Navigating the Intersection of Cyber Risk Management and Governance

November 13, 2024 | 2-3 PM ET

Webinar will begin shortly

American Bankers Association®

BRC

BOARD RISK COMMITTEE

NAVIGATING THE INTERSECTION OF CYBER RISK MANAGEMENT AND GOVERNANCE

BOARD RISK COMMITTEE

BRC SERVICES

CONSULTING AND TRAINING

We have a variety of options to provide expertise on emerging technologies, potential risks, and best practices in risk governance for corporate and nonprofit boards.

SPEAKERS BUREAU

The BRC provides to member companies and other board-related organizations well-recognized speakers on a broad range of risk topics for programs and events-in-person or virtual. The speakers may be keynotes, panelists, or moderators to lead roundtable and breakout group discussions.

WEBINARS AND EVENTS

The BRC offers monthly webinars, regional roundtables and annual in-person events with sponsors.

BRC
BOARD RISK COMMITTEE

SPEAKERS

SUSAN C. KEATING

BRC CEO

CATHERINE A. ALLEN

BRC chair and Founder

LISA O'CONNOR

Managing Director, Global Security Research and Development, Accenture

CRISTIN FLYNN GOODWIN

Founder, Advancing Cyber and Advanced Cyber Law

JONATHAN DAMBROT

CEO, Cranium AI, Inc.

BRC

BOARD RISK COMMITTEE

DOES INSTITUTION HAVE CISO ROLE; YES OR NO

BRC
BOARD RISK COMMITTEE

WHAT IS THE BOARD RISK COMMITTEE?

The Board Risk Committee is a nonprofit that focuses on education and peer exchanges for board directors who are dealing with risk issues. Whether you are on a risk committee, technology, or audit committee, all of us are concerned about risk and that is why we exist and we are here to help.

BoardRisk Committee.org

Accenture Responsible AI

Establish AI Governance & Principles

Business executives see boundless possibilities in AI innovation

76%

of executives view gen AI as an opportunity for revenue growth

Accenture, Pulse of Change

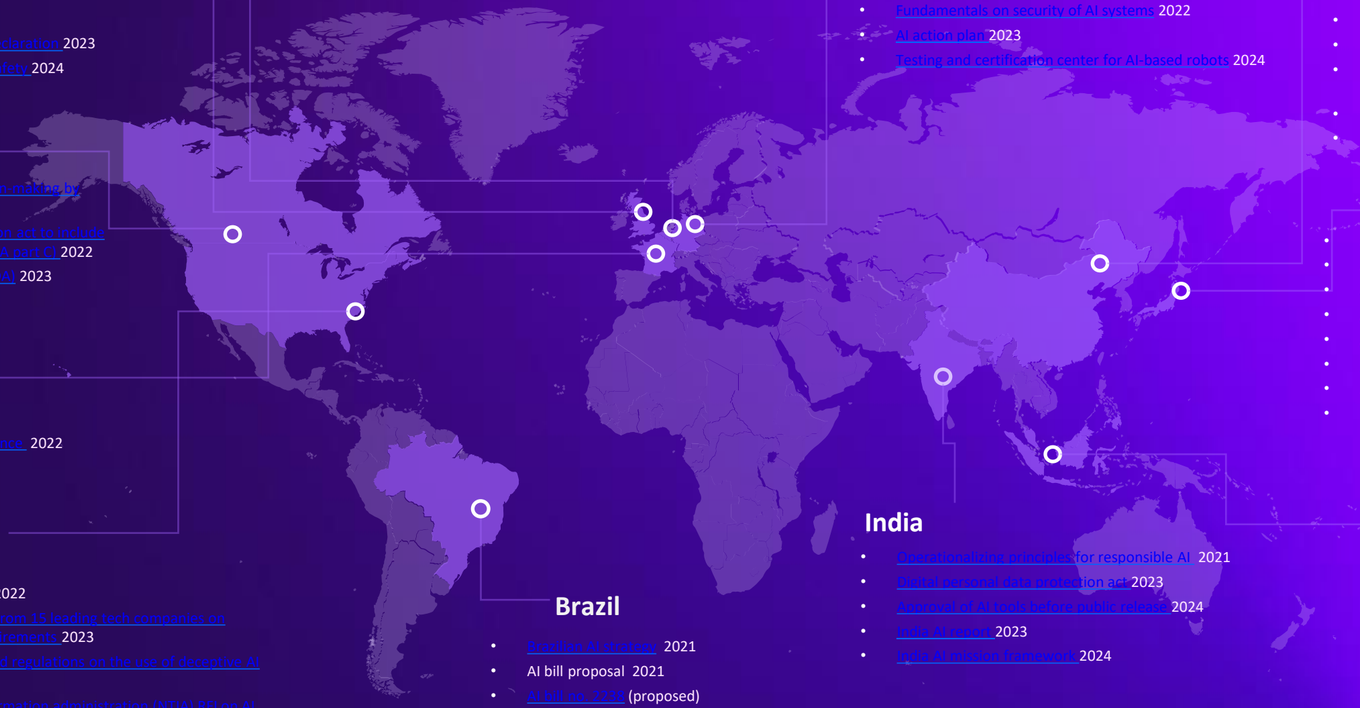
But they're not ready to efficiently manage AI-related risks

49%

of executives lack full confidence in their risk management processes for enterprise-wide integration of gen AI

Avanade, AI Readiness Report

Ever-evolving regulations by country and industry continue to alter the risk landscape



UK

- Artificial intelligence regulation white paper 2023
- Generative artificial intelligence in education 2023
- Frontier AI taskforce 2023
- UK AI safety institute 2023
- UK AI safety summit and Bletchley declaration 2023
- US-UK partnership on science of AI safety 2024

EU

- Artificial intelligence liability directive 2022
- Data governance act 2022
- Digital markets act 2023
- EU AI act 2024

Germany

- National AI strategy 2018
- Regulatory sandboxes enabling innovation and advancing regulation 2018
- Fundamentals on security of AI systems 2022
- AI action plan 2023
- Testing and certification center for AI-based robots 2024

China

- Governance principles for responsible AI 2019
- Guidelines for building new generation AI standard system 2020
- Trustworthy AI certifications 2021
- Ethical norms for the new generation artificial intelligence 2021
- Data security law 2021
- Personal information protection law 2022
- Internet information service algorithm 2022 recommendation management regulations 2022
- China's deep synthesis provisions 2023
- Draft measures for the management of generative AI services 2023

Canada

- Directive on use of automated decision-making by federal government 2021
- Bill C-27 digital charter implementation act to include artificial intelligence and data act (AIDA part C) 2022
- Artificial intelligence and data act (AIDA) 2023

Japan

- Social principles of human-centric AI 2019
- AI utilization guidelines 2019
- AI governance guidelines 2022
- AI strategy 2022
- AI strategy council 2023
- Hiroshima process 2023
- Japan AI safety institute 2024
- Legislation to regulate generative AI (proposed)

France

- Franco-German roadmap on AI 2021
- Conseil d'etat approach on AI governance 2022
- France AI commission report 2024

United States

- Blueprint for an AI bill of rights 2022
- NIST AI risk management framework 2022
- White house voluntary commitments from 15 leading tech companies on certain security and transparency requirements 2023
- Federal election commission – proposed regulations on the use of deceptive AI in campaign ads 2023
- National telecommunications and information administration (NTIA) RFI on AI accountability 2023
- Executive order on the safe, secure, and trustworthy development and use of artificial intelligence 2023

Brazil

- Brazilian AI strategy 2021
- AI bill proposal 2021
- AI bill no. 2338 (proposed)

India

- Operationalizing principles for responsible AI 2021
- Digital personal data protection act 2023
- Approval of AI tools before public release 2024
- India AI report 2023
- India AI mission framework 2024

Singapore

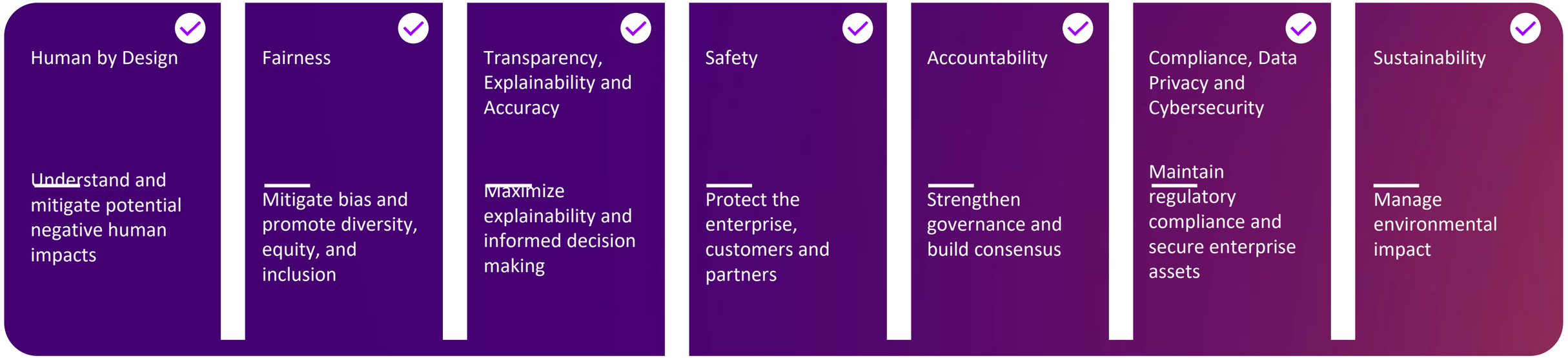
- AI governance approach + implementation self-assessment guide 2020
- AI governance testing framework minimum viable product (MVP) 2021
- A.I. Verify 2022
- Singapore national AI strategy 2.0 (NAIS 2.0) 2023

List of initiatives is non-exhaustive

Responsible AI

is the practice of designing, building, and deploying AI in a manner that is human-centered, fair, trusted, transparent, safe, secure, open and accountable while balancing the considerations around workforce and sustainability.

Governing Principles



GOOD HARBOR | Cyber Security Risk Management

ADVANCED CYBERLAW

Cybersecurity & AI Regulations

Intersection of Cybersecurity, Risk Management, & Governance

American Bankers Association
Board Risk Committee
November 14, 2024

Cristin Flynn Goodwin

Regulation in Cybersecurity & AI Arrives

- The era of best practices is over; time to shift to a “regulatory compliance” mindset
- Regulation impacts the negligence standard – even if you’re not required to meet it, the rising regulatory tide is lifting all boats
- AI acceleration factor is real; pressure on the regulator, but unclear goals and outcomes – and AI is converging privacy & cybersecurity

Cyber & AI - Areas of Regulatory Activity

Cybersecurity

- Incident response and reporting
- Governance and Risk Management
- Customer Information Protection and Breach Notification
- Information Security Policies and Programs
- Business Continuity
- Vulnerability disclosure

Artificial Intelligence

- High Risk AI
- Digital Replicas
- Countering Deepfakes
- Government use of AI

Financial Firms Need to Focus on Cyber Risks Posed by AI, New York Regulator Says

Story by Mengqi Sun • 3w • 2 min read

US Cyber regulation on the rise

SEC Cyber Rules:

- Incident reporting, governance, and risk management

NYDFS Cybersecurity Regulation (23 NYCRR Part 500):

- Most important regulation for Boards, CISOs, and cyber leaders from a practical standpoint
- Applies to financial services entities in NY, but will be setting a “floor” for others
- Incredibly detailed in what it requires of CISOs, leaders, and Boards

NYDFS details 14 priority policy areas, including:

Information security	Asset inventory	Identity management
Business continuity	Risk assessment	App development
Incident response	3p service providers	Customer data

Additional US Cybersecurity regulations

FTC Safeguards Rule - May 2024

- Non-banking financial institutions must protect customers information through a comprehensive security program
- Must notify the FTC over breaches involving 500 customers or more

SEC Regulation S-P Update – June 2024

- For regulated entities, increased requirements to protect customer information and established process for notice to individuals impacted by cyber incidents.

Conference of State Bank Supervisors Nonbank Model Data Security Law

- V2 published February 2024
- Requirements to secure customer information and update information security program

US AI Challenges and Churn

- **Legislative activity – at the state level**
  - 45 US states considered 700 AI bills in 2024; passed 113
    - Focus: high risk AI; digital replicas; countering deepfakes; and gov’t use of AI.
    - Legislative sessions begin in January
  - Federal legislation dabbles at the edges
- **Federal Policy, rather than legislation**
  - AI National Security Memo released Oct. 24, 2024
  - NIST AI Safety Institute – Calls for Congressional funding and support
- **Litigation draws attention**
  - Cases pending against OpenAI, Microsoft, Anthropic, Midjourney, Stability AI, Perplexity AI, DeviantArt, Nvidia, Intel and X / Twitter – just to name a few
    - Fight concerns the use of data to train AI models
  - Cases also developing around poor deployment or use of AI
    - Company or government deploying has been held liable for damages

EU Cybersecurity & AI Regulations

AI Act (EU 2024/1689) – August 2024

- First major regulation – applies to companies designing or using AI in the EU
- Subject to fines of up to €35 million ($51.6 million) or up to seven percent of their global annual profits, whichever is higher

NIS Directive 2.0 (EU 2022/2555) – October 2024

- Applies to “essential service providers” including banks and investment firms; steeper penalties for non-compliance
- Stronger requirements for incident reporting within 24 hours

Cyber Resilience Act – November 2025

- *Any product vulnerability exploited by a malicious actor must be reported within 24 hours*, with a general follow-up within 72 hours, and a detailed follow-up within 14 days.
- Imposes *fines of 15 million EUR or 2.4% of the previous year’s global turnover*; grants the EU the right to ban or recall non-compliant products

Digital Operational Resilience Act (DORA) – January 2025

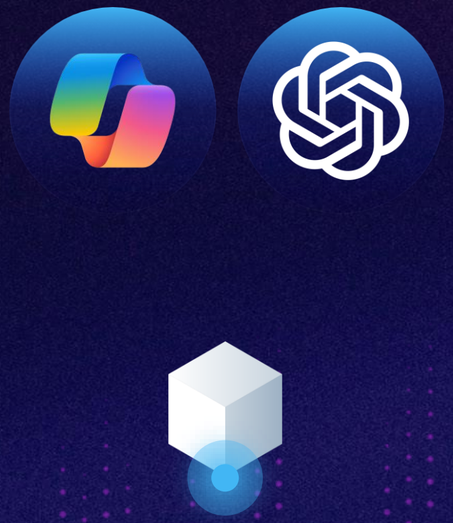
- Requires implementation of risk management framework and operational testing including pen testing on live systems and incident reporting on recurring bases
- Significant fines – 2% of global annual revenue or suspension of operations

Recommendations for Leaders and Boards

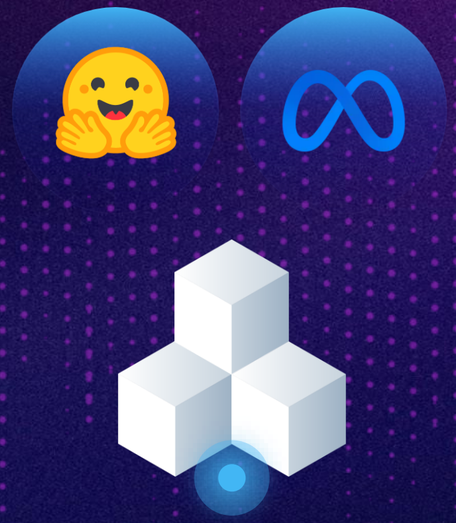
- **Most important**: Develop a ***cybersecurity risk management program*** with relevant policies, including incident response, and document key processes; review / update annually (**repeat for AI**)
- Ensure the ***company has a CISO*** and "qualified personnel or third parties" to support cybersecurity
- Boards and leaders need a ***clear process to learn about company risks and incidents***, under privilege if necessary
- Consider ***tabletop exercises to train Boards and leaders*** to practice decision-making and identify gaps
- Engage counsel now as a part of your product development, incident response, and threat intel process; ***expect your lawyers to be a part of your technical teams – not intimidated by technical issues***

ADVANCED CYBERLAW

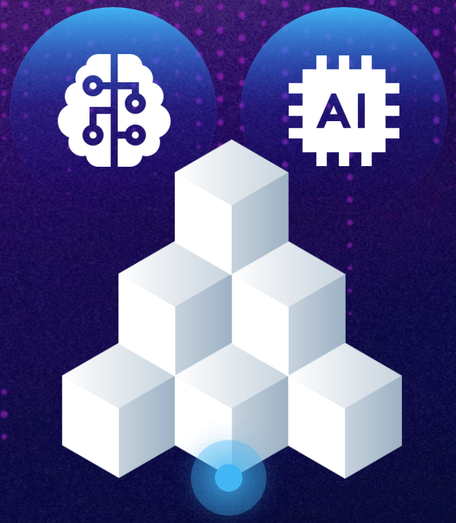
AI adoption exists on a spectrum.



Experimenting
with Generative AI,
LLMs, Copilots



Training open-source
models on company data
to build new products & services



Building enterprise
ML models with advanced
data science teams

What Analysts Are Saying

"AI will contribute **$19.9 trillion** to the global economy through 2030 and drive **3.5% of global GDP** in 2030."

IDC

The Global Impact of Artificial Intelligence on the Economy and Jobs. Sep 2024.

80%

of companies will leverage GenAI enabled applications in production by 2026

Gartner

50%

improvement in AI adoption for organizations that operationalize AI transparency, trust and security by 2026

Gartner

New challenges. New risk.

>60%

of CIOs say AI is part of their innovation plan, yet fewer than half feel their organization can manage its risks.

Gartner

96%

of executives say adopting AI makes a security breach likely in their organization in the next 3 years

IBM

24%

of AI projects will include a cybersecurity component within the next six months

Gartner

BRC

BOARD RISK COMMITTEE

NAVIGATING THE INTERSECTION OF CYBER RISK MANAGEMENT AND GOVERNANCE

BRC

BOARD RISK COMMITTEE

ARE YOU CURRENTLY USING AI IN YOUR ORGANIZATION OR BUSINESS?

YES OR NO

BRC
BOARD RISK COMMITTEE

WHAT IS THE AVERAGE EXPENDITURE PER YEAR ON CYBERSECURITY:

a. LESS THAN $50,000
b. $100-300,000
c. $300-500,000
d. $500,000+