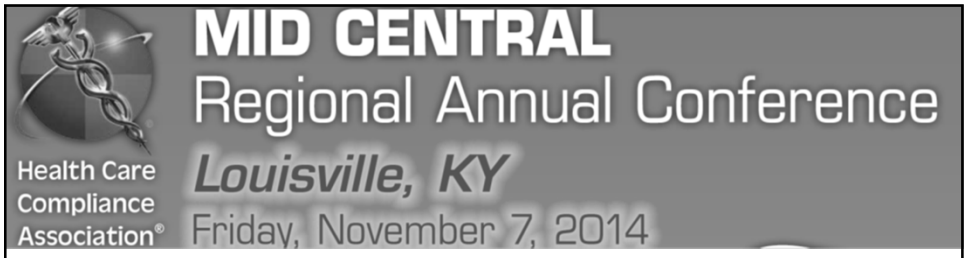


Designing Monitoring and Auditing Plans: Best Practices and Innovations

Urton Anderson Ph.D., CCEP, CIA
Director and EY Professor
Von Allmen School of Accountancy
University of Kentucky

Agenda

- Auditing and monitoring
- Why we need an auditing/monitoring plan
- Approaches to plan development
  - Assurance mapping
  - 3 lines of defense
  - Combined assurance

2

Auditing vs. Monitoring

Monitoring

- A process that assesses the quality of the internal control system's performance over time

	Non-independent	Independent
Periodic		
On-going		

3

Internal Control

…a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- Effectiveness and efficiency of operations.
- Reliability of financial reporting.
- Compliance with applicable laws and regulations.

COSO

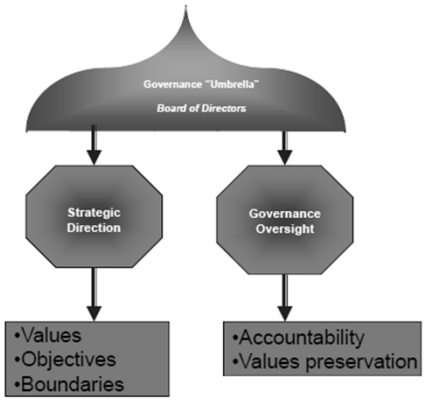
4

Why we need an auditing/monitoring plan

5

The Demand for Assurance

- Board
- Executive Management



Rising Demand for Compliance Assurance

Factors Increasing Complexity of the Legal and Regulatory Environment

- Technological Advancements
- Globalization
- Increased Interdependency of Organizations
- Demand for Accountability

Risk Management and Compliance Requirements

The Board's Role in Compliance

2) (A) The organization's governing authority shall be knowledgeable about the content and operation of the compliance and ethics program and shall exercise reasonable oversight with respect to the implementation and effectiveness of the compliance and ethics program.

Fed. Sent. Guidelines Chapter 8

Reasonable Oversight

A director has a duty to attempt in good faith to assure that

(1) a corporate information and reporting system exists, and

(2) this reporting system is adequate to assure the board that appropriate information as to compliance with applicable laws will come to its attention in a timely manner as a matter of ordinary operations.

In re Caremark International Inc. Derivative Litigation, 698 A.2d 959 (Del. Ch. 1996).

The Executive Management's Role in Compliance

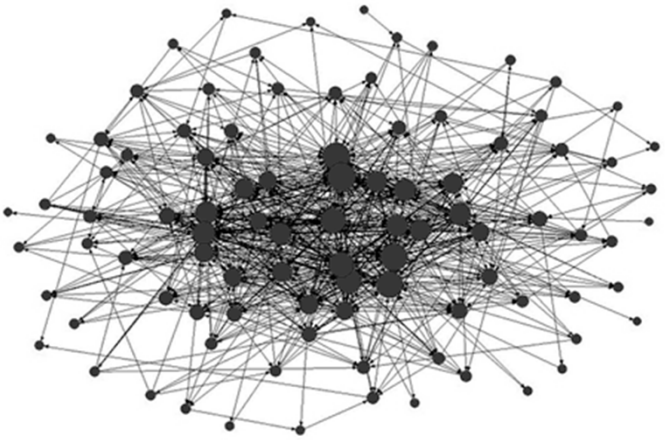
To ensure that all operations are conducted in accordance with applicable law, regulations and policies, including internal policies.

Compliance Programs are designed to establish a culture within a organization that promotes prevention, detection and resolution of instances of conduct that do not conform to federal and state law, as well as the organization's ethical and operations policies.

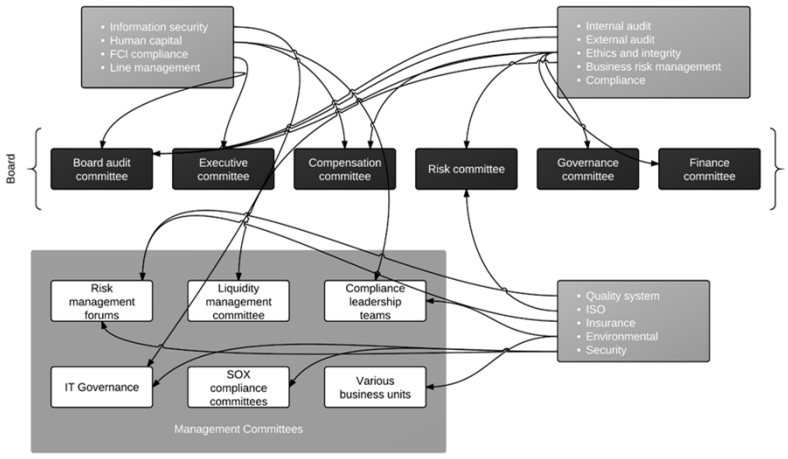
IIA Practice Advisory 2050-2 - Assurance Maps

- **One of the key responsibilities of the board is to gain assurance that processes are operating within the parameters it has established to achieve the defined objectives.**
- **It is necessary to determine whether risk management processes are working effectively and whether key or business-critical risks are being managed to an acceptable level.**

Organization as a Web of Assurance



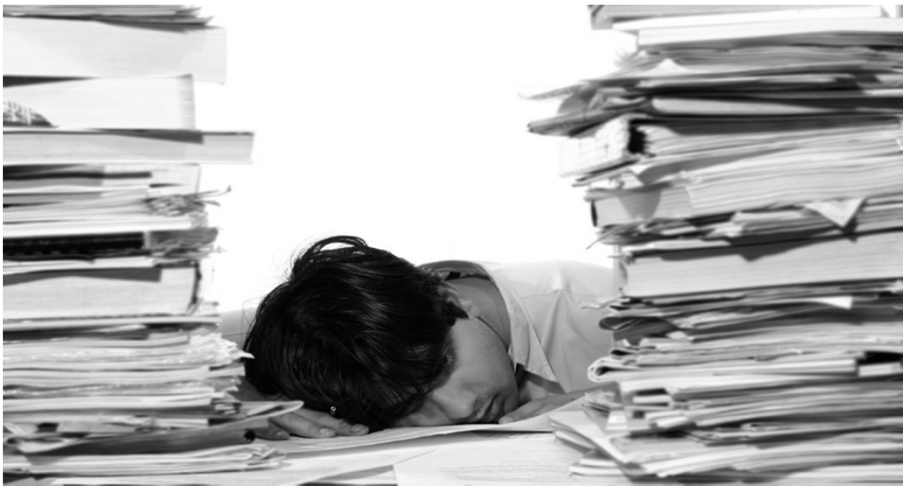
Assurance Network



Sources of Assurance

- Line management and employees (management provides assurance as a first line of defense over the risks and controls for which they are responsible.)
- Senior management
- Internal and external auditors
- Compliance
- Quality assurance
- Risk management
- Billing
- Environmental auditors
- Workplace health and safety auditors
- Government performance auditors
- Financial reporting review teams
- External financial statement auditors
- Other external assurance providers, including surveys, specialist reviews (health and safety), etc.

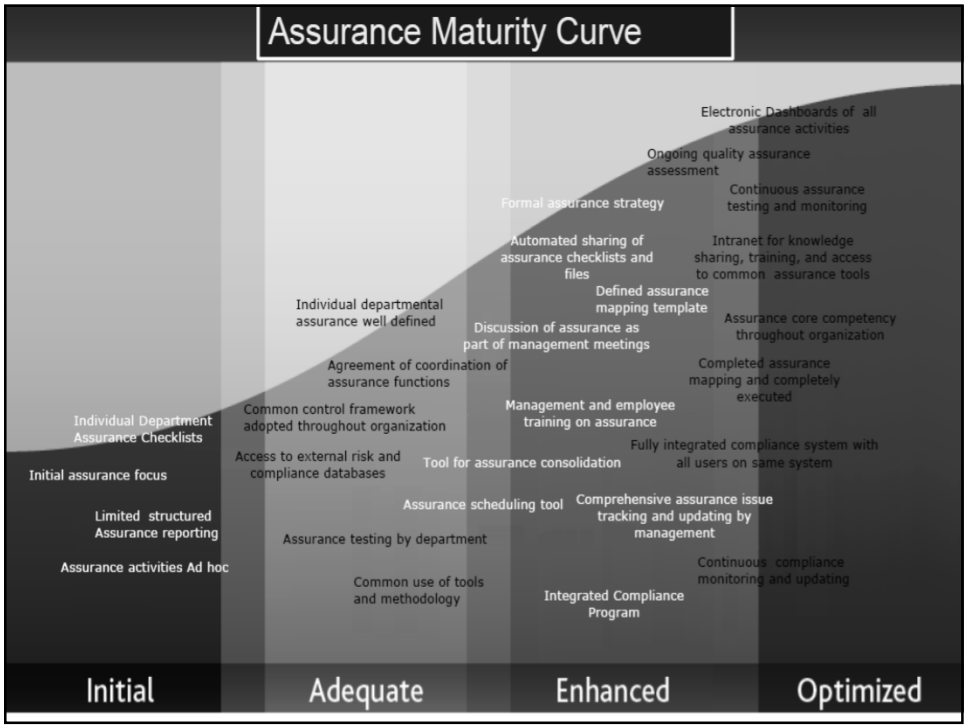
Assurance Fatigue



Business Unit 1– Auditing and Monitoring Schedule

Assurers	J	F	M	A	M	J	J	A	S	O	N	D
Compliance		√					√					
Risk Management	√									√		√
Internal Audit			√						√			
EH&S				√								
Info Security		√					√					
Privacy			√									
Billing	√	√	√	√	√	√	√	√	√	√	√	√
SOX	√					√				√		
CMS			√									
External Financial	√	√								√		√
3rd party payers				√					√			
State Medicaid								√	√			
EEOC									√	√		

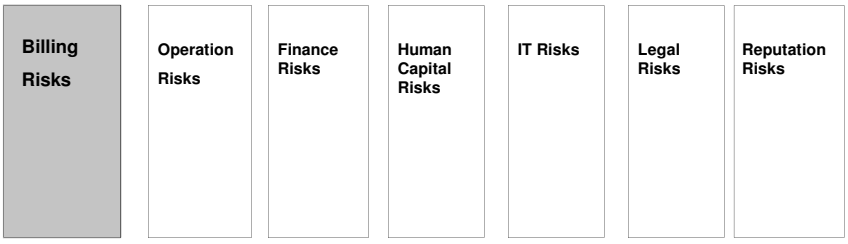
17



Initial

- Assurance activities are fragmented and ad hoc
- Managed in silos and reactive
- Limited formal policies and procedures
- Individual department/function driven
- Limited direct reporting to the board by providers
- High costs due to inefficiencies

Silo Approach to Assurance

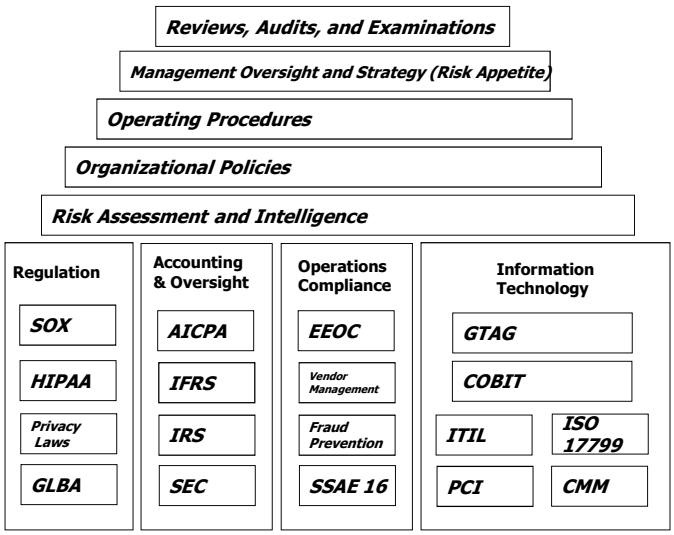


Adequate

- Individual assurance activities are well defined
- Limited integration to reduce duplication
- Agreement that there should be coordination of assurance activities
- Adoption of common framework (e.g., COSO)
- Key assurance providers have direct reporting to board
- Attempt to use common tools and methodologies

Traditional Assurance Approach

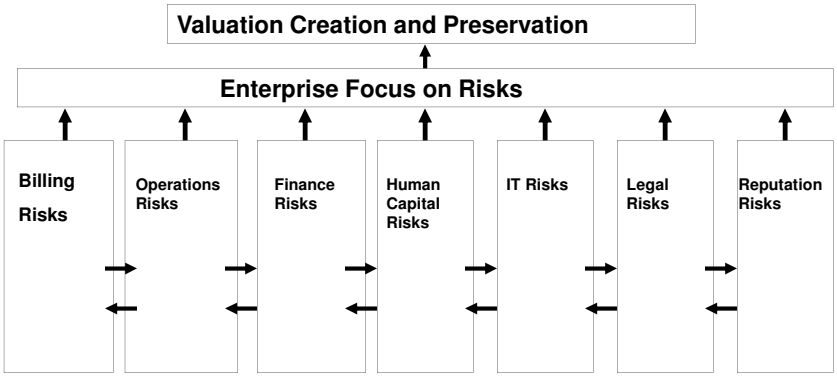
Enterprise Risk Management (ERM) / Governance, Risk, & Compliance (GRC)



Enhanced

- Formal assurance strategy
- Inventory of all organizational assurance activities
- Comprehensive assurance issue tracking
- Integrated compliance program
- Period reporting of assurance activities to board by assurance providers
- Managers are trained in the role of assurance

Integration Approach



Optimized

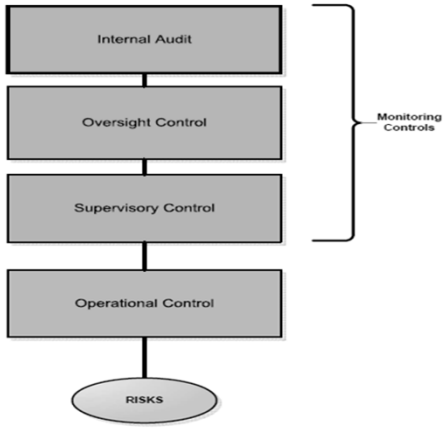
- Electronic dashboard of assurance activities for management and board
- Comprehensive assurance mapping
- Comprehensive assurance issue tracking
- Continuous assurance testing and monitoring
- Assurance is a core competency throughout the organization

Assurance Mapping

Fundamental Assurance Activity

Monitoring Function - Actions taken by management and others to assess the quality of internal control system performance over time

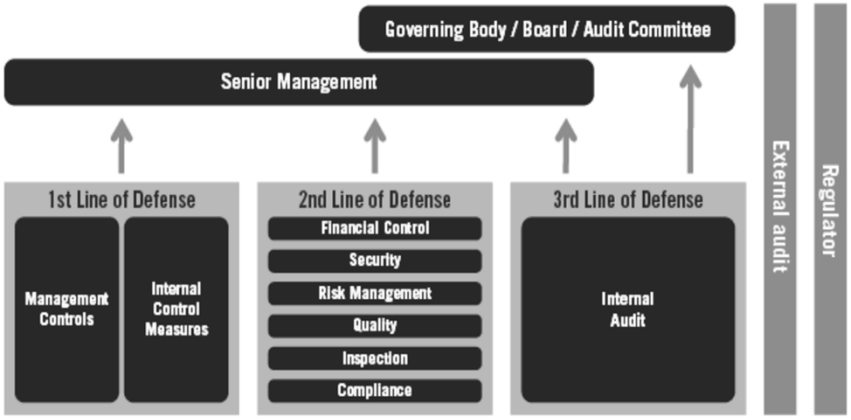
Assurance Activities and Risk



Assurance Map

Risk	Risk Owner	Inherent Risk Rating	Operational Control	Assurance Supervisory	Assurance Oversight	Assurance Internal Audit	Assurance External Provider

The Three Lines of Defense Model



3 Lines of Defense

- Basel II - Basel Committee on Banking Supervision, UK, ECIIA

Line 1	Management oversight - management review, control self-assessment, and continuous monitoring mechanisms
Line 2	Staff functions – Risk management, SOX review, compliance
Line 3	Independent and objective assurance – IA, EA, ISO, regulatory audits and other impendent reviews

Lines of Defense

First line of defence	Second line of defence	Third line of defence
Management oversight	**Management of risk**	**Independent assurance**
Objective: Setting strategy, performance measurement, and establishing and maintaining risk management, control and governance across the business.	**Objective:** Providing a risk framework to improve decision making, planning and prioritisation of the business activities.	**Objective:** Provides independent and objective assurance of the overall adequacy and effectiveness of governance, risk management and control within the organisation as established by the first and second layers of defence.
Reporting Lines: Executive Management Committees and Operational Committees providing direction, guidance and oversight over the focus the areas.	**Reporting Lines:** Risk Committees, Compliance Committee, Audit Committees, Regulatory Forums, etc.	**Reporting Lines:** Regulators, Board and Audit Committees.
Assurance Providers: Management Quality assurance functions ***Other:*** Project Management Office	**Assurance Providers:** ***Risk:*** Risk Management, Regulatory Risk Management, Legal Risk Management, ***Other:*** Forensics, Consultancies within the business, e.g. Tax.	**Assurance Providers:** Internal Audit External Audit/Advisors External regulators

How is assurance provided

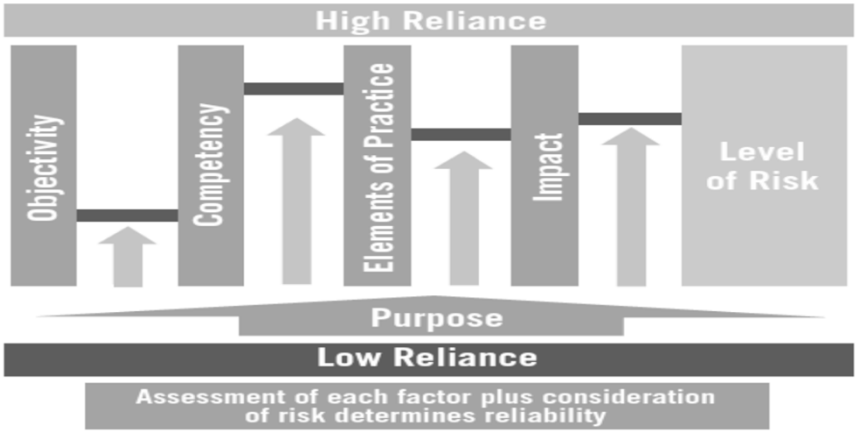
Assurance Provider	Health & Safety (H&S)
How is assurance provided	Self assessment
	Incident tracking and remediation
	H&S analysis and reporting
How is assurance measured	Number and scores of self assessments performed
	Number of BUs ISO 14001 certified
	Number of OHSAS pre-audits performed
	Number of recommendations made to CEOs for improvement

Five Principles in Determining Reliance

1. Purpose
2. Independence and Objectivity
3. Competence
4. Elements of Practice
5. Communication of Results & Impactful Remediation

IPPF – Practice Guide Reliance by Internal Audit on Other Assurance Providers

Assurance Reliance



IPPF – Practice Guide Reliance by Internal Audit on Other Assurance Providers – December 2011

COMBINED ASSURANCE

King III

Principle 3.5

The audit committee should ensure that a combined assurance model is applied to provide a coordinated approach to all assurance activities.

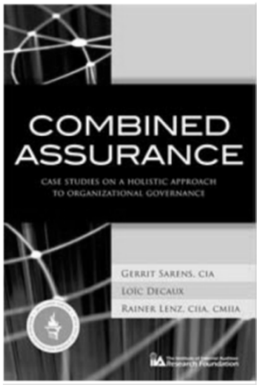
Combined Assurance Benefits

- Provides Board/Governance Body and senior management with assurance needed to carry out their responsibilities
- Reduce “assurance fatigue”

Assurance Map (PWC)

Processes	Three lines of defence assurance providers											
	First line of defence			Second line of defence				Third line of defence				
	Management-based assurance			Risk and legal-based assurance				Independent assurance				
	Control self assess-ment	Special project	Manage-ment review	Risk manage-ment	Health and safety	SOX	Com-pliance	External audit	Internal audit	ISO certifica-tion	Consult-ing engineers	Special project
Strategic												
Cash/finance and treasury												
Funding												
Sustainability												
Growth / mergers & acquisitions												
Alliances												
Operational												
Financial												
IT												
Treasury												
Human resources												
Supply chain management												
Quality												
Environment												
Customers												
Products & services												

IIA Research Foundation - Research Report



Implementing

Step 1: Establishing the business case

Step 2: Assurance reality check – what risk, source of assurance, how

Step 3: Risk mapping

Step 4: Combined assurance design

Step 5: Implement

Risk Assurance Mapping Activities at Large Utility

- IA assisted in coordinating the initial development of business unit and consolidated risk assurance maps
- IA met with risk owners to develop business unit risk and assurance maps
- IA coordinated with Risk Management to develop preliminary assumptions and harmonize business unit and consolidated assurance maps

Risk Assurance Map – Starting Template

	Performance Provider										Assurance Provider														Results				
	Management 1st Line										Functional Oversight 2nd Line										Independent 3rd Line				Regulatory Oversight 4th Line	Corrective Actio			
	Finance	Human Resources	Treasury	Operations	IT	Procurement	Legal	Commercial	Planning	Communications	Risk Management Processes	Compliance	Performance Review Meeting	Safety Review Board	Environmental Management Group	Network Development Forum	SOX	IT Steering Group			Internal Audit	External Audit	Quality Audit \ Compliance	Investigations - Proactive Safety Monitoring	Regulators	Assurance Provision	Obtain Independent Assurance	Review Other Assurance Providers	Remove Duplicate
Asset Safeguarding																													
Business Continuity																													
Crisis Management																													
Competitive Environment																													
Economic Environment																													
Hedging/Liquidity Management																													
Financial Reporting																													
Finance Processing																													
International Operations																													
Information Technology																													
Labor Relations/Staff																													
Legal																													
Operations																													
Regulator & Stakeholders																													
Revenue & Reputation																													
Environment																													
Suppliers & Key Relationships																													

Provider Assessment

Low Assurance | Medium Assurance | High Assurance

Overall Provision

Assurance Gap | Opportunity to Remove / | Maintain Current Status

BU Risk Assurance Map – Illustrative Example

Illustrative

Risk Universe			Top Tier Risks	Performance Provider: Management 1st Line												Assurance Provider: Functional Oversight 2nd Line								Indepen-dent 3rd Line		Regulatory Oversight 4th Line						
			Business Unit "A"	Operations/Constr/Engr	Fuel Management	Regulatory	Legal	Planning & Analysis	Accounting	Environmental Services	Safety & Health	Community Relations	Communications	HR	RMF	I/T	Compliance	Contracts/Supply Chain	Corp Accounting	Corp Tax	SOX	Corp Fin Planning	Internal Audit	External Audit	ERCOT / PUC	NRC	RRCT	NLRB	State of Texas	SEC	OSHA / MSHA
Strategic Risks	External	Change in Laws/Regulations	·	·	·	·	·			·	·			·	·			·		·			·		·	·	·			·	·
		Competitor		·	·										·							·			·					·	
		Concentration						------- N/A -------																							
		Economic						------- N/A -------																							
		Industry		·	·										·			·				·			·	·	·			·	
		Reputation	·	·		·							·	·	·											·					
		Stakeholder		·	·			·		·		·	·		·						·	·			·	·					
		Technology		·	·	·				·					·	·									·	·					
	Internal	Business Strategy		·	·			·		·					·			·		·		·									
		Customer Satisfaction										·	·		·																
		Goal Setting/Alignment		·				·							·							·	·								
		Governance		·		·								·	·								·	·							
		Market Intelligence		·	·	·				·	·				·	·		·													
		Pricing																													
		Product/Service Failure		·	·										·			·													
		Resource Allocation		·	·			·							·			·				·	·								

Lessons Learned

- Implementation can become a very time-consuming exercise
- Important to keep focused on what you are trying to achieve
- Business Unit owns its mapping
- Once developed, the mapping was passed over to Risk Management to administer
- IA uses the mapping as an input in developing its annual audit plan
- Shared ownership of any risk presents an opportunity for the ball to be dropped
- Who should be the owner of the assurance map?

Questions?

Urton Anderson
Von Allmen School of Accountancy
The University of Kentucky
(859)218-1788
urton.anderson@uky.edu