ACUA WEBINAR

Importance of Internal Audit Building a Strong Partnership with Billing Compliance, Privacy, and Information Security Functions

February 16, 2017

Glen C Mueller, MBA, CPA, CIA, CISA, CISM

Webinar Moderator

Don’t forget to connect with us on social media!

ACUA Distance Learning Director

Jana Clark

Senior Internal Auditor
Kansas State University

Today's Presenter

Glen C. Mueller
Chief Audit Executive, Cornell University

glen.mueller@cornell.edu

The Call to Action

As higher education and health care providers continue to face significant cost pressures it is increasingly important for Internal Audit, Compliance & Privacy, and IT Security to demonstrate they are working together and leverage their combined resources and skillsets to maximize the effectiveness of these overlapping functions.

Whether your organization has these functions combined in one department or are separate departments doesn't change the imperative to increase coordination and maximize the use of resources and technologies.

Today's Learning Objectives

- Gain insights into the mission and key activities of internal audit and compliance/privacy & IT security functions and how to better leverage combined resources and activities.

- Better understand the advantages of co-developing *continuous (timely) assurance software* and leverage technologies in a more effective manner by understanding the needs and capabilities of internal audit and compliance/ privacy and IT security.

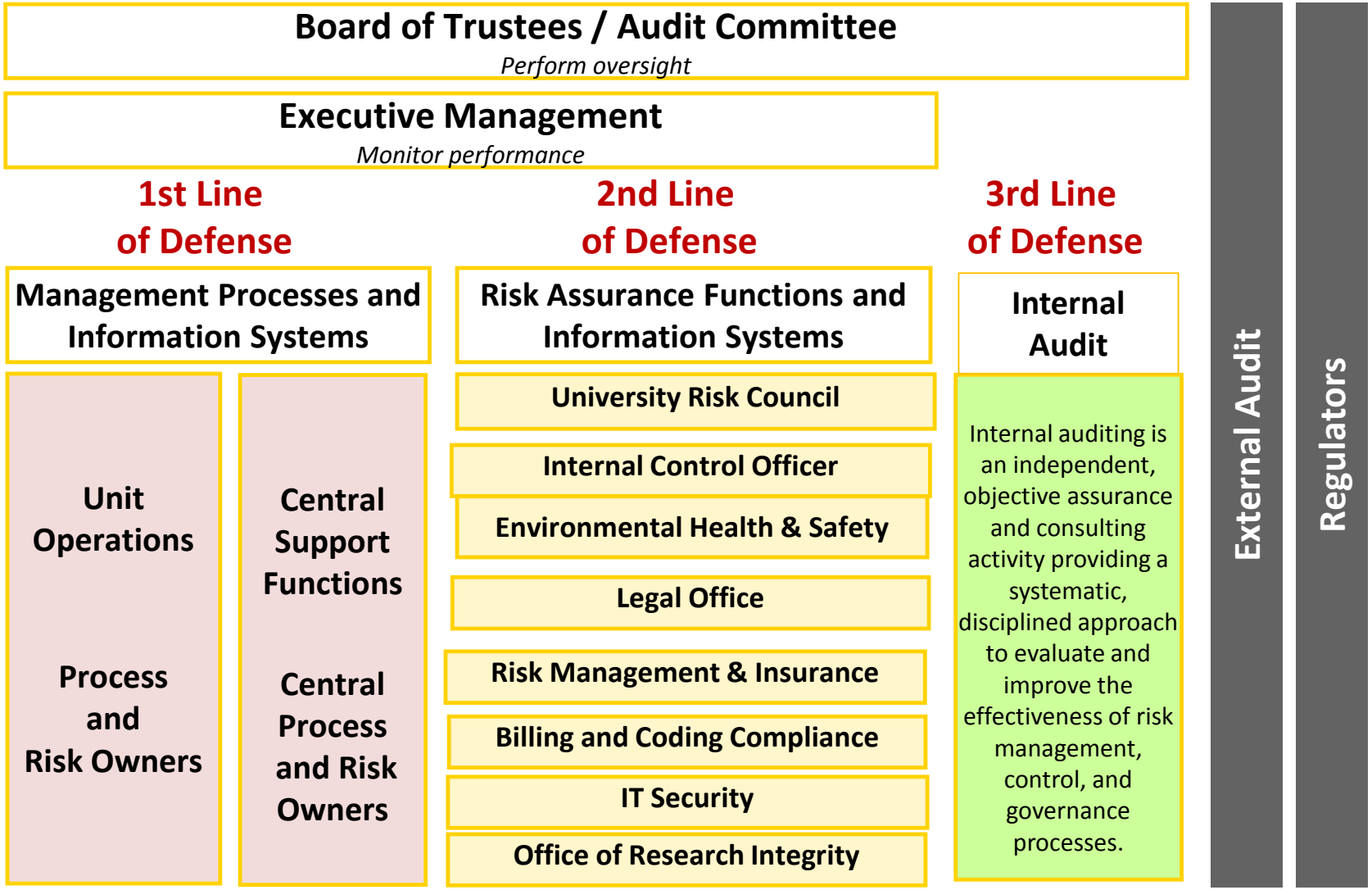
- Obtain an understanding of how to develop annual work plans that are integrated and complementary in terms of risk coverage and consistent reporting to management governance and the Board.

Polling Question #1

Which selection describes your current position?

- Chief Audit Executive (CAE)
- Chief Compliance Officer (CCO)
- Internal Audit Management & Staff
- Compliance Management & Staff
- IT Security Management and Staff

Roles in Risk Management: 3 Lines of Defense



Adapted from "Guidance for boards and audit committees", ECIIA and FERMA, 2010.

Prepare a roadmap for working closer together.

- Establish joint bi-weekly meeting of Privacy, IT Audit, and Information Security functions to discuss privacy and security issues and new systems in the implementation pipeline.
- Look at key steering and oversight committees together to see the optimal way to cover the needs of both functions and demonstrate coordination of activities.
- Provide training and education for each others' staff on key topics, tools, and techniques.
- Joint development and coordination of Annual Work Plans can avoid duplication of effort and gaps in coverage.

Benefits of IA conducting/participating in more compliance and IT Security related reviews (examples)

- ✓ IA gains more understanding of clinical operations, IT operations and other key regulatory areas.
- ✓ IA has opportunity for increased interactions with clinical leadership at department and executive level.
- ✓ Corporate compliance and IT Security can benefit from additional data mining/ analytics and "staff time" from IA for testing of controls or compliance with policies.
- ✓ IT Audit expertise can be leveraged by Compliance an IT Security to better understand key controls in complex areas and related automated (configurable) controls

Polling Question #2

Are Internal Audit and compliance in the same department reporting to the same executive?

- Yes
- No
- Unsure

Opportunities for Internal Audit, Compliance, and IT Security to work together

Projects, Audits and Risk Assessments (examples)

- Revenue Cycle Audits and Reviews
- Privacy and IT Audit coordination on risk assessment objectives
- Privacy risk assessment questions added to all internal audits
- IT Audit conducting reviews of “compliance” with IT Security Policies
- Conflicts of interest reviews
- Application controls reviews for key compliance related clinical systems

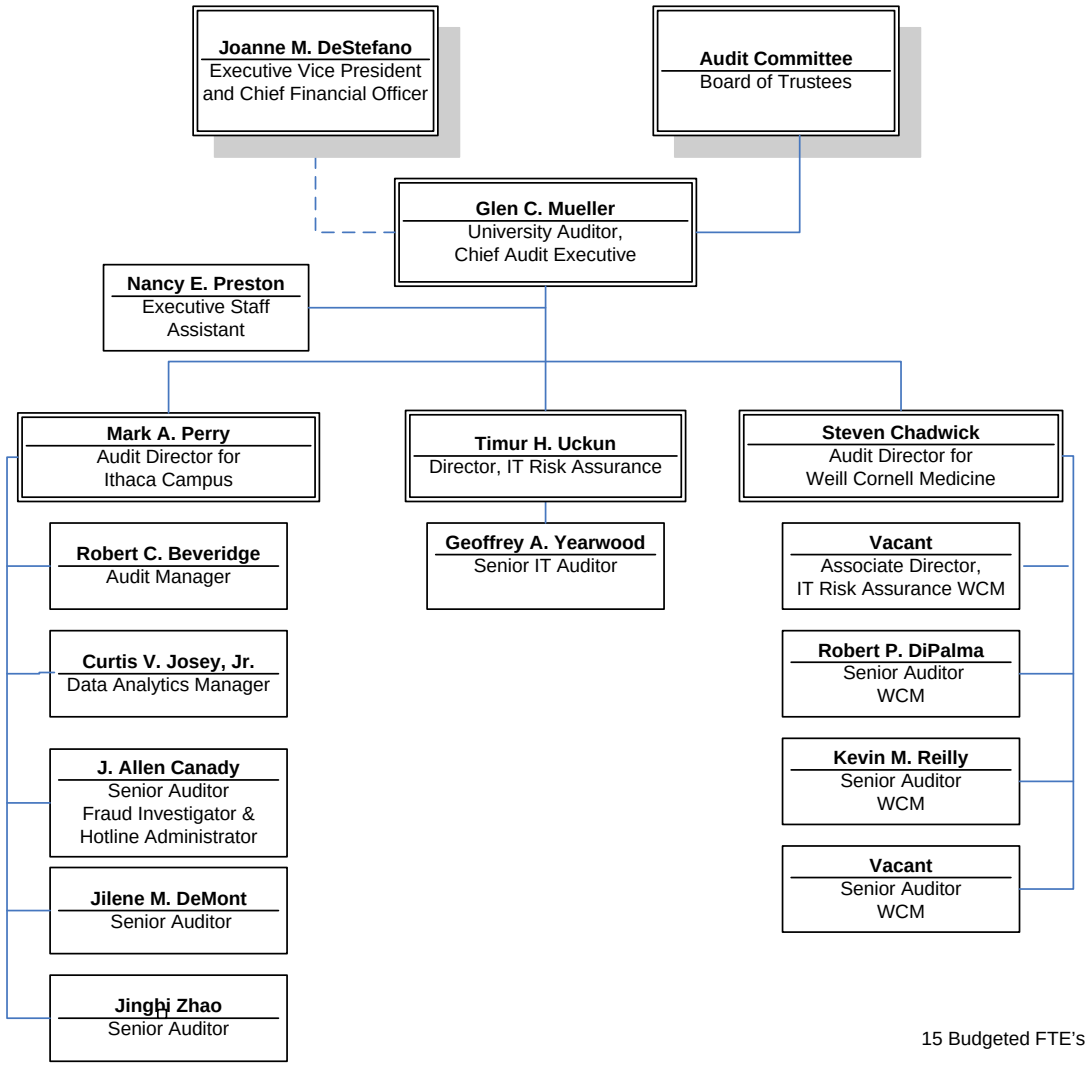
Tools & Techniques (examples)

- Statistical sampling software (use common tool/ subject matter expert)
- On-line survey tools (use common tool/ subject matter expert)
- Consistent formats in reports going to Board oversight committee
- Agree on consistent definitions for “high”, “medium”, and “low” risks

Cornell University
FY17 Annual Internal Audit Work Plan
FIVE KEY ASSURANCE STRATEGIC PRIORITIES

- Proactive Risk Advisory and Assurance Activities
- COSO Internal Control Framework Advancement
- Continuous Assurance Activities
- IT Risk Assurance Activities and Areas of Emphasis
- Weill Cornell Medicine Physician Organization EPIC Patient Care and Revenue Cycle Baseline Controls Reviews

Cornell University Audit Office
Organization Chart



15 Budgeted FTE's as of 07-01-16

"It's not all about audits"

Pro-active Internal Controls & Risk Assurance Advisory Activities

- ✓ Education and awareness activities
- ✓ Committees/workgroups participants
- ✓ Providing self-assessment checklists/guides
- ✓ Facilitating control self assessments
- ✓ Process redesign controls advising
- ✓ New IT systems implementations risks advising
- ✓ Policy and procedure controls related advising
- ✓ Participating in root cause analysis processes

Audits, Reviews, Risk Assessments, and Compliance Testing

- ✓ Conducting risk assessments
- ✓ Conducting audits & reviews
- ✓ Continuous (Timely) Auditing Software
- ✓ Investigating Fraud, Conflicts of Interest, and Hotline Complaints

IA, Compliance, and IT Security Should all Have Working Knowledge of COSO 17 Principles of Effective Internal Control

Control Environment **"Tone at the Top"**	1. Demonstrates commitment to integrity and ethical values 2. Exercises oversight responsibility 3. Establishes structure, authority and responsibility 4. Demonstrates commitment to competence 5. Enforces accountability
Risk Assessment	6. Specifies suitable objectives 7. Identifies and analyzes risk 8. Assesses fraud risk 9. Identifies and analyzes significant change
Control Activities	10. Selects and develops control activities 11. Selects and develops general controls over technology 12. Deploys through policies and procedures
Information & Communication	13. Uses relevant information 14. Communicates internally 15. Communicates externally
Monitoring Activities	16. Conducts ongoing and/or separate evaluations 17. Evaluates and communicates deficiencies

Polling Question #3

Who does IT Security report to at your institution?

- Chief Information Officer (CIO)
- Chief Compliance Officer (CCO)
- Chief Audit Executive (CAE)
- Chief Executive Officer (CEO)
- Other

Technology Tools & Techniques Can Enhance IA, Compliance and IT Security Program Effectiveness

Leveraging requisite direct information system access, data mining capabilities, and data analytics and visualization capabilities can greatly benefit all three functions. Examples are as follows:

Academic Medical Center Examples

- Review for provider, employee, and vendor Medicare excluded parties
- Statistical Sampling Software (i.e. OIG RAT-STATS)
- Physician payment audits
- Verification of user status (termed vs. active) for critical clinical systems
- E&M code utilization for all physicians in a division to identify outliers
- Search for missing charges by comparing daily schedule to daily charges

Non- Healthcare Examples

- Determine what percentage of laptops and desktops are encrypted
- Accounts payable duplicate payments reviews
- Purchasing Card proper utilization (what vendors) and card limits reviews
- Research late equipment purchases
- Research unallowable salaries
- Research unallowable expense

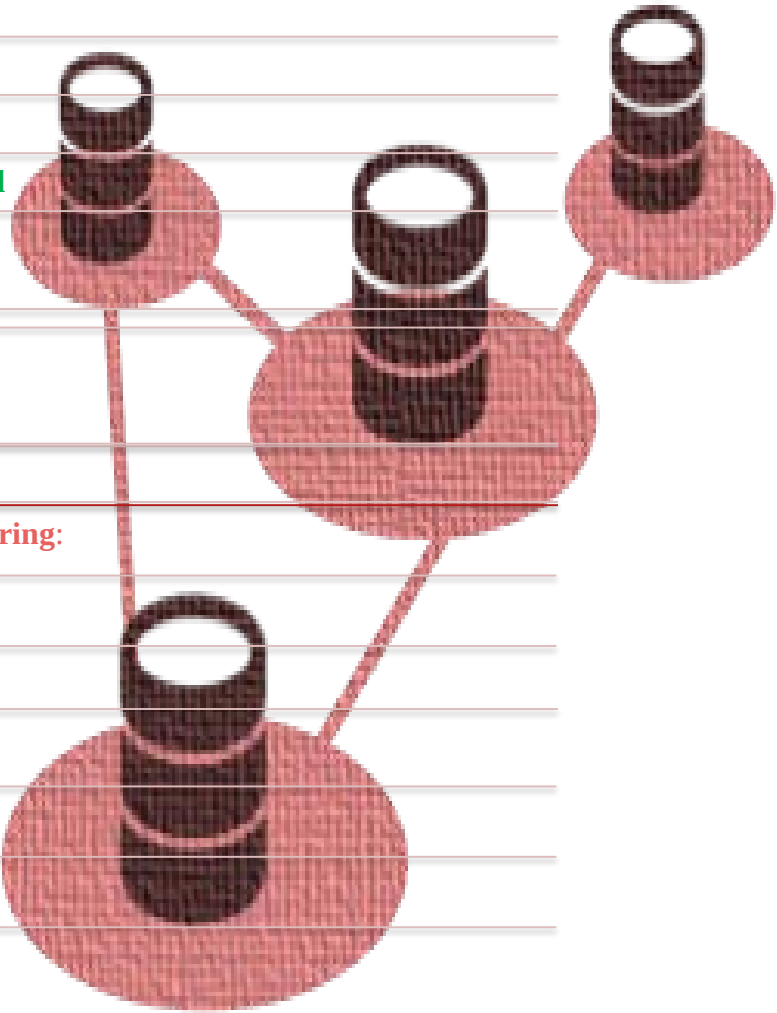
Cornell Audit Office Data Access Priorities

UAO Current Direct Access

- **Active Directory**
- **Business Service Center Management System**
- **CU Person**
- **Kronos**
- **Kuali Data Warehouse (KDW), includes P-Card**
- **Kuali Labor Data**
- **Kuali Near Real-Time (NRT)**
- **PeopleSoft (Payroll)**
- **Research Administration DataMart**
- **Travel Portal**

UAO Planned Future Direct Access

- **Microsoft BitLocker Administrator and Monitoring**:
  Windows – BitLocker Encryption
- **Jamf**:
  Apple Devices - Encryption
- **System Center Configuration Management**:
  Windows – Admin Rights, Screen Locks, Other Encryption
- **Flexera**:
  Software Security Patching
- **Identity Finder**:
  Scanning for Confidential Data
- **Concur**:
  Executive Travel Compensation
- **Student DataMart**:
  Title IV Compliance
- **Workday Timekeeping**:
  Supervisor Sign-offs



Timely Risk Assurance FY17 Plan

Initial Focus Has Been on Research Expenditures & IT Metrics

Focus Areas	FY2017 Planned Routines*	FY 2017 Status
Research Expenditures	**4**	**5**
I.T. Security Metrics	**4**	**IN PROGRESS**
Accounts Payable	4	SPRING 17
Procurement Cards	4	SPRING 17
Payroll & Timekeeping	4	-
	20	5

1. Late Equipment Purchases
2. Unallowable Expenses
3. Timeliness of Award Closeout
4. Transactions after Award End
5. Unallowable Salaries

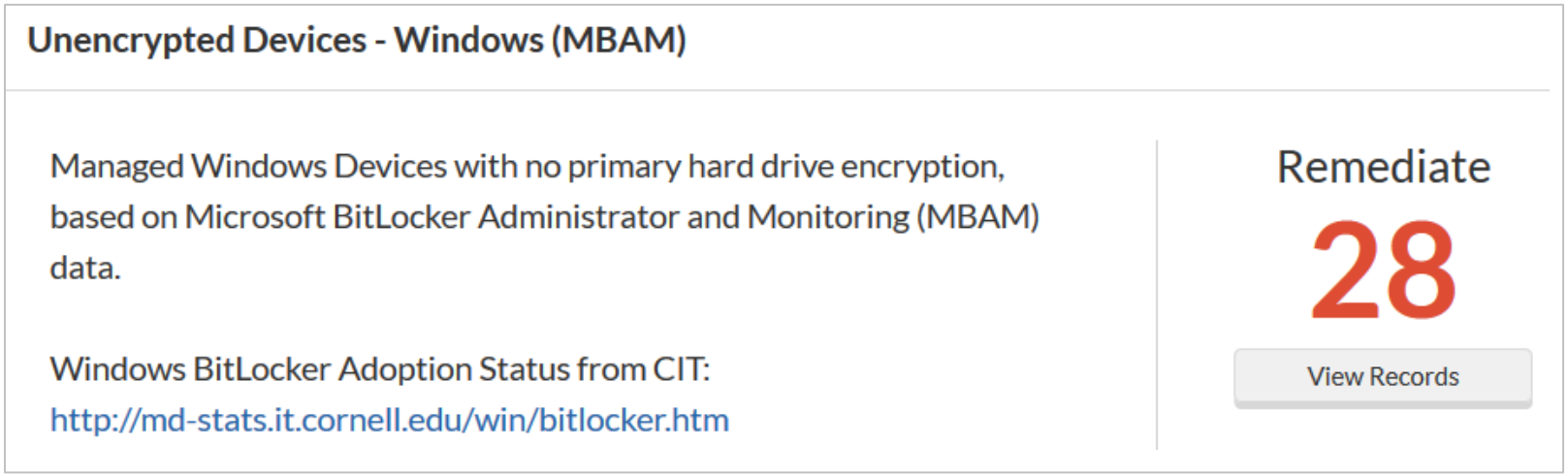
* - each routine results in 3 – 5 data visualizations and at least 1 control test

Current Project: Policy 5.10, Information Security Planned Compliance Testing

Managed Devices Compliance Review (aka Endpoints):

- Device Encryption
- Local Administrative Rights
- Scanning for Confidential Data
- Security Patch Compliance
- Automatic Screen Locks

Testing Only Administrative Data and Devices in Phase I



Excluded Provider Screening at Weill Cornell Medicine (WCM)

Weill Cornell Medicine
Audit Office

- Effect of an Office of Inspector General (OIG) exclusion is that no Federal health care program payment will be made for any items or services furnished by an excluded person; or at the medical direction or on the prescription of an excluded person.

- In addition to having to return any related revenue received as a result of using an excluded provider, the OIG can impose civil monetary penalties (CMPs) against the organization.

- Payment exclusion applies to all methods of Federal health care program payment, whether from itemized claims, cost reports, fee schedules, capitated payments, a prospective payment system or other bundled payment, or other payment system and applies even if the payment is made to a state agency or a person that is not excluded.

- Weill Cornell Audit Office performs monthly excluded provider testing on behalf of Weill Cornell Medicine Office of Billing Compliance (OBC). Results are presented by OBC at the monthly Billing Compliance Committee meeting.

Government data files used to match with internal data files from WCM databases:

Weill Cornell Medicine
Audit Office

- **U.S. Department of Health & Human Services (HHS) – Office of Inspector General (OIG)**
  A data file that enables users to download the entire List of Excluded Individuals and Entities (LEIE) to a personal computer. If a name is a match, the database website can be used to verify the match using a Social Security Number or Employee Identification Number.

  http://oig.hhs.gov/exclusions/index.asp

- **New York State Office of Medicaid Inspector General (OMIG)**
  The OMIG is an independent entity created by the New York State Department of Health to promote and protect the integrity of the Medicaid program in New York State.

  https://omig.ny.gov/fraud/medicaid-exclusions

- **System for Award Management (SAM)**
  Publicly available data for all active exclusion records entered by the Federal government identifying individuals and vendors excluded from receiving Federal contracts, certain subcontracts, and certain types of Federal financial and non-financial assistance and benefits.

  https://www.sam.gov/portal/SAM/#1

WCM data files used to match to excluded provider files from government data files and websites above:

- Comprehensive WCM application Centerwide ID (CWID) user account database. Individuals include: faculty, staff, students, contractors, temporary employees and employees of affiliated physician practices.
- All physicians, WCM employees and voluntary referring physicians maintained in SAP.
- All vendors and merchants who provide WCM with supplies and services maintained in SAP.

Polling Question #4

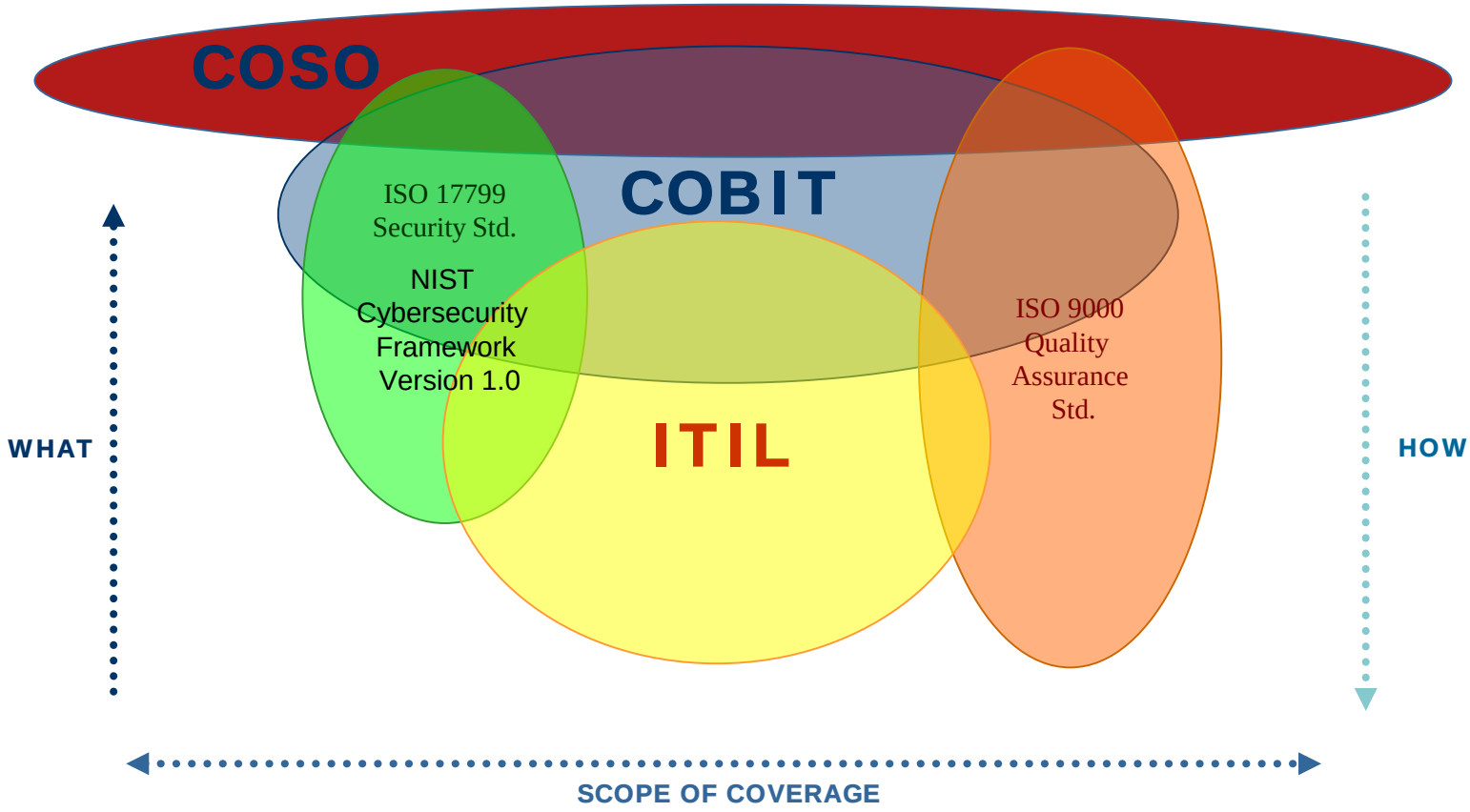
Do you believe Internal Audit independence would be impaired by increasing collaboration with compliance and information security?

- Yes
- No
- Undecided/Unsure

Viewing Information Technology Through Common Frameworks Is Critical to Enabling/ Facilitating IT Audit, IT Security, and IT Leadership Partnerships

COSO, COBIT and Other Frameworks Mean Common Language

IT Audit must be frameworks driven in how we view the world and how we communicate with our key stakeholders as we conduct our business.



IT Related Reviews, Risk Assessments, & Audits Scope Considerations

Effectiveness — Deals with information being relevant and pertinent to the business process as well as being delivered in a timely, correct, consistent and usable manner

Efficiency — Concerns the provision of information through the optimal (most productive and economical**)** use of resources

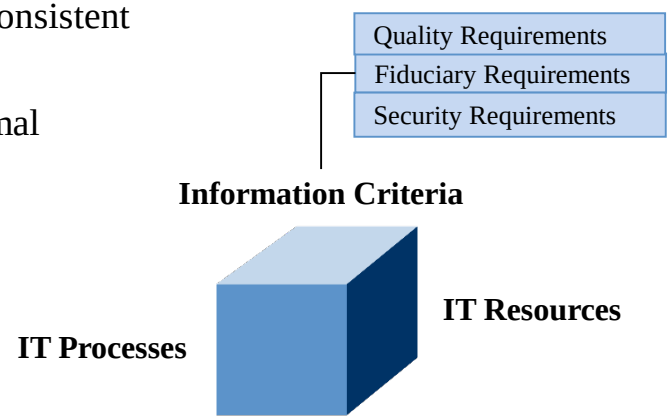
Confidentiality — Concerns the protection of sensitive information from unauthorised disclosure

Integrity — Relates to the accuracy and completeness of information as well as to its validity in accordance with business values and expectations

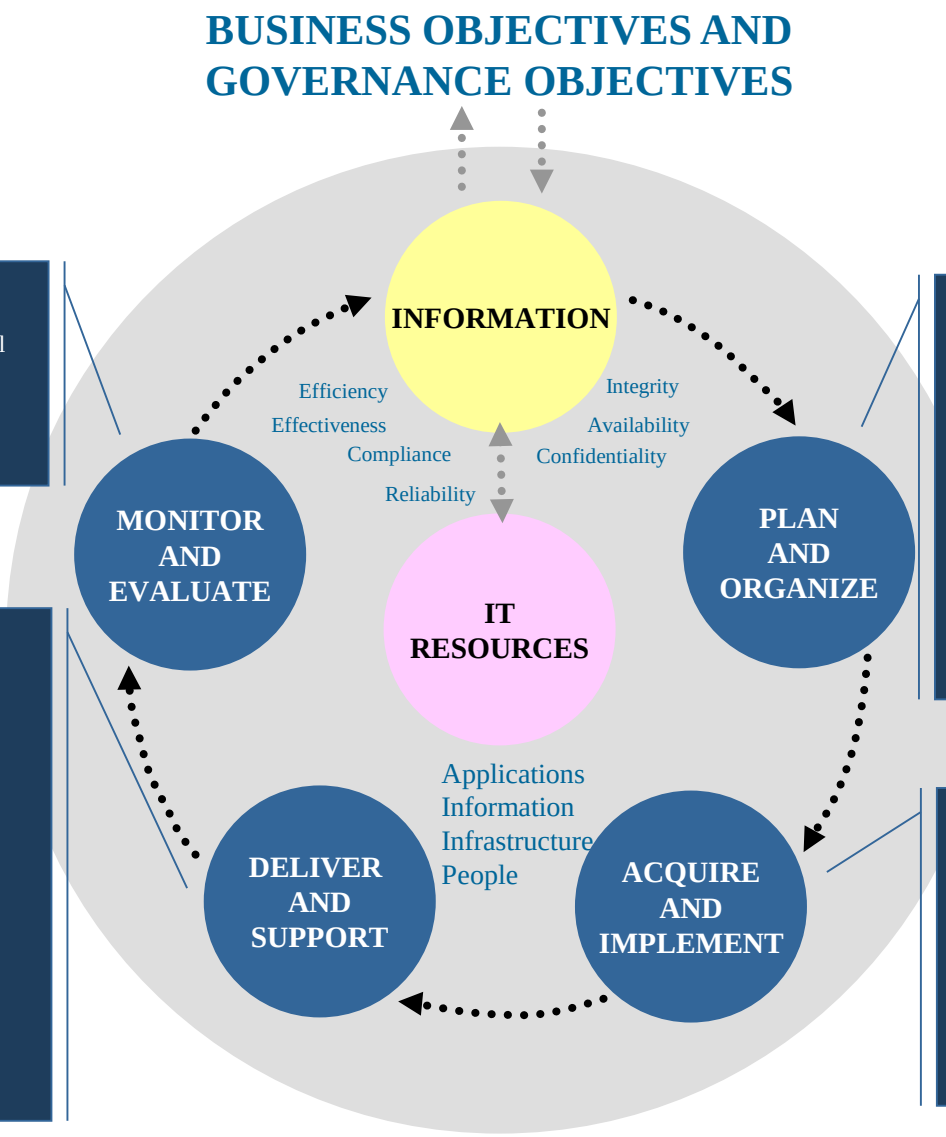
Availability — Relates to information being available when required by the business process now and in the future. It also concerns the safeguarding of necessary resources and associated capabilities.

Compliance — Deals with complying with those laws, regulations and contractual arrangements to which the business process is subject, i.e., externally imposed business criteria as well as internal policies

Reliability — Relates to the provision of appropriate information for management to operate the entity and to exercise its fiduciary and governance responsibilities



COBIT Framework as 4 Domains and 34 Processes



ME1 Monitor and evaluate IT performance.
ME2 Monitor and evaluate internal control.
ME3 Ensure compliance with external requirements.
ME4 Provide IT governance.

PO1 Define a strategic IT plan.
PO2 Define the information architecture.
PO3 Determine technological direction.
PO4 Define the IT processes, organization and relationships.
PO5 Manage the IT investment.
PO6 Communicate management aims and direction.
PO7 Manage IT human resources.
PO8 Manage quality.
PO9 Assess and manage IT risks.
PO10 Manage projects.

DS1 Define and manage service levels.
DS2 Manage third-party services.
DS3 Manage performance and capacity.
DS4 Ensure continuous service.
DS5 Ensure systems security.
DS6 Identify and allocate costs.
DS7 Educate and train users.
DS8 Manage service desk and incidents.
DS9 Manage the configuration.
DS10 Manage problems.
DS11 Manage data.
DS12 Manage the physical environment.
DS13 Manage operations.

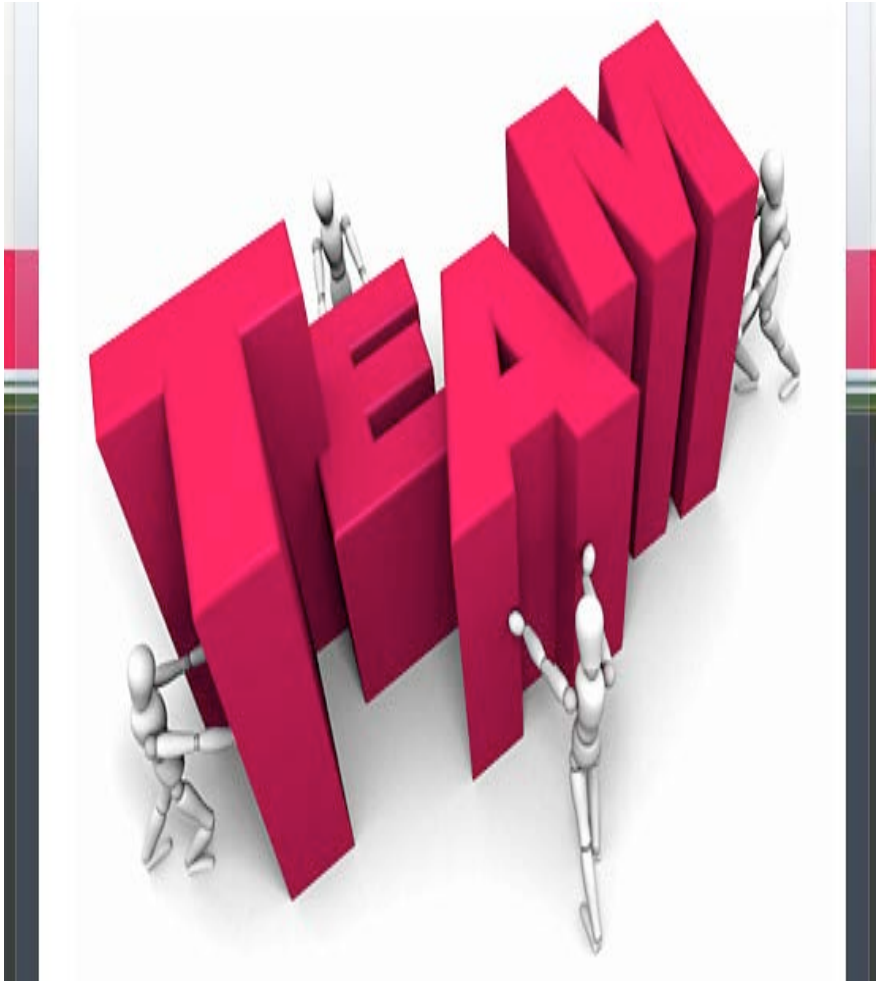
AI1 Identify automated solutions.
AI2 Acquire and maintain application software.
AI3 Acquire and maintain technology infrastructure.
AI4 Enable operation and use.
AI5 Procure IT resources.
AI6 Manage changes.
AI7 Install and accredit solutions and changes.

Annual Work Plan Coordination

Develop annual work plans that:

- Agree on the same planning horizon (i.e. fiscal or calendar year)
- Consider the annual risk assessments and preliminary priorities of each separate team;
- Look for common themes and discuss scope overlap to better leverage combined resources;
- Develop individual plans that are integrated and complementary in terms of risk coverage and timing of reviews; and
- Strive for consistent reporting formats to senior management governance and the Board.

By Working Together, IA, Compliance, and IT Security Can Be a Championship Team!!



Summary Comments and Q&A

Glen C. Mueller,
Chief Audit Executive
glen.mueller@cornell.edu

Contact Information

Glen C. Mueller
Chief Audit Executive, Cornell University

glen.mueller@cornell.edu

Upcoming ACUA Events

Title IX Auditing (encore performance)

- March 8, 2017

Intersection of ERM, Compliance, and Internal Audit

- March 21, 2017

2017 ACUA Midyear Conference – Austin, TX

- March 26-29, 2017

Using Interns in the Audit Shop

- April 19, 2017

ACUA
ASSOCIATION OF COLLEGE & UNIVERSITY AUDITORS
Advancing Auditing in Higher Education