhances alignment between performance and enterprise risk management.
- Accommodates expectations for governance and oversight.
- Recognizes the globalization of markets and operations and the need to apply a common, albeit tailored, approach across geographies.
- Presents new ways to view risk to setting and achieving objectives in the context of greater business complexity.
- Expands reporting to address expectations for greater stakeholder transparency.
- Accommodates evolving technologies and the growth of data analytics in supporting decision-making.

It also sets out core definitions, components and principles, and direction for all levels of management involved in designing, implementing, and conducting enterprise risk management practices. As well, for those who are looking for an overview of these topics (boards of directors, chief executive officers, and other senior management), we have prepared this Executive Summary.

Readers may also wish to consult a complement to this publication, COSO's *Internal Control—Integrated Framework*. The two publications are distinct from each other and provide a different focus; neither supersedes the other. However, they do overlap. *Internal Control—Integrated Framework* encompasses internal control, which is referenced in part in the updated publication, and remains viable and suitable for designing, implementing, conducting, and assessing internal control, and for consequent reporting.

The COSO Board would like to thank PwC for its significant contributions in developing *Enterprise Risk Management—Aligning Risk with Strategy and Performance*. Their full consideration of input provided by many stakeholders and their insight were instrumental in ensuring that the strengths of the original publication have been preserved, and that text has been clarified or expanded where it was deemed helpful to do so. The COSO Board and PwC together would also like to thank the Advisory Council and Observers for their contributions in reviewing and providing feedback.

Robert B. Hirth Jr.
COSO Chair

Dennis L. Chesley
PwC Project Lead Partner
Global Risk Leader

Back To Agenda

Committee of Sponsoring Organizations of the Treadway Commission

Board Members

Robert B. Hirth Jr.
COSO Chair

Richard F. Chambers
The Institute of Internal Auditors

Mitchell A. Danaher
Financial Executives International

Charles E. Landes
American Institute of Certified Public Accountants

Douglas F. Prawitt
American Accounting Association

Sandra Richtermeyer
Institute of Management Accountants

PwC—Author

Principal Contributors

Miles E.A. Everson
Engagement Leader and US Advisory Leader
New York, USA

Dennis L. Chesley
Project Lead Partner and Global Risk Leader
Washington DC, USA

Frank J. Martens
Project Lead Director
Vancouver, Canada

Matthew Bagin
Director
Washington DC, USA

Hélène Katz
Director
New York, USA

Sallie Jo Perraglia
Manager
New York, USA

Kate T. Sylvis
Manager
McLean Virginia, USA

Kathleen Crader Zelnik
Manager
Washington DC, USA

Maria Grimshaw
Senior Associate
New York, USA

Back To Agenda

The Changing Risk Landscape

1. Our understanding of the nature of risk, the art and science of choice, lies at the core of our modern economy. Every choice we make in the pursuit of objectives has its risks. From the day-to-day operational decisions to the fundamental trade-offs in the boardroom, dealing with uncertainty in these choices is a part of decision-making.

2. As we seek to optimize a range of uncertain outcomes, decisions are rarely binary, with a right and wrong answer. That's why enterprise risk management may be called both an art and a science. And when uncertainty is considered in the formulation of an organization's strategy and business objectives, enterprise risk management helps to optimize outcomes.

3. Our understanding of risk and our practice of enterprise risk management have improved greatly over the past few decades. But the margin for error is shrinking. The World Economic Forum writes of the "increasing volatility, complexity and ambiguity of the world."[1] That's a phenomenon we all recognize. Organizations find challenges impacting reliability, relevancy, and trust. Stakeholders are more engaged today, seeking greater transparency and accountability for managing risk. Even success can bring with it risk—the risk of not being able to fulfill unexpectedly high demand or the ability to maintain business momentum that has become an expectation, for example.

4. Organizations need to become more adaptive to change. They need to think strategically about how to manage the increasing volatility, complexity, and ambiguity of the world, particularly at the senior levels in the organization and in the boardroom where the stakes are highest.

5. *Enterprise Risk Management—Aligning Risk with Strategy and Performance* includes a Framework for boards and management in organizations of all sizes. It demonstrates how integrating enterprise risk management into an organization helps to accelerate growth and enhance performance by more closely linking strategy and objectives to both risk and opportunity. The Framework contains principles they can apply—from strategic decision-making through to execution. Integrating enterprise risk management throughout an entity provides a clear path to creating, preserving, and realizing value.

6. Below, we describe why the enterprise risk management framework makes sense for use by senior management and in the boardroom, what enterprise risk management has achieved, and how it can do more to inform and help shape strategy and improve decision-making.

The Board's Guide to Enterprise Risk Management

7. The board of directors[2] has a risk oversight responsibility, and its mix of skills, experience, and business knowledge need to be appropriate to assess risk in light of the business's strategy and objectives. All boards need to satisfy themselves that enterprise risk management practices are consistent with the entity's[3] strategy and risk appetite, and that a culture of risk-aware decision-making is embedded throughout the organization.

8. Boards have an opportunity, however, to go further: to use enterprise risk management to enhance the conversation with management and stakeholders. Enterprise risk

[1] *The Global Risks Report 2016*, 11th edition, World Economic Forum (2016).

[2] The Framework uses the term "board of directors" or "board," which encompasses the governing body, including board, supervisory board, board of trustees, general partners, or owner.

[3] This Executive Summary uses the term "entity" when referring to any form of for-profit company, not-for-profit organization, or government body.

Back To Agenda

management—one of the best frameworks available for decision-making in the face of uncertainty—should be deployed as part of the critical process of selecting and refining a strategy.

9. Most notably, boards gain a better understanding of how risk may impact the choice of strategy. Enterprise risk management enriches boardroom dialogue by providing a comprehensive sense of a strategy's strengths and weaknesses as conditions change, and of a strategy's fit with the organization's mission. Directors can feel more confident that they've looked at alternative strategies with a critical eye and can have a more robust discussion with management.

10. Once strategy is set, enterprise risk management provides an effective way for a board to fulfill its risk oversight role by knowing that the organization is attuned to risks that can impact strategy and is managing them well. Boards are under greater scrutiny than ever before about how they oversee risk. They need to create trust and instill confidence in their stakeholders—many of whom are growing louder in demanding accountability and transparency. Enterprise risk management is one more step toward fulfilling their responsibility.

What Enterprise Risk Management Has Achieved

11. COSO published *Enterprise Risk Management—Integrated Framework* in 2004. Its philosophy was to help entities better protect and enhance stakeholder value: "Value is maximized when management sets strategy and objectives to strike an optimal balance between growth and return goals and related risks, and efficiently and effectively deploys resources in pursuit of the entity's objectives."[4] Since then, the *Framework* has been used successfully around the world and across industries and in organizations of all types and sizes to identify risks, manage those risks within a defined risk appetite, and support the achievement of objectives.

12. Yet, as we've seen the *Framework* applied in practice, we've recognized that it has the potential to be used more extensively. We realized that certain aspects would benefit from more depth and clarity, as well as greater insight into the links between strategy, risk, and performance. Therefore, the updated Framework in the current publication:

- More clearly connects enterprise risk management with a multitude of stakeholder expectations.
- Positions risk in the context of an organization's performance, rather than as the subject of an isolated exercise.

Clearing up a few misconceptions

We've heard a few misconceptions about the original *Framework* since it was introduced in 2004. To set the record straight:

Enterprise risk management is more than a risk listing. Managing risk across an organization requires more than listing the "top 10" risks or making an inventory of all risks within the organization. Enterprise risk management is broader and includes practices that management puts in place to actively manage risk to appropriate levels.

Enterprise risk management addresses more than internal control. Internal control is an integral subset of enterprise risk management. But enterprise risk management also addresses other topics such as setting strategy, governance, communicating with stakeholders, and measuring performance. Its principles apply at all levels of the organization and across all functions.

Enterprise risk management is not a checklist. It is a set of principles on which processes can be built for a particular organization, and it is a system of monitoring, learning, and improving performance.

Enterprise risk management can be used by organizations of any size. If an organization has a mission, a strategy, and objectives—and the need to make decisions under uncertainty—then enterprise risk management can be applied. Enterprise risk management can and should be applied by all kinds of organizations, from small shops to community-based social enterprises to government agencies to Fortune 500 companies.

[4] *Enterprise Risk Management—Integrated Framework*, Executive Summary, COSO (2004).

Back To Agenda

- Enables organizations to become more anticipatory so they can get ahead of risk. Organizations in this position understand that change creates valuable opportunities, not simply the potential for crises.

13. This update also answers the call for a stronger emphasis on enterprise risk management when informing strategy and its execution.

The Strategic Value of the COSO Framework

14. All organizations need to set and periodically adjust strategy with an awareness of both ever-changing opportunities for creating value and—at the same time—the challenges they will face in pursuit of that value. They need the best possible framework for optimizing strategy and performance.

15. That's where enterprise risk management—defined as *the culture, capabilities, and practices, integrated with strategy and execution, that organizations rely on to manage risk in creating, preserving, and realizing value*—comes into play. Organizations that integrate enterprise risk management can obtain a range of benefits, including (though not limited to):

    - *Increasing the range of opportunities*: By considering all possibilities—both positive and negative aspects of risk—management can identify new opportunities and unique challenges associated with current opportunities.
    - *Identifying and managing risk entity-wide*: Every entity faces myriad risks that can affect many parts of the organization. Sometimes a risk can originate in one part of the entity but impact a different part. Consequently, management identifies and manages these entity-wide risks to sustain and improve performance.
    - *Reducing negative surprises and increasing gains*: Enterprise risk management allows entities to improve their ability to identify risks and establish appropriate responses, reducing surprises and related costs or losses, while profiting from advantageous developments.
    - *Reducing performance variability*: For some, the challenge is less with surprises and losses and more with variability in performance. In addition, performing ahead of schedule or beyond expectations may cause as much concern as performing short of scheduling and expectations. Enterprise risk management allows entities to anticipate the risks that would impact performance and enable them to put in place the actions needed to minimize disruption.
    - *Improving resource deployment*: Obtaining robust information on risk allows management to assess overall resource needs and enhance resource allocation.

16. Further, an entity's medium and long-term viability depends on its ability to anticipate and respond to change, not only to survive but also to evolve and thrive. That capability is called "enterprise resilience," and it is increasingly important as the business environment becomes more uncertain and the pace of change accelerates. Fortune 500 companies with multiple business units and loyal customers cannot easily "pivot" their strategies in the face of change the way smaller organizations can. Regardless of size, strategies need to stay true to their mission. And all organizations need to exhibit traits that drive an effective response to change, including agile decision-making, the ability to respond in a cohesive manner, and the adaptive capacity to pivot and reposition while maintaining high levels of trust among stakeholders.

17. These benefits highlight the fact that risk should not be viewed solely as a potential constraint or challenge to executing a strategy. Rather, the change that underlies risk and the organizational responses to risk also give rise to strategic opportunities and key differentiating capabilities. As such, the role of risk in selecting and evaluating a strategy requires deeper consideration.

Back To Agenda

The Role of Risk in Strategy Selection

18. Strategy selection is about making choices and accepting trade-offs. So it makes sense to apply enterprise risk management, the best approach for untangling the art and science of making well-informed choices, to strategy.

19. Risk is a consideration in many strategy-setting processes. But risk is often evaluated primarily in relation to its potential effect on an already-determined strategy. In other words, the discussions focus on *risks to* the strategy: "We have a strategy in place, what could affect the relevance and viability of our strategy?"

20. Organizations are getting better at asking the right questions and putting practices in place to deal with those kinds of risks. Have we modeled customer demand accurately? Will our supply chain deliver on time and on budget? Will new competitors emerge? Is our technology infrastructure up to the task? These are the kinds of questions that executives grapple with every day and that are fundamental to executing a strategy.

21. However, risk to the chosen strategy is only one aspect of risk to consider. As this Framework emphasizes, there are two additional aspects to enterprise risk management that can have far greater effect on an entity's overall risk profile.

22. Central to decisions that underlie selection of a strategy, the second aspect is the possibility of strategy not aligning with an organization's mission, vision, and core values. Every entity has a mission, vision, and core values that define what it is trying to achieve and how it wants to conduct business. Some are skeptical about organizations truly embracing their corporate credos. But mission, vision, and core values have been demonstrated to matter—and they matter most when it comes to managing risk and remaining resilient during periods of change.

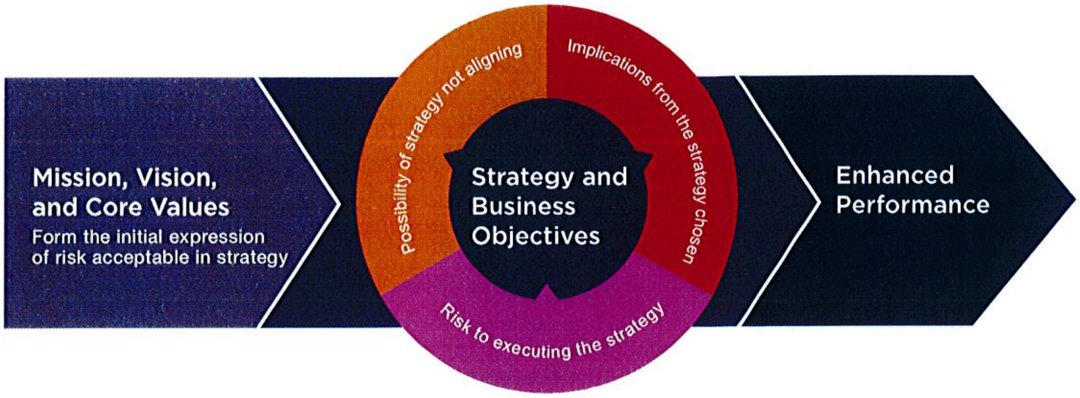
23. A chosen strategy must support the organization's mission and vision. A misaligned strategy increases the possibility that the organization may not realize its mission and vision, or may compromise its values, even if a strategy is successfully executed. Therefore, enterprise risk management considers the possibility of strategy not aligning with the mission and vision of the organization.

24. Then there is a third aspect. When management develops a strategy and works through alternatives with the board, they make decisions on the trade-offs inherent in the strategy. Each alternative strategy has its own risk profile—these are the implications from the strategy. The board of directors and management need to consider how the strategy works in tandem with the organization's risk appetite, and how it will help drive the organization to set objectives and ultimately allocate resources efficiently.

25. Additionally, alternative strategies are built on different assumptions, and those assumptions are sensitive to change in different ways. Change may come in the form of rates of innovation, customer behaviors, shifting employee capabilities, competitive responses, regulatory shifts, geopolitical developments—or just about any other factor that upends the assumptions behind a strategy. Boards should want to understand these sensitivities—the implications from the strategy—before they approve a strategy. They should also monitor business developments to ascertain whether these assumptions continue to remain valid, and if not, what actions need to be taken, including revisiting strategy.

26. Here's what's important: Enterprise risk management is as much about understanding the *implications from the strategy* and the *possibility of strategy not aligning* as creating an inventory of all risks within the organization. These considerations are why enterprise risk management, as depicted below, can be so valuable in the strategy-setting process.

Back To Agenda


Mission, Vision, and Core Values
Form the initial expression of risk acceptable in strategy
Possibility of strategy not aligning
Implications from the strategy chosen
Strategy and Business Objectives
Risk to executing the strategy
Enhanced Performance

27. Enterprise risk management, as it has typically been practiced, has helped many organizations identify, manage, and mitigate risks to the strategy. But the most significant causes of value destruction are embedded in the possibility of the strategy not supporting the entity's mission and vision and the implications from the strategy. Analyses of underperforming organizations reveal that they lost their way because of strategic blunders (*possibility of* and *implications from*), rather than operational errors, compliance faults, or external events (*risks to*).

28. Enterprise risk management helps to make the evaluation of strategy rooted in the decisions made by senior management much clearer. It clarifies how strategy selection can be enhanced. Choosing a strategy calls for structured decision-making that analyzes risk and aligns budgets and activities with the mission and vision of the organization.

Aligning Risk with Strategy and Performance

29. *Enterprise Risk Management—Aligning Risk with Strategy and Performance* clarifies the importance of enterprise risk management's role in strategic planning and demonstrates that it is more easily embedded throughout an organization—because risk influences and aligns strategy and performance across all departments and functions.

30. The Framework itself is a set of principles organized in five interrelated components:

    1. **Risk Governance and Culture:** Risk governance sets the organization's tone, reinforcing the importance of, and establishing oversight responsibilities for, enterprise risk management. Culture pertains to ethical values, desired behaviors, and understanding of risk in the entity.

    2. **Risk, Strategy, and Objective-Setting:** Enterprise risk management, strategy, and objective-setting work together in the strategic-planning process. A risk appetite is established and aligned with strategy; business objectives put strategy into practice while serving as a basis for identifying, assessing, and responding to risk.

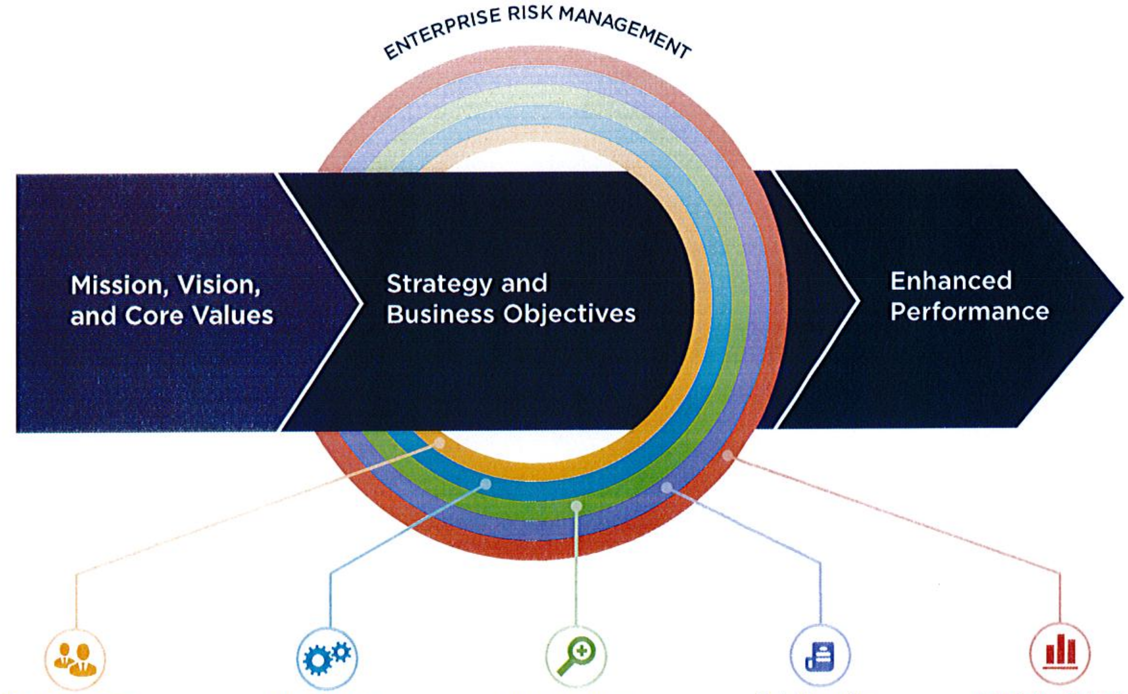
    3. **Risk in Execution:** Risks that may impact the achievement of strategy and business objectives need to be identified and assessed. Risks are prioritized by severity in the context of risk appetite. The organization then selects risk responses and takes a portfolio view of the amount of risk it has assumed. The results of this process are reported to key risk stakeholders.

    4. **Risk Information, Communication, and Reporting:** Enterprise risk management requires a continual process of obtaining and sharing necessary information, from both internal and external sources, which flows up, down, and across the organization.

Back To Agenda

5. **Monitoring Enterprise Risk Management Performance:** By monitoring risk management performance, an organization can consider how well the enterprise risk management components are functioning over time and in light of substantial changes.

31. There are 23 principles, noted below, that support the five components.[5] These principles cover everything from governance to monitoring. They're manageable in size, and they describe practices that can be applied in different ways for different organizations regardless of size or sector. Adhering to these principles can provide a reasonable expectation to management and the board that the organization understands and is able to manage the risks associated with the strategy and business objectives to an acceptable level.


ENTERPRISE RISK MANAGEMENT
Mission, Vision, and Core Values
Strategy and Business Objectives
Enhanced Performance

Risk Governance and Culture

1. Exercises Board Risk Oversight
2. Establishes Governance and Operating Model
3. Defines Desired Organizational Behaviors
4. Demonstrates Commitment to Integrity and Ethics
5. Enforces Accountability
6. Attracts, Develops, and Retains Talented Individuals

Risk, Strategy, and Objective-Setting

7. Considers Risk and Business Context
8. Defines Risk Appetite
9. Evaluates Alternative Strategies
10. Considers Risk while Establishing Business Objectives
11. Defines Acceptable Variation in Performance

Risk in Execution

12. Identifies Risk in Execution
13. Assesses Severity of Risk
14. Prioritizes Risks
15. Identifies and Selects Risk Responses
16. Assesses Risk in Execution
17. Develops Portfolio View

Risk Information, Communication, and Reporting

18. Uses Relevant Information
19. Leverages Information Systems
20. Communicates Risk Information
21. Reports on Risk, Culture, and Performance

Monitoring Enterprise Risk Management Performance

22. Monitors Substantial Change
23. Monitors Enterprise Risk Management

[5] A fuller description of these 23 principles is provided on the inside back cover.

Back To Agenda

Looking Forward

32. Enterprise risk management helps boards do their job better. Every board has an oversight role, helping to prevent the destruction of value. Traditionally, enterprise risk management has played a strong supporting role. Now, boards are increasingly expected to contribute to value creation through oversight and involvement in vetting strategy. *Enterprise Risk Management—Aligning Risk with Strategy and Performance* makes the connection clearer.

33. An important way that directors fulfill their responsibilities is through probing dialogue that not only tests assumptions but also draws out insights into strategy selection and ultimately enables better decisions. Specifically, boards should consider asking different kinds of questions about risk and resilience to their leadership in order to enhance the dialogue with management to include the more strategic aspects of enterprise risk management.

34. For example, can the leaders in entities—not just the chief risk officer—articulate how risk factors into business decisions? Can they clearly articulate the entity's risk appetite and how it might influence a specific decision? The resulting conversation may shed light on what the mindset for risk taking is really like in the organization.

35. Boards can also ask senior management to talk not only about risk processes but also about risk culture. How does the culture enable or inhibit responsible risk taking? What lens does management use to monitor the company's risk culture and how has that changed? As things change—and things will change whether or not they're on the entity's radar—how can the board be confident of an appropriate and timely response?

36. Over the longer term, enterprise risk management can also enhance enterprise resilience—the ability to anticipate and respond to change. It helps organizations identify factors that represent not just risk but change, and how that change could impact performance and necessitate a shift in strategy and objectives. By seeing change more clearly, an organization can fashion its own plan; for example, should it defensively pull back or invest in a new business? Enterprise risk management provides the right framework for boards to assess risk and embrace that mindset of resilience.

Back To Agenda

Acknowledgments

37. A special thank you to the following companies and organizations for allowing the participation of Advisory Council Members and Observers.

Advisory Council Members

Companies and Organizations

- Athene USA (Jane Karli)
- Edison International (David J. Heller)
- First Data Corporation (Cynthia Armine-Klein)
- Georgia-Pacific LLC (Paul Sobel)
- Invesco Ltd. (Suzanne Christensen)
- Microsoft (Jeff Pratt)
- US Department of Commerce (Karen Hardy)
- United Technologies Corporation (Margaret Boissoneau)
- Zurich Insurance Company (James Davenport)

Higher Education and Associations

- North Carolina State University (Mark Beasley)
- St. John's University (Paul Walker)
- The Institute of Internal Auditors (Doug J. Anderson)

Professional Service Firms

- Crowe Horwath LLP (William Watts)
- Deloitte & Touche LLP (Henry Ristuccia)
- Ernst & Young (Anthony J. Carmello)
- James Lam & Associates (James Lam)
- Grant Thornton LLP (Bailey Jordan)
- KPMG LLP Americas (Deon Minnaar)
- Mercury Business Advisors Inc. (Patrick Stroh)
- Protiviti Inc. (James DeLoach)

Former COSO Board Member

- COSO Chair, 2009–2013 (David Landsittel)

Observers

- Federal Deposit Insurance Corporation (Harrison Greene)
- Government Accountability Office (James Dalkin)
- Institute of Management Accountants (Jeff Thompson)
- Institut der Wirtschaftsprüfer (Horst Kreisel)
- International Federation of Accountants (Vincent Tophoff)
- ISACA (Jennifer Bayuk)
- Risk Management Society (Carol Fox)

Back To Agenda

23 principles

1. **Exercises Board Risk Oversight**—The board of directors provides oversight of the strategy and carries out risk governance responsibilities to support management in achieving strategy and business objectives.
2. **Establishes Governance and Operating Model**—The organization establishes governance and operating structures in the pursuit of strategy and business objectives.
3. **Defines Desired Organizational Behaviors**—The organization defines the desired behaviors that characterize the entity's core values and attitudes toward risk.
4. **Demonstrates Commitment to Integrity and Ethics**—The organization demonstrates a commitment to integrity and ethical values.
5. **Enforces Accountability**—The organization holds individuals at all levels accountable for enterprise risk management, and holds itself accountable for providing standards and guidance.
6. **Attracts, Develops, and Retains Talented Individuals**—The organization is committed to building human capital in alignment with the strategy and business objectives.
7. **Considers Risk and Business Context**—The organization considers potential effects of business context on risk profile.
8. **Defines Risk Appetite**—The organization defines risk appetite in the context of creating, preserving, and realizing value.
9. **Evaluates Alternative Strategies**—The organization evaluates alternative strategies and impact on risk profile.
10. **Considers Risk while Establishing Business Objectives**—The organization considers risk while establishing the business objectives at various levels that align and support strategy.
11. **Defines Acceptable Variation in Performance**—The organization defines acceptable variation in performance relating to strategy and business objectives.
12. **Identifies Risk in Execution**—The organization identifies risk in execution that impacts the achievement of business objectives.
13. **Assesses Severity of Risk**—The organization assesses the severity of risk.
14. **Prioritizes Risks**—The organization prioritizes risks as a basis for selecting responses to risks.
15. **Identifies and Selects Risk Responses**—The organization identifies and selects risk responses.
16. **Assesses Risk in Execution**—The organization assesses operating performance results and considers risk.
17. **Develops Portfolio View**—The organization develops and evaluates a portfolio view of risk.
18. **Uses Relevant Information**—The organization uses information that supports enterprise risk management.
19. **Leverages Information Systems**—The organization leverages the entity's information systems to support enterprise risk management.
20. **Communicates Risk Information**—The organization uses communication channels to support enterprise risk management.
21. **Reports on Risk, Culture, and Performance**—The organization reports on risk, culture, and performance at multiple levels of and across the entity.
22. **Monitoring Substantial Change**—The organization identifies and assesses internal and external changes that may substantially impact strategy and business objectives.
23. **Monitors Enterprise Risk Management**—The organization monitors enterprise risk management performance.

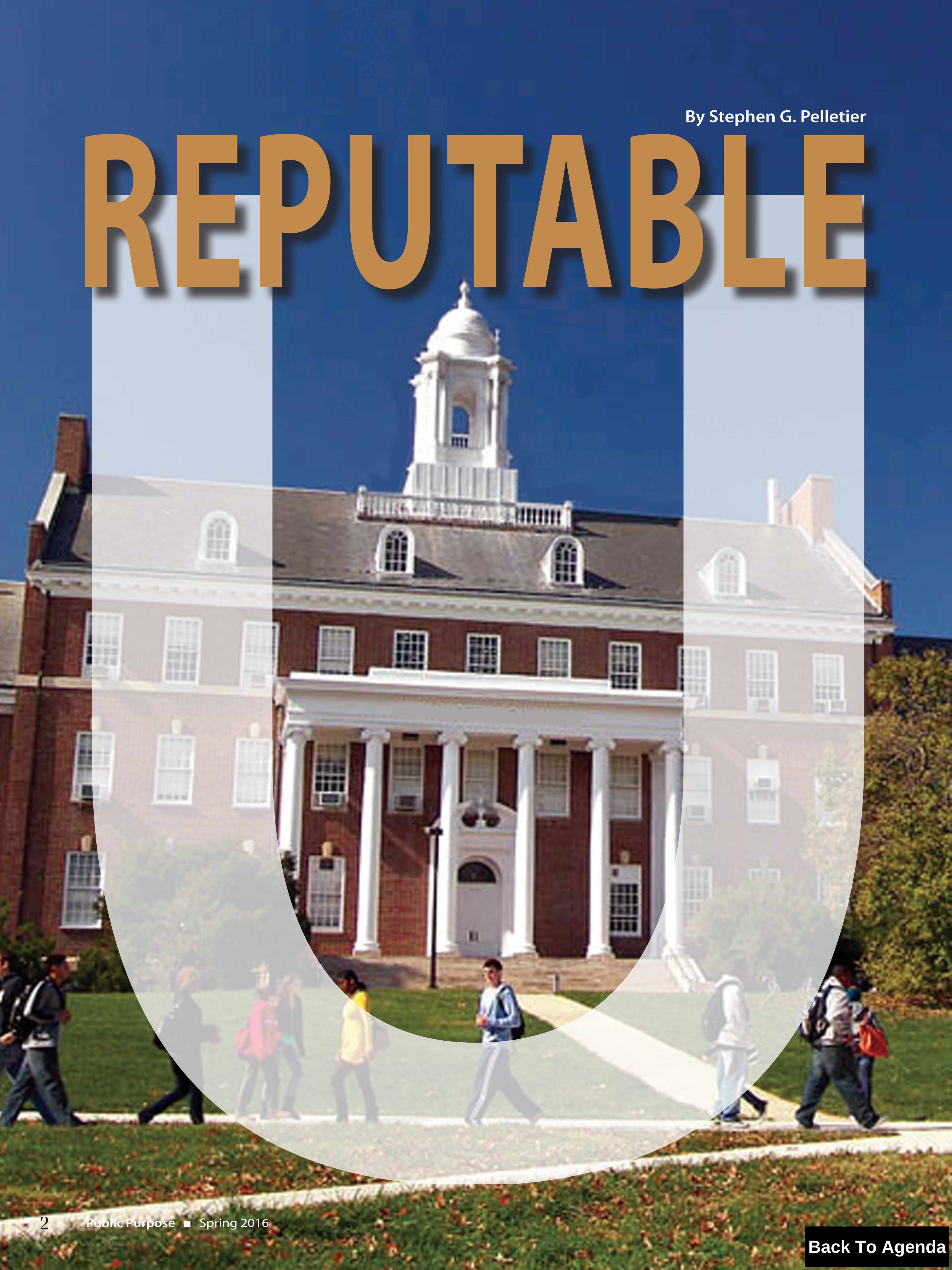
Back To Agenda

A full version of *Enterprise Risk Management—Aligning Risk with Strategy and Performance* can be purchased by visiting www.coso.org.

Back To Agenda

By Stephen G. Pelletier

REPUTABLE U



Back To Agenda

Building, polishing and protecting a university's reputation takes vigilance, hard work—and a strategy.

Every university leader knows how fragile an institution's reputation can be. From misuse of funds and student misbehavior to sex scandals and campus shootings, any number of threats can quickly undermine years of hard work to define, promote and protect an institution's image. The fallout might be quickly repairable—or cause long-lasting damage.

Crisis management strategies can help a university triage specific threats. But arguably more important is what an institution does before a crisis strikes. It's when the institution is not in crisis mode that it needs to invest in defining and polishing its reputation.

Countless Angles

Examining institutional reputation is like looking through a prism: There are countless angles to consider. One common measure of a university's reputation might be its position in national rankings. For public universities, however, a better measure of reputation might be how well the institution serves its various communities. Serving as "stewards of place," public universities must particularly assess their reputations in terms of how they are perceived by students, trustees, legislators, alumni, the media, local and regional communities, and other stakeholders.

Arlethia Perry-Johnson, vice president for strategic communications and marketing at Kennesaw State University in Georgia, says that reputation has to do with how an institution distinguishes itself in the marketplace. "When people hear your institution's name," she says, "what do they associate with that in terms of the quality of your graduates, the academic programs you have that are stellar or niches of excellence, and how are your students received by employers?" Perry-Johnson says an institution's reputation is defined by how responsive its academic programs are to community needs at the local, regional, state or even national levels.

Mark Kinders, vice president for public affairs at the University of Central Oklahoma, says that some of the factors that feed a public university's reputation have to do with how well they enable their graduates to be socially and economically mobile. "Do we give students opportunities to step up in life?" he says. "For students who may be first-generation or at risk, do we provide them with the means necessary to be successful?" Fundamentally, a university's reputation pivots on the institution's vision for itself, and on its mission. Robert Moore, president and chief executive officer at Lipman Hearne, a marketing and communications agency for higher education and nonprofit organizations, says that too many institutions settle for a vision for their reputation that is insufficiently bold or distinctive. For example, he says, it's not enough to merely tout that "we are doing a really good job at getting our students in and getting them through to graduation." Rather, he argues, "reputation needs to be about something that has some level of distinction. You need to isolate something not that you are really good at, but something where you are uniquely or differentially good."

Framework for Reputation

Framing one construct for strategizing about an institution's reputation, Julia Weede, executive vice president and education sector leader at the Edelman communications marketing firm, suggests focusing on three facets: evolving reputation, promoting reputation and protecting reputation. Which facet an institution should focus on, she says, depends on that institution's particular situation at a given time.

Research by Edelman consistently shows that one key driver of a university's reputation is that the public is keenly interested in knowing how a college education contributes to creating personal and professional opportunities for alumni. The research also shows that the public wants to know more about how a university impacts society at large.

Borrowing a phrase from business, Weede says universities need to "live their brand." By that she means institutions need to pursue their goals authentically and find effective ways to convince a public that is increasingly skeptical about higher education that the institution is delivering value. "I think we can no longer rely on people believing that what we do is self-evidently important to our communities and to society," Weede says. "We need new ways to demonstrate the great work that a university does and communicate that in ways that connect with our most important audiences. It is really about demonstrating how universities live their value."

"Learning how to tell that story well, in a media environment that is completely changed from where it was five to seven years ago, is a new art," Weede says. "And that universities do that authentically is absolutely critical."

Weede suggests that thoughtfully seeding an institution's reputation during relatively placid times can pay dividends when inevitably the wolves come to the door. Universities that have learned to live their brand authentically and communicate their value well stockpile goodwill among the public, she believes, that can help an institution weather crises.

Still, Weede says, universities have to be ready to proactively protect their reputation when a crisis does strike. "Perhaps the most important part of reputation management in higher education right now is understanding and watching for how issues and crises evolve," she says. Weede believes that

Back To Agenda

> "Reputation needs to be about something that has some level of distinction. You need to isolate where you are uniquely or differentially good." —Robert Moore

university leaders can learn a lot from studying what she calls "the anatomies of crises." According to Weede, "Many times you can see a reputational crisis coming 24 to 48 hours in advance if you are listening, and in many cases much longer."

Enterprise Reputation Management?

Some institutions strive to protect their reputation on an ongoing basis through strategic or enterprise risk management. In that regard, for example, William T. Wiseman, the assistant vice chancellor for enterprise risk management and military programs at East Carolina University, views reputational risk in context with four other risk categories: strategic, financial, operational and compliance-related.

Wiseman quotes Mary Schulken, ECU's executive director of communication, public affairs, and marketing, who says that in order to be effective, reputation management needs to be systematic, not episodic. "You cannot manage reputation just through public relations," Wiseman says. "It has to be integrated into the university's operating principles, so that actions align consistently and over time with desired outcomes." Wiseman advocates for an enterprise-wide risk management framework that includes information and communications on a regular basis, not just during or after a crisis. "When emotions are running high and you're trying to respond and react to questions and partial information," he says, "that is not the time to build your framework for managing the risk associated with crisis events."

Assessing Institutional Reputation

To be able to manage its reputation, a university needs to thoroughly understand what its reputation actually is. That's sometimes easier said than done.

"It is hard for an institution to objectively assess whether its reputation is great or good," says Gary Langsdale, who has served as university risk officer at The Pennsylvania State University since 2003. "We tend to believe our own press releases." Langsdale advocates that a university reach intentionally "beyond its own good PR" to understand as objectively as possible how it is perceived in the community and by the media." Part of that process, he says, is to discern what all of the institution's varied constituents think—parsing the differences in how potential students perceive an institution, for example, versus the perspectives of parents or alumni. Sometimes too, Langsdale observes, "you need a reality check from somebody who is more objective."

To triangulate and manage input about its reputation, risk management staff at ECU regularly convene meetings across the university's operational functions, pulling in expertise from such areas as communications and the university counsel's office. Part of the agenda is to review ongoing risks and emerging areas of concern and bring as much perspective to bear in assessing risks, including threats to reputation. The meetings create a means for ECU to take a holistic look at reputational threats and a channel for sharing critical information across departmental silos, Wiseman says. That's important because it enables the university to strategize broadly about risks, weighing implications that can get overlooked when individuals are reacting to immediate crises. Moreover, collaborating when crises are not imminent helps prepare staff to work together effectively when trouble strikes. Overall, Wiseman says, the process "can help us get upstream of negative risk events and intercede early in the process while time is on our side, rather than waiting for a reaction to an incident or crisis mode when you really don't have the luxury of time for some thoughtful analysis."

Sometimes, though, there is no substitute for hard data. Perry-Johnson strongly argues that research is a fundamental tool for plumbing the true perceptions of an institution. Campus administrators often get so caught up in their day-to-day responsibilities, she says, that it becomes difficult to assess where an institution stands with its various internal and external audiences. "In order to truly be effective and not push marketing money down black holes," she says, "you have to at some point pause to say, let me talk to my stakeholders.

Back To Agenda

Ask them a set of critical questions. Find out what the true perceptions are about your institution, then engage that against what it is you are trying to do or how you are trying to present the institution." Such research, she says, provides invaluable intelligence both about an institution's perceived "warts," which can then be addressed, as well as feedback about what the institution is doing right. If institutions find a disconnect between how they are being perceived and how they wish to be perceived, she says, "you can create effective strategic communications to help close those gaps."

Impact of Social Media

A key factor in managing reputation today is that thanks to social media and electronic communication, information can travel fast. Social media particularly changes the calculus in that it enables loud voices, including ones that may espouse contrary opinions or erroneous information, to quickly find a prominent bully pulpit.

Institutions and their leaders need to be proactive about managing those fast-moving communications channels. From his office at Penn State, for example, Langsdale has a unique perspective on the dangers of getting behind in the flow of information. "There are many who would say that Penn State didn't adequately communicate at the time that Jerry Sandusky was indicted and that as a result of that, the media got ahead of the university in terms of the story" he says. "And that our reputation was impacted by our inability to communicate our message."

One potential upside of social media is that it can help universities mine information that can help them better understand what constituents think about an institution. Kinders, for example, says that "students will speak truth to power through social media, so if we really want to know what our students and others are thinking, keeping an eye on social media helps us get a sense of any problems." The challenge, of course, is to wade through all the input to separate what is valuable intelligence from what is merely chatter.

"One of the things that many institutions in higher education are doing right now to manage reputational risk is to try to get out in front of some of the headlines that might come from certain events and put them into perspective," Wiseman says. "I call it 'expectation setting.'" To that end, for example, ECU monitors social media and chat sites that are popular with university constituents. The university will actively step in when needed to clarify what people might be saying about the university, particularly when ECU believes that misinformation or partial information is starting to build an inaccurate picture of the facts. "We try to engage in a respectful manner but proactively provide the additional factual basis that would put things in context," Wiseman says. "We can no longer be silent and let the general public or stakeholders in the institution's future arrive at conclusions that may or may not be based on the full facts in a given situation."

Role of Leaders

Experts say that while operational details can be delegated, university leaders must play a strong ongoing role in shaping and advancing the institution's reputation. "It's up to the president to set the tone, but also to empower the entire institution so that everyone understands what the message is so that everybody's singing the same song," Langsdale says. Equally important is that university leaders invest time in representing the institution in public settings—in essence serving as the public persona of an institution's reputation.

> "You cannot manage reputation just through public relations. It has to be integrated into the university's operating principles, so that actions align consistently and over time with desired outcomes." —William T. Wiseman

Another imperative is that institutions develop both a well-honed sense for what its different constituencies want to know and effective channels to communicate with those audiences. "Governors, legislators, Main Street, nonprofit organizations, our partners in K-12—we have to be very astute in understanding what matters to them," Kinders says. To those ends, he says, "having clear data and being transparent and showing that we're very willing to be accountable will go a long way."

Ultimately, maintaining a strong institutional reputation takes consistency and constant effort. "Stay on message," Kinders says. "Be very clear about who you are as an institution and in what ways you are unique and in the ways you express that through your branding platform. What is your personality as an institution? What is the promise that you are going to deliver every day? You need to be very thoughtful about that and you need to say it over and over and over again to everyone."

Stephen G. Pelletier is a writer and editor based in Rockville, Md.

Back To Agenda

East Carolina University
Board of Trustees
Audit, ERM, Compliance and Ethics Committee
July 14, 2016

Session	Audit, ERM, Compliance and Ethics Committee
Responsible Person	Kel Normann, Chair
Agenda Item	V.
Item Description	Other Business
Comments	
Action Requested	Information
Disposition	
Notes	

Back To Agenda

East Carolina University
Board of Trustees
Audit, ERM, Compliance and Ethics Committee
July 14, 2016

Session	Audit, ERM, Compliance and Ethics Committee
Responsible Person	Kel Normann, Chair
Agenda Item	VI.
Item Description	Closed Session
Comments	
Action Requested	Information
Disposition	
Notes	

Back To Agenda