

AI Governance
Turning Accountability Into Action

October 2026

forvis mazars

Today’s Presenters

Zach Shelton, CISA, CDPSE

Principal | IT Risk & Compliance

- 19 years in Public Accounting
- Focus areas:
  - IT Consulting / Compliance
  - IT Audit / SOX
  - Cybersecurity Consulting
  - AI Governance / Use Case Development
  - AI Voice Cloning (Deepfake) Assessments



© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

Today’s Presenters

Jennifer Taylor

Director | IT Risk & Compliance

- 19 years in banking, regulatory oversight, and IT prior to joining the firm in 2022
- Focus areas:
  - Virtual CIO / CISO Advisory Servies
  - IT Risk & Compliance Consulting
  - Cybersecurity Consulting
  - AI Governance / Use Case Development
  - AI Risk Assessment, Due Diligence, Adoption, & Implementation

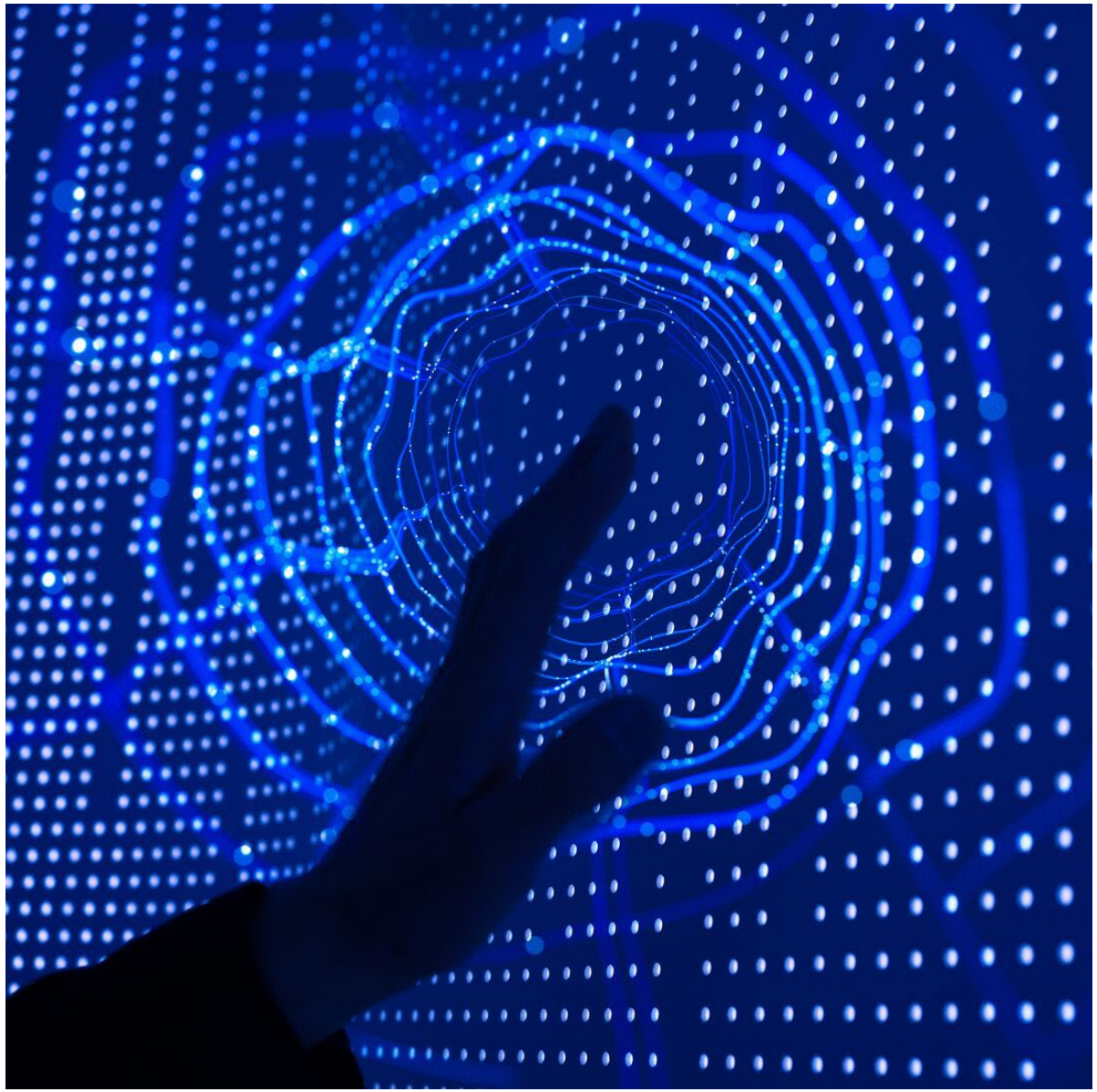


© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

Agenda

1. AI Adoption & Governance
2. Framework Alignment & Ownership
3. Control Design & Implementation
4. Third-Party AI Risk
5. Building Trust & Accountability
6. Q&A & Closing



© 2026 Forvis Mazars, LLP. All rights reserved.

AI Adoption & Governance

Implementing AI successfully in a professional setting should involve a structured AI process and a solid AI governance framework to help the technology be trustworthy, aligned with business goals, and compliant with ethical and legal standards. This requires:

- Oversight
- Data Governance
- Risk Management & Compliance
- Ethical Guidelines & Principles
- Monitoring & Reporting

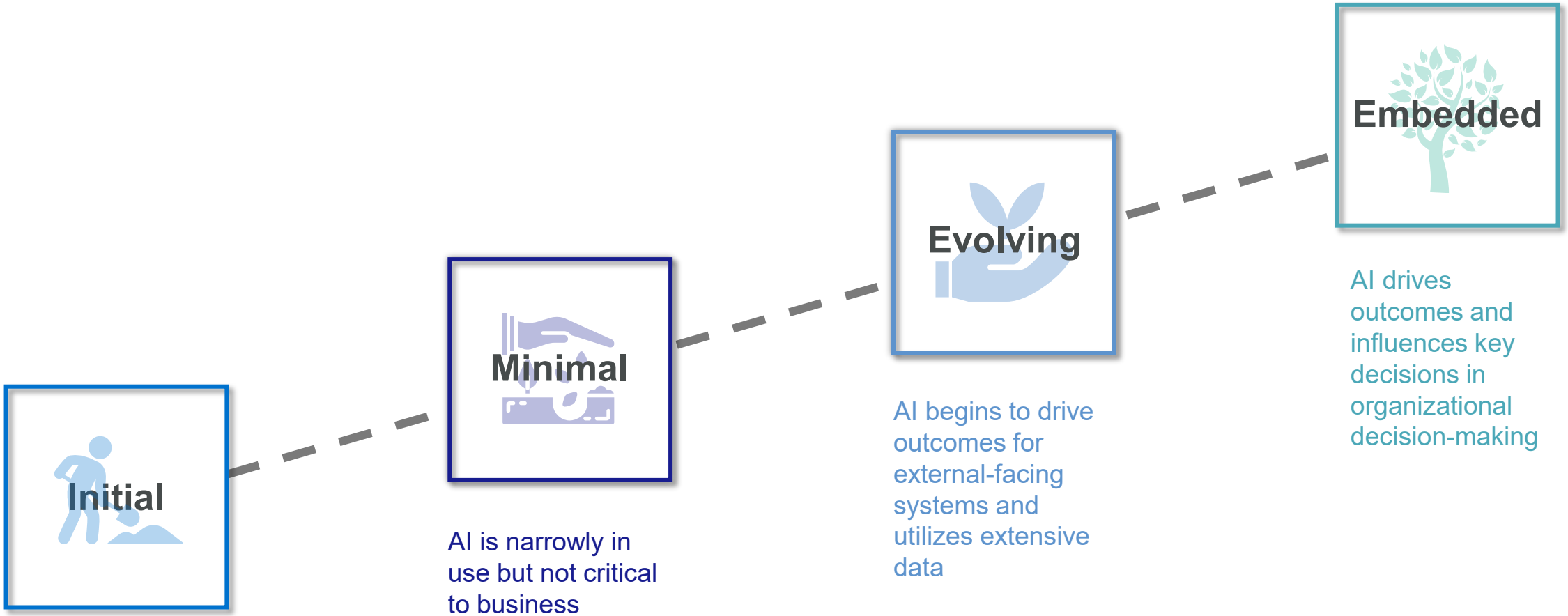


© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

AI Adoption & Governance

Governance Should Evolve With Adoption & Risk



© 2026 Forvis Mazars, LLP. All rights reserved.

AI Adoption & Governance
Why Governance Is Critical

As AI reshapes how organizations operate, real success lies in aligning innovation with accountability, clarity, and trust.

AI is transforming business.

From productivity gains to improved customer experiences, but without proper governance innovation quickly becomes exposure. Organizations need a clear, scalable approach to managing AI risks, aligning with internal values, and meeting evolving regulatory expectations.

AI governance can go beyond compliance to help provide organizational confidence.

From risk mitigation and control design to model transparency and use case oversight, effective governance enables safe, responsible, impact-driving AI adoption across the organization.

Strong AI governance turns risk into readiness—and readiness into results.



It's important to:

- **Design and build** governance programs that enable safe, effective AI use
- **Evaluate and enhance** existing frameworks to meet regulatory and business expectations
- **Assess governance maturity** against leading industry practices and regulations
- **Operationalize governance** through practical implementation of controls, roles, and oversight

© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

EVALUATE

Perform evaluations of AI systems, including performance assessments, bias detection, and validation of model accuracy and fairness.



DEVELOP

Design customized AI solutions tailored to their specific business needs.



IMPLEMENT

Manage the deployment of AI systems, considering smooth integration with existing systems and controls to enable ethical, transparent, and compliant use of AI technology.



SECURE

Identify and manage AI-specific threats, enhance data security, and test access controls to protect sensitive information used by AI Systems.



AUDIT

Audit AI systems for compliance with relevant regulations, effectiveness, and potential risks, providing recommendations for improvements.



IDENTIFY

Identify areas where AI can create value, optimize processes, and drive innovation, providing strategic insights and feasibility of different solutions.



AI GOVERNANCE

Organizations of all sizes are looking to harness the power of AI to help increase efficiency, enhance processes, & empower their teams.

At Forvis Mazars, we assist organizations with developing AI frameworks, infrastructure, & solutions in a structured & controlled manner for sustainable growth.

AI Governance

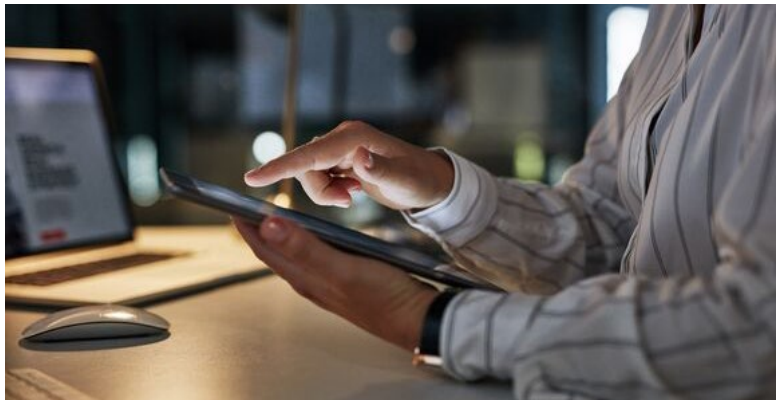
Create and implement robust governance frameworks that align with risked-based best practices and address relevant or upcoming regulations.

© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

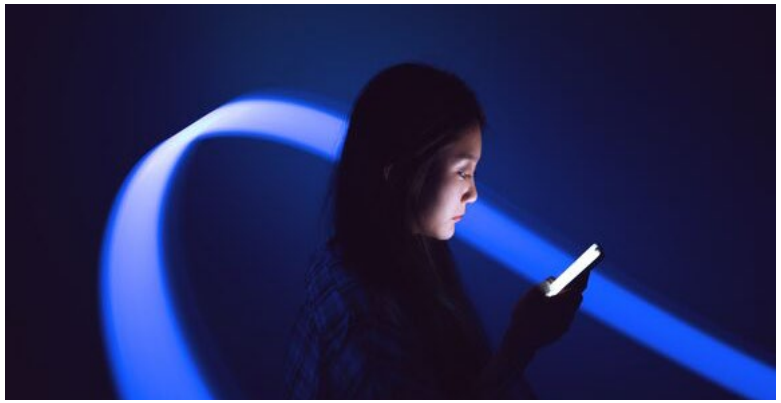
Why Governance Is Critical
AI Governance Is More Than Policy

Policy sets expectations. Governance puts them into operation.



Oversight & Accountability

Know what AI is in use, who owns decisions, and when issues should escalate.



Risk & Data Governance

Apply risk, privacy, security, and data expectations throughout the AI lifecycle.



Monitoring & Evidence

Track performance, exceptions, and changes, and retain evidence that controls operate.

© 2026 Forvis Mazars, LLP. All rights reserved.

Framework Alignment

Three Frameworks, One Governance Strategy

Think of CSF as the board-level governance language, AI RMF (Risk Management Framework) as the AI risk framework, and CRI as the financial-services implementation guide.

Framework	What It Does	Why Executives Care
NIST CSF 2.0 Govern	Provides enterprise governance and risk oversight outcomes.	Connects AI to existing cyber, risk, and governance programs.
NIST AI RMF 1.0	Provides AI-specific guidance for managing risk and supporting trustworthy AI across the lifecycle.	Helps organizations map context, measure risk, and manage priorities over time.
CRI Financial Services AI RMF	Translates AI RMF concepts into financial-services-specific control objectives and maturity stages.	Provides financial institutions with an implementation roadmap.

© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

Framework Alignment

NIST CSF Govern Is the Connective Thread

01

Organizational Context

AI priorities connect to mission, risk appetite, and stakeholder expectations.

02

Risk Strategy

AI risks are prioritized within enterprise risk management.

03

Roles & Policy

Decision rights, accountability, and policy expectations are explicit.

04

Oversight

Performance, exceptions, and risk decisions reach leadership.

05

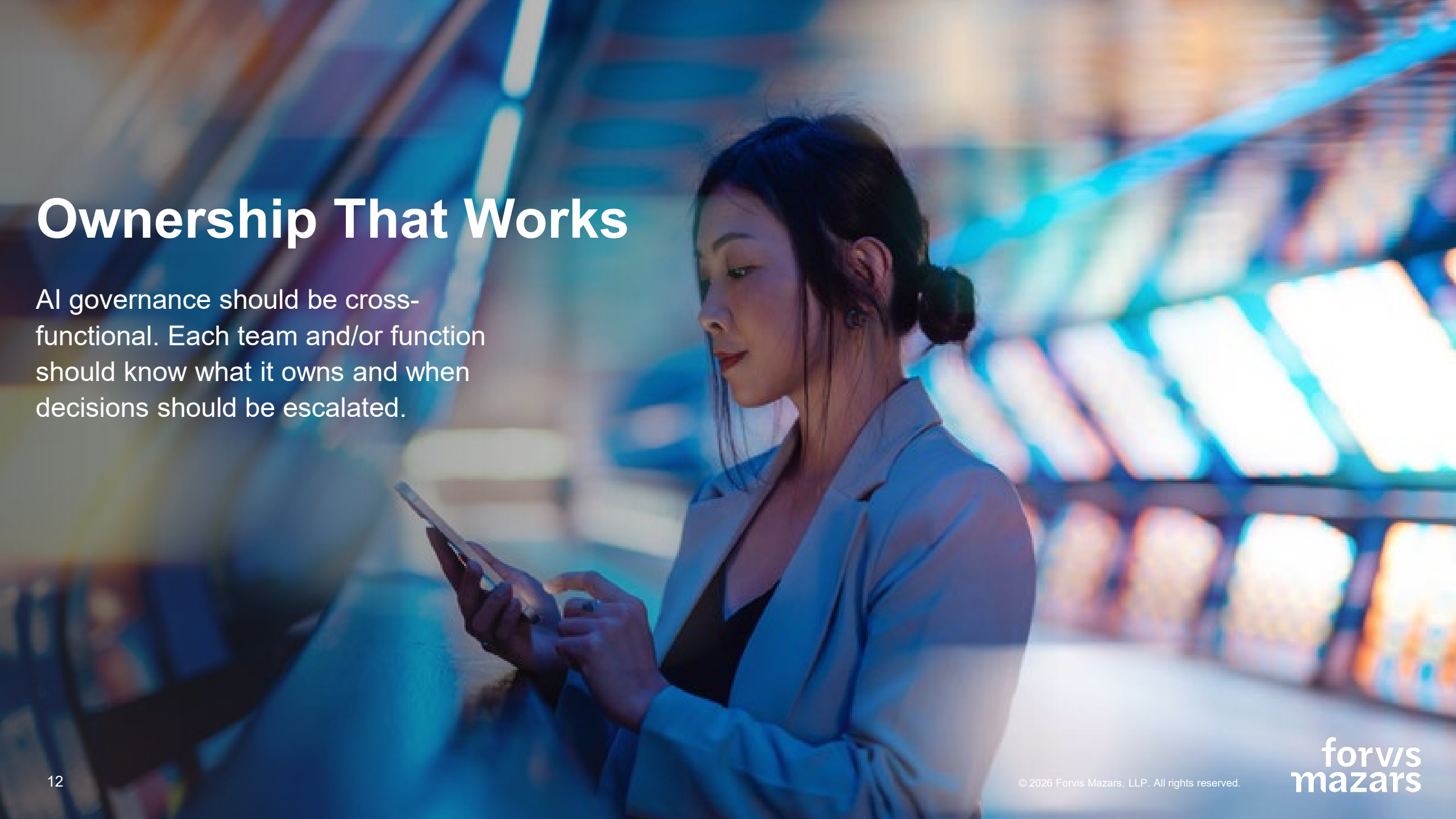
Supply Chain

Third-party AI expectations are integrated into vendor oversight.

© 2026 Forvis Mazars, LLP. All rights reserved.

Ownership That Works

AI governance should be cross-functional. Each team and/or function should know what it owns and when decisions should be escalated.



© 2026 Forvis Mazars, LLP. All rights reserved.

Ownership

Shared Ownership Helps Prevent Siloed Accountability

Board & Executive Leadership

Set risk appetite, receive reporting, resolve enterprise tradeoffs

AI Steering Committee

Prioritize use cases, approve standards, resolve cross-functional issues

Business & Product Owners

Own intended use, outcomes, human oversight, and process controls

Risk, Compliance, & Legal

Interpret obligations, provide independent challenge, and set second-line oversight expectations

Technology, Data, & Security

Manage architecture, access, data, resilience, testing, and logging

Internal Audit

Provide independent assurance over design and operating effectiveness

© 2026 Forvis Mazars, LLP. All rights reserved.



Control Design & Implementation

Control design translates governance expectations into repeatable, day-to-day operating practices, supported by evidence that shows controls are working.

© 2026 Forvis Mazars, LLP. All rights reserved.

Control Design
From Framework to Daily Operations

You cannot govern what you have not identified.

01	02	03	04	05	06
Inventory	**Classify**	**Approve**	**Control**	**Monitor**	**Respond**
What AI exists?	What could go wrong?	Who accepts the risk?	How is exposure reduced?	What signals matter?	Who acts when thresholds are crossed?

Evidence follows the loop: owner, rationale, approval, test result, exception, and response.

© 2026 Forvis Mazars, LLP. All rights reserved.

Control Design

Control Examples by Risk Area

Inventory & Intake

Inventory approved tools, shadow AI, and embedded AI features; name business and technical owners

Data & Privacy

Approved data sources; classification; retention; access and leakage controls

Model & Output

Performance thresholds; bias and robustness testing; human review; change control

Security & Resilience

Least privilege; logging; incident playbooks; fallback and decommissioning

Third Party

Data-use terms; model and feature changes; monitoring evidence; incident duties; exit plans

© 2026 Forvis Mazars, LLP. All rights reserved.

Implementing AI Governance

Implementing AI governance means taking key steps so AI systems are developed and used responsibly. Following best practices can help organizations build a strong governance structure that supports responsible AI.

01

Use a Solid Framework

- Define roles & responsibilities for AI oversight
- Create a governance structure that aligns with institutional values

02

Define Governance & Acceptable Use

- Set standards for data quality, security, & privacy
- Document data sources & maintain transparency

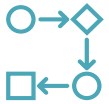
03

Integrate Operational Strategy & Risk Management

- Embed governance into workflows & decision-making
- Monitor AI tools for compliance, bias, & unintended outcomes

© 2026 Forvis Mazars, LLP. All rights reserved.

Implementing AI Responsibly
AI Governance & Risk Management



01

AI Governance

- Develop clear AI policies & procedures
- Establish a governance structure with defined roles
- Identify & manage AI risks
- Promote transparency & fairness
- Implement security controls
- Align AI use with ethical standards



02

NIST Framework

- Apply NIST guidelines to manage AI risks
- Define & uphold AI trustworthiness & security
- Support compliance & follow regulations
- Promote responsible AI practices



03

IT Audit

- Assess AI model implementation
- Analyze data handling & security
- Review governance effectiveness
- Recommend improvements
- Provide assurance to stakeholders

© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

Discussion

Where Accountability Becomes Real



1. Who can approve an AI use case, and who can stop it?
2. What evidence should executives receive without drowning in detail?
3. Where do existing controls already cover AI risk?
4. Which AI risks require new controls or new ownership?

© 2026 Forvis Mazars, LLP. All rights reserved.

Third-Party AI Risk

Explore how to govern the model, the vendor, the data path, and the dependency.



© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

Third-Party AI Risk

The Vendor Is Only One Layer of the Dependency

Provider	Model	Data Path	Integration	Operations
Contract, ownership, financial, and operational stability	Training sources, limitations, evaluation, and change	Inputs, retrieval sources, storage, retention, and residency	APIs, plugins, identities, permissions, and downstream actions	Monitoring, incidents, support, continuity, and exit

© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

Third-Party AI Risk
Questions That Reveal Control Posture

Transparency
What model, data sources, and subprocessors support the service?

Change
How will we learn about material model, feature, or control changes?

Control
What can we configure, restrict, monitor, and independently test?

Evidence
What documentation, logs, validation, and assurance can the provider supply?

Resilience
What happens during degradation, outage, compromise, or provider exit?

Accountability
Who owns the decision when model behavior and business process intersect?

© 2026 Forvis Mazars, LLP. All rights reserved.

Financial Services
CRI, AI RMF, Control Objectives

The CRI Financial Services AI RMF translates NIST AI RMF outcomes into sector-specific control objectives, matched to adoption stage and supported by evidence.

Adoption Stage

Initial → Minimal → Evolving → Embedded

Risk & Control Matrix

230 control objectives linked to risks and guidance

Reference Material

Illustrative controls and evidence to support implementation



How to use it:

- **Confirm** the organization's adoption stage
- **Select** control objectives that match risk and maturity
- **Map** current evidence and control ownership
- **Prioritize** gaps and sequence remediation
- **Reassess** as AI use and dependencies change

Building Trust & Accountability

Accountability Should Be Visible at Three Levels

Trust grows when each level receives the information and authority needed to act.

Executive	Risk appetite, strategic tradeoffs, material exceptions, and trends
Program	Inventory, decisions, ownership, control status, and third-party posture
Use Case	Intended use, data, testing, human oversight, monitoring, and response

© 2026 Forvis Mazars, LLP. All rights reserved.

Key Takeaways

Accountability is clearer when ownership, controls, and evidence work together.

Identify & Govern

Inventory approved tools, shadow AI, embedded features, use cases, and third-party providers.

Assign Decision Rights

Name business, technical, and risk owners. Define challenge, escalation, and stop authority.

Extend Oversight

Treat third-party AI, model changes, dependencies, and exit planning as ongoing governance matters.

© 2026 Forvis Mazars, LLP. All rights reserved.

AI Governance Framework Enablement

Establish the foundational AI governance structure for responsible adoption

We build on a governance enablement approach used in similar engagements to stand up an initial AI governance framework tailored to your current maturity, strategic priorities, and operating model. The framework provides a practical starting point that supports responsible adoption and ongoing oversight, rather than a one-size-fits-all end state.

Phase 1: Structure & Stakeholders

Define the governance structure, sponsorship, and decision rights for AI:

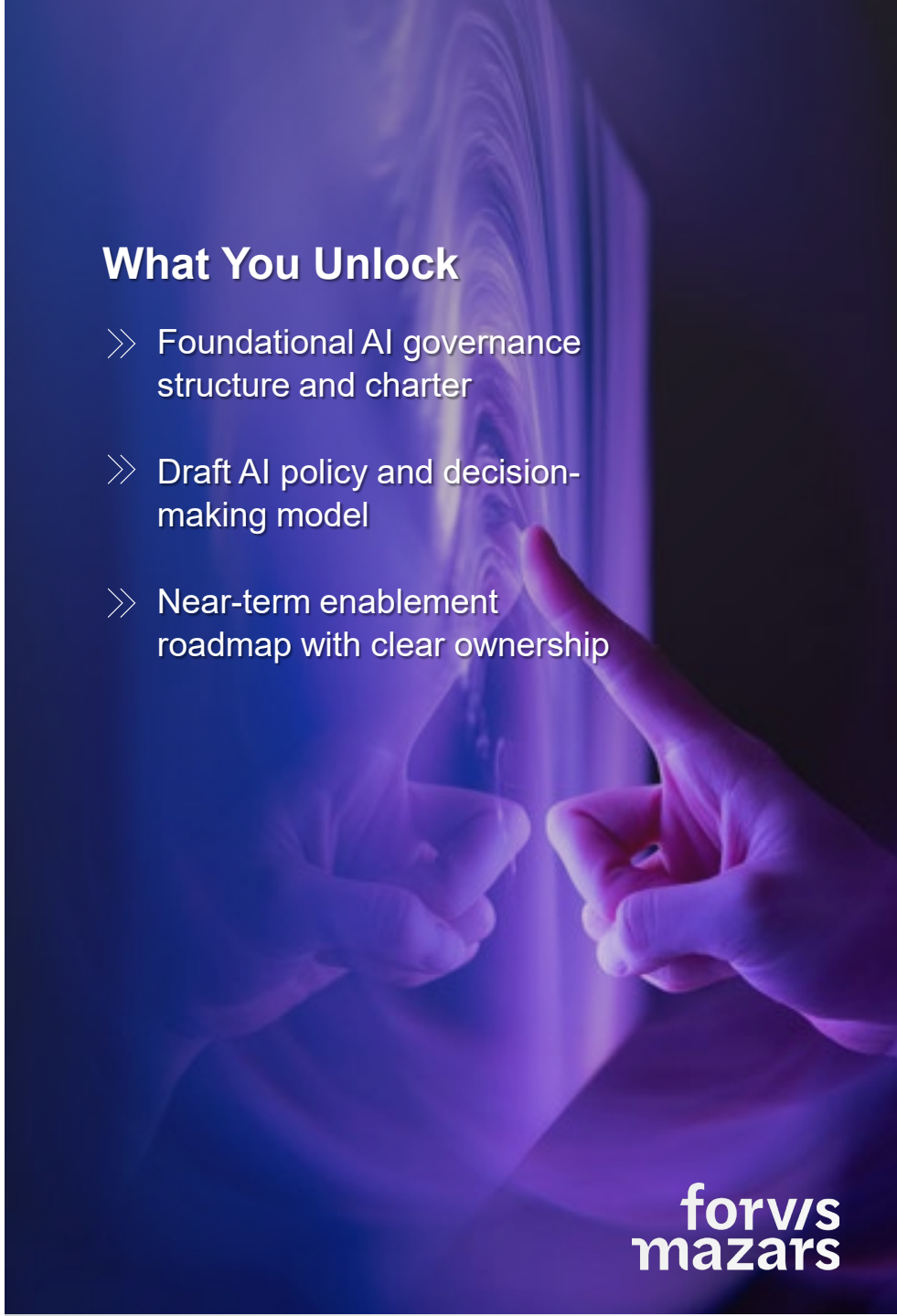
- **Sponsorship & Committee -** Define executive sponsorship, steering committee scope, working group participation, and escalation paths
- **Stakeholder Alignment -** Confirm roles across business, risk, compliance, IT, and data teams and align on decision rights
- **Operating Model -** Align governance to strategic priorities, regulatory environment, and functional use cases across clinical, operational, and support areas

Phase 2: Artifacts & Policy

Develop foundational artifacts including an AI governance charter, steering committee purpose statement, draft policy hierarchy, and decision-making model, plus draft or review AI-focused policy aligned to organizational needs and best practice

Phase 3: Operating Model & Roadmap

Stand up AI inventory, risk intake, use case review, third-party oversight, and documentation processes, and deliver a governance enablement roadmap with near-term foundational actions, ownership, and priorities



AI Risk Management Framework Gap Assessment

Evaluate AI governance and risk management maturity against NIST AI RMF

We deliver a structured, phased engagement that assesses AI governance maturity against the NIST AI RMF v1.0, leveraging the CRI Financial Services AI RMF Profile to map functions to specific, implementable controls. This combination helps us assess the organization's current state and identify considerations for improvement.

Phase 1: Document Requests & Discovery

Establish a baseline and validate observations against actual practices:

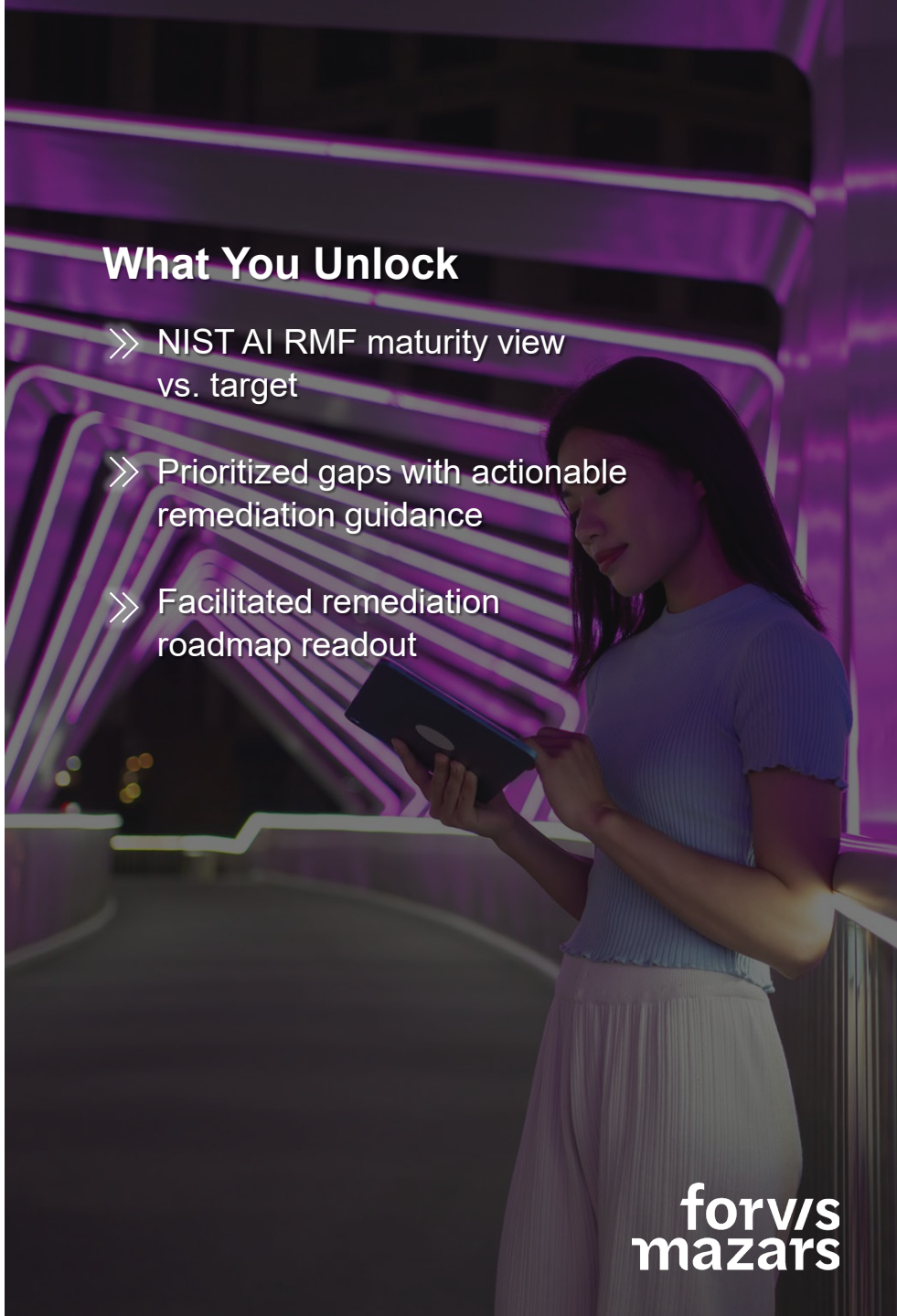
- **Document Requests -** AI policies, system inventories, risk assessments, training materials, and vendor agreements
- **Stakeholder Interviews -** Walkthroughs across business, risk, compliance, IT, and data teams structured around Govern, Map, Measure, and Manage
- **Maturity Tier Goal -** Define target maturity tier for gap identification and assess governance structures, third-party oversight, and monitoring practices

Phase 2: Processing & Gap Assessment

Score each subcategory against CRI maturity tiers (Initial through Embedded), catalog gaps across Govern, Map, Measure, and Manage, and develop prioritized, actionable recommendations

Phase 3: Presenting Results

Deliver an executive-ready assessment report with overall maturity view, domain observations, prioritized gaps mapped to NIST subcategories, and a facilitated readout to align on a remediation roadmap. Following the Gap Assessment, Forvis Mazars can assist in the integration and ongoing review of the appropriate controls.



Q&A



IT Risk & Compliance

Questions?

© 2026 Forvis Mazars, LLP. All rights reserved.



Don’t Miss the Next Session of the

2026 Cybersecurity Virtual Symposium

Ransomware & Extortion: Preparing for Multifront Attacks

Today at 11:15 a.m. - 12:15 p.m. ET

© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

Contact

Forvis Mazars

Zach Shelton
Principal
zach.shelton@us.forvismazars.com

Jennifer Taylor
Director
jennifer.taylor@us.forvismazars.com

The information set forth in this presentation contains the analysis and conclusions of the author(s) based upon his/her/their research and analysis of industry information and legal authorities. Such analysis and conclusions should not be deemed opinions or conclusions by Forvis Mazars or the author(s) as to any individual situation as situations are fact-specific. The reader should perform their own analysis and form their own conclusions regarding any specific situation. Further, the author(s)' conclusions may be revised without notice with or without changes in industry information and legal authorities.

© 2026 Forvis Mazars, LLP. All rights reserved.