



ADVANCED
CYBER
SECURITY
CENTER

Corporate Boards, Risk Frameworks and AI Risks

Cyber Risk Governance Program Executive Practice Guide

May 2024



TRUSTED NETWORKS.
ADVANCING CYBER STRATEGIES.



On May 1 at the **ACSC Cyber Risk Governance Workshop**, hosted by **Google** in Cambridge, featured expert presentations from leading ACSC members **Manulife** and **Tenable**, and our **AI Co-Chairs**. This Executive Practice Guide includes key takeaways from the board-level risk frameworks presented along with the new AI risks that challenge existing risk assessments.

Risk Frameworks: A Starting Point For Collaboration

Risk frameworks provide the basis for business, technology, and security leaders to make collaborative decisions balancing risk against business opportunities – and agree on priorities to mitigate risk. They give security, risk executives, and ultimately boards a consistent, common view on risk across the organization. Once decisions are made, priorities become a ‘single source of truth’ for leadership and boards.

Fundamental principles emerged from the ACSC Cyber Risk Governance Workshop

- Risk frameworks don’t set priorities or make decisions, they shape a process
- It’s the process and risk priority-setting that are critical and should be clear to boards
- Consistent frameworks give boards a lens to understand risk and evaluate performance
- AI risk will require a distinct framework in these early stages, within an established risk governance program – which regulators will want to see

What’s Needed, What’s Changing - From Our Executives

Workshop Participants Reported:

- More than 60% said their #1 challenge was setting risk priorities
- Almost 80% rated their frameworks with a 3 or higher (on a 1-5 scale)
- Almost 70% are developing a separate AI risk framework within their current frameworks

What’s needed to manage AI risk at the operational level:

- Next generation IAM that detects misuse of models and data, even where access is permitted
- Time-based controls that enable models and data to be backed up/checkpointed
- Resources to help define materiality for AI risks

For management and boards, a GRC tool that rolls up AI risks and adds threat intel

What’s changing in board presentations to reflect AI adoption:

- AI risk is impacted by deployment models and third-party mix. Capture these associated risks and tradeoffs.
- As AI technical controls are in flux, focus on controls the board understands. How do we evaluate vendors? How are applications tested? How do our threat models change?

Contact Us

(617) 485-1112

wguenther@acscenter.org

CYBER RISK FRAMEWORK CASE STUDIES



Jenn Cook

Global Leader of IRM Strategy,
Planning and Governance
Manulife



Bob Huber

Chief Security Officer
Tenable

Presenting Risk to the Board

ACSC members and senior Cyber Risk and Security Executives **Jenn Cook** and **Bob Huber** shared material from recent board-level presentations and guidance for effective risk governance.

Risk executives must keep the board informed of how risk is categorized as well as progress towards mitigation. Consistency in reporting will drive confidence over time, even as details change.

- Targets will change, although the process to set priorities shouldn't
- There will never will be single structure that will work for every organization or audience
- Use existing, familiar structures to get people confident and comfortable
 - They combine CMMI maturity levels (initial, defined, managed, quantitatively managed, optimized) and the NIST IPDRR framework

Risk assessments and priority-setting are a snapshot in time, while risk reporting should communicate continuous progress towards maturity.

- The NIST frame helps leadership understand where efforts are functionally focused, while CMMI metrics lets them know how well efforts are progressing
- Changes in maturity levels are to be expected, both positive gains and declines
 - Be prepared to speak to both
 - Give board an easy way to judge progress year to year (or event to event)
- Extending frameworks to include new risks, including AI, provides the opportunity to engage executives across the organization

Both presenters emphasized the importance of clear and easy to consume information.

Risk Frameworks In Post-incident Reporting

While risk frameworks are essential to daily risk confidence, they're also essential to effective post-incident board briefings.

For that Executive Practice Guide, visit the [ACSC Workshop page](#).

Contact Us

(617) 485-1112

wguenther@acscenter.org

“The business conversation is the risk conversation.”

Moving From Strategic To Operational Risk Management Is A Challenge

Frameworks have three levels: strategic, engineering, operational. The engineering layer, which translates from strategy and policy to operational controls and solutions, is a critical element but least developed. We need better methods to identify solutions, prioritize investments, and then measure and demonstrate their impact on strategic risks.

Risk frameworks must help stakeholders, executives, and board members understand how core assets are being protected.

- Start with common sense: what are our ‘crown jewels’ and how do we protect them?
- Map these “priority assets” to security/risk investment dollars
- Focus on where the budget is currently overweighted and where additional resources might speed mitigation
- Assure the use of engineering frameworks – without them there is no visibility into the effectiveness of controls

This is where business and risk thinking come together: what’s most important and what are we doing to protect the organization?

Risk Management Case Studies - Sample Board Presentation Material

Tell the Risk Story

Jenn Cook presented the Manulife framework, heavily coded with color and other visual aids, helps quickly tell the risk story.

Inventory, Assess, Register

Bob Huber shared his Tenable framework and board presentation to assess and communicate risks across three phases: inventory, assessment, and register.

[Click to see board presentation samples](#)



AI RISKS AND BOARD-LEVEL GOVERNANCE



Mark Maybury
Vice President,
Commercialization
Lockheed Martin



Marc Zissman
Associate Head, Cyber Security and
Information Sciences Division
MIT Lincoln Laboratory

Managing AI Risk and Rewards with Frameworks

ACSC AI co-chairs **Marc Zissman** and **Mark Maybury** launched a discussion on managing leadership conversations and collaboration around AI risk. **Key takeaways:**

- AI risks can be integrated into existing governance, but regulators will require a distinct risk framework
- Focus on both “tight controls and strong enablers”

AI is reshaping software development as first an enabler and then a risk. An infographic is available [on ACSC Workshop webpage](#).

Third party risk is about to get more complicated, making trusted partners even more valuable. See ACSC’s AI Vendor Assessment Toolkit

A Core Challenge: Infinite Threats and Finite Resources

AI is supercharging old threats and creating new ones

- AI is making both automated and human-led attacks more effective
- AI and deep fakes are already linked to high profile financial and fraud cases
- Gen AI-driven attacks will target AI systems, including spoiling training data

Your AI systems are now a crown jewel subject to greater risk

- AI brings together core business assets and sensitive information, including customer data
- Risk isn’t just traditional data loss, but now includes exfiltration from models and GenAI applications

All IT and business systems are also at risk from AI-assisted attacks

- Human users remain the weakest link, especially as our ability to detect AI lags behind attacks and errors
- AI will make complex, multistage attacks harder to detect and deflect

Despite these changes, stay focused on what hasn’t changed in managing risk—much of the process applies to AI risks as well.

Contact Us

(617) 485-1112

wguenther@acscenter.org

AI Development: Closer to R&D than Traditional IT

“Balance strong controls and powerful enablers”

Managing, not limiting access, is key

- Eliminate “Shadow AI” by creating managed access and transparency for users/use cases
- Drive education-led adoption - users are trained on risks and best practices

Recent guidance from the Five Eyes -- US intelligence and its closest allies -- provides a good, layered formula for building secure environments

- Start with appropriate use policies around applications and sensitive data and IP
- Build secure local environments that let teams safely develop and iterate
- Assure data integrity and security

Evaluating vendors and partners will be a continuous challenge

- A lot of risk is determined by environment: hosted versus hybrid cloud, etc.
- Commercial application and model opacity will impede visibility and security

Framing AI Threats: The Cyber CIA Triad and New Challenges

		Threats from an adversary attacking my use of GenAI	Threats from an adversary using GenAI Against me
Conventional Cyber Threats	Confidentiality	<ul style="list-style-type: none"> • Training data are exfiltrated • models are exfiltrated • models are reverse engineered, exposing IP of PHI or PII • IP or PHI or PII leaked into commercial AI system 	<ul style="list-style-type: none"> • Social engineering or speed, scale and with high fidelity to gain unauthorized access
	Integrity	<ul style="list-style-type: none"> • Training data are poisoned • models are corrupted 	<ul style="list-style-type: none"> • Fake training data generated with high-fidelity at speed and scale leaning to poor performance and other GenAI systems
	Availability	<ul style="list-style-type: none"> • Data and/or models are held for ransom 	<ul style="list-style-type: none"> • Extremely high fidelity email and website safe flood at speed and scale
GenAI-specific Threats		<ul style="list-style-type: none"> • System underperforms due to inadequate training or incomplete testing • IP infringement due to insufficient licensing of training data • Lack of protecting for GenAI-generated material • GenAI output misleads recipients into thinking it was human generated 	<ul style="list-style-type: none"> • Disinformation campaign at hitherto unexperienced speed and scale

For the Full Presentation: AI Threat Framework



During the session, we were given a helpful framework for identifying potential threats from AI.



For a more complete view of the AI data lifecycle and threats, see these slides.

Contact Us

(617) 485-1112

wguenther@acscenter.org

AI: A Distinct Framework, Embedded In Traditional Governance

AI presents a challenge for organizations attempting to simply extend existing risk management structures.

Regulators and stakeholders will expect new frameworks and guidance

- AI feels new and different enough to require new ways of organizing and understanding risk
- Existing frameworks (MITRE ATLAS, NIST AI RMF) are incomplete but good starting points
- All the best practices around frameworks still apply: consistency, clarity, extendibility

Everything still needs to connect back to strategic business and risk decisions

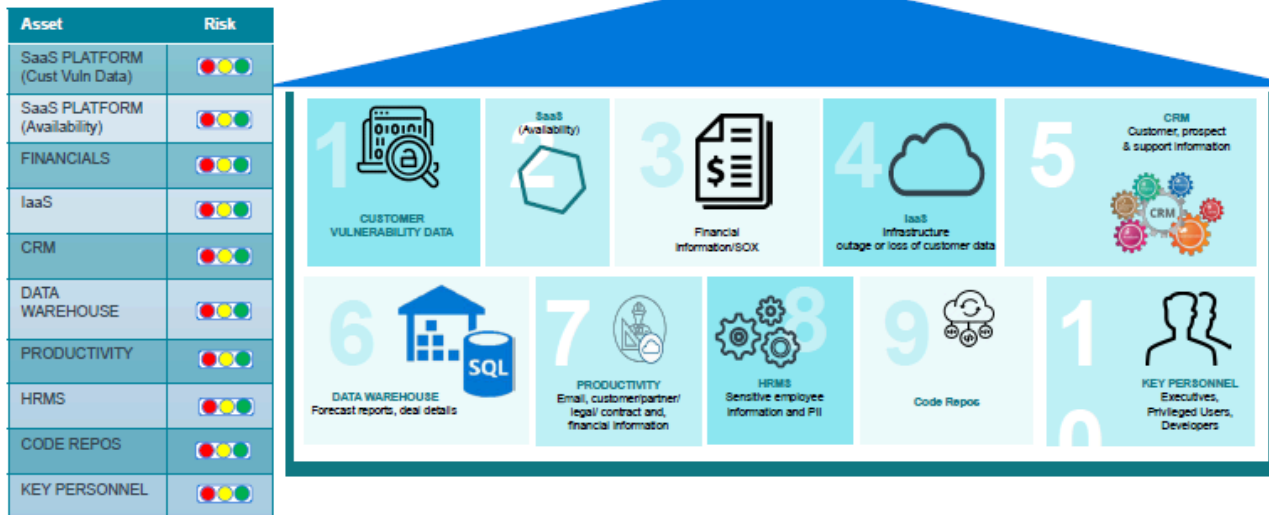
- The gap between strategic and operational controls might feel wider
- Global risk frameworks may have less visibility into some AI risk

Model providers are working to increase trust and transparency, including model cards

- Model providers and other vendors are working towards model transparency and labeling via model cards
- Expect these efforts to improve—vendors know transparency is critical to credibility

Protect the House

Company TOP 10 CRITICAL FUNCTIONS, ASSETS & SERVICES



About the ACSC

The Boston-based ACSC advances member cyber defense strategies through regional, national and global practice-sharing networks of industry leaders and provides professional opportunities for rising talent. This Executive Practice Guide reflects key takeaways, with proprietary information redacted, from this NDA-covered session and its case studies.

Contact Us

(617) 485-1112

wguenther@acscenter.org