Privacy + Security Forum, Fall 2024

Managing AI and Privacy Risks: Developing a Coordinated Risk Management Framework

Christine Lyon, Partner and Global Co-Head, Data Privacy & Security,
Freshfields Bruckhaus Deringer

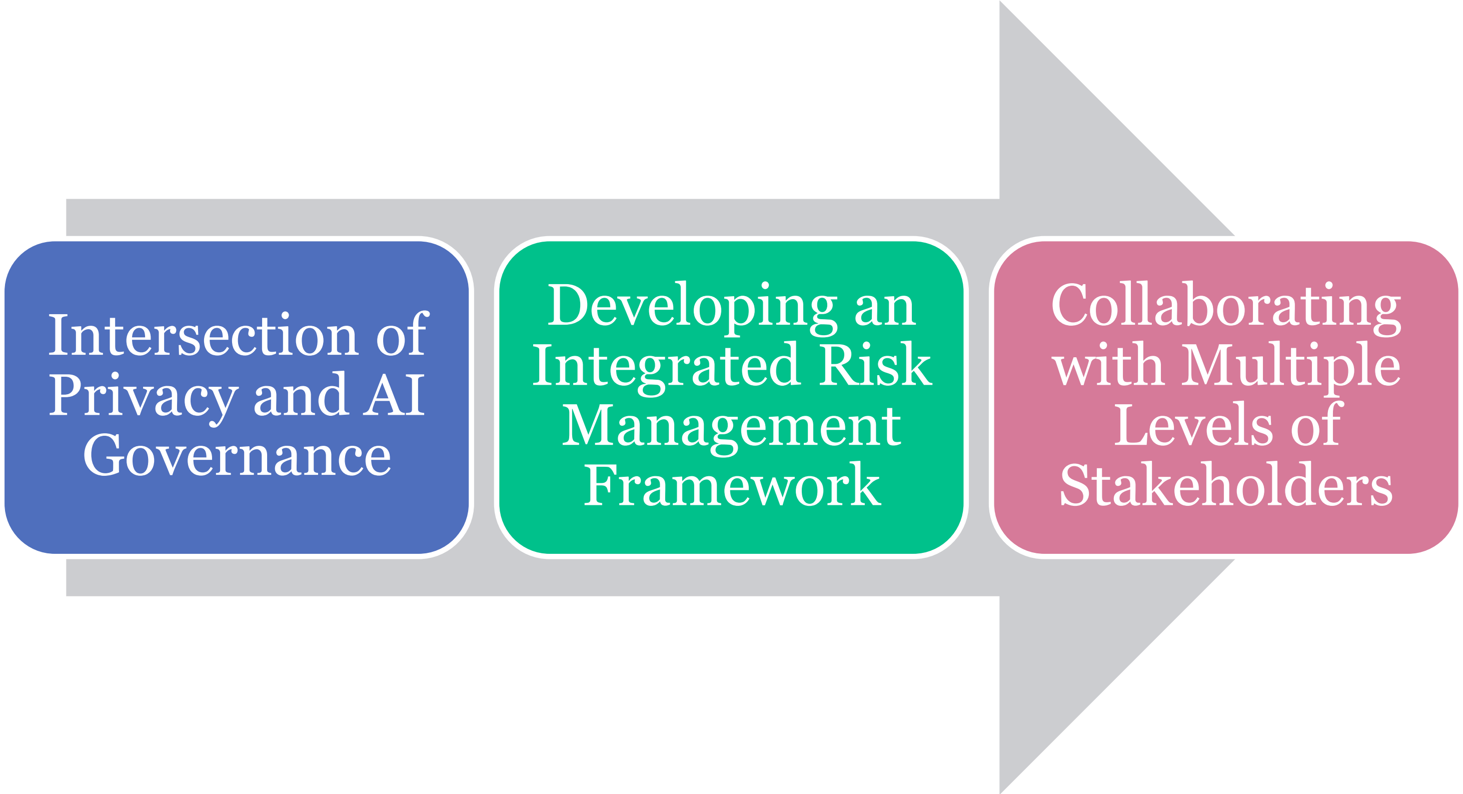
Hilary Wandall, Chief Ethics and Compliance Officer,
Dun & Bradstreet

Freshfields

dun&bradstreet

© Dun & Bradstreet, Inc. 2024

Agenda



Intersection of Privacy and AI Governance

Developing an Integrated Risk Management Framework

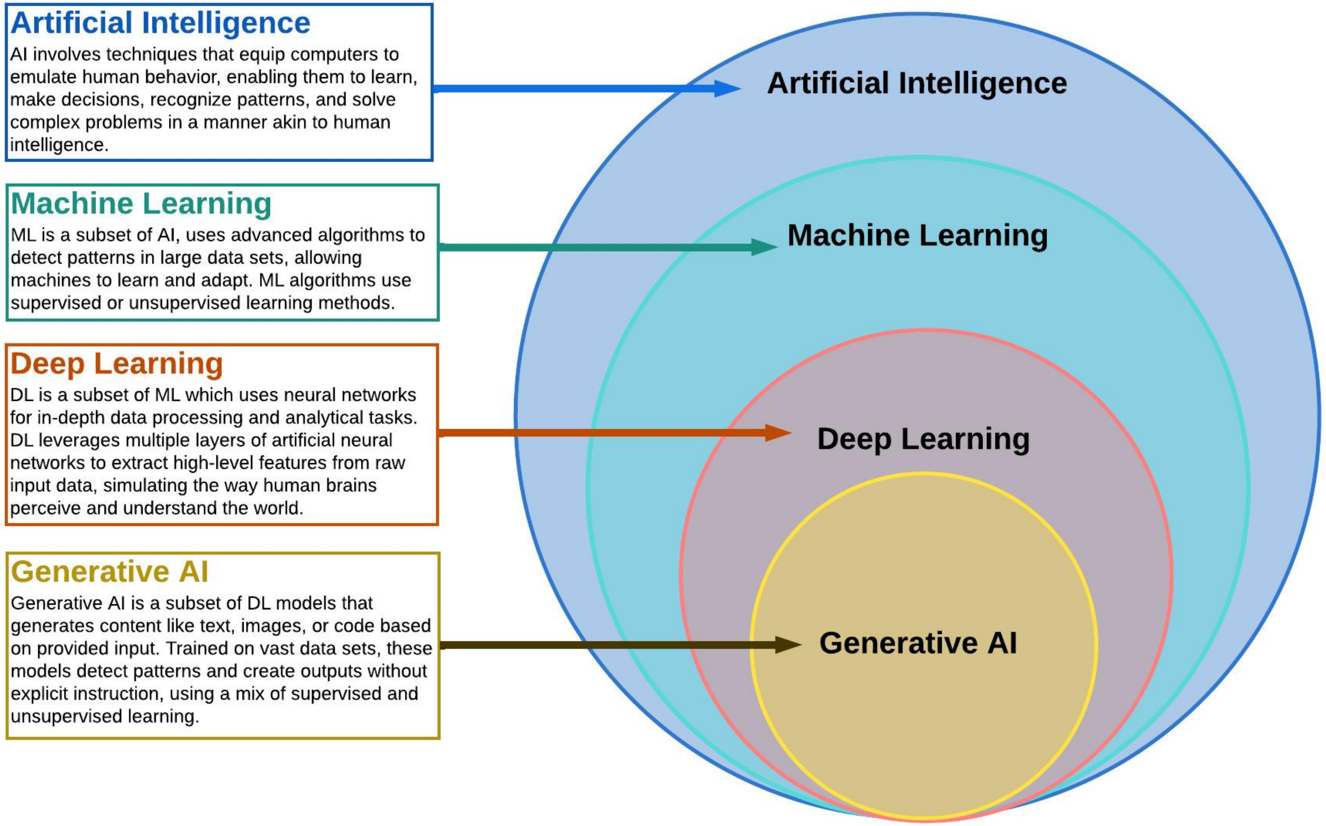
Collaborating with Multiple Levels of Stakeholders

Intersection of Privacy and AI Risks

Levels of Artificial Intelligence

An AI system is a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.

- OECD Definition



Artificial Intelligence
AI involves techniques that equip computers to emulate human behavior, enabling them to learn, make decisions, recognize patterns, and solve complex problems in a manner akin to human intelligence.

Machine Learning
ML is a subset of AI, uses advanced algorithms to detect patterns in large data sets, allowing machines to learn and adapt. ML algorithms use supervised or unsupervised learning methods.

Deep Learning
DL is a subset of ML which uses neural networks for in-depth data processing and analytical tasks. DL leverages multiple layers of artificial neural networks to extract high-level features from raw input data, simulating the way human brains perceive and understand the world.

Generative AI
Generative AI is a subset of DL models that generates content like text, images, or code based on provided input. Trained on vast data sets, these models detect patterns and create outputs without explicit instruction, using a mix of supervised and unsupervised learning.

Unraveling AI Complexity - A Comparative View of AI, Machine Learning, Deep Learning, and Generative AI.

(Created by Dr. Lily Popova Zhuhadar, 07, 29, 2023)

AI Risks are Cross-Disciplinary

They combine existing risk categories and introduce novel threats and challenges

Product Safety

Intellectual Property

Human Rights

Cybersecurity

Privacy and Data Protection

Equity, Non-Discrimination and Fairness

Governance and Accountability

AI Risks Contributing to the AI Trust Gap

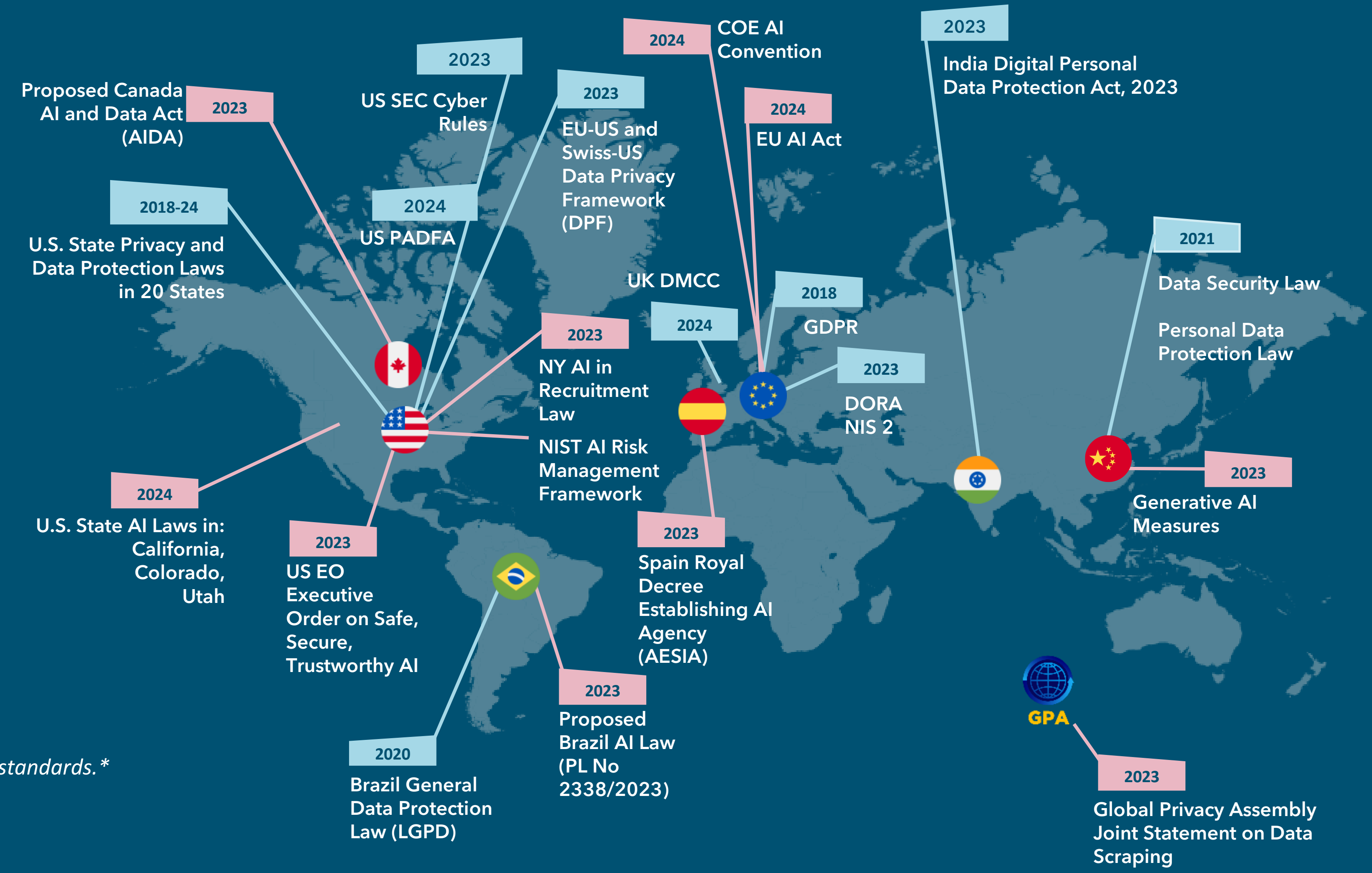
- Disinformation
- Safety & Security
- Black box problem
- Ethical Concerns
- Bias
- Instability
- Hallucination
- Unknown Unknowns
- Job and social inequalities
- Environmental impact
- Industry concentration
- Government overreach

Source: AI's Trust Problem. Harvard Business Review. 3 May 2024.

Regulations affecting AI and digital responsibility are rapidly evolving

Privacy, data and digital regulations* are expanding and proliferating

AI-focused regulation* has begun



2023 Proposed Canada AI and Data Act (AIDA)

2023 US SEC Cyber Rules

2018-24 U.S. State Privacy and Data Protection Laws in 20 States

2024 US PADFA

2023 EU-US and Swiss-US Data Privacy Framework (DPF)

2024 COE AI Convention

2024 EU AI Act

2023 India Digital Personal Data Protection Act, 2023

2021 Data Security Law

Personal Data Protection Law

UK DMCC

2024

2018 GDPR

2023 DORA NIS 2

2023 NY AI in Recruitment Law

NIST AI Risk Management Framework

2024 U.S. State AI Laws in: California, Colorado, Utah

2023 US EO Executive Order on Safe, Secure, Trustworthy AI

2023 Spain Royal Decree Establishing AI Agency (AESIA)

2023 Generative AI Measures

2020 Brazil General Data Protection Law (LGPD)

2023 Proposed Brazil AI Law (PL No 2338/2023)

GPA

2023 Global Privacy Assembly Joint Statement on Data Scraping

*Map displays a sample of related regulations and standards.**

dun & bradstreet

© Dun & Bradstreet, Inc., 2024. All rights reserved.

CIPL
Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

AI and Data Protection Principles

Data Protection Requirements	Tensions To Resolve	Artificial Intelligence
Legal basis for processing		Insufficient/limited variety of legal bases may undermine full range and stages of AI
Consent		Not practical to obtain consent for the processing of personal data (including sensitive data)
Data minimisation		Needs sufficient volumes and diversity of data for research, analysis, operation, training and to avoid bias
Purpose specification and limitation		Uses data for new and unforeseen purposes beyond original scope
Transparency		May produce unexplainable and unanticipated outcomes; hard to provide meaningful notice
Retention limitation		Needs to retain data for AI training, traceability, audit and oversight
Individual rights		Difficult to facilitate access, correction, deletion or explanation of the logic involved
Rules on automated decision-making		Automated decision-making capabilities are inherent to AI
Cross border data transfer restrictions		Needs to use diverse and geographically disperse data

Developing an Integrated Risk Management Framework

Elements of Effective AI Governance

Tools and approaches to help your organization govern effectively

1 AI Governance Framework

- Define and adopt a **set of AI principles** that align with your company’s values and adopt an **AI governance framework**.
- Establish **oversight structures, including appointing an AI Leader and a cross-functional AI steerco of senior leaders to direct the governance of AI** across your organisation. Reporting to the Board.

2 AI Legal and Compliance Framework

- Conduct a **global AI regulatory assessment** to understand the current and emerging AI regulations or AI-related obligations that may apply to your organisation.
- Periodically review and update **legal and governance systems and policies** and **assess gaps and areas for improvement (including with a view to maximising IP protection and minimising data risks)**.

3 AI Product Development

- Conduct an **AI product evaluation assessment** to understand the opportunities and risks of each current or future product or use case of your organisation.
- Conduct a **supplier diligence assessment** to understand how your organisation is reliant on third parties for its AI tools (and the legal terms that underpin those arrangements).
- Create **“rules of the road”** for engaging with third party AI tool suppliers.

4 AI Deployment

- Implement **an annual systemic risk assessment and AI audit** to ensure that products and services are being developed and deployed in accordance with your AI principles and governance framework.
- Implement a process for **sign-off of proposed new use cases for AI tools and their output**.

86% of organizations adopting AI view responsible AI guidelines as indispensable[1]

51% of organizations have a governance framework in place for Gen AI[2]

23% of organizations highly prepared for AI risk management and governance[2]

Sources: [1]2023 AI Ethics and Corporate Responsibility Report. Conversica.; [2]Deloitte's State of Generative AI in the Enterprise Q3 2024

Commercial in Confidence

© Dun & Bradstreet, Inc. 2024

Building AI into an Integrated Program

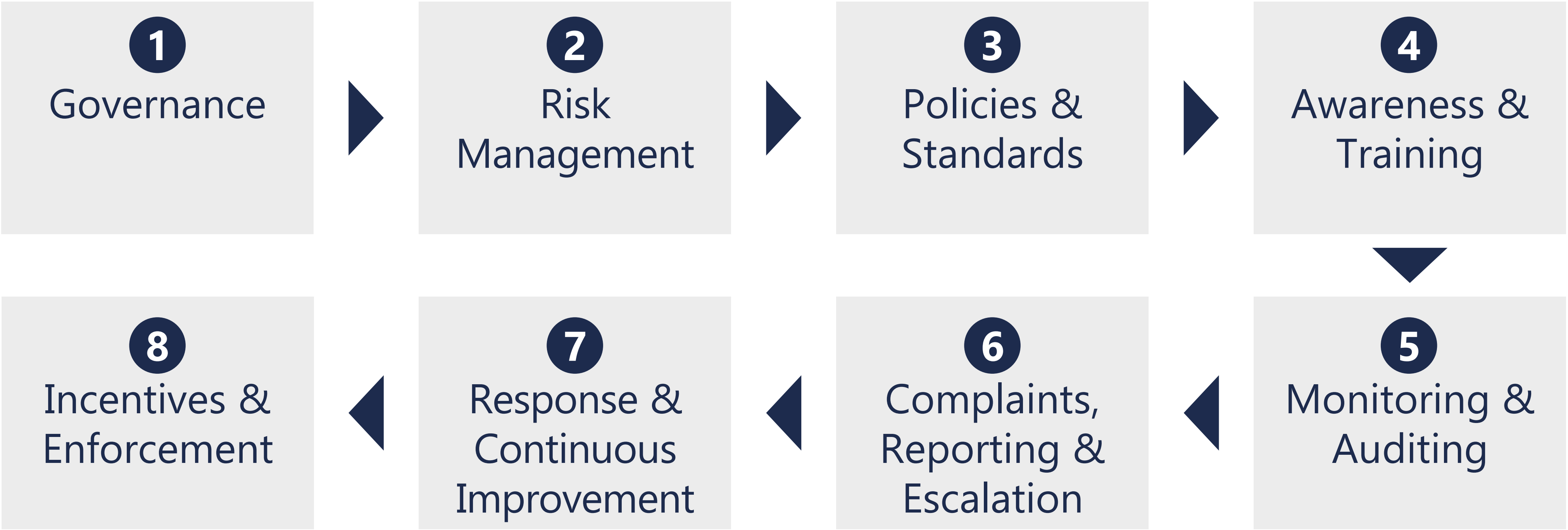
Data Compliance, Ethics and Risk

- Privacy
- Data and Cybersecurity
- IP/Trade Secrets
- Data Protection
- Consumer Protection
- Export Controls
- Credit Reporting
- Artificial Intelligence

© Dun & Bradstreet, Inc. 2024

Program Components

Based on the 8 Elements of an Effective Compliance & Ethics Program



1 Governance

2 Risk Management

3 Policies & Standards

4 Awareness & Training

5 Monitoring & Auditing

6 Complaints, Reporting & Escalation

7 Response & Continuous Improvement

8 Incentives & Enforcement

© Dun & Bradstreet, Inc. 2024

Integrated Privacy and AI Program Components

Program Element	Data Protection Requirement	Special Considerations
Governance	Appoint a Data Protection Officer (DPO) AI Governance Leader or Function	Similar to the role of a Chief Compliance Officer, the DPO is expected to be independent and have direct reporting to the highest level of the organization. Relationship to the Chief Privacy Officer/Counsel: strategic, operational, both? Relationship to/with the CISO, CRO, CSO

Integrated Privacy and AI Program Components

Program Element	Data Protection Requirement	Special Considerations
Policies and Standards Awareness and Training	Provide a Notice of Information of Privacy Practices AI Requirement – Transparency and Explainability	Privacy Notices are fundamentally about Transparency, so while they are derived from policies and often share common characteristics, they are also about Awareness of the organizations' practices by key constituents. In this way, they align with aspects of CSR and ESG. AI and System Model Cards add a new dimension to Transparency requirements.

Integrated Privacy and AI Program Components

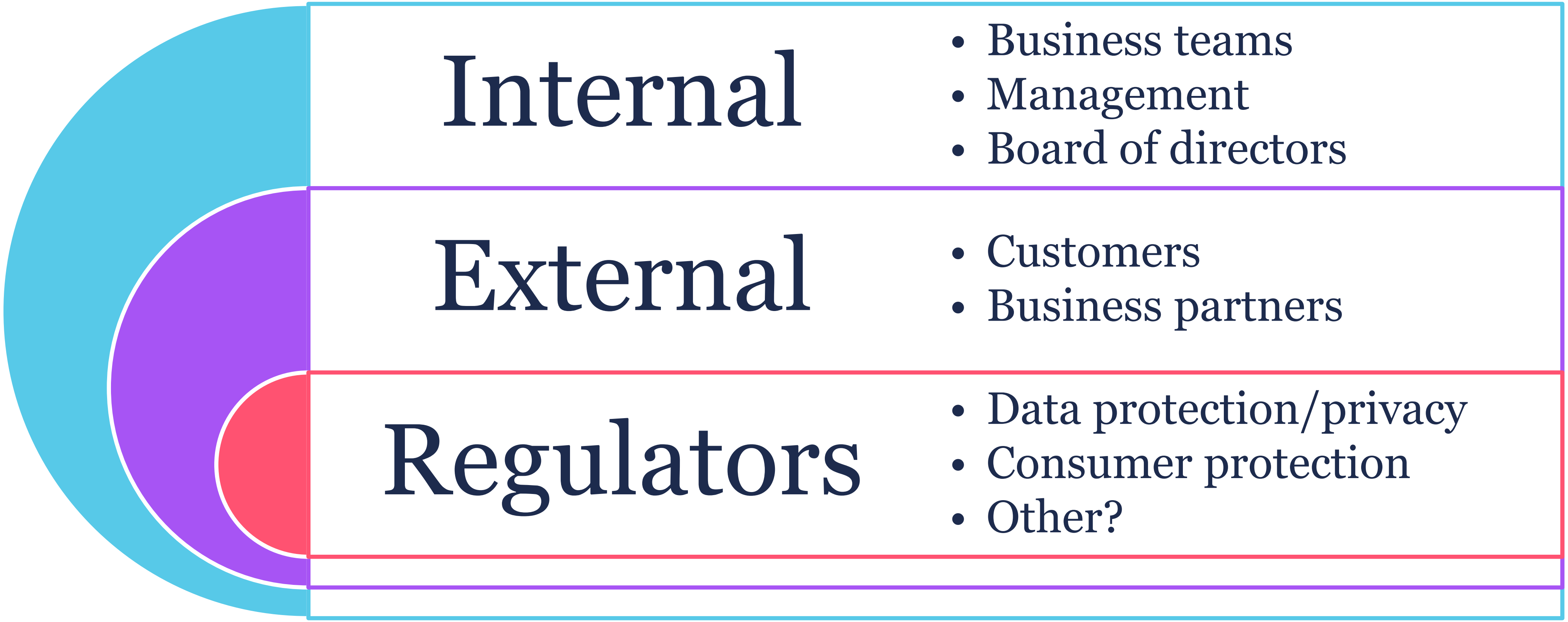
Program Element	Privacy and Data Protection Requirement	Special Considerations
Risk Assessment	Data Protection Impact Assessments (DPIAs), Transfer Impact Assessment (TIA) and similar forms of Impact Assessment (IA), such as an Algorithmic Impact Assessment	DPIAs, PIAs, LIAs, EIAs, TIAs, and other IAs (e.g., AIAs and HRIAs) are transaction or activity-level risk assessments. In the aggregate they provide a similar view to a compliance risk assessment and align to enterprise risk management (ERM). Alignment with third party risk assessments; Relationship between transactional and aggregate risks.

Integrated Privacy and AI Program Components

Program Element	Privacy and Data Protection Requirement	Special Considerations
Complaints, Reporting, and Escalation	Data Subject Requests Cookies and Preferences Concern and Incident Management Engagement and Contestability	Obligations, exceptions, and response times vary by jurisdiction. Is a baseline standard and process possible for your organization? Relationship among data incidents, privacy incidents, security incidents, compliance concerns. Is a common standard and process possible?

Collaborating with Multiple Levels of Stakeholders

Wide Range of Potential Stakeholders



Internal

- Business teams
- Management
- Board of directors

External

- Customers
- Business partners

Regulators

- Data protection/privacy
- Consumer protection
- Other?

AI – Questions For Your Business

Collaborating with your business to identify AI risks and opportunities

1 Governance Framework

How do we identify and evaluate potential AI tool use cases?

How do we currently identify, evaluate and manage AI risk?

How does AI fit into our corporate governance framework, including our corporate mission and values?

2 Legal & Compliance Framework

Are we subject to any AI-specific regulations?

What existing compliance functions are dealing with AI-related issues?

What steps do we take to align our compliance efforts with best practice?

3 Product Development

What is our AI product development lifecycle?

What third party suppliers do we rely on for our AI tools?

What data do we share with AI tools and what safeguards have we put in place?

4 Deployment

How do we currently deploy AI tools?

How do we manage, monitor and evaluate our use of AI tools and their output?

How do we manage risk associated with passing through third party AI tools or their functions to customers?

Day to day contracting

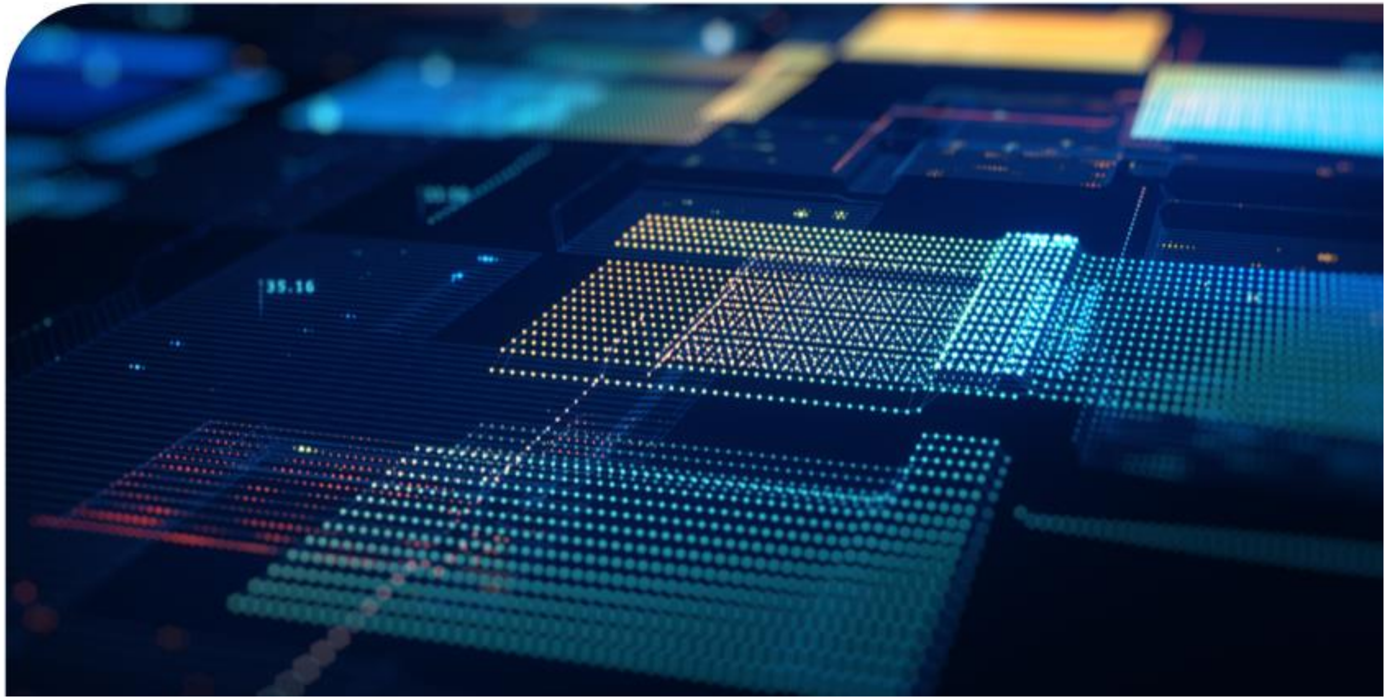
- Contracting with GenAI vendors
  - Ownership of prompts
  - Inputs not used as training data
  - Own IP in outputs
  - Output remains confidential to customers
- Contracting with other AI suppliers
  - Enhanced supplier diligence
  - Limiting risk vis a vis customers

Governance toolkit

- AI governance framework
- Oversight structures
- Global AI regulatory assessment
- AI product evaluation assessment
- Supplier diligence assessments and “rules of the road” for engaging suppliers
- Annual risk assessments and audits
- Process for sign-off of proposed new use cases for AI tools and their output

External Reporting on Responsible AI and Performance

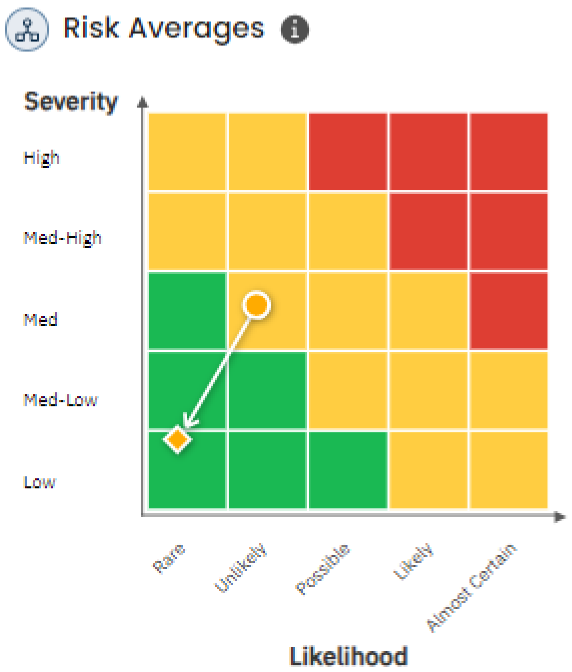
- Trust Centers
- ESG / CSR Reporting
- Codes of Conduct
- AI System Cards
- AI Model Cards
- Privacy Notice
- Others?



© Dun & Bradstreet, Inc. 2024

Metrics and Reporting

- Operational Metrics. Risk Metrics. Maturity Metrics.



27 New Applicable Data Laws Adopted

1 New certification obtained (CBPRs)

92 Ethical Culture Score

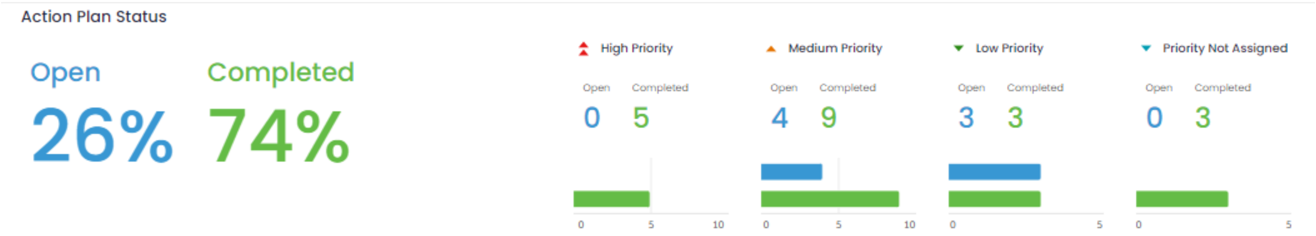
95% ▲ Employee Training Completion Rate

1 Reported Breaches or Incidents

2 Regulatory Inquiries

3,300▼ Data Subject Rights Requests

10▼ Medium-High Severity Incidents

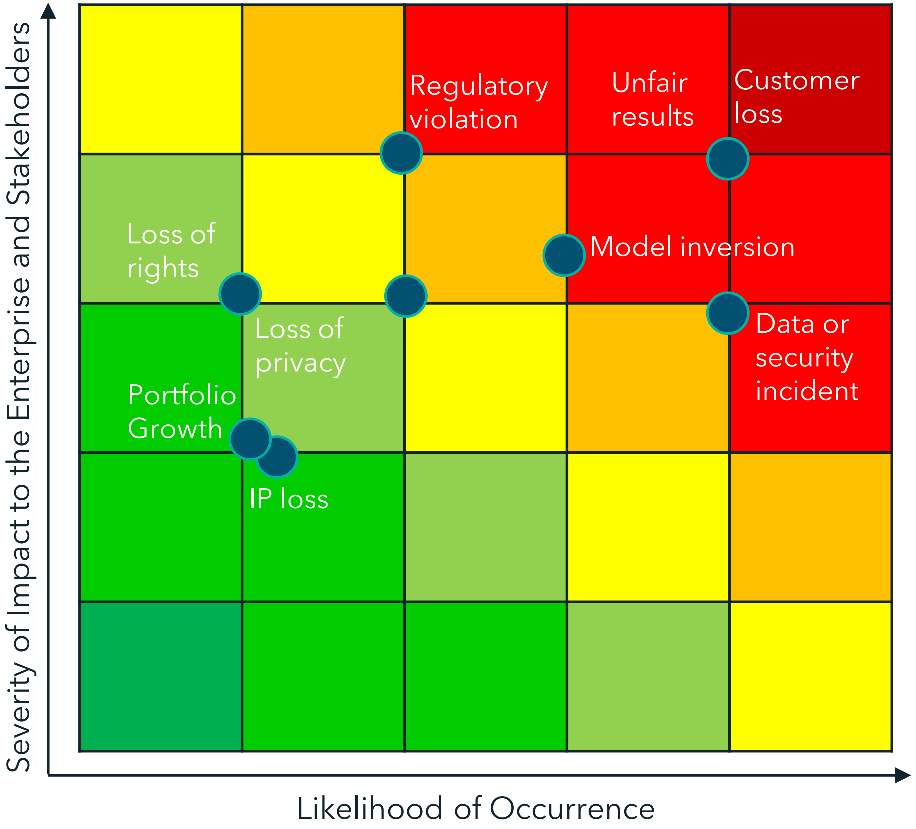

Action Plan Status

Open	Completed
26%	74%

	Open	Completed
▲ High Priority	0	5
▲ Medium Priority	4	9
▼ Low Priority	3	3
▼ Priority Not Assigned	0	3

AI Risk Management: Leveraging ERM*

- Defining a consistent risk management scale enables relative comparison of different types of risks during the AI lifecycle
- Balance Value/Benefit with Risks
- Value/Benefit: Strategic opportunities, prioritization, resource allocation, alignment with impact to stakeholders, societies, and sustainability goals
- Risks
  - Inherent
  - Residual
- Factors:
  - Severity / Impact
  - Likelihood
  - Control Effectiveness



*Heat map is a hypothetical example. Results will vary.

AI – Questions from the Board

1 AI Governance Framework

- How do we identify and evaluate potential AI tool use cases?
- How do we currently manage AI risk?

2 AI Legal & Compliance Framework

- Are we subject to any AI-specific regulations? If so, are they likely to affect our core business operations?
- What existing compliance functions are dealing with AI-related issues?
- What steps are we taking to ensure our compliance efforts are aligned with best practice?

3 AI Product Development

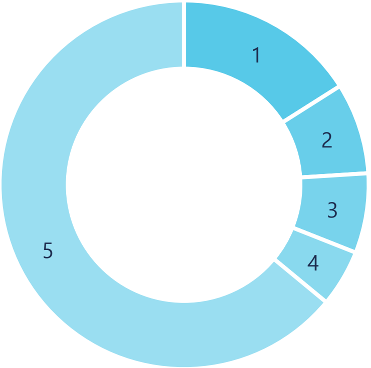
- What is our AI product development lifecycle?
- What third party suppliers do we rely on for our AI tools?
- What data do we share with AI tools?

4 AI Deployment

- How do we currently deploy AI tools?
- How do we manage, monitor and evaluate our use of AI tools and their output?

Emerging Trends in Board Oversight of AI

Board or Committee Oversight of AI*



1	Audit committee or similar	16%
2	Full board	8%
3	Risk committee	7%
4	Technology committee	5%
5	No express delegation or N/A	64%

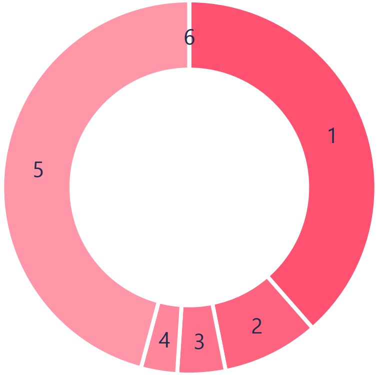
Director Expertise in AI**

13

% of S&P 500 have at least one director with AI expertise

This increases to **30%** of S&P companies in information technology (and up to **60%** in the automobile space)

Frequency of AI Topics on Board Agendas*



1	Ad hoc or as-needed basis	37%
2	Semi-annually	8%
3	Every regular meeting	4%
4	Quarterly	3%
5	Not yet an agenda item	44%
6	Other	N/A

Sources: *Deloitte and Society for Corporate Governance: Board Practices Quarterly: Future of Tech: Artificial Intelligence (2023): **ISS-Corporate AI and Board of Directors Oversight: AI Governance Appears on Corporate Radar (2024)*

Concluding Thoughts

Thank you

This material is for general information only and is not intended to provide legal advice.

© Freshfields Bruckhaus Deringer US LLP 2024