AuditCon

by ACUA

Louisville Kentucky | September 14-18, 2025

ACUA

IT AUDIT ROUNDTABLE

Facilitator: Johan Lidros
CISA, CISM, CGEIT, CRISC, HITRUST CCSFP, CDPSE, ITIL-F
President Eminere Group

Date: Tuesday, September 16, 2025

Start time: 11:05:00 AM

End time: 12:20:00 PM

Contents

- Introduction
- Discussion and Knowledge Sharing
- Referenced Material

Presenter/Facilitator

Johan Lidros, Founder and President of Eminere Group

- Over 30 years of experience providing information technology audit, security, privacy, compliance and IT governance services in for many healthcare and higher education institutions. Johan has worked with more than 100 universities in the US and northern Europe.
- Well-versed in accepted IT and information security standards/frameworks (ISO27000, HITRUST, NIST, COBIT, CIS, TIR, DRII, etc.) and has participated in several related committees.
- Certifications: CISA, CISM, CGEIT, CDPSE, ITIL-F, CRISC, HITRUST CCSFP
- ISACA certified instructor CISA, CISM, CRISC, CGEIT

DX AUDIT ROUNDTABLE

Facilitator: Johan Lidros
CISA, CISM, CGEIT, CRISC, HITRUST CCSFP, CDPSE, ITIL-F
President Eminere Group

RESILIENCE AUDIT ROUNDTABLE - 2024

Facilitator: Johan Lidros
CISA, CISM, CGEIT, CRISC, HITRUST CCSFP, CDPSE, ITIL-F
President Eminere Group

2024 Educause Top 10

- ***#1. Cybersecurity as a Core Competency:*** Balancing cost and risk
- ***#2. Driving to Better Decisions:*** Improving data quality and governance
- ***#3. The Enrollment Crisis:*** Harnessing data to empower decision-makers
- ***#4. Diving Deep into Data:*** Leveraging analytics for actionable insights to improve learning and student success
- ***#5. Administrative Cost Reduction:*** Streamlining processes, data, and technologies
- ***#6. Meeting Students Where They Are:*** Providing universal access to institutional services
- ***#7. Hiring Resilience:*** Recruiting and retaining IT talent under adverse circumstances
- ***#8. Financial Keys to the Future:*** Using technology and data to help make tough choices
- ***#9. Balancing Budgets:*** Taking control of IT cost and vendor management
- ***#10. Adapting to the Future:*** Cultivating institutional agility
- Honory Issue: AI .... Friend or Foe **Go deeper…** **https://er.educause.edu/articles/2023/10/2024-educause-top-10-honorary-issue-ai-friend-or-foe**

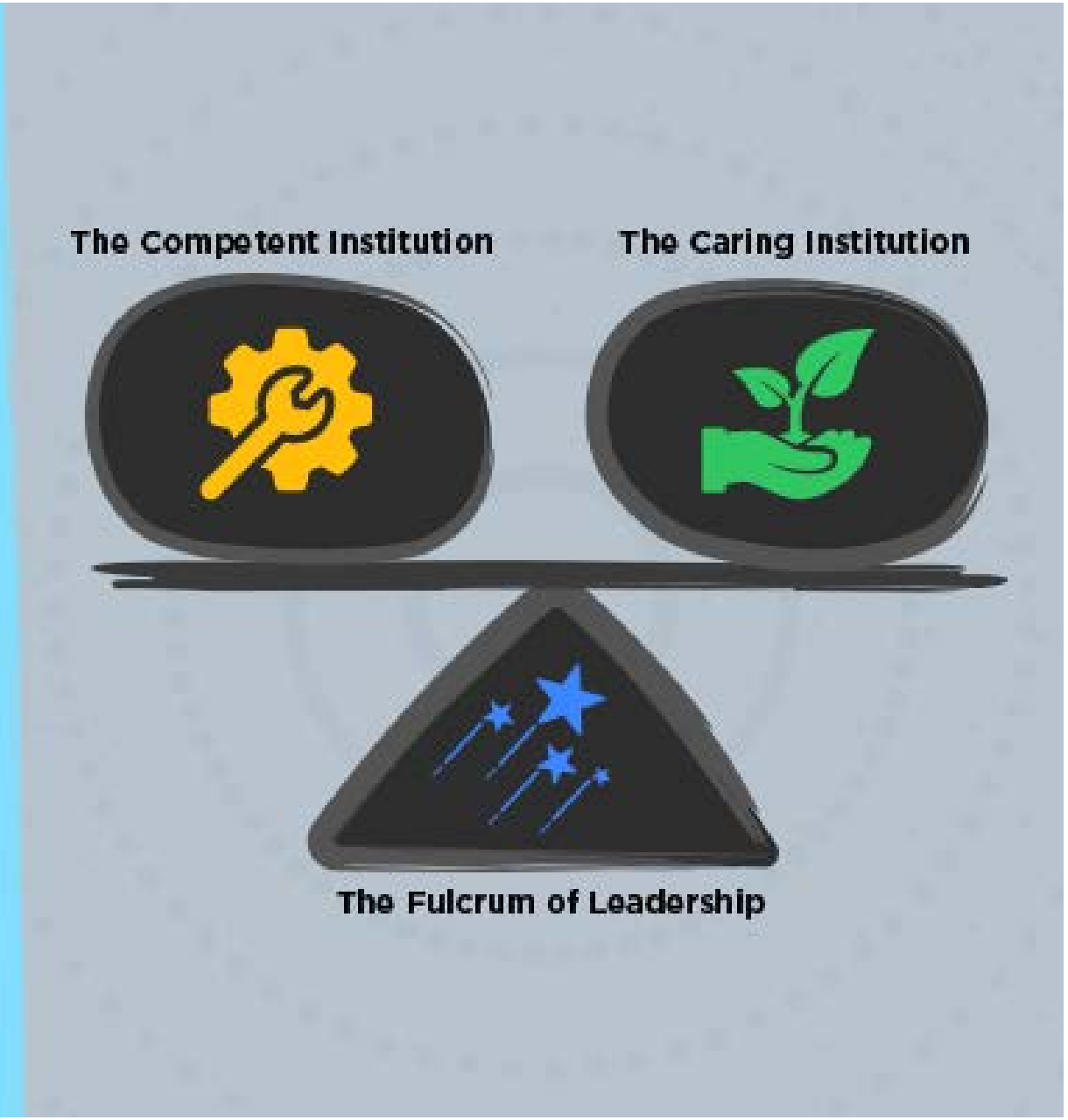
Educause Top Ten 2024 - Resilience

RESTORING TRUST AUDIT ROUNDTABLE - 2025

Facilitator: Johan Lidros
CISA, CISM, CGEIT, CRISC, HITRUST CCSFP, CDPSE, ITIL-F
President Eminere Group

2025 EDUCAUSE Top 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)

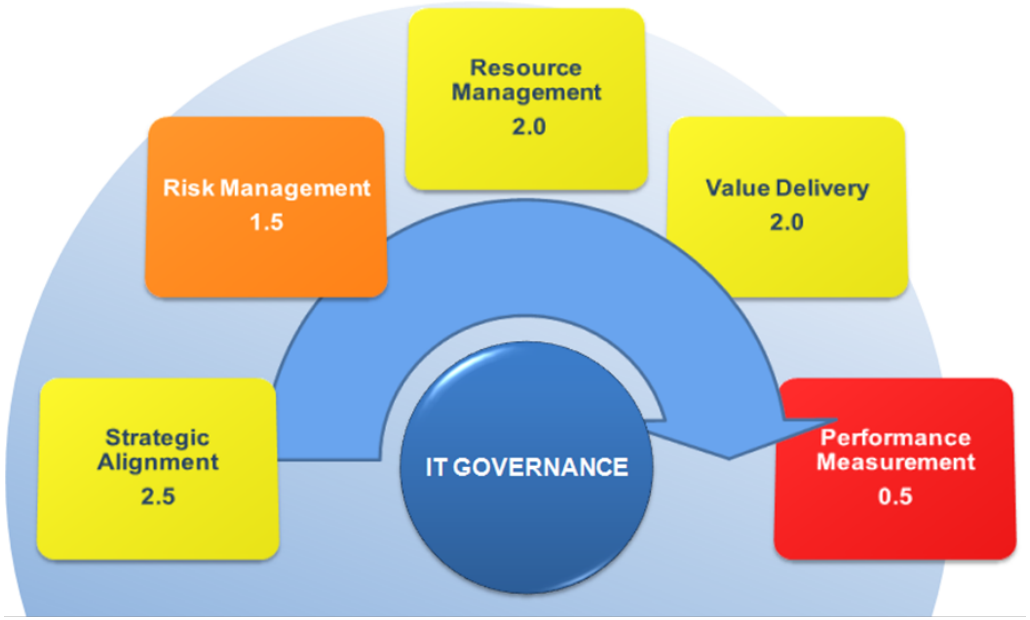
THE CARING INSTITUTION

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

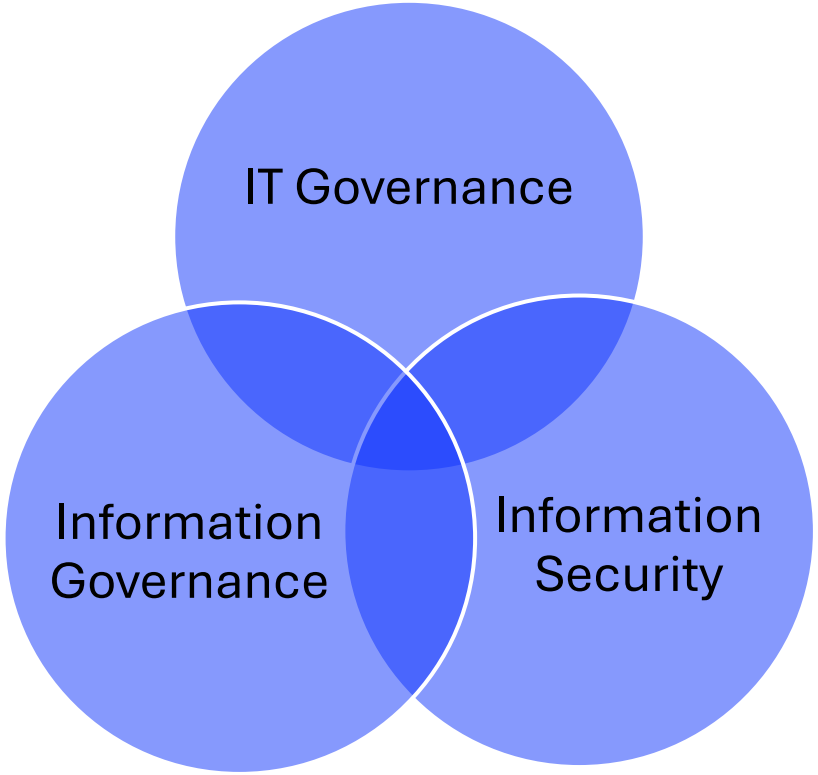
THE FULCRUM OF LEADERSHIP

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

The 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.



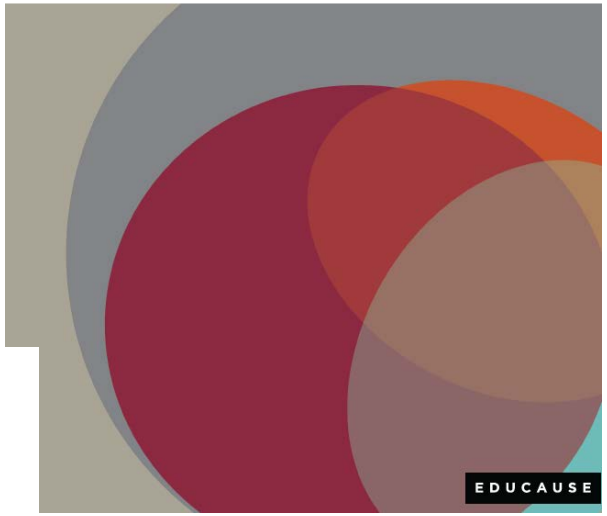
Educause IT GCR Report

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

1/5 say

The gaps between the importance of and the effectiveness in addressing these IT risks are large.

Educause IT GRC Report Conclusion

- Informal processes and procedures for risk management and compliance
- Half 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 have an adequate budget devoted to IT risk management.

Objective I

Opportunity to discuss issues unique to their role, share ideas and best practices and network with peers from many leading organizations that understand higher education.

Objective II

- 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 me measuring them?
  - Have we defined metrics?
- IT Audit results - What are the root causes?
- How to create change, massive change?
- Conformance versus Performance
  - Does your audit plan include both?

Objective III

IT Auditing

- National Association of Corporate Directors (NACD):

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

Internal Auditing Competency Framework™ Global Practice Guide

Skills required for 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

Coming

- Third-party – Q3 2025
- Culture
- Organizational Resilience

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.

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
- …

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…

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

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
- Many regulatory requirements with more state/federal requirements coming and more “guidelines” (due care)
- Immature IT/Information Security

Key Drivers - Impacting Areas

Regulatory requirements

Cloud

PII/EPHI Theft or misuse

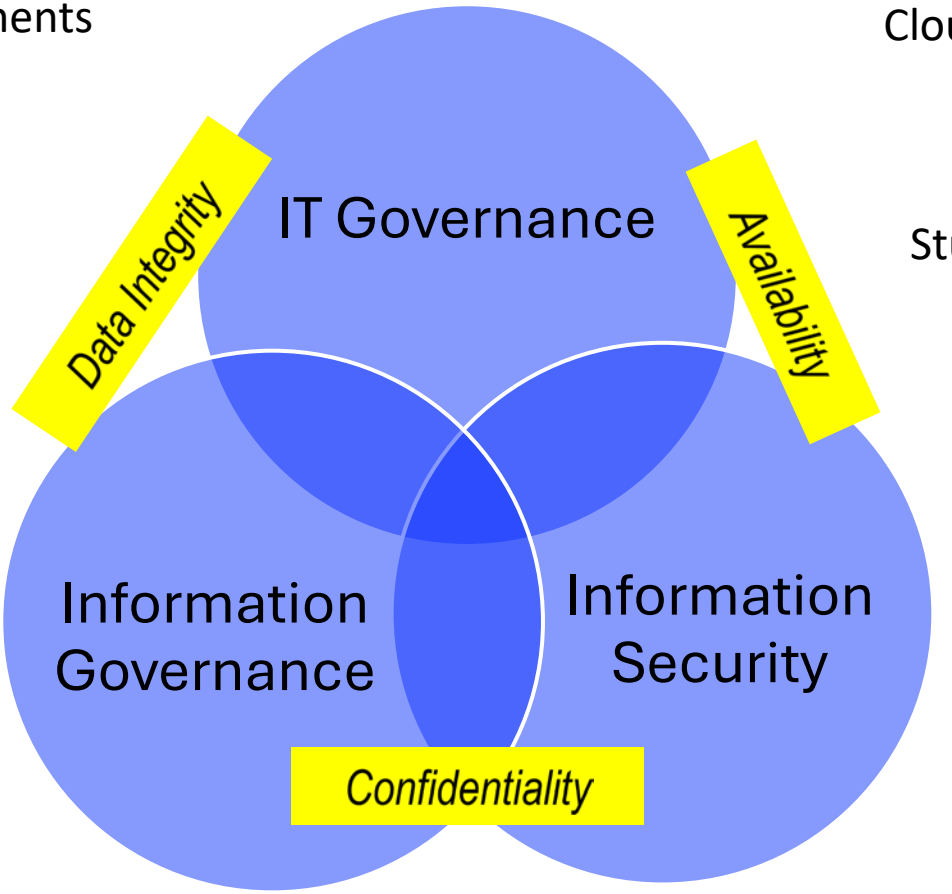
Student interaction

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?

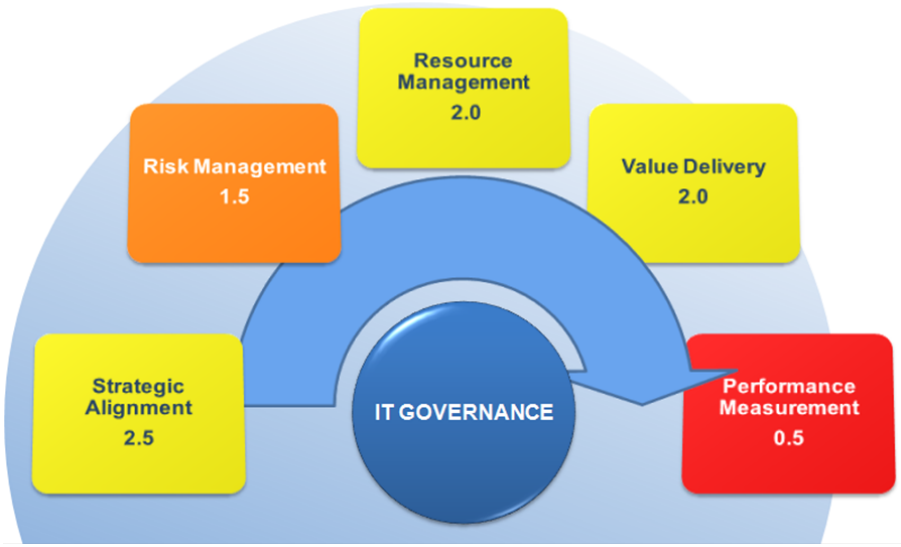
Resource Management

- 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: o Strategic alignment, o Value delivery, and o Resource management.

Contents

- Introduction
- Discussion and Knowledge Sharing
- References

Potential Key Topics to Discuss - (to be rated by participants)

- IT Governance
- Resilience
- AI
- Cyber Risk / Cyber Security and frameworks (NIST CSF, etc.)
- Identity and Access Management – Privilege Account Management
- IT Vendor management
- Distributed IT – Shadow IT
- Third party and Supplier Risk Management
- IT asset management - All IT assets (hardware, software, data, interfaces, with criticality, classifications, etc.)
- SIEM and log management
- PCI security and compliance
- Cloud Management and Security
- IT Risk Scoreboard/Measurements/Metrics
- Cybersecurity Performance Goals (CPG)
- How to create needed change in a higher education environment
- CMMC
- Information Security Program
- Research Security
- Medical devices (and Internet of Things)
- Information Governance/Data Governance/Big Data/Research
- End-User Devices/BYOD
- News on IT standards (ISO27000, NIST, CIS, etc…)
- How to communicate with your Board and Executive Management about IT Risks/Cyber Risks
- IT Strategy
- IT Cost
- Security Awareness Training/Education
- Risk Assessments
- IT Audit Plan Areas/Root Causes/Key Controls
- Privacy – GDPR, CCPA – California Consumer Privacy Act (Jan 1, 2020)
- Root Causes

Topics to be discussed

We will discuss a selected number of topics based on the result from the survey and input during the meeting.

Discussed 2024

- AI
- IT risk assessment – Your Most Important Control
- Third Party Risk Management – TPRM
- Standards and best practices
- IT Governance

Referenced Material

Depending on the topics different references will be provided during the session and after. After the session we will send out an updated ppt what was discussed and references to material. The Following slides are examples of what will be provided.

News on Standards

- Proposed HIPAA Security Rule – December 2024
- NIST Cybersecurity Framework (CSF) 2.0
- NIST Privacy Framework (2.0 Draft)
- NIST.SP.800-234. High-Performance Computing (HPC) Security Overlay
- NIST SP 1326 - NIST SP 1326 (Initial Public Draft) NIST Cybersecurity Supply Chain Risk Management: Due Diligence Assessment Quick-Start Guide
- NIST 800-55 Measurement Guide for Information Security
- 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
- IIA – Update to Internal Audit Standard and the Topical Requirement Cybersecurity
- NIST Special Publication 800-221A Information and Communications Technology (ICT) Risk Outcomes: Integrating ICT Risk Management Programs with the Enterprise Risk Portfolio
- ISO 27001:2022 Information Security Management Systems
- ISO 27002:2022 Information Security Controls
- 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

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)
- …

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 https://www.cisecurity.org/insights/white-papers/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
- Educause
  - Educause Top Ten https://er.educause.edu/articles/2024/10/2025-educause-top-10-restoring-trust#issue1
  - *Getting Your Ducks in a Row: IT Governance, Risk, and Compliance Programs in Higher Education.* http://www.educause.edu/library/resources/it-governance-risk-and-compliance-higher-education
  - Security and Privacy in Higher Education. https://www.educause.edu/content/2025/2025-educause-cybersecurity-and-privacy-workforce-in-higher-education

Resources (continued)

- 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.
- 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 (see recommended measurements)
  - 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
- Joint Commission.
  - Joint Commission Leadership standard http://www.jointcommission
  - The Big Book of Checklists 2023
    - Cybersecurity Risk Assessment Checklist
    - New Emergency Management Standards for Hospitals Compliance Checklist

Resources (continued)

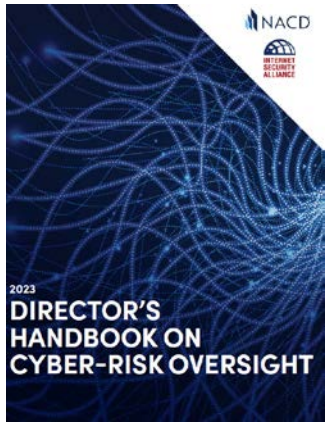
- Health Industry Cybersecurity Practices (HICP) https://405d.hhs.gov/information
  - Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients
  - Managing Threats and Protecting Patients
  - Cybersecurity Practices for Small Health Care Organizations
  - Cybersecurity Practices for Medium and Large Health Care Organizations
  - Hospital Cyber Resilience Initiative – Landscape Analysis **https://405d.hhs.gov/Documents/405d-hospital-resiliency-analysis.pdf**
- ISO
  - ISO/IEC 23894:2023 Information technology — Artificial intelligence — Guidance on risk management
- MIT Sloan Management Review
  - How Digitally Savvy Top Teams Drive Performance – MIT White paper
  - It Pays to Have a Digitally Savvy Board – MIT White paper https://sloanreview.mit.edu/article/it-pays-to-have-a-digitally-savvy-board/?use_credit=e0373081c8bd92f7458e2d3a5ed6e2e7#article-authors
  - 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

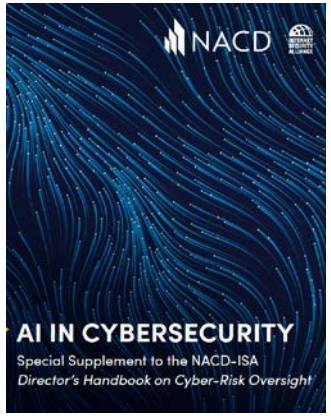
  (NACD nonmembers can access this publication by creating a guest account)
  - Principles for Board Governance of Cyber Risk (NACD and World Economic Forum) Principles for Board Governance of Cyber Risk | World Economic Forum (weforum.org)
  - Special Supplement to the NACD-ISA Director's Handbook on Cyber-Risk Oversight https://www.nacdonline.org/globalassets/public-pdfs/nacd_ai-cybersecurity-handbook.pdf

NACD – 2023 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

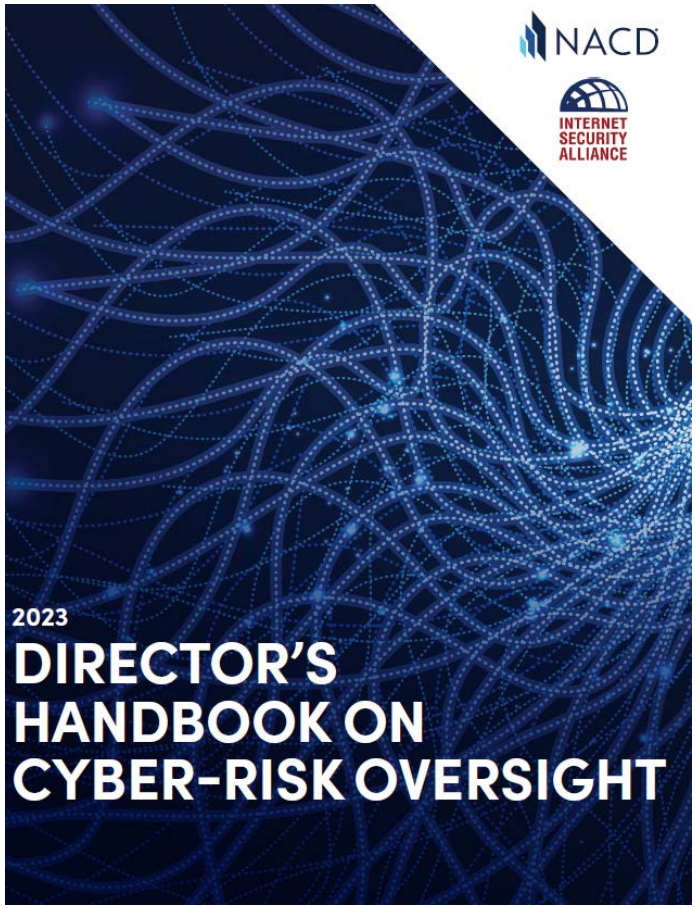
Nonmembers can access this publication by creating a guest account.

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

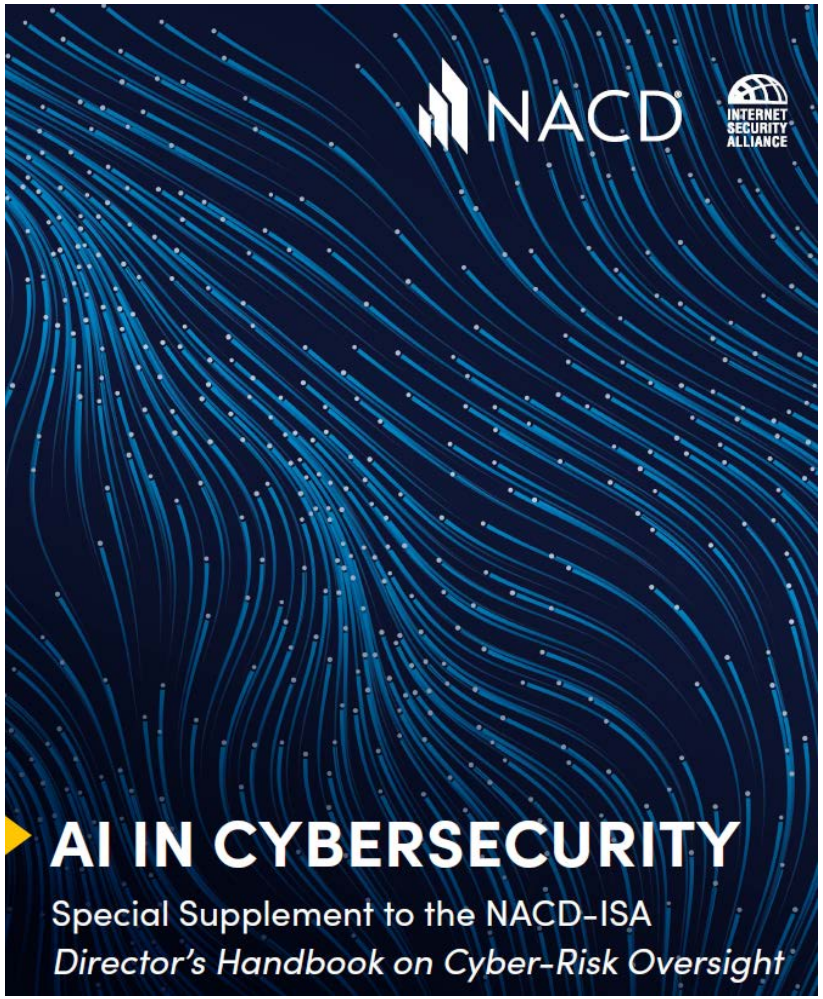
NACD – 2023 Directors Handbook on Cyber-risk Oversight

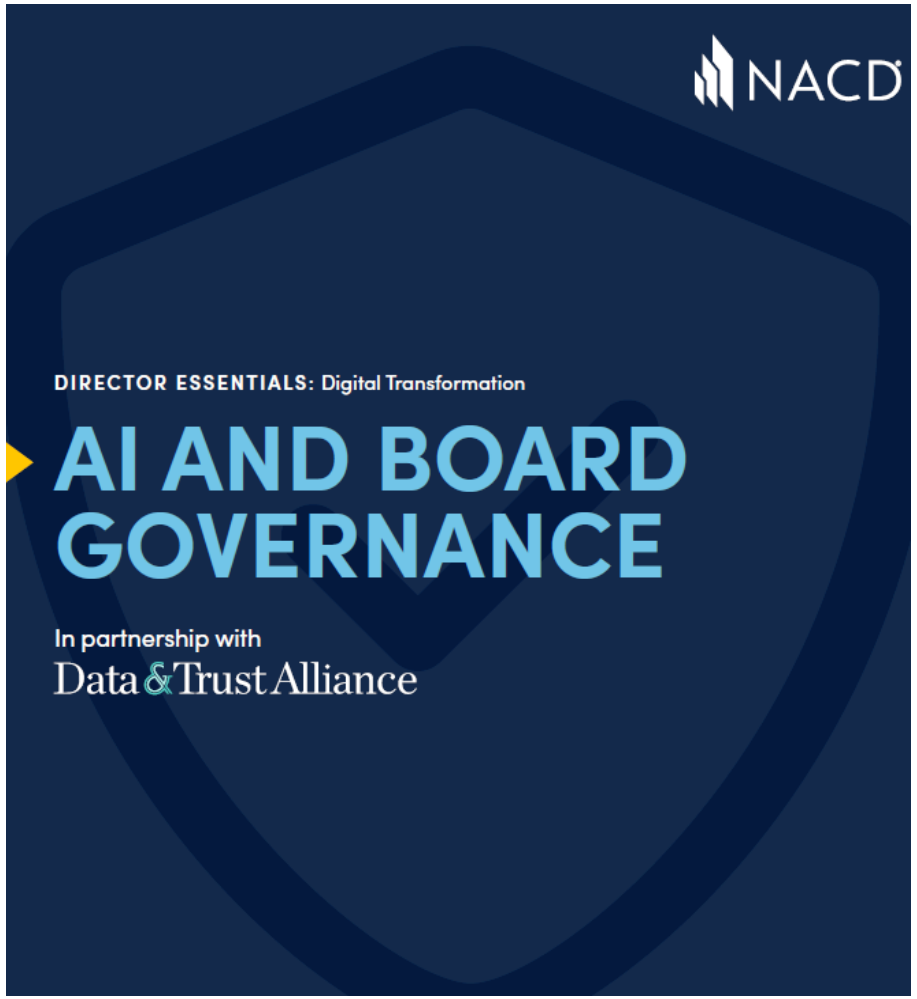
Tools:

- TOOL A: Ransomware Readiness
- TOOL B: Assessing the Board's Cyber-Risk Oversight Effectiveness
- TOOL C: The Cyber-Insider Threat
- TOOL D: Supply-Chain and Third-Party Risks
- TOOL E: Incident Response
- TOOL F: Board-Level Cybersecurity Metrics
- TOOL G: Cybersecurity Concerns During M&A Phases
- TOOL H: Building a Relationship with the CISO
- TOOL I: Enhancing Cybersecurity Oversight Disclosures—10 Questions for Boards
- TOOL J: Securing Cloud Services
- TOOL K: Working with CISA and Having a Conversation with Your CISO
- TOOL L: Incident Response and Reporting to the FBI
- TOOL M: Board Decisions on General Use of AI
- TOOL N: US Secret Service's Role in Stopping Financial Loss



AI and Board Governance





Resources (continued)

- 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/
- NIST
  - NIST's AI Risk Management Framework (AI RMF 1 .0)
  - NIST Privacy Framework
  - NIST IR 8286C Staging Cybersecurity Risks for Enterprise Risk Management and Governance Oversight
  - Cybersecurity Framework - Framework for Improving Critical Infrastructure Cybersecurity 2.0 https://www.nist.gov/document/csf-20-concept-paper
  - Cybersecurity Resource Center https://csrc.nist.gov/
  - 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
  - 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
- 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

Q & A

Contact information

Johan Lidros

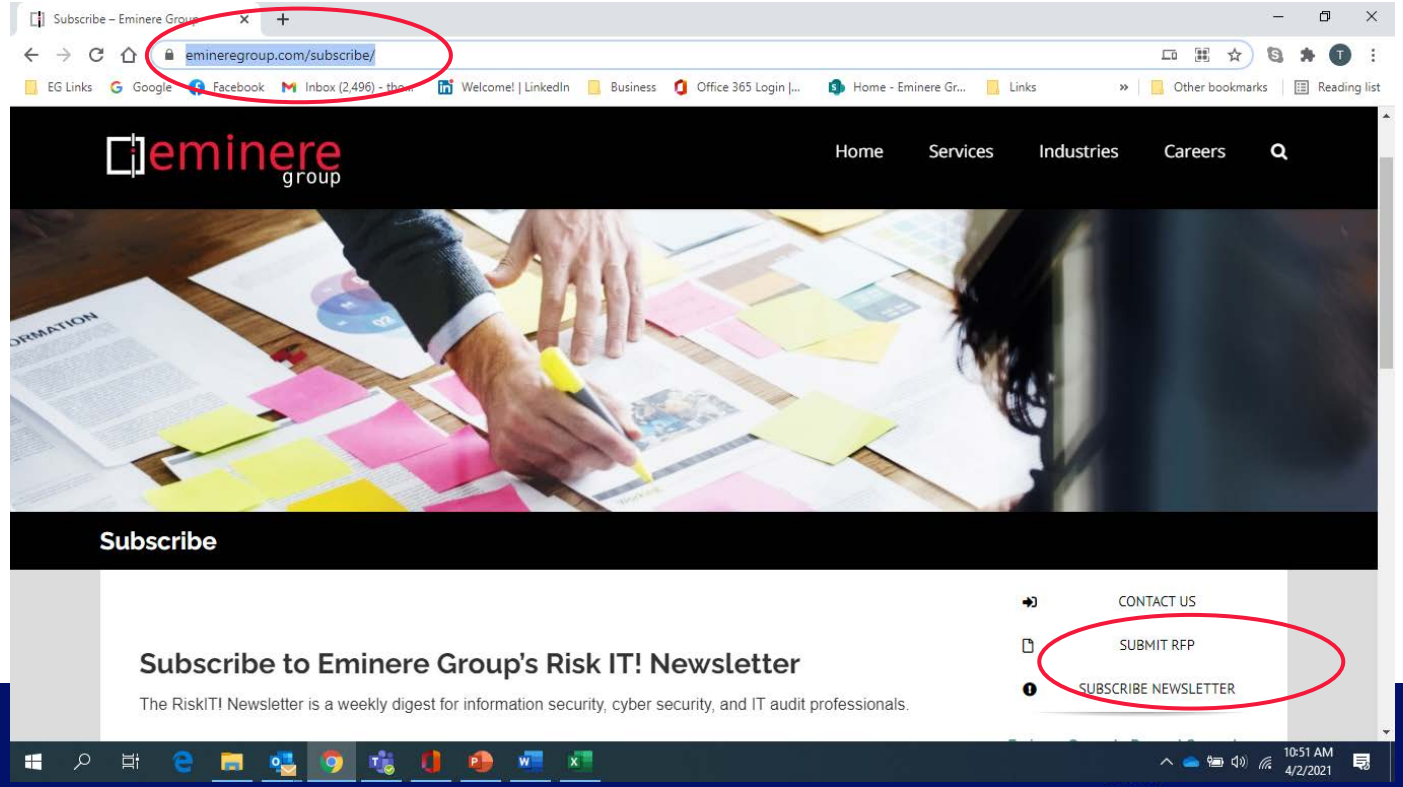
johan.lidros@emineregroup.com

+1 813) 832-6672 x-9101

+1 (813) 355-6104 (cell)

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



AuditCon 2026 – See You All