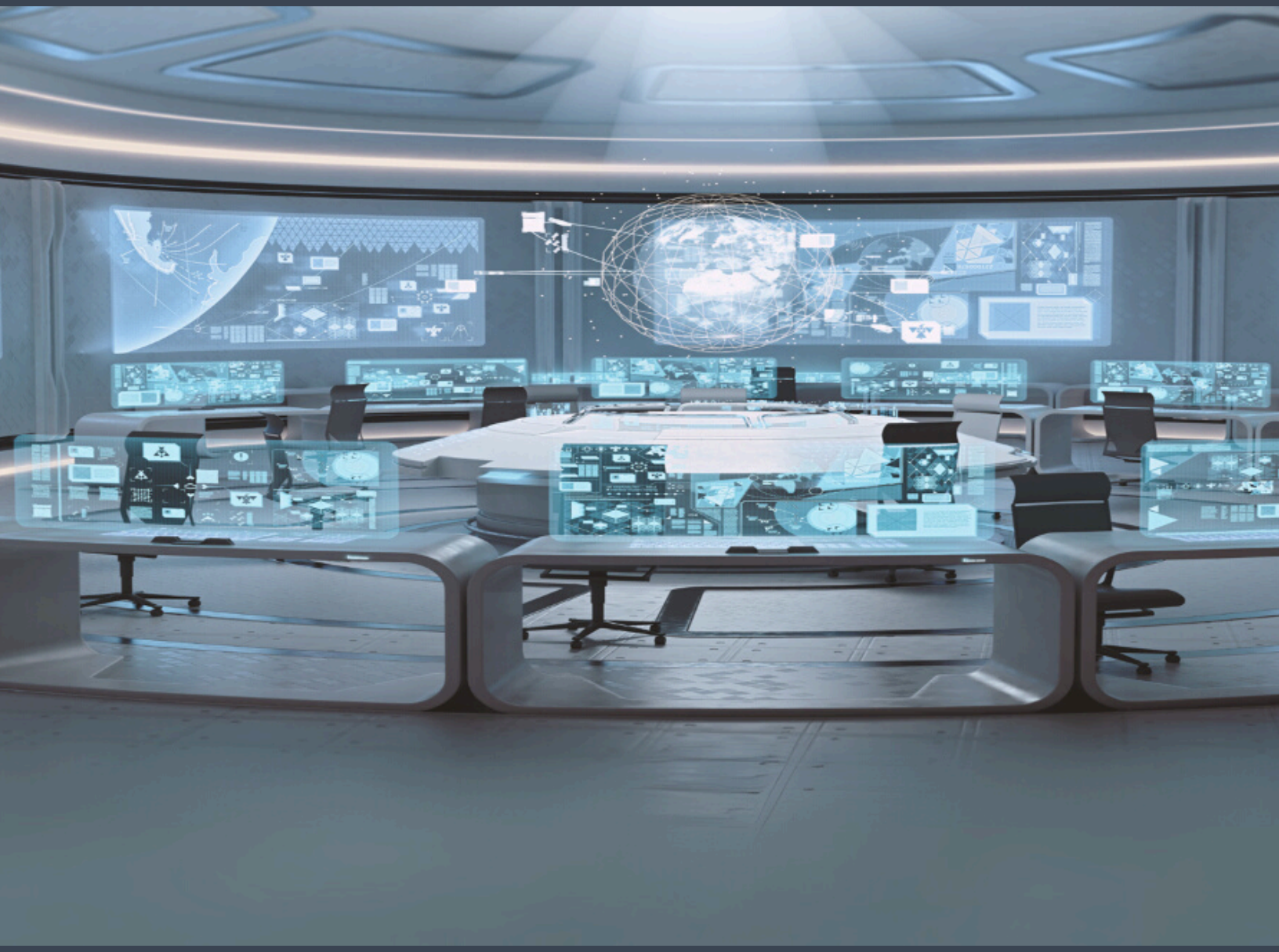
The Board's Command Center:

Boardroom Toolkit in the Age of AI and Cyber Risk



Prepared By:
ARC Hybrid

1/16/25
ISACA Chicago
Companion Resources

ISACA
Chicago Chapter

ARTIFICIAL INTELLIGENCE

The Board's Command Center:

AI Governance

Why this matters:

Artificial Intelligence (AI) will transform how our orgnization supports its business, but it also introduces new risks and oversight responsibilities for the board.

What is AI?

AI refers to systems that perform tasks requiring human intelligence, such as analyzing data, making predictions, or generating content. AI could be used to:

- Analyze customer/market data
- Automate financial reporting and compliance
- Enhance software development
- Optimize supply chain logistics
- Support resource allocation decisions
- Enhance and expedite communication

Opportunities:

- Improve data-driven decision-making
- Automate routine administrative tasks
- Enhance outreach and engagement
- Enable earlier detection of business trends and risks
- Support innovation in service delivery

Challenges:

- Risk of bias and inequity in AI outputs
- Data privacy and confidentiality concerns
- Difficulty explaining "black box" AI decisions
- Unclear or evolving regulatory requirements
- Limited internal expertise for oversight

The Board's Command Center:

AI Governance

Board Discussion Prompts:

- How does management ensure AI systems are fair and support equity across the organization?
- What safeguards are in place to protect employee, customer, and third-party data used by AI?
- How are AI-driven decisions explained to stakeholders and business partners?
- What is the board's role if an AI-related incident or failure occurs?

Management's Role:

- Maintain an AI inventory (purpose, data sources, owners)
- Implement robust privacy controls
- Monitor AI outputs for bias and fairness
- Document and explain AI models and decisions
- Prepare and test response plans for AI failures

Board's Oversight Role:

- Ensure AI risks are in the risk register
- Oversee privacy and bias controls
- Require regular reporting on AI risk metrics and incidents
- Confirm AI governance aligns with Heluna's mission and risk appetite

Key Takeaways / Board Checklist:

- ☑ AI risks are identified and integrated into ERM
- ☑ Privacy and bias controls are in place and monitored
- ☑ Board receives regular AI risk updates
- ☑ Incident response plans for AI failures are tested

AI Governance

Strategic Direction:

- How does our AI strategy align with our mission, and what metrics measure this alignment?
- What is management's framework for evaluating new AI opportunities against potential risks?

Risk Management:

- How are AI risks formally integrated into our enterprise risk register, and which ones pose the greatest threat to our mission?
- What process exists to identify and address potential bias in AI systems that could affect business outcomes or create inequities?

Oversight & Accountability:

- Who has explicit accountability for AI governance across our organization, and does this individual(s) have sufficient authority and resources?
- What independent validation occurs for AI systems that influence decision-making?

Privacy & Ethics:

- How are we protecting sensitive data when using AI across the organization, and have we evaluated privacy impacts?
- What ethical framework guides our AI usage?

Future Readiness:

- How is management monitoring emerging AI regulations that could impact our organization?
- What investments are needed to ensure our AI governance remains effective as both technology and our business evolves and scales?

CYBERSECURITY

Cybersecurity

Why this matters:

Cyber threats are increasing, making board oversight essential to protect the organization's mission and reputation.

What is Cybersecurity?

Cybersecurity is the practice of protecting systems and data from digital attacks. This may involve safeguarding:

- Sensitive data (e.g. PII, PHI, etc.).
- Intellectual Property (IP)
- Financial records and revenue-generating availability
- Mission-critical communications
- Internal systems and vendor connections

Opportunities:

- Protect sensitive data
- Build trust with business partners and funders
- Reduce risk of costly service disruptions
- Meet regulatory compliance needs
- Leverage new security technologies

Challenges:

- Increasing frequency and sophistication of attacks
- Limited resources for robust security measures
- Vulnerabilities from third-party vendors
- Keeping staff trained and vigilant
- Balancing security with operational needs

The Board's Command Center:

Cybersecurity

Board Discussion Prompts:

- How does management assess and prioritize the most significant cyber risks?
- What steps are taken to ensure vendors and business partners meet the organization's cybersecurity standards?
- How are staff and project teams trained to recognize and respond to cyber threats?
- What is the board's role during a major cyber incident?

Management's Role:

- Regularly assess and update the cyber risk profile
- Develop, test, and update incident response plans
- Provide ongoing security awareness training
- Implement and monitor technical controls
- Evaluate and monitor vendor/partner security posture

Board's Oversight Role:

- Ensure cyber risks are included in the risk register
- Oversee management's implementation of cyber controls
- Require regular updates on cyber incidents and lessons learned
- Confirm cyber risk management aligns with the organization's risk appetite

Key Takeaways / Board Checklist:

- ☑ Cyber risks are integrated into ERM
- ☑ Incident response plans are tested and current
- ☑ Board receives regular cyber risk and incident updates
- ☑ Security awareness is promoted at all levels

Cybersecurity

Risk Assessment:

- What are the top 3-5 cyber threats specifically targeting organizations like ours, and how are we mitigating each?
- How does our cybersecurity program address the unique risks of our organization?

Incident Preparedness:

- When was our incident response plan last tested with a realistic scenario, and what key lessons emerged?
- How quickly would we know if a breach occurred, and what is our communication protocol with sponsored projects?

Resource Allocation:

- How does our cybersecurity budget and staffing compare to similar organizations, and is it sufficient for our risk profile?
- What cybersecurity expectations do we place on our sponsored projects, and how do we verify compliance?

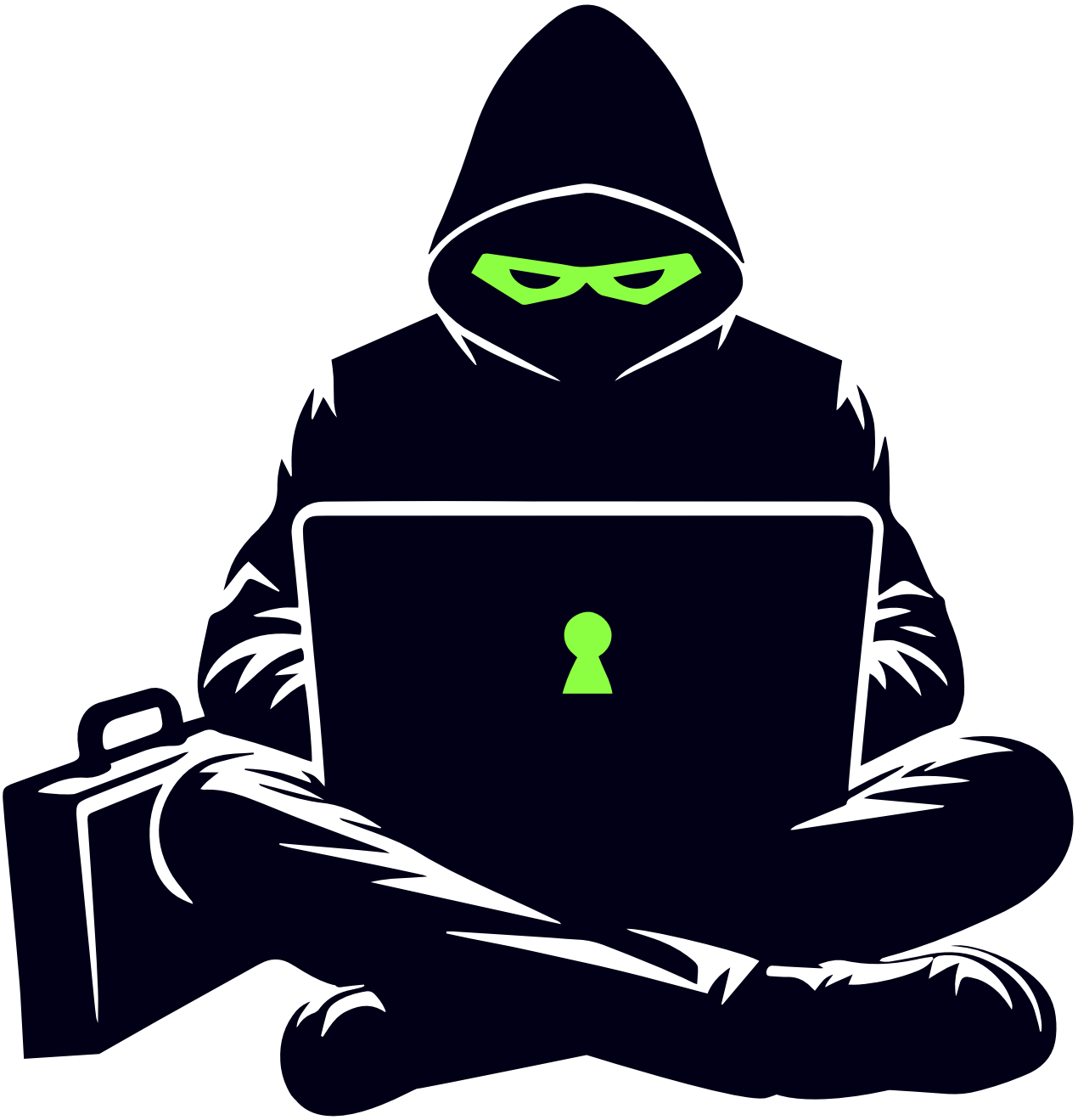
Third-Party Risk:

- What process exists to evaluate and monitor our security posture and risks of our key technology vendors and partners?

Resilience Planning:

- What is our recovery time objective for critical systems following a major cyber incident?
- How comprehensive is our cyber insurance coverage, and what exclusions could expose us to financial risk?

INCIDENT MGMT



The Board's Command Center:

Incident Management

Why this matters:

Effective incident management limits harm, speeds recovery, and protects Shareholder Value, Brand Reputation, and Fiduciary Duty.

What is Incident Management

Incident management is the process of preparing for, detecting, responding to, and recovering from disruptive events, such as cyberattacks, data breaches, or AI system failures. This may involve:

- Compromised business data
- Disruption of business operations
- AI used to automate, enhance, and scale cyberattacks
- Natural disasters impacting operations
- Reputational events affecting brand or public trust

Opportunities:

- Minimize impact of disruptions and breaches
- Strengthen organizational resilience
- Improve stakeholder and public trust
- Meet legal and regulatory response requirements
- Foster a culture of continuous learning

Challenges:

- Rapid escalation of incidents (e.g., ransomware)
- Communication breakdowns during crises
- Resource constraints for response and recovery
- Ensuring lessons learned are implemented
- Coordinating across multiple teams, regions, and vendors

The Board's Command Center:

Incident Management

Board Discussion Prompts:

- How often are incident response plans tested and updated?
- How does management ensure lessons learned from incidents are implemented?
- What mechanisms ensure timely and transparent communication during incidents?
- How does the organization coordinate response across multiple business units, regions, and business partners?

Management's Role:

- Develop, maintain, and test incident response plans
- Monitor for threats and escalate incidents promptly
- Inform board, staff, partners, and regulators with timely updates
- Document actions and lessons learned
- Implement corrective actions and report progress

Board's Oversight Role:

- Ensure the organization has a current, tested incident response plan
- Confirm clear roles, responsibilities, and escalation paths
- Oversee insurance coverage and regulatory compliance
- Support management during incidents, avoid micro-management

Key Takeaways / Board Checklist:

- ☑ Incident response plan reviewed and tested annually
- ☑ Board receives timely updates during incidents
- ☑ Post-incident reviews include board participation
- ☑ Lessons learned are implemented and tracked

The Board's Command Center:

Incident Management

Preparation:

- How do our incident response plans address our organizational structure, operations, and fiduciary duties?
- What criteria determine when the board should be notified of an incident, and are these thresholds appropriate?

Response Capabilitites:

- What specialized resources (internal or external) can we access during a major incident?
- How are roles and responsibilities defined during an incident?

Communication Protocols:

- What communication templates and protocols exist for notifying different stakeholders (e.g. funders, vendors, regulators) during an incident?
- How do we balance transparency with legal protection during crisis communications?

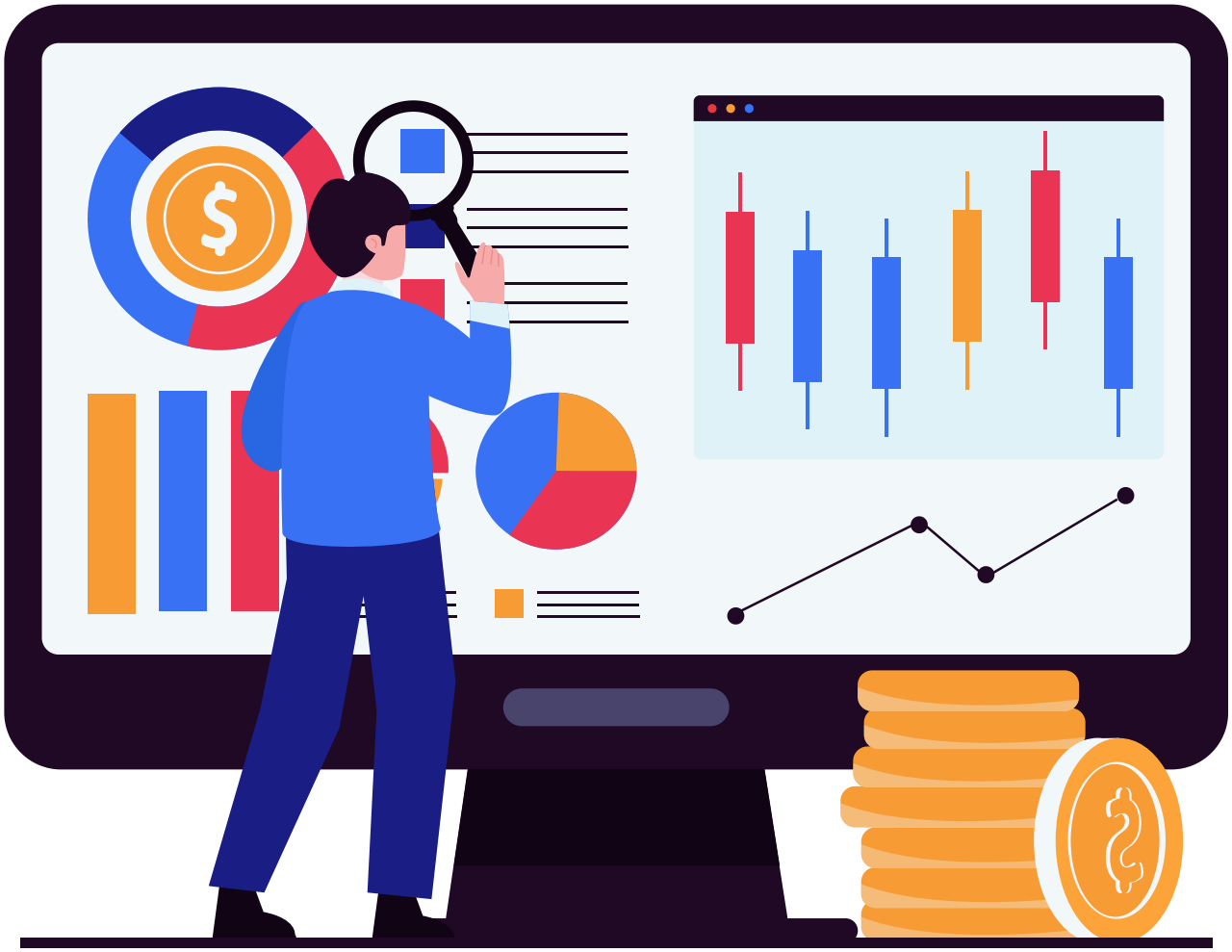
Learning & Improvement:

- How are lessons from incidents (both our own and those in similar organizations) systematically incorporated into our practices?
- What metrics do we track to assess the effectiveness of our incident response capabilities over time?

Board Engagement:

- What is the specific role of board members during a major incident, and are they adequately prepared for this role?
- How does management ensure the board receives appropriate information during an incident without overburdening the response team?

RISK MGMT (ERM)



⚠ Enterprise Risk

Why this matters:

Enterprise Risk Management (ERM) enables the board to balance innovation with risk, ensuring the organization's mission is protected and advanced.

What is ERM?

ERM is a holistic approach to identifying, assessing, managing, and monitoring risks, strategic, operational, financial, cyber, and AI, across the organization. ERM may:

- Provide a unified view of key risks
- Prioritize risks that could impact business goals
- Support informed decision-making
- Integrate risks from AI, cyber, and operations
- Enable proactive planning and resource use

Opportunities:

- Gain a holistic view of organizational risks
- Align risk management with mission and strategy
- Enable proactive, rather than reactive, risk response
- Support responsible innovation (AI, tech adoption)
- Enhance board engagement and oversight

Challenges:

- Siloed or fragmented risk management practices
- Rapidly changing risk landscape (AI, cyber, compliance)
- Limited risk management resources or tools
- Unclear risk appetite or tolerance
- Difficulty integrating risk information into decision-making

The Board's Command Center:

⚠ Enterprise Risk

Board Discussion Prompts:

- How does management ensure risks from AI, cyber, and operations are integrated?
- What is the organization's risk appetite, and how is it communicated?
- How does the board receive updates on emerging risks?
- How is risk management aligned with the organization's mission and strategy?

Management's Role:

- Continuously scan for emerging risks across the business
- Evaluate risks and update the risk register regularly
- Develop and implement controls, policies, and training
- Provide the board with clear, actionable risk dashboards
- Foster a culture of risk awareness and collaboration

Board's Oversight Role:

- Review and set the organization's risk appetite and tolerance
- Ensure all major risks are identified and assessed
- Oversee integration of risk management into strategic planning
- Monitor risk mitigation efforts and receive regular risk reports

Key Takeaways / Board Checklist:

- ☑ Risk register includes AI and cybersecurity risks
- ☑ Regular risk assessments and updates are conducted
- ☑ Board reviews risk reports at least twice per year
- ☑ Clear ownership of risk management processes

⚠ Enterprise Risk

Integration & Alignment:

- How are emerging risks from AI and cybersecurity integrated into our overall ERM framework?
- How does our risk management approach reflect our organization and industry?

Risk Appetite & Tolerance:

- Have we formally defined our risk appetite for innovation versus security, and is it appropriate for our mission?
- How does management ensure risk decisions across projects align with our established risk appetite?

Governance Structure:

- Is accountability for risk management clearly defined, with appropriate separation from operations?
- How does our governance structure ensure risks aren't managed in silos, particularly across technology, operations, and finance?

Risk Assessment Process:

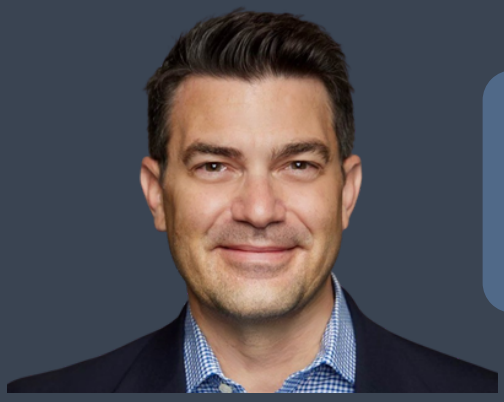
- How often are our risk assessments updated, and what triggers an out-of-cycle review?
- How do we incorporate external perspectives and emerging threats into our risk assessments?

Board Effectiveness:

- What training should the board receive to stay current on evolving risks in technology like AI?
- How do our board dashboards provide meaningful risk insights rather than just data points?

Scott Madenburg

ADVISOR | SPEAKER | TRAINER



Founder of ARC*Hybrid*
20+ Years of Industry Experience
CIA, CISA, and CRMA
Recognized Speaker and Author

ARC Hybrid

Empower your teams and elevate your impact with Scott:

- *Internal audit, risk, and compliance consulting*
- *Group training for internal audit and risk management*
- *Training for Boards and Committees*
- *Team-building workshops*
- *Career coaching sessions*
- *Inspiring keynote presentations*

Get in touch

Multiple ways to get in touch

Email

Send a message
info@thearchybrid.com

Phone

Call to discuss directly
+1-949-384-5355

Let's Connect