ACUA
Association of College & University Auditors

March 24-26, 2026

ACUA VIRTUAL SPRING SUMMIT

Audit in Action

“Performance vs. Conformance”– Elevating Your IT Audits

Johan Lidros

CISA, CISM, CDPSE, CGEIT, ITIL-F, CRISC, HITRUST CCSFP

March 25, 2026
1:00 PM – 2.50 PM

Contents

- Introduction
- What is High Value IT Audits
- High Value IT Audits
- Q&A
- Referenced Material

Presenter

Johan Lidros, Founder and President of Eminere Group

- Over 25 years of experience providing information technology security, compliance and governance services in Europe and in the United States, at many healthcare and higher education institutions.
- Well-versed in accepted IT and information security standards/frameworks (ISO27000, HITRUST, NIST, COBIT, CIS, TIR, etc.) and has participated in several related committees
- Certifications: CISA, CISM, CDPSE, CGEIT, ITIL-F, CRISC, HITRUST CCSFP
- ISACA certified instructor CISA, CISM, CRISC, CGEIT

Why We are Here

Is your organization performing the “right” IT audits?

Is it conformance or performance-focused?

Does your risk-based IT audit plan incorporate opportunity areas and root causes?

By who and how has your risk appetite been defined?

How do we provide management, the audit committee, and the board with relevant information to provide input and/or select the “right” audit plan?

This interactive session will provide valuable insight into these areas and several other topics that increase the value of your IT audits.

Session Objectives

- Are we doing the right things?
- Get you thinking !!!
- Is there another way to do this?
- What are our biggest risks?
- What are the key controls?
- Are we auditing them?
- Are we measuring them?
- Have we defined metrics?
- What are the root causes?
- How to create change, massive change?
- What are the most “high” value audits we can perform

Objectives

Introduction

- Information technology (IT) is critically important for most organizations.
- The complexity and rate of change of technology can dramatically impact risk, compliance and success.
  - Research
  - Education
  - Communication outreach
  - Administration
- The latest IT and cyber threats can challenge a higher education provider's ability to deliver quality outcomes and resilience.
- Improvements in IT Governance can help prepare organizations to manage new and traditional IT risks
- A wealth of best practices and industry standards is available to help organizations improve their cybersecurity, IT audit, and IT Risk compliance.

Internal Auditing Competency Framework™ Global Practice Guide

Skills required for Auditors.

See also skills required for the Audit Committee !!!!! B.10

See https://www.theiia.org/en/resources/internal-audit-competency-framework/

IIA Standard 9.1 Understanding Governance, Risk Management, and Control Processes

Requirements

To develop an effective internal audit strategy, charter, and plan, the chief audit executive must understand the organization's governance, risk management, and control processes.

International Professional Practices Framework® (IPPF)

To understand governance processes, the chief audit executive must consider how the organization:

- Establishes strategic objectives and makes strategic and operational decisions.
- Oversees risk management and control.
- Promotes an ethical culture.
- Ensures effective performance management and accountability.
- Structures its management and operating functions.
- Communicates risk and control information throughout the organization.
- Ensures the coordination of activities and communications among the board, internal and external providers of assurance services, and management.

To understand risk management and control processes, the chief audit executive must consider how the organization identifies and assesses significant risks and selects appropriate control processes. This includes understanding how the organization identifies and manages the following key risk areas:

- Reliability and integrity of financial and operational information.
- Effectiveness and efficiency of operations and programs.
- Safeguarding of assets.
- Compliance with laws and Regulation

IIA Standard 2024: Standard 9.4 Internal Audit Plan

<u>The internal audit plan must</u>:

- Consider the internal audit strategy and the full range of internal audit services.
- Specify internal audit services that support the **evaluation** and improvement of the organization's governance, **risk management,** and control processes.
- **Consider coverage of information technology governance,** fraud risk, and the **effectiveness** of the organization’s compliance and ethics programs.
- Identify the necessary financial, human, and technological resources.
- Be dynamic and updated timely in response to changes in the organization’s business, risks, operations, **programs**, **systems**, controls, and organizational culture.

IIA Standard 2024

<u>The new Standards now include requirements for IA to communicate to senior management and the Board</u>:

- **Any high risk areas** where an assurance engagement **is not** included on the IA plan.
- Impact of resource limitations on IA coverage
- Demonstrate that IA considered coverage of IT governance, fraud risk, the effectiveness of the compliance and ethics programs in addition to other high risk areas.

IIA Standard 2024: Topical Requirements

Cybersecurity February 2025

- GOVERNANCE: Evaluating and Assessing Cybersecurity Governance
- RISK MANAGEMENT: Evaluating and Assessing Cybersecurity Risk Management
- CONTROLS: Evaluating and Assessing Cybersecurity Control Processes

Third-Party Topical Requirement Effective September 15, 2026

Organizational Behavior Topical Requirement Effective December 15, 2026

Organizational Resilience Topical Requirement – Coming 2026

IIA Standard 2024: Topical Requirements

Topical Requirements are applicable when a risk assessment leads to the topic being one of the following:

1.The subject of an assurance engagement in the internal audit plan.
2.Identified while performing an engagement.
3.The subject of an engagement request not on the original internal audit plan.

IT Auditing

National Association of Corporate Directors (NACD):

“The board must require internal audit to provide health check of the organizations cybersecurity program”

Higher Education IT Characteristics

- Higher Education is a “target”
- Constantly new and changing threats/risks related to the use of technology
- IT solutions become critical for core services – education, etc.
- Diversified IT environment and legacy debt
- Shadow IT/Decentralized IT
- Data governance in critical state - Value of Information increasing– Information Governance – Creating new “in-house” critical systems
- Many regulatory requirements with more state/federal requirements coming and more “guidelines” (due care)
- Immature IT/Information Security

Key Drivers - Impacting Areas

Regulatory requirements

AI

Cloud

PII/EPHI Theft or misuse

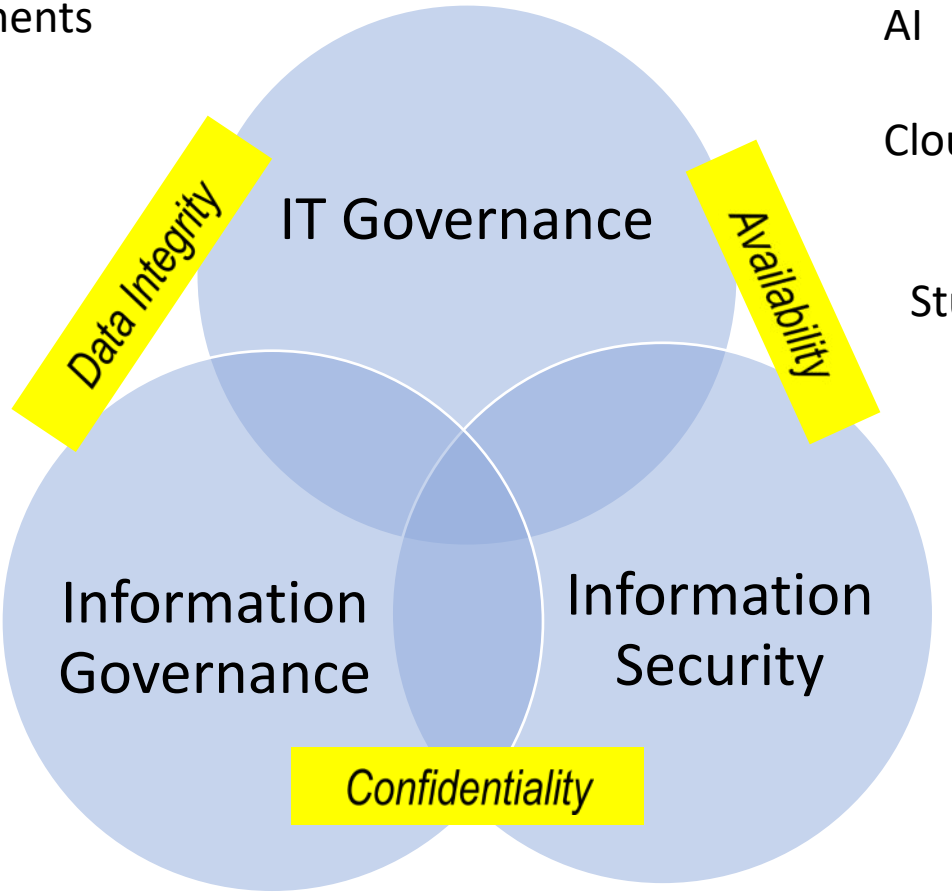
Student interaction

Research

Social media

Big data Analytics

Portable devices



Root Causes

1. IT and information security is not an IT issue anymore – ERM key business risk – Tone from the Top
2. IT and Information Security Governance
3. Weak IT / IT Security Risk Management
4. Lack of well defined Goals/Measurements/Reporting
5. Management and Business/Information Owner's responsibilities for IT risk is not well defined and communicated
6. Weak Critical Foundational IT Processes (asset management, IAM, resilience, etc.)
7. Lack of Resources in Key Areas e.g. IT Governance, networks, system administrators, disaster recovery, security governance, IAM, vendor management
8. Awareness and Training
9. Lack of Policies in Key Areas, no IT Security Standards and Limited Formal Procedures in Most Areas
10. Decentralized IT, "Shadow" IT (lack of governance/controls)
11. Weak Compliance and Assurance

Key Questions

Tone from the top

- Does the Board take leadership for the IT Governance?
- Does the board understand the organization's dependency on IT? How is that understanding reflected in the strategic plan?
- Does the Board define clear objectives?
- Are directives in place?

Strategic Alignment

- Does an IT Strategy exist?
- Is the IT Strategy up to date?
- Is the IT Strategy aligned with the business objectives?

Risk Management

- Is an IT Risk Management process in place?
- Are the risks identified, evaluated, assigned and mitigation actions taken?
- Is the Board aware about the IT Risks?
- Are incidents tracked and reported?
- Who is overseeing risk management and control?

Organization

- Is the IT organization adequate?
- Are the processes defined (maturity level)?
- Are the roles, responsibilities and duties defined and assigned?
- Is a project Portfolio Management in place and effective?

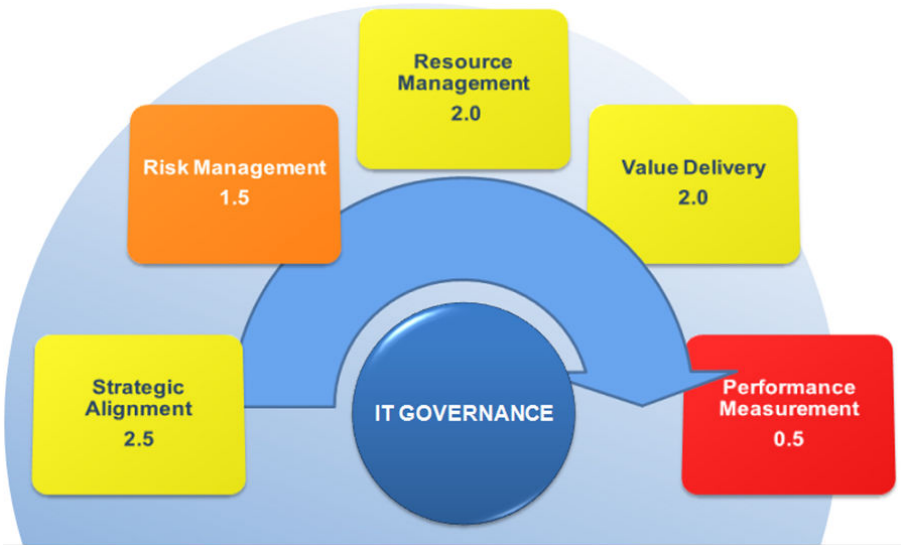
Resource Management

- Are the resources adequate?
- Are IT resources managed effectively?

Performance Management

- Are meaningful metrics defined?
- Is IT performance defined, measured and reported using the defined metrics?

Reporting – Key for Success



Process Maturity Rating	
0	**Non-existent:** The process (control/procedures) does not exist.
1	**Initial/Ad hoc:** The process is informal, undocumented and reactive.
2	**Repeatable:** The process is repeatable but may be applied inconsistently as needed.
3	**Defined:** The process is documented and communicated.
4	**Managed:** The process is implemented and measurable.
5	**Optimizing:** Managed process with continuous performance improvements utilizing best practices.
N/A	**Not Applicable:** The process is not applicable to the review or has not been reviewed for other reasons.

IT Governance Area	Key Strengths	Key Areas for Improvement
Strategic Alignment Ensure IT is aligned with the organization's mission, strategic goals/direction, and business needs.	• IT Road Map, and • Executive team involvement.	• Formalize IT strategy, and • Information Technology Committee implementation.
Risk Management Understand and be aware of IT risks and the organization's risk appetite and how to effectively and appropriately manage the identified risks.	• Enterprise Risk Management (ERM) program, • Annual IT risk assessment, • Information Security Committee and Program, • Business Continuity/Disaster Recovery Program and • Comprehensive IT policies	• Further integrate IT risk management with ERM. • Improve asset management and defined owners and responsibilities. • Weak IT procedures in several areas • Supply chain management • Regular IT audits and Information Security Review
Resource Management Optimal investment in and proper management of IT resources, including infrastructure, applications, information, and people.	• Weekly IT department meetings	• Communication and prioritization of IT projects, and • Business value analysis for projects can be improved together with TCO .
Value Delivery IT delivers the promised benefits against the strategy, concentrating on optimizing costs and proving the intrinsic value of IT.	• Vendor IT infrastructure delivery (Service Level Agreement).	• Project management, • Limited project value delivery follow ups, • Limited processes for IT cost analysis, and • Customer satisfaction.

Performance Measurement
Ongoing key IT measurements, such as Key Goal Indicators (KGI) and Key Performance Indicators (KPI), that supports the Board's and managements understanding of IT strategic alignment, IT risk management, resource management, and value delivery.
	• Service desk measurements,
	• IT risk management,
	• IT security reporting, and
	• Regular IT status reporting to the Board and Executive Management.
		• Limited and/or lack of performance measures in the following IT governance areas:
		  ○ Strategic alignment,
		  ○ Value delivery, and
		  ○ Resource management.

Threat Models:

Higher Education is a target… & Easy Target ….

- Remote workforce
  - Staff
  - Contractors
  - Vendors
- Remote Student/researchers
  - Email
  - Collaboration tools
- Increased dependency to remote technology and infrastructure
  - VPN
  - Education solutions
  - Collaboration tools
  - Cloud infrastructure
- Supply Chain

The weakest link….

- **People**
- **Tools**
- **Process**

The top six industries in our casework stayed the same this year, and they accounted for 63% of our cases:

1. Professional and legal services
2. High technology
3. Manufacturing
4. Healthcare
5. Finance
6. Wholesale and retail

Paloalto UNIT42 2024 Incident response report

Cyber Common Attack Vectors: the Weakest Links

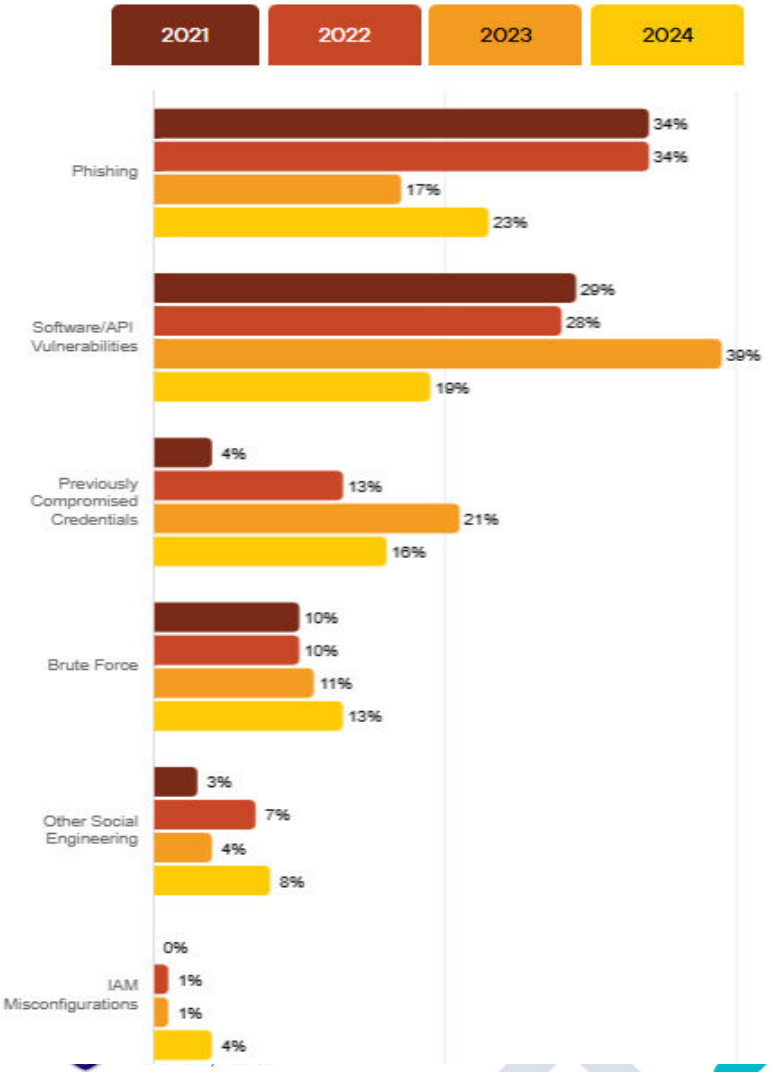
- Email
- Authentication
- Privileged Accounts
- Web Application
- Supply Chain/Partner Breach

Paloalto UNIT42 2024 Incident response report:
How Threat Actors Succeed: Common Effective Tactics, Techniques and Procedures

Fronts of Attack	Percentage of Cases
Endpoints	72%
Human	65%
Identity	63%
Network	58%
Email	28%
Cloud	27%
Application	21%
SecOps	14%
Database	1%

Cyber Common Attack Vectors: the Weakest Links

- Email (phishing, DMARC, SPF, etc.)
- Authentication
- Privileged Accounts
- Web Application
- Supply Chain



What happened in 2025 from an IT Risk Perspective

- Incidents
  - …
- Resilience
- New or Technology Shifts
  - Business Technology – AI
    - Administration
    - Education
    - Research
  - IT Infrastructure Technology
- Regulatory changes
- IT Security and Privacy Practices/Standards Updates
- Insurance
- Data …
- …

Other Trends

- Cybersecurity and Infrastructure Security Agency and HHS Cybersecurity Performance Goals - CPG
- AI – New operational usage and requirements
  - FDA New Requirements
  - EU AI Act
  - New areas use of AI
- GLBA Gramm-Leach-Bliley Act
  - Prescriptive security requirements
- Privacy Legislation and Enforcements
  - State
  - Federal
- Research Requirements
  - NIH - Data management plan
  - DoD – CMMC
  - Fedramp, StateRamp
- Privacy and Information Security Integration
- OT – Operational Technology
- Technology Debt - IT Legacy Debt
- Standards
  - CIS – Reasonable Cybersecurity
  - NIST CSF 2.0
  - NIST Privacy 2.0
  - Hitrust
- Information/Data Governance
- Cyber insurance - Increased requirements and cost …
- IT Cost … Value … IT Governance
- Training – 88% of Cybersecurity breaches due to human error…

Valuable Resources & Regulatory Changes

1. Cybersecurity Performance Goals
   - Critical Infrastructure – CPGs
   - Healthcare - CPG Incentive programs and new cybersecurity requirements

2. Free Services from the Cybersecurity and Infrastructure Security Agency (CISA)
   1. Risk and Vulnerability Assessment (RVA).
   2. Cyber Security Performance Goals Assessment

3. Health Industry Cybersecurity Practices 2023 – HICP

Cybersecurity Performance Goals

Essential Goals: *To help healthcare organizations address common vulnerabilities by setting a floor of safeguards that will better protect them from cyber attacks, improve response when events occur, and minimize residual risk.*

- **Mitigate Known Vulnerabilities**
- **Email Security**
- **Multi-factor Authentication**
- **Basic Cybersecurity Training**
- **Strong Encryption**
- **Revoke Credentials for Departing Workforce Members:**
  Employees, Contractors, Affiliates, Volunteers
- **Basic Incident Planning and Preparedness**
- **Unique Credentials**
- **Separate User and Privileged Accounts**
- **Vendor/Supplier Cybersecurity Requirements**

Enhanced Goals: To help healthcare organizations mature their cybersecurity capabilities and reach the next level of defense needed to protect against additional attack vectors.

- ❑ **Asset Inventory**
- ❑ **Third Party Vulnerability Disclosure**
- ❑ **Third Party Incident Reporting**
- ❑ **Cybersecurity Testing**
- ❑ **Cybersecurity Mitigation**
- ❑ **Detect and Respond to Relevant Threats and Tactics, Techniques, and Procedures**
- ❑ **Network Segmentation**
- ❑ **Centralized Log Collection**
- ❑ **Centralized Incident Planning and Preparedness**
- ❑ **Configuration Management**

2. CISA Free Services

- Free Risk and Vulnerability Assessment (RVA).
- Free Cybersecurity Performance Goals (CPG) assessments
- An RVA is a two-week penetration test of an entire organization, with one week spent on external testing and one week spent assessing the internal network.
  - The objectives:
    - Identify weaknesses through network, system, and application penetration testing.
    - Test stakeholders, using a standard, repeatable methodology to deliver actionable findings and recommendations.
    - Analyze collected data to identify security trends across all RVA stakeholder environments.
    - See example https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-349a
  - See Fact Sheet: https://www.cisa.gov/sites/default/files/publications/VM_Assessments_Fact_Sheet_RVA_508C.pdf

Foundation

- Identify and understand “new” technologies
  - Evaluate the potential use for the organization
  - Define a plan and objectives
  - Risk Assessment with stakeholders and Subject Matter Experts (SME)
  - Asset inventory (data, hardware, attributes (RTO, RPO, owner, etc.))
- Identify and understand trending risk areas
  - Asset inventory
  - BIA results
  - Risk studies/reports
  - Silo – Integration – ERM

Contents

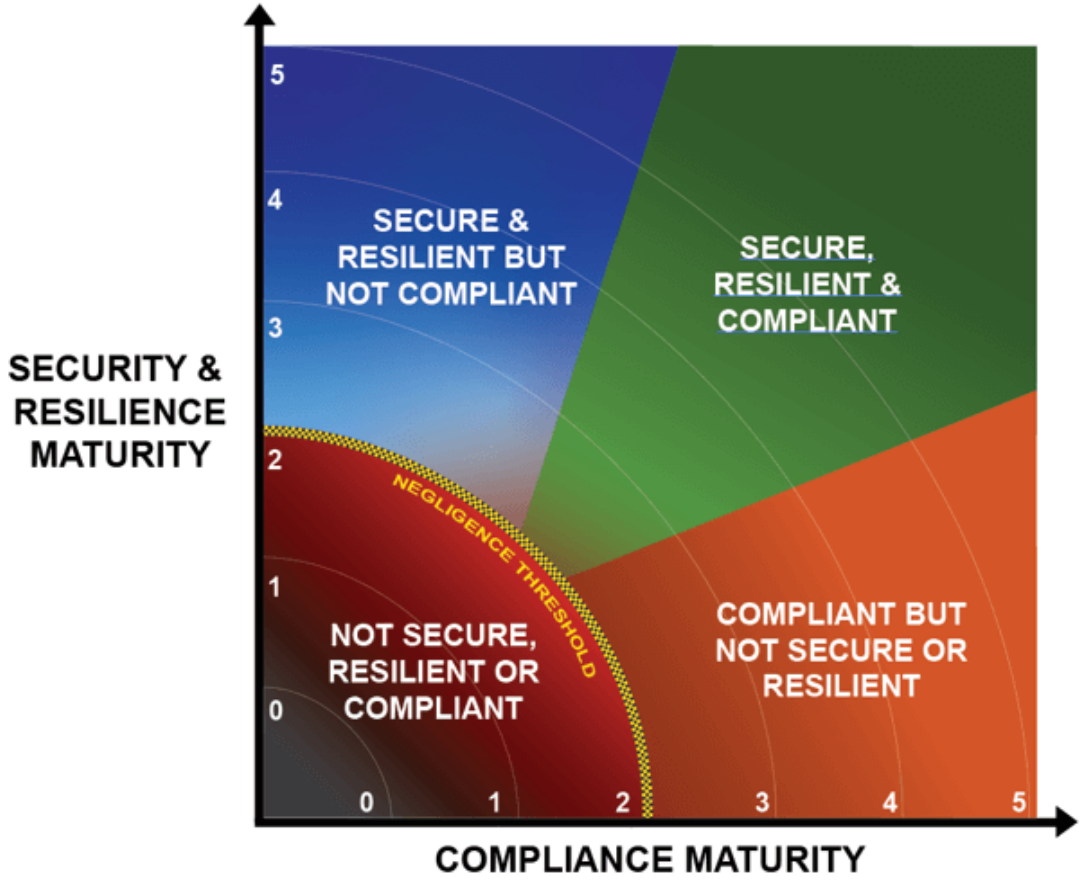
- Introduction
- What is High Value IT Audits
- High Value IT Audits
- Q&A
- Referenced Material

High Value Audits?

- Risk based
  - Negative and positive/opportunities
- Root Causes
- Understand your stakeholders
- Programs
- Key Controls
  - People
  - AD
  - Utilities …

What is Good Enough – Compliance or Resiliency?

- Compliance does not mean good risk management?
- What are the key risks?
- What is the status of key programs?
- Where does Quality come in?

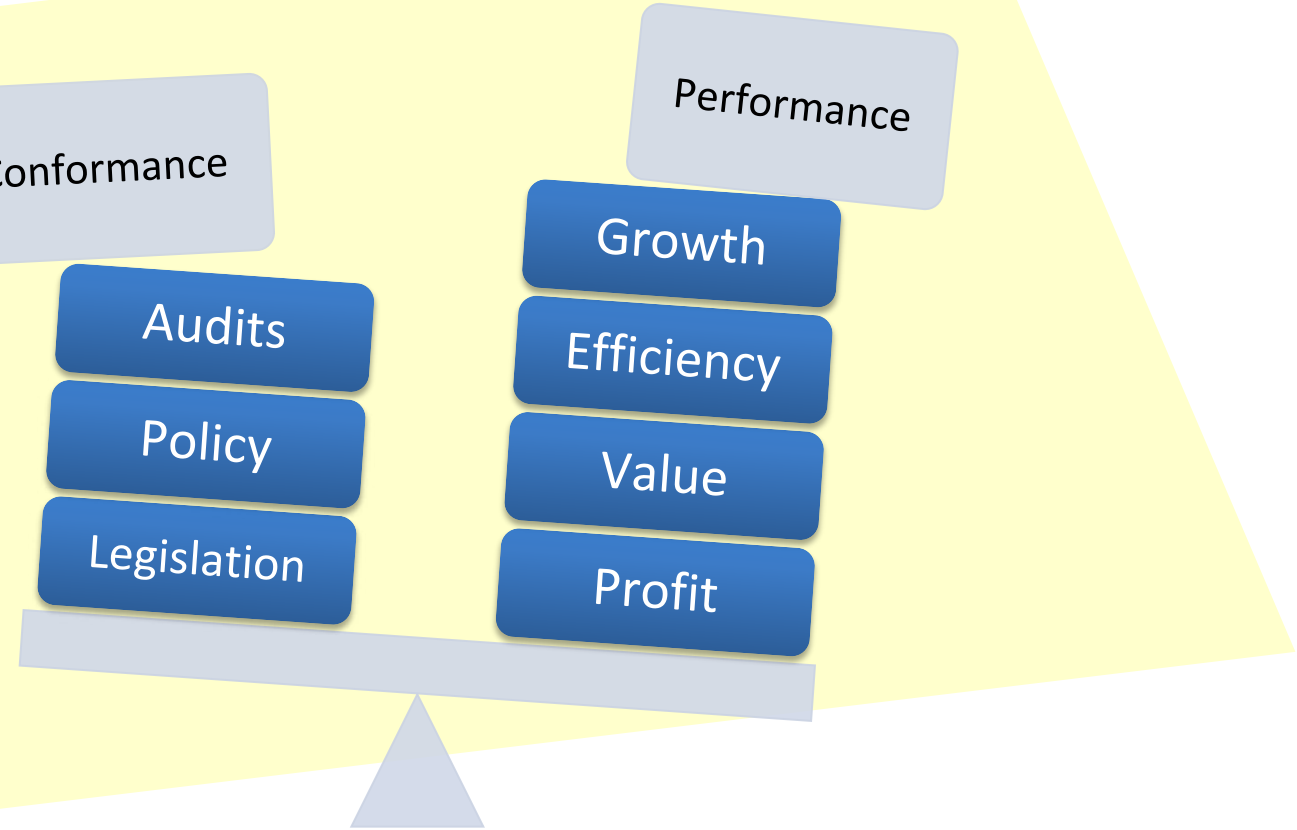


IT Governance Goals

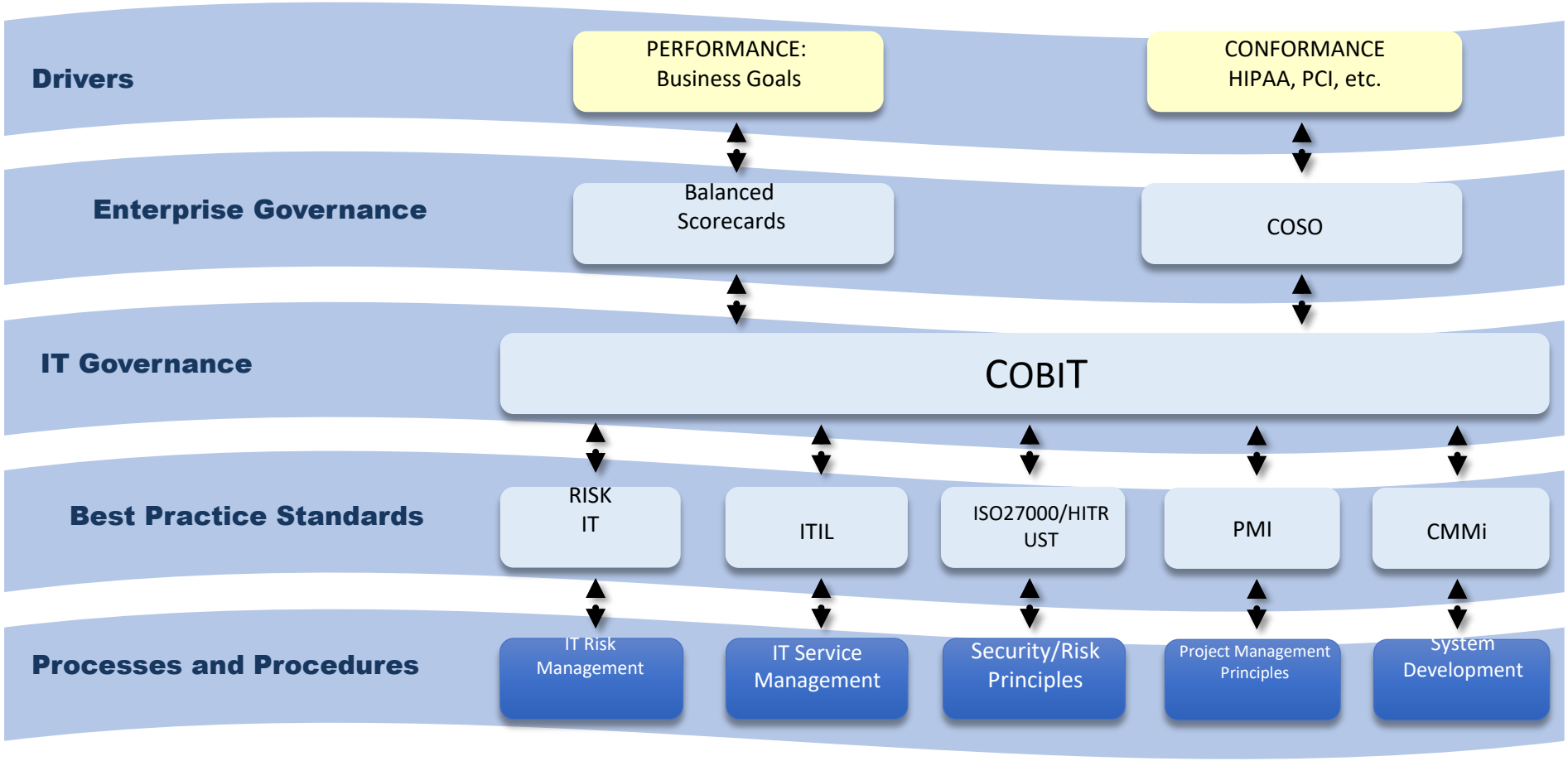
- "… is a set of responsibilities and practices exercised by the board and executive management with the goal of
  - "Providing strategic direction
  - "Ensuring that objectives are achieved
  - "Ascertaining that risks are managed appropriately
  - "Verifying that the enterprise's resources are used responsibly"
- "… is about
  - "Conformance: adhering to legislation, internal policies, audit requirements, etc.
  - "Performance: improving profitability, efficiency, effectiveness, growth, etc."

Balance of IT Governance Goals

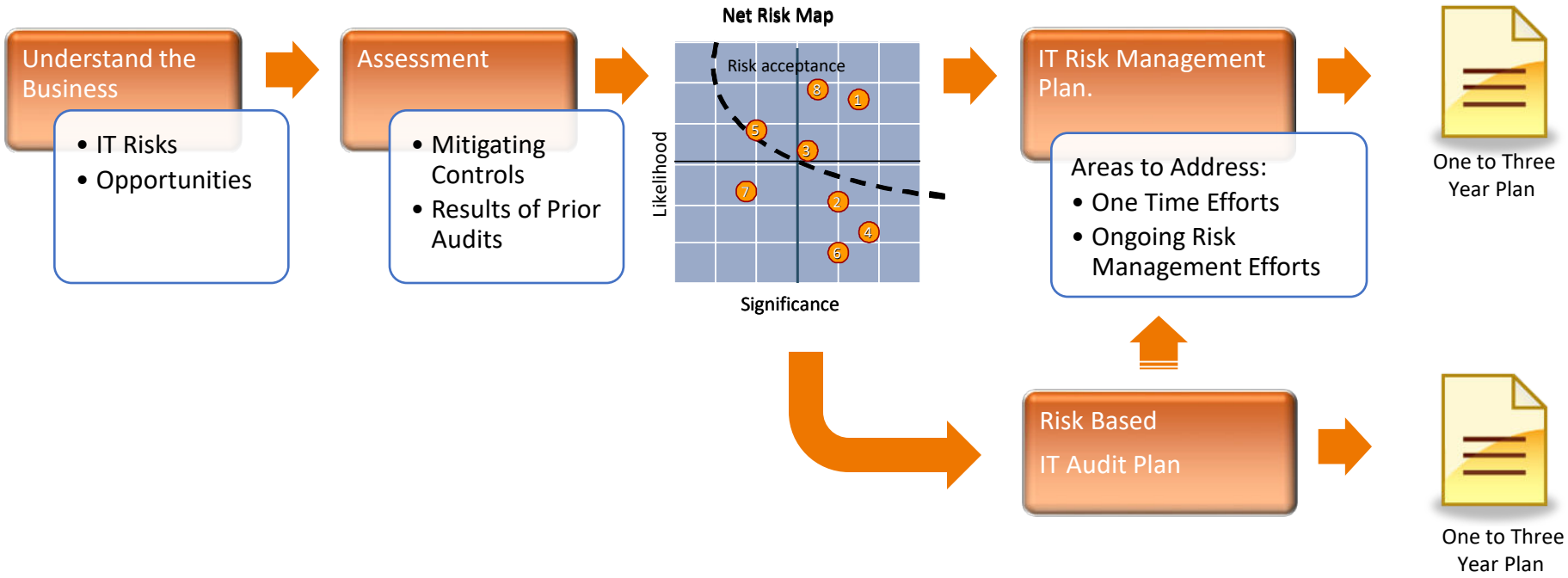
The board must direct the balance between conformance and performance goals.



IT Governance Framework



IT Risk Management



IT Related risk = materialised business impact because of IT related event

Risk Management Approach

Identify high risk areas

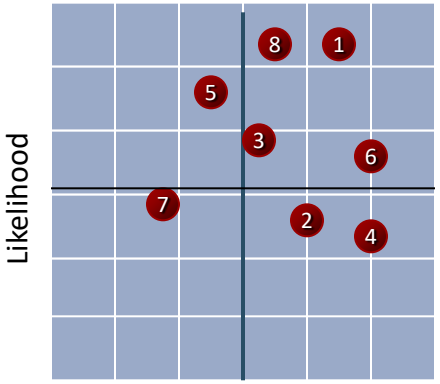
Assess risk management

Risk acceptance – Can management accept the existing risk level?

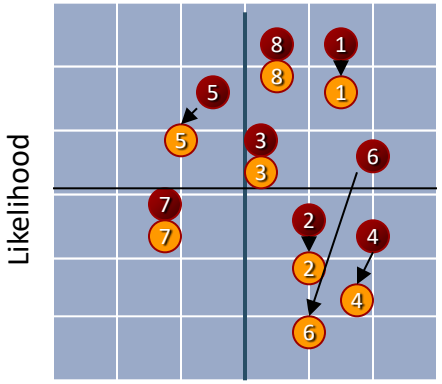
Gross risk

Net risk

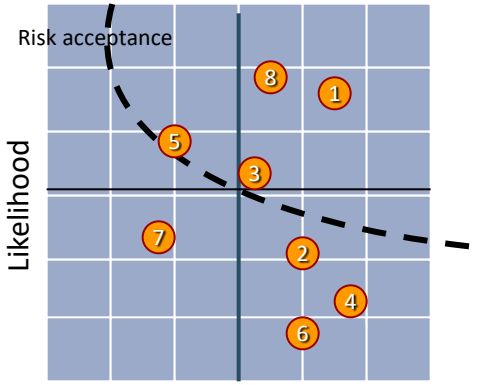
Gross Risk Map



Risk Management



Net Risk Map

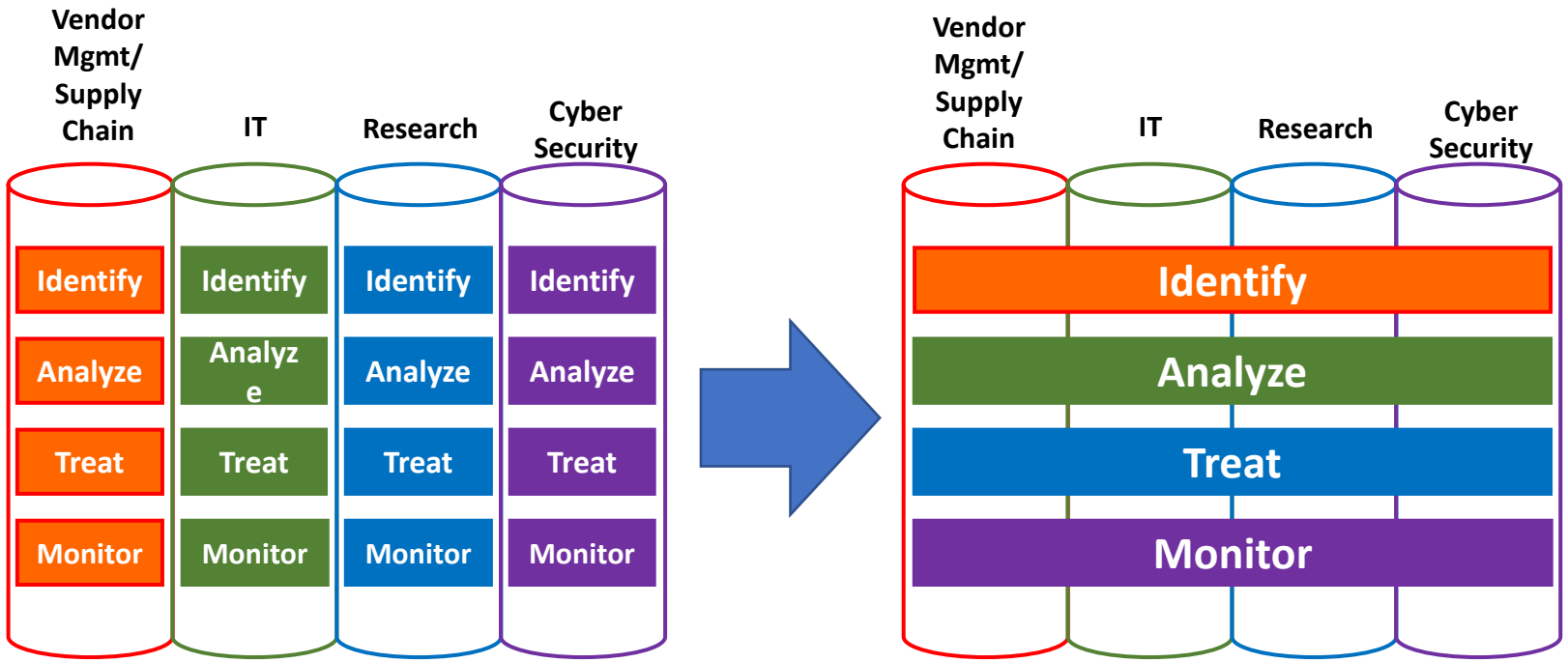


Example Risk Universe (Risk Landscape)

Root Causes

1. It is not an IT issue anymore – Key business risk - Accountability
2. IT and Information Security Governance
3. Weak IT / IT Security Risk Analysis
4. Lack of Risk Management Plan and Goals/Measurement/Reporting
5. Management and Business/Information Owner's responsibilities for IT risk is not well defined and communicated
6. Asset Management (hardware, software, data, interfaces, CI, and criticality…)
7. Weak Critical Foundational IT Processes
8. Lack of Resources in Key Areas e.g. networks, system administrators, disaster recovery, cyber, governance, IAM, vendor management
9. Awareness and Training
10. Lack of Policies in Key Areas, no IT Security Standards and Limited Formal Procedures in Most Areas
11. Decentralized IT, "Shadow" IT (lack of governance/controls)
12. Weak Compliance and Assurance

Risk Management Silos



Science and Information Security

Tool / Attribute	Availability	Integrity	Authenticity	Accepted Techniques	Authorization	Confidentiality	Credible Source	Reproducibility
3rd party data repo	O	O	O				O	O
Policy for network/cloud storage	N	O			N		N	
Archival storage	N	O					O	O
Workflow integrity checking		S						N
Access controls	N	N			S	N		
Physical security protections	N	N			N	N		
Network controls	N	N			N			
Logging	O	O			O			
Multifactor Authentication	O	O			O			
Intrusion detection/protection	O	O			O			
File/host integrity check	O	N			O			
RAID file system	N	N						
External backups	N	O						

Symbol	Meaning
S	Sufficient: This tool/technology alone can establish an assertion of the desired attribute, however weak it may be.
N	Necessary: This tool/technology is required to provide a stronger, credible assertion of the desired attribute.
O	Optional: This tool/technology can help strengthen the assertion of the desired attribute, however that is not its design intent.

Guidance for Trustworthy Data Management in Science Projects

https://trustedci.org/2020-trustworthy-data

September 30, 2020

Distribution: Public

Trustworthy Data Working Group

Andrew Adams, Kay Avila, Jim Basney, Laura Christopherson, Melissa Cragin, Jeannette Dopheide, Terry Fleury, Calvin Frye, Florence Hudson, Manisha Kanodia, Jenna Kim, W. John MacMullen, Mats Rynge, Scott Sakai, Sandra Thompson, Karan Vahi, John Zage

https://blog.trustedci.org/2020/10/tdwg-guidance-report.html

Key Discussion Topics for the Board/Executives

- IT Governance
- IT – Legacy Debt
- AI
- Information Security
- Information Governance
- IT Standards (NIST CSF, SCF, HITRUST, etc.)
- Measurements and Metrics
- Exception Management – Risk Tolerance

- Board and Management Digital Smarts
  - Does your C-suite have enough digital smarts? – **MIT Sloan Management Review**:
    - Magazine: Spring 2021 Issue Research Highlight

      Digitally Savvy Top Teams Deliver Performance Premiums: companies with such executive teams have 48% higher revenue growth and higher valuations(share price to sales ratio) and 15% higher net margins than the rest of the companies we studied.
  - **It Pays to Have a Digitally Savvy Board – MIT Sloan Management Review:**

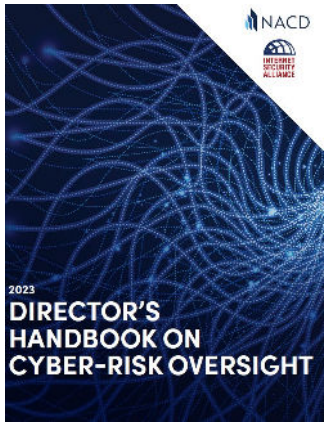
    Magazine: Spring 2019 Issue Research Highlight March 12, 2019

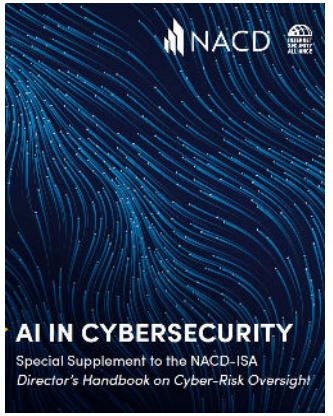
    https://sloanreview.mit.edu/article/it-pays-to-have-a-digitally-savvy-board/
  - **IIA**

NACD – Directors Handbook on Cyber-risk Oversight

The Six Principles:

- PRINCIPLE ONE: Cybersecurity as a Strategic Risk
- PRINCIPLE TWO: Legal and Disclosure Implications
- PRINCIPLE THREE: Board Oversight Structure and Access to Expertise
- PRINCIPLE FOUR: An Enterprise Framework for Managing Cyber Risk
- PRINCIPLE FIVE: Cybersecurity Measurement and Reporting
- PRINCIPLE SIX: Encourage Systemic Resilience and Collaboration



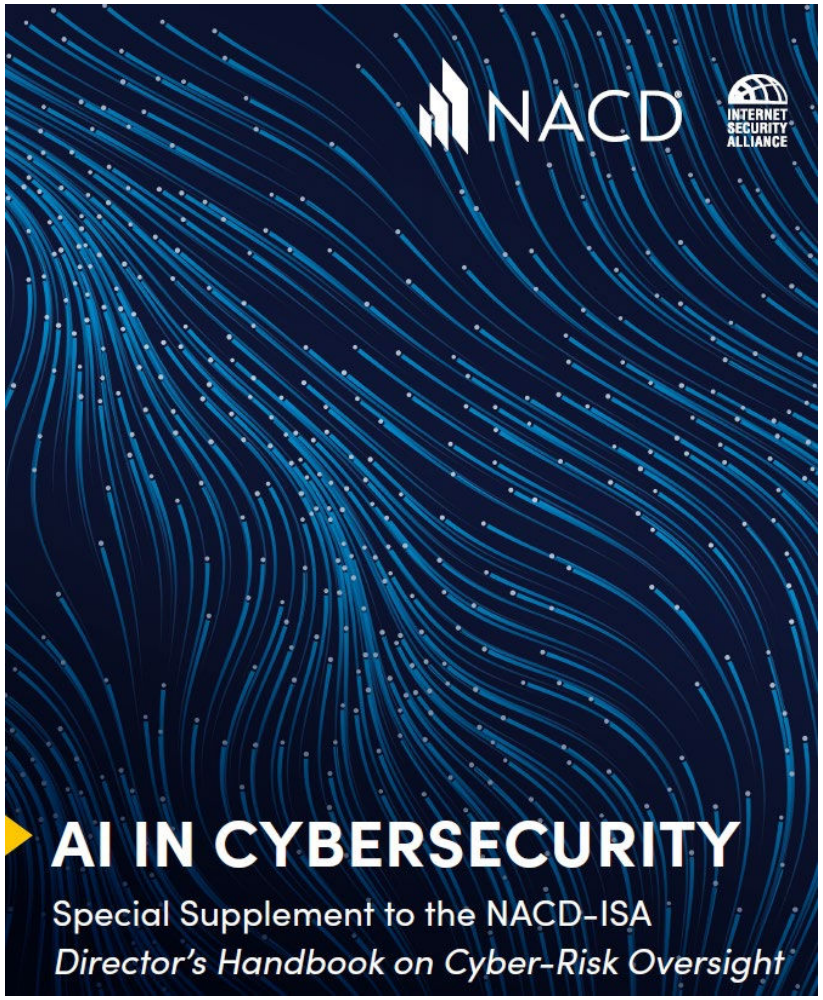


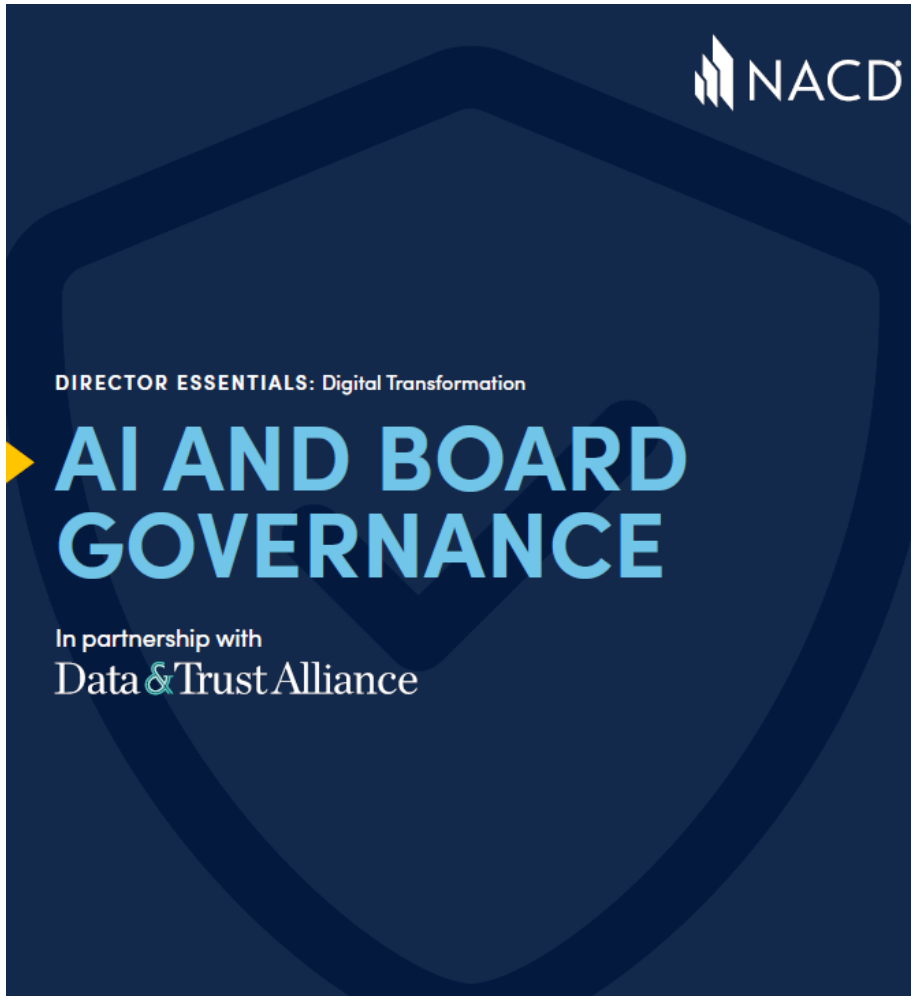
https://www.nacdonline.org/insights/publications.cfm?ItemNumber=74777

Nonmembers can access this publication by creating a guest account.

https://www.nacdonline.org/globalassets/public-pdfs/nacd_ai-cybersecurity-handbook.pdf

AI and Board Governance





How Important is it that your board improves in the following Cyber-risk areas

Areas Related to Cyber-Risk Oversight	Not at all important	Slightly important	Moderately important	Very important	Extremely important	n
Alignment of compensation incentives with corporate cybersecurity objectives	32.94%	18.82%	27.06%	16.47%	4.71%	85
Quality of board-CISO relationship	15.48%	20.24%	23.81%	33.33%	7.14%	84
Board cybersecurity expertise	10.71%	15.48%	28.57%	34.52%	10.71%	84
Committee oversight responsibility	14.29%	11.90%	25.00%	35.71%	13.10%	85
Quality of cybersecurity education plans and access to outside expertise	9.30%	18.60%	24.42%	36.05%	11.63%	86
Linking cybersecurity to strategic priorities	9.41%	18.82%	20.00%	43.53%	8.24%	84
Acquiring metrics to accurately measure and assess cybersecurity	3.53%	15.29%	29.41%	41.18%	10.59%	85
Quality of management reporting	3.53%	15.29%	24.71%	37.65%	18.82%	85

This table comes from the Cybersecurity section of the 2025 NACD Private Company Board Practices and Oversight Survey.

ACUA
Association of College & University Auditors

Notpetya - Warstory

THE UNTOLD STORY OF NOTPETYA, THE MOST DEVASTATING CYBERATTACK IN HISTORY

-Maersk Andy Greenberg – Wired August 22, 2018

"It cost us between 250-300 million dollars, and yet I argue it was a very important wake-up call…."

- https://www.youtube.com/watch?v=VaqIYlYmDbA

COSO Risk Appetite – Critical to Success

4

RISK APPETITE IS AT THE HEART OF DECISION-MAKING

It is germane to decision-making. It is equally important in determining that a decision is necessary.

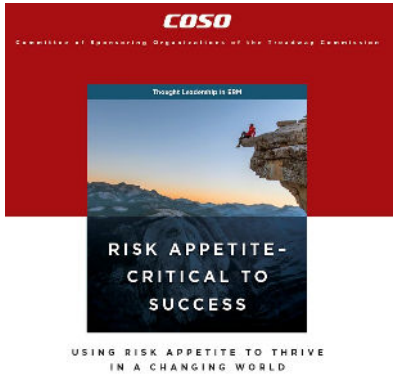
RISK APPETITE AND RISK TOLERANCE DIFFER

Various documents use the terms "risk appetite" and "risk tolerance" in different ways, even interchangeably. This adds to the confusion in understanding their meaning. Though related, they are different ideas.

6

RISK APPETITE HELPS INCREASE TRANSPARENCY

A well-formed and communicated risk appetite provides awareness of the risks the organization wishes to assume as well as those it wishes to limit.



https://www.coso.org/Documents/COSO-Guidance-Risk-Appetite-Critical-to-Success.pdf

Cause of Cyber risks?

Consider a simple example: **A bank is robbed; that's the "what." The "how" might be that the burglar alarm failed to go off.** And that's usually the end of the story: There was an unfortunate malfunction.

But digging deeper, we might learn that the **alarm system was known to be old and unreliable. Funds had been allocated to replace it, but someone in management decided to instead use them for a marketing campaign to attract more customers.**

I call this **semiconscious decision-making**, because **someone made a decision** — not to replace the burglar alarm — **without considering the possible consequences of that choice, namely, losing all the cash**. In essence, that decision created the circumstance for the robbery.

The Rest of the Cybersecurity Story

Semiconscious decision-making is a common but too often unacknowledged cause of cyber risks.

Cause of Cyber risks?

Semiconscious decision-making is a common but too often unacknowledged cause of cyber risks.

The methodology is based on three core concepts:

(1) Identify the crown jewels — that is, what is it that you are trying to protect or prevent;

(2) (2) identify controllers for processes that are intended to protect the crown jewels; and

(3) (3) identify controllers for controllers, hierarchically.

In essence, an attack can only succeed if the needed controls were defective or simply not in place—and if a higher-level controller overlooked this security gap.

Applying the Cybersafety methodology in order to reveal the what, how, and why of the cyber event, we identified many cases of semiconscious decision-making that contributed to the Equifax data breach. These semiconscious decisions were made at all levels of the organization, from the middle management of technical groups to top executives and the board. Let's consider just some of those decisions.

- **Unencrypted data:** System out of scope. Management decided system out of scope for PCI audit i.e. not require encrypt data and be audited to ensure key controls in place.
- **Outdated certificates;** company's intrusion detection and prevention process (IDPP), which was supposed to be monitoring internet traffic for any messages that were suspicious or invalid, had not been functioning for at least nine months

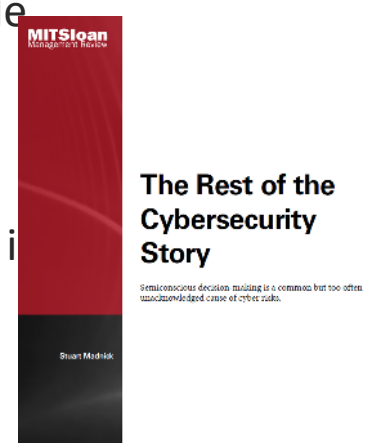
The Rest of the Cybersecurity Story

Semiconscious decision making is a common but too often unacknowledged cause of cyber risks.

Cause of Cyber risks?

Why wasn't the IDPP functioning? It required certain security certificates to give it permission to access the internet traffic, but the certificates had expired — so it was not able to monitor any traffic or sound an alarm.

Why hadn't the certificates been updated long ago? Well, Equifax had hundreds, if not thousands, of such certificates, and tracking each one's expiration date and updating the certificates was an error-prone, manual task (not unlike the defective burglar alarm process i the bank robbery example).



The Rest of the Cybersecurity Story

Semiconscious decision-making is a common but too often unacknowledged cause of cyber risks.

This problem had been noted in the past; in fact, a proposal had been made to develop an automated, centralized certificate-management process. **But the managers responsible for the numerous applications requiring security certificates, scattered throughout the organization, did not consider this a priority. Furthermore, providing centralized support for managing the certificates would require some organizational changes that were likely to be resisted by those who had overlooked the danger created by expired certificates.**

Cause of Cyber risks?

Conscious Risk Assessment

Apparently, no one at Equifax considered the possibility that these two isolated decisions, along with many other similar semiconscious management decisions, might cost the company dearly. The **company's board essentially allowed management to take unmeasured, and thereby unlimited, risks** in order to pursue an aggressive growth strategy.

Although all of Equifax's board members had considerable experience in areas such as executive leadership and strategy development, **only two of the 10 had any expertise in cybersecurity**, according to company reports. (We found this to be a common element at the top of most of the organizations we studied.)

It is fine for management to have a "risk appetite," but when it comes to cybersecurity, the risk potential must be consciously and realistically evaluated. Most attacks that we studied stemmed from decisions made without any explicit consideration of risk. **The connections between decisions that might seem minor and the significant consequences those decisions can invite are rarely considered.**

While some risks are true surprises unlikely to be recognized in advance, many are more like the burglar alarm known to be defective. Indeed, in almost every case that we studied there were **red flags — often many of them — that management chose to ignore,** with disastrous consequences.

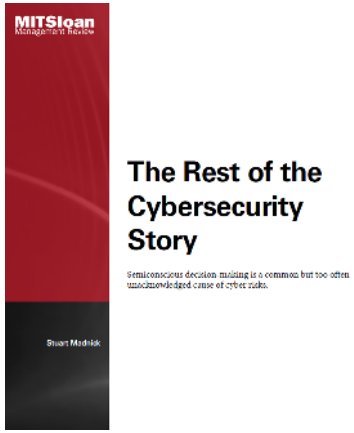
The Rest of the Cybersecurity Story

Semiconscious decision-making is a common but too often unacknowledged cause of cyber risks.

Cause of Cyber risks?

What to do

- **Management at every level must gain knowledge about how cyber risks arise and hone their skills in assessing the potential consequences of breaches**. Reading detailed analyses of past cyberattacks, such as those at Equifax and Capital One, and participating in tabletop exercises and cyber fire drills, are a couple of ways to accomplish this.
- When managers at all levels are developing plans to improve revenues or reduce costs, they **must consciously and deliberately assess the potential cyber risk of the planned changes — and then, only if the risk is acceptable, proceed.** Taking these steps can dramatically reduce the number of cyberattacks your company faces while minimizing the impact of any attacks that do successfully breach your systems.



Learning points

- Identify key Controls
- Risk versus cost
- Risk management process
- Who is involved make these “risk” decisions
- Politics
- Exception management
- Measurements and metrics

How Digitally Savvy Top Teams Drive Performance

		Top 25% of Savvy Top Management Teams	Bottom 25% of Savvy Top Management Teams
RESULTS	**Innovation** (% of revenues from new offerings in the past three years)	59%	18%
	% of revenues from **cross-selling**	53%	15%
	% complete on **transformation**	69%	30%
PRACTICES	**Rapid learning** (for example, test and learn, minimum viable products, sharing lessons, evidence-based decisions)	80%	25%
	Modular, open and agile	80%	33%
	Automated decision-making	80%	35%
LEADERSHIP	Moving from **command-and-control** to a **coach-and-communicate** orientation	83%	28%
	Creating a **digital culture**	85%	30%
	Holding people **accountable**	85%	41%
	Encouraging **innovation**	85%	30%

Does your C-suite have enough digital smarts? – **MIT Sloan Management Review**: Magazine: Spring 2021 Issue Research Highlight

Make Cybersecurity a Strategic Asset

The study found that the biggest mistake by executive management were:

- to not treat cybersecurity as an operational issue
- cyber-attacks cannot be prevented but most be prepared for
- the impact of an cyber-attack is not limited to IT but affects the whole business.

What these executives came to understand is that organizational resilience to cyberattacks require a fundamental change of mindset. Although executives acknowledge cybersecurity as important part of IT planning, the misunderstood the strategic character of cyberattacks both as a severe threat to earnings and operations and as an **opportunity**.

- What is the opportunity? A mature cyber strategy provides a basis for security of critical assets, business processes, enhancing organizational learning and noticing and capturing **new** strategic opportunities. Among the companies researched some found that it **paved the way to a fully digital business model** or help them to **establish a new value proposition around security (confidentiality, availability, integrity) for customers**.


MITSloan Management Review

MAGAZINE FALL 2020 ISSUE · RESEARCH FEATURE

Make Cybersecurity a Strategic Asset

By elevating cybersecurity from an operational necessity to a source of opportunity, leaders can boost resilience and business advantage.

Manuel Hepfer and Thomas C. Powell · September 08, 2020 READING TIME: 14 MIN

Image courtesy of Gary Waters/theispot.com

On June 27, 2017, employees in more than 80 global

Why Do Cybersecurity Efforts Fail?

- Cybersecurity is delegated to IT
- Cybersecurity focused on protection and to a lesser extent to plan cyber responses. In addition, “these investments were largely wasted…”
- Organizations misunderstand the strategic nature of cybersecurity risks because the mischaracterize the threat as a random unpredictable event.
- **Executives assign strategic priorities based on their own areas of expertise (finance, engineering, marketing, etc.)**
- **Cybersecurity was treated by management as a tick-the-box exercise instead of really understanding it.**
- Organizations keep attacks under wraps i.e. best practices for responding to attacks are not shared and executives cannot learn from cyberattacks from other companies.
- **Executives were viewing cybersecurity investments as a lose-lose situation (i.e. investment in this areas would be wasted if no incidents) and as a result under-invested in cybersecurity.**

How Do Organizations Become Strategic?

- Increased the understanding of the strategic value of cybersecurity and strengthening the core strategic capabilities of the organization.
- It showed the organizations areas of strong leadership and weak leadership. I.e. what leaders need better training in handle cyber responses.
- With better understanding of its critical processes the **organization changed from protecting its IT infrastructure to protecting its most critical processes**
- **A strategic understanding of cybersecurity creates the opportunity for closer integration and understanding between business and IT.**
- A more strategic approach lead to a layered approach designed to minimize an organizations consequences of a cyberattack.

Key Actions to Reduce Risk

Leadership

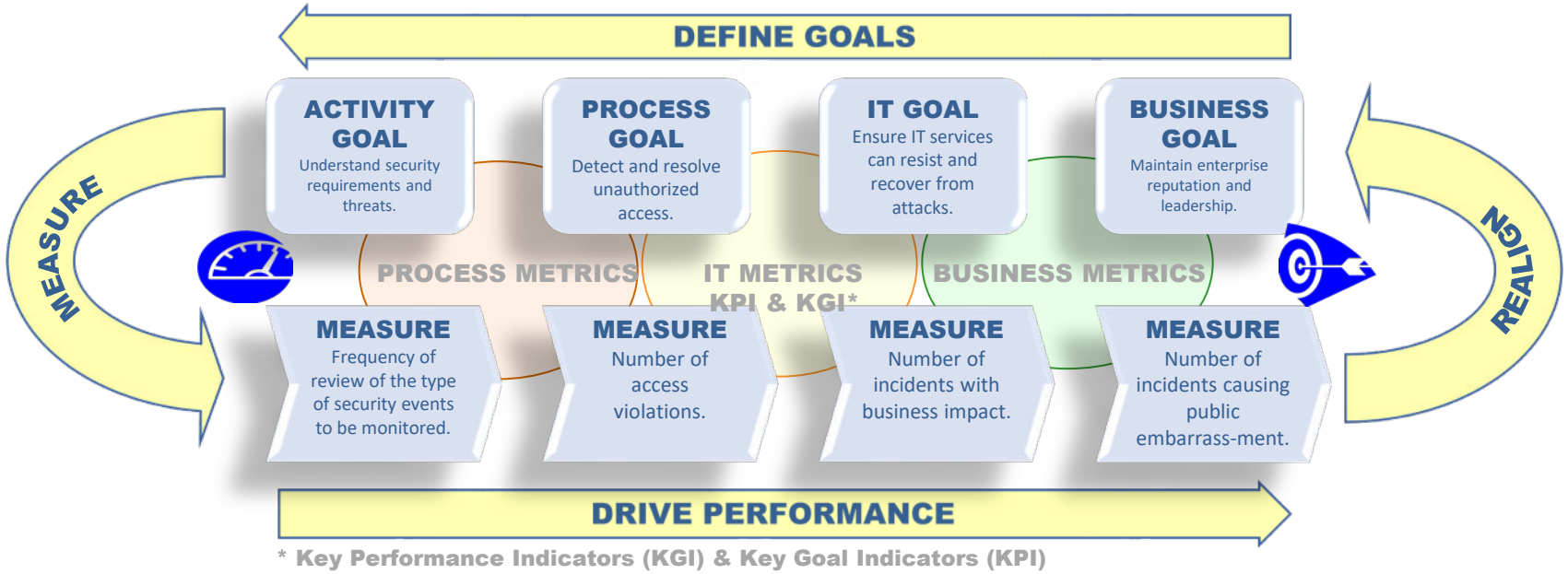
- Governance !!!
- Multidisciplinary Involvement
- Vendor selection and Involvement
- Change management
- Control effectiveness and efficiency

Safety culture and process improvement

- Comprehensive system analysis/risk assessments/failure mode and effects analysis
- Shared involvement and responsibility
- System implementation and upgrades

IT Goals and Metrics (Key Performance Indicators)

You cannot manage what you do not measure!



* Key Performance Indicators (KGI) & Key Goal Indicators (KPI)

Board / Executive IT Risk Dashboard

Capability	Key Risks	Risk Level	Risk Mgm Plan	Regulatory Findings	Trend
IT Risk Management	IT risks are not defined IT risks are not managed to acceptable levels		7	5	▲
Information & Asset Inventory	Processes and procedures for classifying, labelling and handling information and assets are not managed Identification and assignment of ownership for assets containing sensitive information has not been performed.		6	3	▬
Information Protection	Processes for monitoring and tracking sensitive information throughout its lifecycle is not established Failure to restrict collection of personal information for only necessary purposes		~35	~22	▲
Information Security Program Management	The information security program is not aligned with business requirements Policies and procedures have been established for information security		13	13	▬
Identity & Access Management	Privileged access is used to compromise data Terminated user access is not removed appropriately		37	34	▲
Threat & Vulnerability Management	Internal and external vulnerabilities go unmanaged Internal and external security threats go unmanaged		~120	~76	▲
Third Party Security	Security risks are not identified with third parties Security risks are not managed to acceptable levels with third parties		39	39	▬
IT Operations	Information security practices are not integrated into IT operations (change mgm, incident mgmt., etc.) IT operations are not performing their Information security responsibilities		~26	~19	▲
Business Continuity & Disaster recovery	Disaster recovery processes and procedures are not defined Ability to recover from an outage has not been tested		38	34	▬
Physical & Environmental Controls	Physical perimeter controls at IT facilities are not established IT environmental controls (power, temp, etc.) to support IT operations are not sufficient		20	14	▬
Organization Security & Awareness	Users do not perform their security responsibilities Users do not understand their security responsibilities		5	4	▬
IT Compliance Management	Adequate mechanisms to monitor and remediate compliance issues are not implemented Compliance with legislative, regulatory or contractual obligations are not identified		~12	~2	▲

Legend			
Risk Rating		Trend	
	Low	▲	Risk increasing
	Medium	▼	Risk decreasing
	High	▬	No change

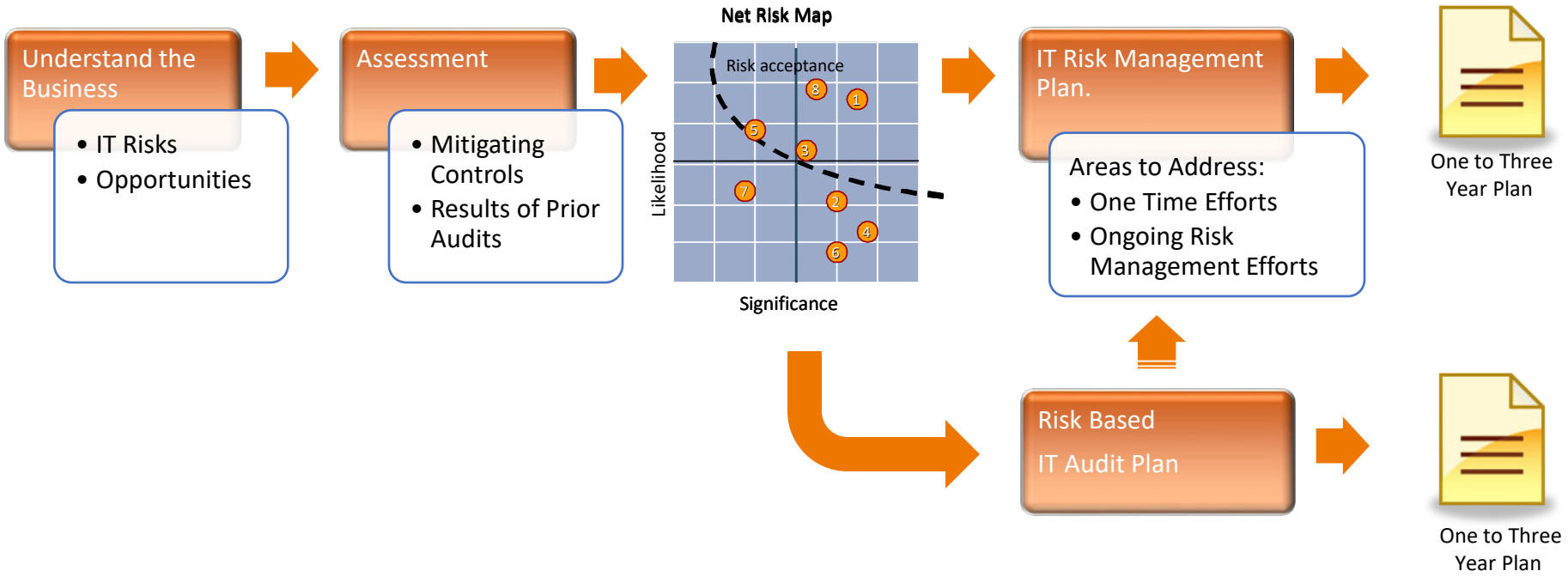
Regular Reporting of Key Measurements towards Metrics

- **Risk Management Program**
  - Status management program – see example previous page – Dash board
  - Number of risk assessments performed – Defined assessments and analysis per IT and organization projects, to include change control.
  - Time to remediate issues – The time between identification and remediation.
- **Vulnerability Management**
  - Issues by Status – When a vulnerability is identified on a system the first time, it is a new data point that should inform and, depending on the situation, drive an action.
  - Remediation Time - Measure the length of time from identification to remediation and is a measure of the efficiency of the patch and remediation cycle.
  - Mean time to Patch – The time between identification of a needed patch and the installation of the required patch.
- **Exceptions**
  - The number of information security and IT policy exceptions requested and granted
- **Incident Management**
  - Number of Events - Events are activities or indicators that warrant further investigation and can be indicators of incidents.
  - Number of Incidents - Incidents occur when a material event or events have occurred and require a formal response activity.
- **Specific Initiatives**
  - Program/projects
- **Cost and Value**
  - IT cost per business areas with trending
  - IT cost per patient with trending
  - Number of systems per business area

Contents

- Introduction
- What is High Value IT Audits
- High Value IT Audits
- Q&A
- Referenced Material

IT Risk Management



IT Related risk = materialised business impact because of IT related event

Risk Management Approach

Identify high risk areas

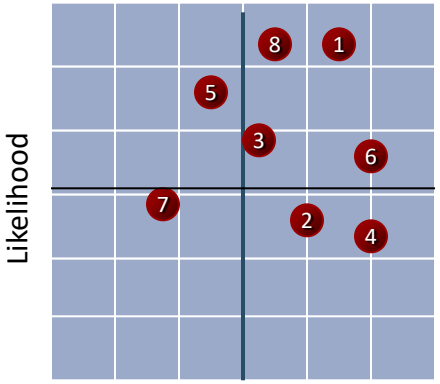
Assess risk management

Risk acceptance – Can management accept the existing risk level?

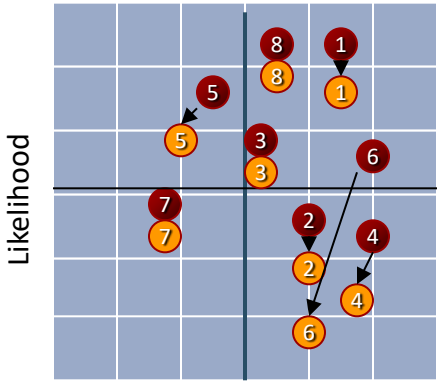
Gross risk

Net risk

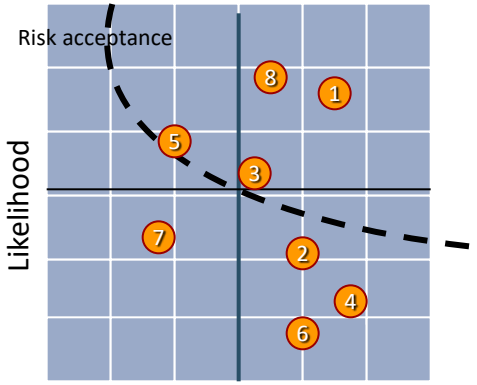
Gross Risk Map



Risk Management



Net Risk Map



Typical Key IT Risks

Risk List	Risk List	Risk List
1. Vendor/Supplier Management	13. Data Warehouse and Other Data Repositories	25. PCI-DSS Compliance
2. Change Management	14. Internal and External Intrusion	26. Problem and Incident Management
3. Identity and Access Management	15. IT Governance / IT Security Governance	27. Resources and IT Skills
4. IT Asset Management	16. Business Continuity (Downtime)	28. Roles and Responsibilities
5. Network Availability	17. Disaster Recovery and Backup Management	29. Facility/Utility Systems
6. Electronic Communication (Email, Texting, Faxing)	18. Disposal of Electronic Media	30. Grants w. IT Security Requirements / Research (CMMC, DFARS, etc.)
7. IT Risk Management	19. Security Incident Management	31. Cybersecurity
8. Medical Devices/Health Technology	20. Information/Data Governance	32. IT Cost
9. Phone Systems	21. Patch management	33. Affiliated Organizations
10. Security Awareness	22. Physical Security, IT Environmental Controls	34. Distributed IT/Shadow IT
11. Internet Usage and Social Media	23. End-User Devices (Workstations, Tablets, Laptops, USBs, Smart phones, etc.)	35. Privacy/GDPR/State Privacy, etc.
12. Audit Trail and Logs	24. IoT	36. Cloud Management

2025 EDUCAUSE Top 10 ~~10~~ 11 Restoring Trust

Educause 2025 Top Ten (11)

- **#1. *The Data-Empowered Institution:*** Using data, analytics, and AI to increase student success, win the enrollment race, increase research funding, and reduce inefficiencies
- **#2. *Administrative Simplification:*** Streamlining and modernizing processes, data, and technologies
- **#3. *Smoothing the Student Journey:*** Using technology and data to improve and personalize student services
- **#4. *A Matter of Trust:*** Advancing institutional strategies to safeguard privacy and secure institutional data
- **#5. *The CIO Challenge:*** Leading digital strategy and operations in an era of frequent leadership transitions, resource limitations, societal unrest, and rapid technology advancements
- **#6. *Institutional Resilience:*** Contributing to institutional efforts to prepare for and address a growing number and range of risks
- **#7. *Faster, Better, AND Cheaper:*** Using technology to personalize services, automate work, and increase agility
- **#8. *Putting People First:*** Helping staff adapt, upskill, and thrive in an era of rapid change and ongoing digital advancements
- **#9. *Taming the Digital Jungle:*** Updating and unifying digital infrastructure and governance to increase institutional efficiency and effectiveness
- **#10. (tie) *Building Bridges, Not Walls:*** Increasing digital access for students while also safeguarding their privacy and data protection
- **#10. (tie) *Supportable, Sustainable, and Affordable:*** Developing an institutional strategy for new technology investments, pilots, policies, and uses

Where is the AI Issue?

AI was embedded in more than half of the 2025 Top 10 issues

- *The Ethics of AI (#11):* Ensuring that implementations and uses of AI are equitable and inclusive
- *AI Goes to School(#14):* Tailoring AI models and tools to support student learning and advising

See the AI Table type of institution.

AI per Type of Institution

Institution Type	In Their Top 10
Public Doctoral, 15,000+ FTEs	•The Ethics of AI: Ensuring that implementations and uses of AI are equitable and inclusive •Digital Differentiation: Investing in digital infrastructure, services, and support to reinforce educational and research priorities and gain a competitive advantage
Private Doctoral, 15,000+ FTEs	•The Ethics of AI: Ensuring that implementations and uses of AI are equitable and inclusive
Public Doctoral, 8,000–14,999 FTEs	•The Ethics of AI: Ensuring that implementations and uses of AI are equitable and inclusive •The Flexible Campus: Managing virtual and physical spaces to sustainably optimize work and learning •Digital Differentiation: Investing in digital infrastructure, services, and support to reinforce educational and research priorities and gain a competitive advantage

The Competent Institution

Competence is an essential component of trust. People trust organizations and people who honor commitments and produce quality results.

- **#2. *Administrative Simplification***
  Streamlining and modernizing processes, data, and technologies
- **#7. *Faster, Better, AND Cheaper***
  Using technology to personalize services, automate work, and increase agility
- **#9. *Taming the Digital Jungle***
  Updating and unifying digital infrastructure and governance to increase institutional efficiency and effectiveness
- **#10. (tie) *Supportable, Sustainable, and Affordable***
  Developing an institutional strategy for new technology investments, pilots, policies, and uses

The Caring Institution

Trust in institutions stems from trust in the people at the institution, and that trust needs to be earned.

- **#3. *Smoothing the Student Journey***
  Using technology and data to improve and personalize student services
- **#4. *A Matter of Trust***
  Advancing institutional strategies to safeguard privacy and secure institutional data
- **#8. *Putting People First***
  Helping staff adapt, upskill, and thrive in an era of rapid change and ongoing digital advancements
- **#10. (tie) *Building Bridges, Not Walls***
  Increasing digital access for students while also safeguarding their privacy and data protection

The Fulcrum of Leadership

Building an institution that is both competent and caring is a balancing act. This is the challenge of leadership: to balance competence and caring and to recognize that the best outcome for the institution is to maintain that balance.

- **#1. *The Data-Empowered Institution***
  Using data, analytics, and AI to increase student success, win the enrollment race, increase research funding, and reduce inefficiencies
- **#5. *The CIO Challenge***
  Leading digital strategy and operations in an era of frequent leadership transitions, resource limitations, societal unrest, and rapid technology advancements
- **#6. *Institutional Resilience***
  Contributing to institutional efforts to prepare for and address a growing number and range of risks

THE COMPETENT INSTITUTION

2. Administrative Simplification
7. Faster, Better, AND Cheaper
9. Taming the Digital Jungle
10. Supportable, Sustainable, and Affordable (tie)

THE CARING INSTITUTION

3. Smoothing the Student Journey
4. A Matter of Trust
8. Putting People First
10. Building Bridges, Not Walls (tie)

THE FULCRUM OF LEADERSHIP

1. The Data-Empowered Institution
5. The CIO Challenge
6. Institutional Resilience

The 2026 EDUCAUSE Top 10

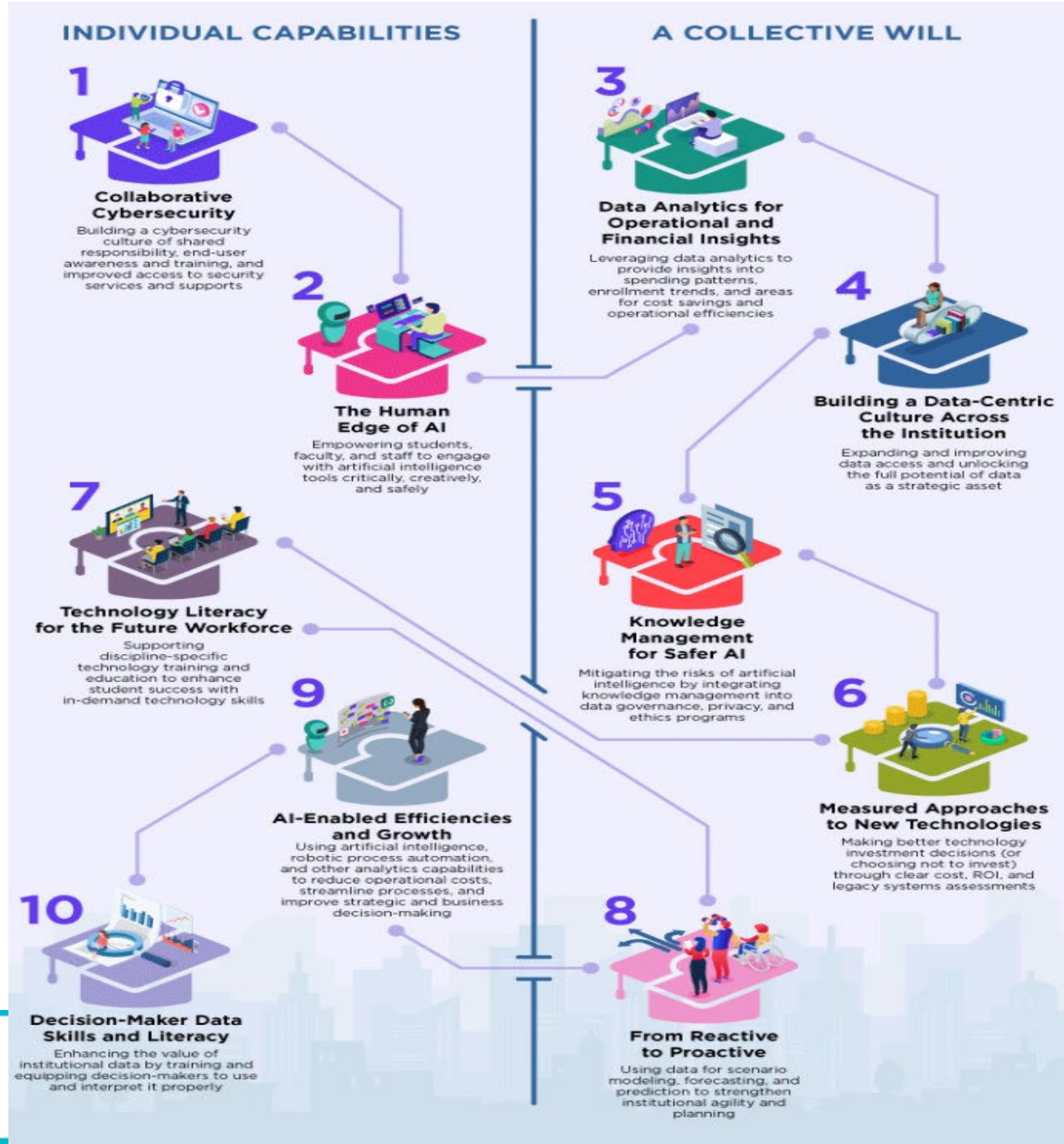
The 2026 EDUCAUSE Top 10 highlights how higher education technology and data leaders can foster a ***collective will*** and support ***individual capabilities***—two deeply connected actions that will help institutions thrive in the year ahead.

Educause 2026 Top Ten

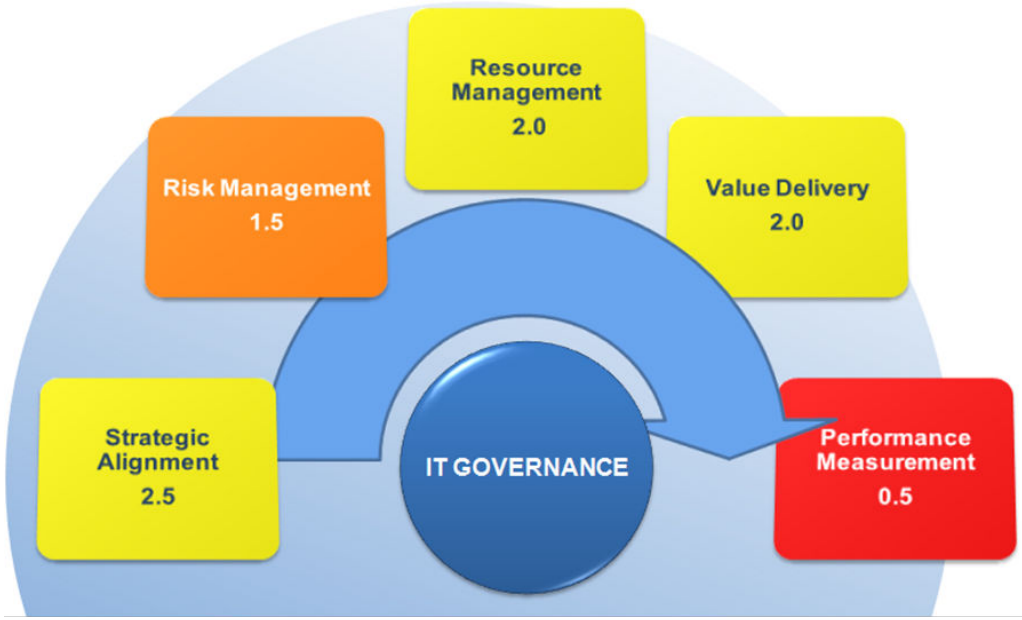
- **#1. *Collaborative Cybersecurity:*** Building a cybersecurity culture of shared responsibility, end-user awareness and training, and improved access to security services and supports
- **#2. *The Human Edge of AI:*** Empowering students, faculty, and staff to engage with artificial intelligence tools critically, creatively, and safely
- **#3. *Data Analytics for Operational and Financial Insights:*** Leveraging data analytics to provide insights into spending patterns, enrollment trends, and areas for cost savings and operational efficiencies
- **#4. *Building a Data-Centric Culture Across the Institution:*** Expanding and improving data access and unlocking the full potential of data as a strategic asset
- **#5. *Knowledge Management for Safer AI:*** Mitigating the risks of artificial intelligence by integrating knowledge management into data governance, privacy, and ethics programs
- **#6. *Measured Approaches to New Technologies:*** Making better technology investment decisions (or choosing not to invest) through clear cost, ROI, and legacy systems assessments
- **#7. *Technology Literacy for the Future Workforce:*** Supporting discipline-specific technology training and education to enhance student success with in-demand technology skills
- **#8. *From Reactive to Proactive:*** Using data for scenario modeling, forecasting, and prediction to strengthen institutional agility and planning
- **#9. *AI-Enabled Efficiencies and Growth:*** Using artificial intelligence, robotic process automation, and other analytics capabilities to reduce operational costs, streamline processes, and improve strategic and business decision-making
- **#10. *Decision-Maker Data Skills and Literacy:*** Enhancing the value of institutional data by training and equipping decision-makers to use and interpret it properly

2026 Top 10

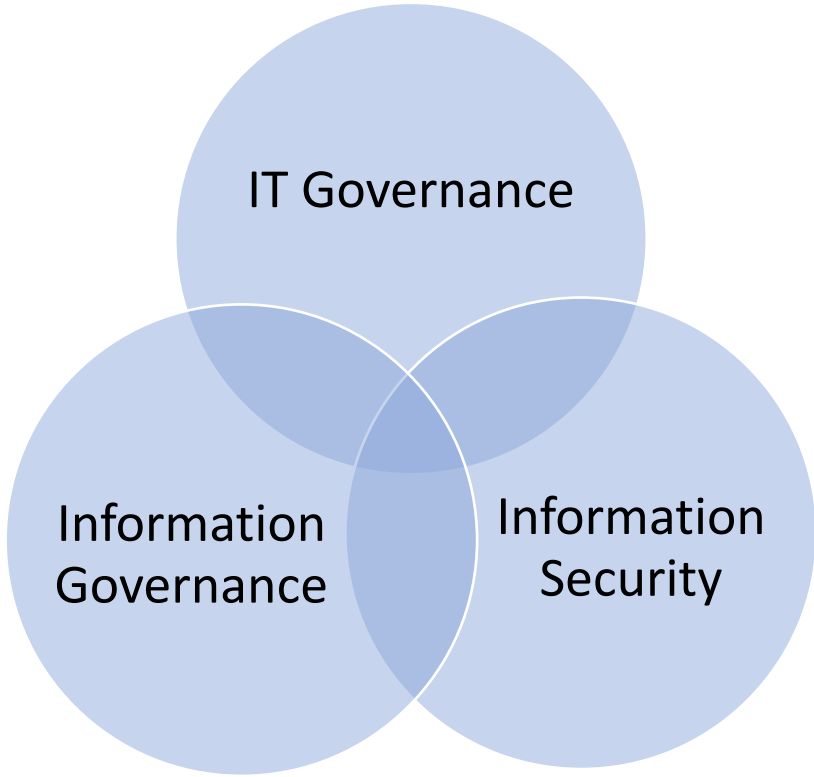
- The integration
- Change, change, change



The Foundational Aspects



Process Maturity Rating	
0	**Non-existent:** The process (control/procedures) does not exist.
1	**Initial/Ad hoc:** The process is informal, undocumented and reactive.
2	**Repeatable:** The process is repeatable but may be applied inconsistently as needed.
3	**Defined:** The process is documented and communicated.
4	**Managed:** The process is implemented and measurable.
5	**Optimizing:** Managed process with continuous performance improvements utilizing best practices.
N/A	**Not Applicable:** The process is not applicable to the review or has not been reviewed for other reasons.



Educause IT GRC Report

EDUCAUSE CENTER FOR ANALYSIS AND RESEARCH

81% of institutions ***do not*** **include IT risk** in their institution's strategic plan

Getting Your Ducks in a Row

IT Governance, Risk, and Compliance Programs in Higher Education

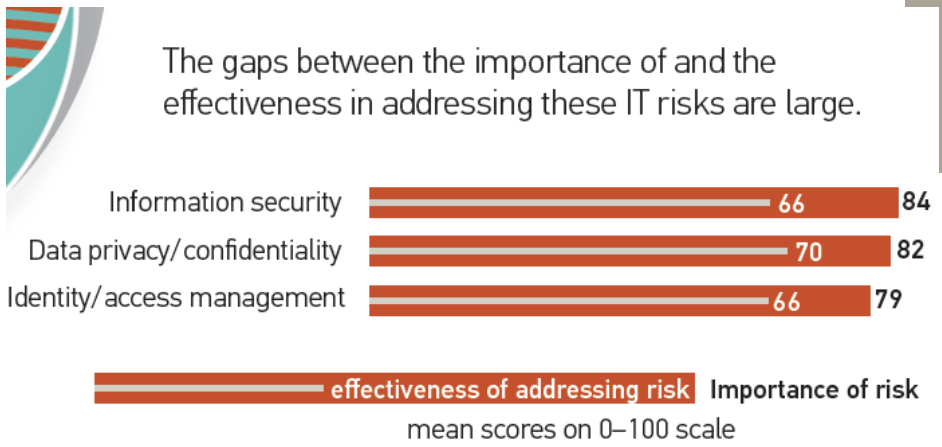
Institutions with formal IT governance bodies

- are more likely to involve others in decision making
- make better investment decisions
- have more support from leadership, faculty, and other stakeholders
- participate more in strategic planning and policy making

When it comes to IT compliance:

2/5 say "We have a process in place for reviewing and updating our IT compliance practices."

1/5 say "We have an adequate budget devoted to IT compliance."



Educause IT GRC Report Conclusion

- **Informal** processes and procedures for **risk management and compliance**
- **Half** of the institutions have a formal IT governance body
- Significant gaps between **perceived importance of the risks** and the **effectiveness** with which they are being addressed
- **Maturity** in risk management is associated with **stronger governance and compliance efforts and processes**
- Less than 50% report **effective communication** about IT risks to all relevant parties
- Institutions with IT Governance body in place are more likely **to involve others** (faculty, students, alumni) in both IT budgeting and other governance decisions.
- **Investment in risk management is associated with more progressive GRC efforts.**
- Only 1 in 10 institutions has an adequate budget devoted to IT risk management.

Root Causes and Key Controls/Programs

- Root causes
- Programs
  - Asset management
  - IAM/PAM
  - BCP/DRP/Resilience
  - Vulnerability Management
  - Incident Management
  - Information Security Program
- Risk Assessment integration
- IT Strategy
- Measurements/Metrics

Most Common IT Audit Areas

- Network Security/Cybersecurity
- Penetration testing
- Identity and Access Management
- ERP Core System
- IT General Controls
- HIPAA/FERPA
- Financial Systems
- Vendor Management/supply chain/TPRM
- Asset Management
- AI
- Business Continuity/Emergency Management and Disaster Recovery
- PCI
- Mobile Device Management
- Patch/Vulnerability Management
- New Systems
- Privacy
- Cloud Management
- Active Directory
- Information Security Program

Additional Key Risks to Audit

- Incident management (Operation, IT, Information Security, Security, Facility, Biomed, Supply Chain)
- Change Management
- Data Warehouse
- Information/Data Governance
- IT Governance
- Student/Patient Communication/Portal
- Backup Management
- Security Awareness and Cyber Training
- Departmental IT/”Shadow IT”

Added Value Audits – Hidden Opportunities

- Life Cycle Management
  - Application/Tool functionality
  - Inventories
  - Cost
  - Age
  - Utilization, ownership
  - Budget/capacity/acquisition processes
  - IT Strategy
- Cloud Management
  - Risk Management
  - Business Case
  - Cost/Maintenance
- Identity and Access Management Program
  - Number of systems
  - Authentication
  - Resources for management of access management (FTE/cost)
- IT Value/IT Cost
  - You cannot manage what you do not measure!

IT Audit Plan Considerations

- Comprehensive IT Risk Assessment
- Root Cause Analysis
- Build Long Term IT Audit Plan
- IT Governance Audit
- Regular Audit of Key Control Areas
  - Value added internal benchmarks
  - Trends
- Framework Based
  - Standard benchmark
- Pro-Active Audits/Value Added Work
  - Pre-implementation
  - Participation in key committees
- Value – Cost – Investment – i.e. Performance
- Tools – Key Component for Effective and Efficient IT Risk Management – need to assess as part of an audit

Key Audits to Consider

- IT Governance (Strategy, Risk, Objectives and Measurements, Value and Resource Management)
- IT Risk Management and Action Plan
- Resilience (BIA, BCM, DRP, Third Party)
- Active Directory / Administrative Credentials
- Asset Management and Critical Data
- Identity/Access Management
- Penetration Tests/Network Security Assessment
- Measurements/metrics
- AI Governance

<u>Other Considerations</u>

- Review Cyber insurance coverage, questionnaire and link to your audits/findings
- Link audit findings to industry standards requirements
- Expand your Business Stakeholders view in your reporting i.e. patient safety, quality, etc.

Contents

- Introduction
- What is High Value IT Audits
- High Value IT Audits
- Q&A
- Referenced Material

Q & A

Johan Lidros Contact Information

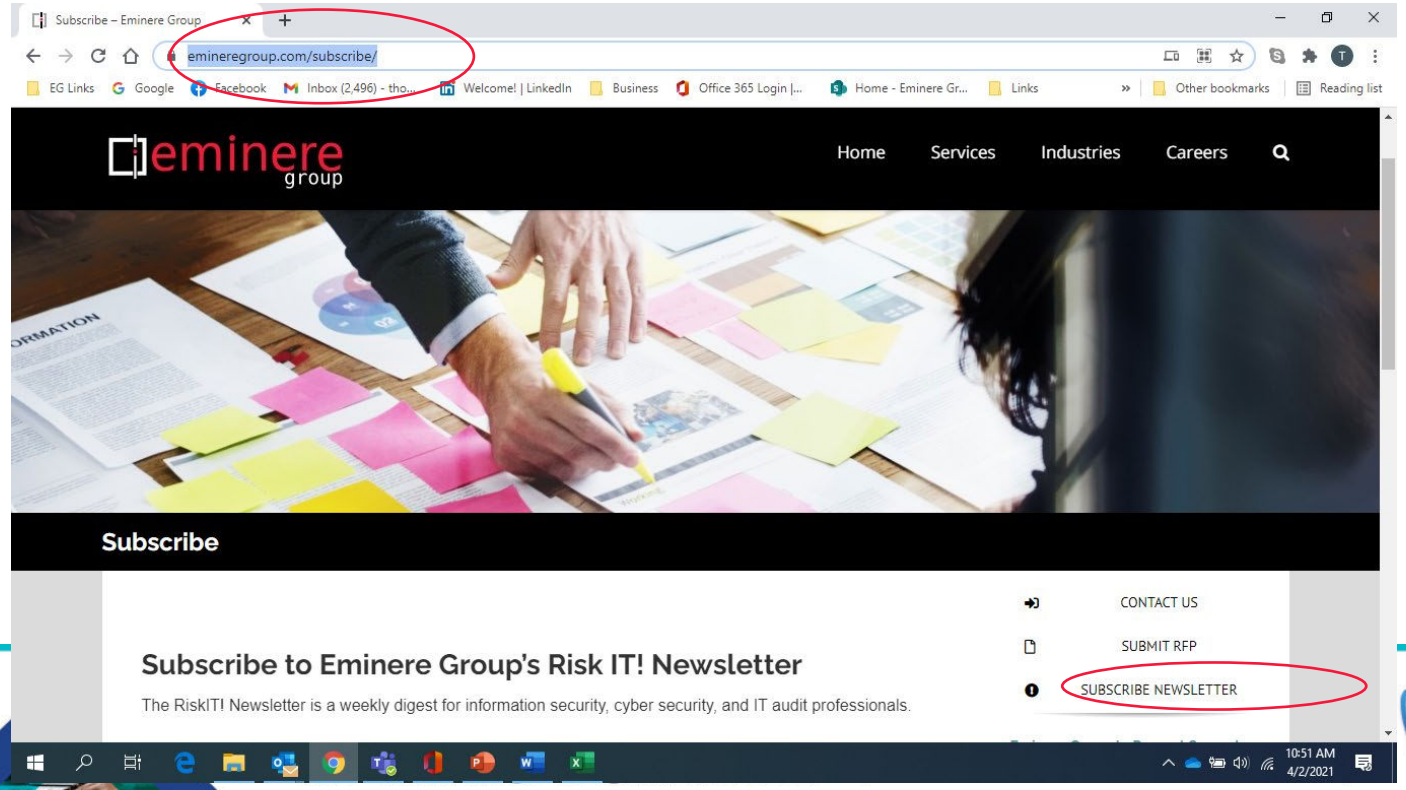
Johan Lidros, President

johan.lidros@emineregroup.com
(813) 832-6672 x-9101
(813) 355-6104 (cell)

Connect on LinkedIn
linkedin.com/in/johanlidros
Or QR-code

Ongoing IT Risk/Cybersecurity Updates

Interested in on-going IT Governance and IT Security updates? Sign up for our weekly newsletter “RiskIT “at https://www.emineregroup.com/subscribe/ or Linkedin Eminere Group Risk IT Newsletter



Contents

- Introduction
- What is High Value IT Audits
- High Value IT Audits
- Q&A
- Referenced Material

News on Standards

- Proposed HIPAA Security Rule – December 2024
- NIST Cybersecurity Framework (CSF) 2.0
- NIST SP 1326 - NIST SP 1326 (Initial Public Draft) NIST Cybersecurity Supply Chain Risk Management: Due Diligence Assessment Quick-Start Guide
- Health Data, Technology, and Interoperability: Certification Program Updates, Algorithm Transparency, and Information Sharing (HTI-1) Final Rule https://www.federalregister.gov/public-inspection/2023-28857/health-data-technology-and-interoperability-certification-program-updates-algorithm-transparency-and
- Health Industry Cybersecurity Practices (HICP) 2023 version https://405d.hhs.gov/information
- NIST Special Publication 800-66r2 Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule Cybersecurity Resource Guide
- NIST 800-55 Measurement Guide for Information Security
- IIA – Update to Internal Audit Standard and the Topical Requirement Cybersecurity, Culture, Third parties
- SAFER Guides - https://www.healthit.gov/topic/safety/safer-guides
- Joint Commission Cybersecurity Risk Assessment, Emergency Management Checklists.
- NIST Special Publication 800-221A Information and Communications Technology (ICT) Risk Outcomes: Integrating ICT Risk Management Programs with the Enterprise Risk Portfolio
- Center for Internet Security https://www.cisecurity.org/controls - Key Controls and Benchmarks
- US Department of Justice – Evaluation of Corporate Compliance Programs (including social media/BYOD)
- Core Cybersecurity Feature Baseline 2 for Securable IoT Devices – NIST 8529
- Cloud Security Alliance – Cloud Security Control Matrix 4.0
- StateRAMP, TX-RAMP
- CMMC updates

News on Standards/Frameworks –AI only

- NIST's AI Risk Management Framework (AI RMF 1 .0)
  - **Alignment with international standards and production crosswalks to related standards**. (e.g., ISO/IEC 5338, ISO/IEC 38507, ISO/IEC 22989, ISO/IEC 24028, ISO/IEC DIS 42001, and ISO/IEC NP 42005.)
- HAIP – Health AI Partnership (guidelines)
- HHS Strategic Plan for the Use of AI in Health, Human Services, and Public Health
- ISACA – Auditing Artificial Intelligence
- IIA
  - Artificial Intelligence Auditing Framework
  - Update to Internal Audit Standard and the Topical Requirement Cybersecurity
- MITRE ATLAS Framework - Adversarial Threat Landscape for Artificial Intelligence Systems
- The CISCO Responsible AI Framework
- Department of Energy's AI Risk Management Playbook (AI RMP)
- SAFER Guides (includes AI aspects)
- Australian Digital Transformation Agency (DTA) guidance for implementing AI *Technical Standard for Government's Use of Artificial Intelligence* (TSGUAI)
- ISO 42001 AI Management Systems, 23894 AI risk management, 38507 AI Governance, 25059 AI Quality management and evaluations
- …

Resources

- Committee of Sponsoring Organizations (COSO)
  - ERM - *Enterprise Risk Management—Integrated Framework* https://www.coso.org/_files/ugd/3059fc_61ea5985b03c4293960642fdce408eaa.pdf
  - COSO INTERNAL CONTROL – INTEGRATED FRAMEWORK: An Implementation Guide for the Healthcare Provider Industry https://www.coso.org/_files/ugd/3059fc_b5232f85f48848a295cc6c168de82006.pdf
  - RISK APPETITE – CRITICAL TO SUCCESS - USING RISK APPETITE TO THRIVE IN A CHANGING WORLD https://www.coso.org/_files/ugd/3059fc_c23aec8adbbd4b2abb4ebee9a8929370.pdf
  - ENABLING ORGANIZATIONAL AGILITY IN AN AGE OF SPEED AND DISRUPTION https://www.coso.org/_files/ugd/3059fc_cef1343e024a43c0b65d23ad0178d41e.pdf
- Center for Internet Security (CIS)
  - Key Security Controls and Benchmark (old SANS 20 expanded with technical security baselines) https://www.cisecurity.org/controls.
  - How to Construct a Sustainable GRC Program in 8 Steps
- Cybersecurity and Infrastructure Security Agency (CISA)
  - Cybersecurity and Infrastructure Security Agency (CISA) CPGs. See https://www.cisa.gov/sites/default/files/2023-03/CISA_CPG_REPORT_v1.0.1_FINAL.pdf and https://www.cisa.gov/sites/default/files/2023-03/20230320-CSF-aligned-Consolidated-Component-Listing.xlsx
  - Free Vulnerability Assessment https://www.cisa.gov/sites/default/files/publications/VM_Assessments_Fact_Sheet_RVA_508C.pdf
- Health-ISA

  Current and Emerging Healthcare Cyber Threat Landscape This report is a collaboration between and Booz Allen Hamilton Cyber Threat Intelligence (CTI). https://h-isac.org/health-isac-report-explores-current-and-emerging-cyber-threats-to-the-healthcare-sector/
- Health Sector Coordinating Council (HSCC)
  - HSCC-HEALTH-INDUSTRY-CYBERSECURITY-STRATEGIC-PLAN-OVERVIEW https://h-isac.org/health-isac-supports-health-industry-cybersecurity-strategic-plan/#:~:text=The%20Health%20Industry%20Cybersecurity%20Strategic%20Plan%20is%20a%20call%20to,over%20the%20next%20five%20years.
  - Coordinated Privacy and Security Partnership https://healthsectorcouncil.org/privacy-security-coordination/
  - Supply Chain Risk Management Guide v2.0

Resources (continued)

- HHS
  - Cybersecurity Performance Goals https://hphcyber.hhs.gov/performance-goals.html
  - Health Care Sector Cybersecurity Strategy https://aspr.hhs.gov/cyber/Documents/Health-Care-Sector-Cybersecurity-Dec2023-508.pdf
  - HPH Sector Cybersecurity Framework Implementation Guide https://aspr.hhs.gov/cip/hph-cybersecurity-framework-implementation-guide/Pages/default.aspx
  - HHS Strategic Plan for the Use of Artificial Intelligence in Health, Human Services, and Public Health
- HHS/OCR
  - Use of Online Tracking technologies by HIPAA Covered Entities and Business associate https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html
  - HIPAA Audit Program (Privacy, Breach and Security)
- HITRUST
  - AICPA Trust Principles and Criteria for security, confidentiality and availability
  - NIST CSF
  - Center for Internet Security Critical Security Controls (CIS CSC)
  - Cybersecurity guidance from the President's Precision Medicine Initiative (PMI)
  - OCR Audit Protocol v2
  - HICP
  - FEDRAMP Support for Cloud and IaaS Service Providers
  - FFIEC IT Examination Handbook for Information Security.

Resources (continued)

- Health Industry Cybersecurity Practices (HICP) https://405d.hhs.gov/information
  - Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients
  - Managing Threats and Protecting Patients
  - Cybersecurity Practices for Small Health Care Organizations
  - Cybersecurity Practices for Medium and Large Health Care Organizations
  - Hospital Cyber Resilience Initiative – Landscape Analysis
- IIA
  - THE IIA'S Artificial Intelligence Auditing Framework https://www.theiia.org/en/content/tools/professional/2023/the-iias-updated-ai-auditing-framework/
  - The IIA's Practice Guides and Global Technology Audit Guides (GTAGs)
  - ChatGPT for Internal Auditors
  - Topical Requirement Cybersecurity https://www.theiia.org/globalassets/site/standards/topical-requirements/cybersecurity/cybersecurity_topical_requirement.pdf
  - Internal Auditing Competency Framework™ Global Practice Guide https://www.theiia.org/en/resources/internal-audit-competency-framework/
- ISACA www.isaca.org
  - COBIT – Leading IT Governance Framework
  - Risk IT Framework ISACA, Risk IT Framework, 2nd Edition, 2020, USA, www.isaca.org/bookstore/bookstore-risk-digital/ritf2
  - Getting Started with Risk Management https://www.isaca.org/bookstore/bookstore-wht_papers-digital/whpgsr
  - IT – Risk Toolset https://store.isaca.org/s/#/store/browse/detail/a2S4w000005EgZbEAK
  - Auditing Artificial Intelligence https://transformingaudit.isaca.org/featured-articles/auditing-artificial-intelligence

Resources (continued)

- Joint Commission.
  - Joint Commission Leadership standard https://www.jointcommission.org/en-us/standards
  - The Big Book of Checklists 2023
    - Cybersecurity Risk Assessment Checklist
    - New Emergency Management Standards for Hospitals Compliance Checklist
- MIT Sloan Management Review
  - Make Cybersecurity a Strategic Asset - MIT Sloan Management Review: Magazine: https://sloanreview.mit.edu/article/make-cybersecurity-a-strategic-asset/
  - AI Risk Repository https://airisk.mit.edu/
- NACD – National Association of Corporate Directors
  - 2023 Cyber Risk Oversight https://www.nacdonline.org/insights/publications.cfm?ItemNumber=74777

  (NACD nonmembers can access this publication by creating a guest account)
  - Principles for Board Governance of Cyber Risk (NACD and World Economic Forum) Principles for Board Governance of Cyber Risk | World Economic Forum (weforum.org)
  - Special Supplement to the NACD-ISA Director's Handbook on Cyber-Risk Oversight https://www.nacdonline.org/globalassets/public-pdfs/nacd_ai-cybersecurity-handbook.pdf
- The National Security Agency (NSA) and the Cybersecurity Infrastructure Security Agency (CISA)
  - Identity and Access Management – Recommended Best Practices for Administrators https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3336001/esf-partners-nsa-and-cisa-release-identity-and-access-management-recommended-be/

Resources (continued)

- NIST
  - Cybersecurity Framework - Framework for Improving Critical Infrastructure Cybersecurity 2.0 https://www.nist.gov/document/csf-20-concept-paper
  - NIST 800-55 Measurement Guide for Information Security
  - NIST 800-66r2 Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule https://csrc.nist.gov/pubs/sp/800/66/r2/final
  - NIST's AI Risk Management Framework (AI RMF 1 .0)
  - Cybersecurity Resource Center https://csrc.nist.gov/
  - Guide for Cybersecurity Incident Recovery NIST Special Publication 800-61, Revision 2, Computer Security Incident Handling Guide https://doi.org/10.6028/NIST.SP.800-61r2
  - NIST IR 8286C Staging Cybersecurity Risks for Enterprise Risk Management and Governance Oversight
  - NIST.IR.8286D-upd1 Using Business Impact Analysis to Inform Risk Prioritization and Response.
  - NIST IR 8286B-upd1 Prioritizing Cybersecurity Risk for Enterprise Risk Management
  - NIST Privacy Framework – Updated Draft
- Assistant Secretary for Technology Policy (ASTP) ONC – Health IT
  - Health IT Playbook - https://www.healthit.gov/playbook/
  - SAFER Guides - https://www.healthit.gov/topic/safety/safer-guides
  - How to Identify and Address Unsafe Conditions Associated with Health IT
  - The Role of Health IT Developers in Improving Patient Safety in High Reliability Organizations

Resources (continued)

- ONC and OCR Office of Civil Rights (OCR)/HHS
  - Security Risk Assessment – Small and Medium Entities https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool

- Secure Controls Framework SCF
  - Cybersecurity & data privacy controls," where there is a selection of 1,000+ controls linked to over 100 statutory, regulatory and contractual frameworks https://securecontrolsframework.com/
- World Economic Forum
  - The Global Risk Report 2025 https://reports.weforum.org/docs/WEF_Global_Risks_Report_2025.pdf

Polling Question #1

What is your organization's top IT Risk Challenge? Select your top 3.

A. Privacy – HIPAA, GDPR, CCPA – California Consumer Privacy Act
B. IT Governance
C. Cyber Risk/Network Security
D. Medical Devices Management / IOT
E. Business Continuity / Disaster Recovery
F. Vendor Management/Supply Chain
G. Silos of Risk Management (structure of roles and accountability)
H. AI
I. IT Cost
J. Legacy IT Debt
K. Resources (tools/skilled personnel)
L. Others

Polling Question #2: Root Causes

Which are the most important root causes that apply to your organization? Select up to 3.

1. IT Governance
2. Risk Management Process (Risk Appetite, Exception to the Policies, integration…)
3. Board and Executive Management Skill Set (Tone at the Top)
4. Weak Foundational IT Processes (Asset mgmt, Change mgmt, Access mgmt,…)
5. Measurements/Metrics Matrix (Objectives, KPIs)
6. Resources (Tools, People, Skills)
7. Culture
8. Supply Chain
9. Technology Debt
10. Cybersecurity program

Polling Question #3

What is your most critical System?

A. ERP (Banner, Peoplesoft, Workday)
B. Data Warehouse
C. Backup utility
D. Password/Encryption key vault
E. Active Directory
F. Online Banking
G. “Asset” Inventory(ies) (data, software, hardware, interfaces, etc.)

Polling Question #4

Has Executive Management and or Board established and implemented **comprehensive** IT governance and risk measurements and metrics?

a. Yes
b. Partly, only a limited number of measurement/metrics
c. No
d. Do not know

Polling Question: #5 Audits

Which of the following audits have you performed in the last 3 years? Pick up to 3.

1. IT Governance (Strategy, Objectives and Measurements, Value and Resource Management)
2. IT Risk Management and Action Plan
3. Resilience (BIA, BCM, DRP, Third Party, cyber)
4. Active Directory / Administrative Credential/governance
5. Asset Management and Critical Data
6. Network security / Penetration Tests
7. AI Governance
8. Information Security Program
9. Identity-Access Management Program
10. PCI
11. Review the Cyber insurance questionnaire and coverage
12. Application Reviews
13. None
14. Do not know