

ERP Security

Protecting an Expanding Attack Surface

October 2026

forvis mazars

Today’s Presenters



Ben Sady
Principal, IT Risk & Compliance
804.474.1267
ben.sady@us.forvismazars.com



Martin van de Pol
Principal, Business Technology Services
615.973.8292
martin.vandepol@us.forvismazars.com

© 2026 Forvis Mazars, LLP. All rights reserved.

Learning Objectives

Everything that follows maps back to these three.



Recognize the cyber risks associated with modern ERP systems, across cloud, integrations, identity, and data.



Identify common ERP security and control gaps before, during, and after go-live.



Apply security and governance practices and tools that support ERP security as systems evolve.

© 2026 Forvis Mazars, LLP. All rights reserved.

ERP Security
Why This Matters Now

Cyber risk isn’t confined to IT. It extends to financial, continuity, privacy, compliance, and audit areas.

Modern Enterprise Resource Planning Technology

- Modern ERP systems have advanced capabilities
- The systems can integrate and support finance, procurement, CRM, and HR functions
- With SaaS systems, there’s generally continual vendor-driven change
- As the technology has become more intricate, your control environment may be lagging



© 2026 Forvis Mazars, LLP. All rights reserved.

The Promise of Modern ERP
Future-State Expectations

Faster

Technology-Driven Operations

Consistent processes across entities and functions, with faster, more reliable reporting to support better decisions.

Automated

Streamlined Workflows

Manual workflows, approvals, and reconciliations move into the system, so controls are enforced by design rather than by reminder.

Scalable

Room to Grow

Greater resilience and access to new capabilities, with connectivity across finance, HR, procurement, operations, customers, and vendors/partners.

Each of these elements also deepens dependence on user/AI access, system integrations, data, cloud services, and more.

© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

The Expanding Attack Surface

Modernization doesn’t just add risk, it adds attack surface. Every cloud tenant, integration, identity, data store, and AI agent is another way in.



© 2026 Forvis Mazars, LLP. All rights reserved.

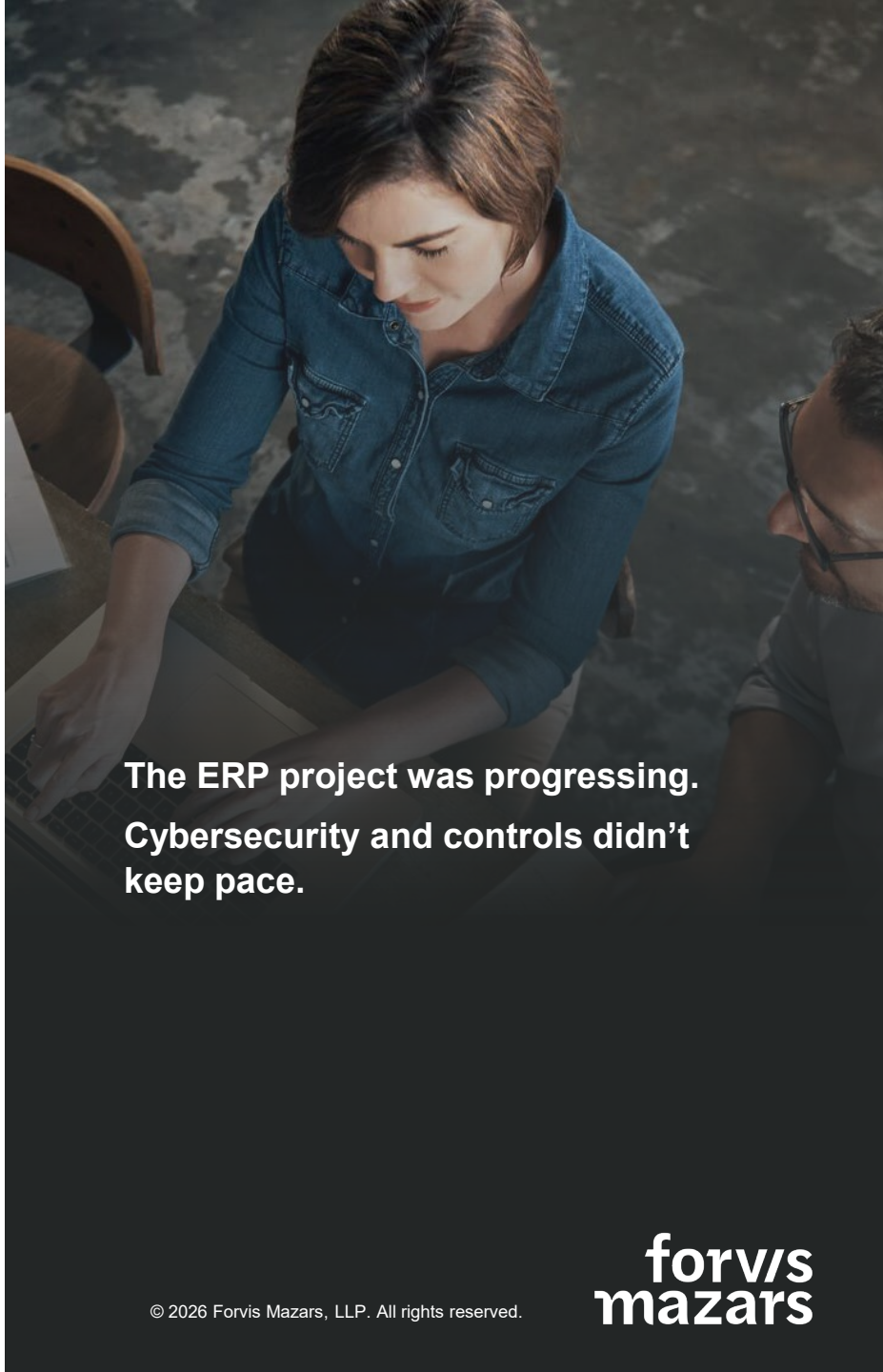
forvis mazars

An Illustrative Story
The ERP Go-Live That Looked Ready

A large organization is weeks from a cloud ERP go-live. The plan is green, processes are mapped, and integrations are being tested.

Cybersecurity Headwinds

- **Excessive Access**: Privileged access is broader than expected
- **Incomplete Segregation of Duties**: Rules haven't been tailored to the business
- **Uncertain Integrations**: Third-party connections haven't been assessed for risk
- **Inconsistent Logging**: Events are captured but exceptions can go unreviewed
- **Scattered Evidence**: Approvals live outside the system and in emails and spreadsheets



© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

Anatomy of the Expanded Attack Surface

Cloud Adoption

The perimeter moves to the vendor. Tenant configuration, identity, and the shared-responsibility seam become the exposed edge.

Guarded by SSPM, tenant baselines, and PAM

Expanding Integrations

Every API, file transfer, and third-party platform is an entry point, often authenticated by a standing service account.

Guarded by API gateways and secrets vaulting

Rapid Change

Continuous vendor releases and emergency changes reopen the surface faster than testing and approvals can close it.

Guarded by release governance and control retesting

Automation & Workflow

Approvals execute without a human in the loop, so one flawed configuration scales a bad decision instantly.

Guarded by configuration change control and SoD analysis

Embedded AI

Copilots and agents reach across ERP data with the user's rights, widening exposure to leakage and unreliable output.

Guarded by scoped agent identities and use-case approval

Data Centralization

One platform concentrates finance, HR, and vendor data, so a single access failure becomes an enterprise-wide loss.

Guarded by IAM, IGA, encryption, and data masking

© 2026 Forvis Mazars, LLP. All rights reserved.

ERP Cyber Risk
Balancing the Equation

A quick diagnostic for an ERP program: what pushes risk up, and what brings it back down.

Risk increases when …

- More users have access
- More systems are integrated
- More data is centralized
- More changes happen quickly
- More vendors support the environment
- More controls depend on configuration and workflows

Risk decreases when …

- Ownership is clear
- Access is governed
- Changes are controlled
- Integrations are monitored
- Evidence is automated
- Exceptions are reviewed
- Governance continues after go-live

© 2026 Forvis Mazars, LLP. All rights reserved.

Controls

Gaps & How to Close Them

Role Design

Built for implementation speed, not least privilege

Rebuild roles from privileges and duties

Segregation of Duties

Rules never tailored to the business

Tune the ruleset, enforce at provisioning

Joiner, Mover, Leaver

Disconnected from ERP role assignment

Wire ERP roles to identity so exits revoke access

Change Evidence

Approvals exist, but evidence is inconsistent

Capture approvals in the system of record

Emergency Changes

Poorly controlled, rarely reviewed after the fact

Time-box access, review every session

Interfaces

Treated as technical tasks, not control points

Inventory, risk-rate, and monitor each

Log Review

Logging enabled, exceptions unreviewed

Alert on what matters, clear the queue on a cadence

Ownership

Unclear once the project team stands down

Name owner, frequency, and evidence up front

© 2026 Forvis Mazars, LLP. All rights reserved.

Access & Identity Management
The Highest-Volume, Highest-Frequency ERP Risk

#1

Access & Identity

Identity governance, role design, privileged access, MFA, and access review.

What Matters

- ERP security depends on identity governance, role design, privileged access, MFA, and periodic access review
- Role-based access control isn't enough if roles are overbuilt or poorly governed
- Segregation of duties should be business-relevant
- Privileged access should be limited, monitored, and approved

Efficient Ways to Manage

- IAM and IGA platforms for provisioning, de-provisioning, and certification
- SSO and MFA integration
- Privileged access management for administrative roles
- Automated SoD analysis and role mining
- Access review dashboards for owners and auditors

© 2026 Forvis Mazars, LLP. All rights reserved.

Access & Identity Management
Microsoft Dynamics 365 Finance

Dynamics 365 pairs role-based access with cloud identity to help protect financial and other data.

1

Role-Based Security

Permissions roll up into privileges, duties, and roles.

2

Segregation of Duties

No single user controls a whole critical process.

3

Temporary Role Management

Time-boxed elevated access that expires automatically.

4

Audit Trails

A tamper-resistant log of who changed access and when.

Cloud & Infrastructure Safeguards

- **Identity Management**: Cloud directories verify logins and block weak credentials
- **Security Snapshots**: Version security settings to compare or roll back changes
- **Continuous Monitoring**: Cloud security teams watch for abnormal activity and help aid recovery

Source: Microsoft Learn, Dynamics 365 Security Architecture & Role-Based Security guides. Illustrative of one platform; principles apply broadly.

© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

An Illustrative Story
Migrating From GP to Dynamics 365 Finance

Moving from on-premises Dynamics GP (v18.8) to cloud Dynamics 365 Finance is a full cloud implementation, not a one-click upgrade.

What Changes

- An on-premises SQL Server system becomes a cloud enterprise platform
- Fixed account segments give way to a main account plus financial dimensions
- Legacy user classes are re-mapped to cloud role-based security
- Customizations and third-party add-ons are reassessed for the cloud

Source: Microsoft Learn, Migration guidance. Illustrative sequence; validate for any specific environment.



Where Security Is Rebuilt

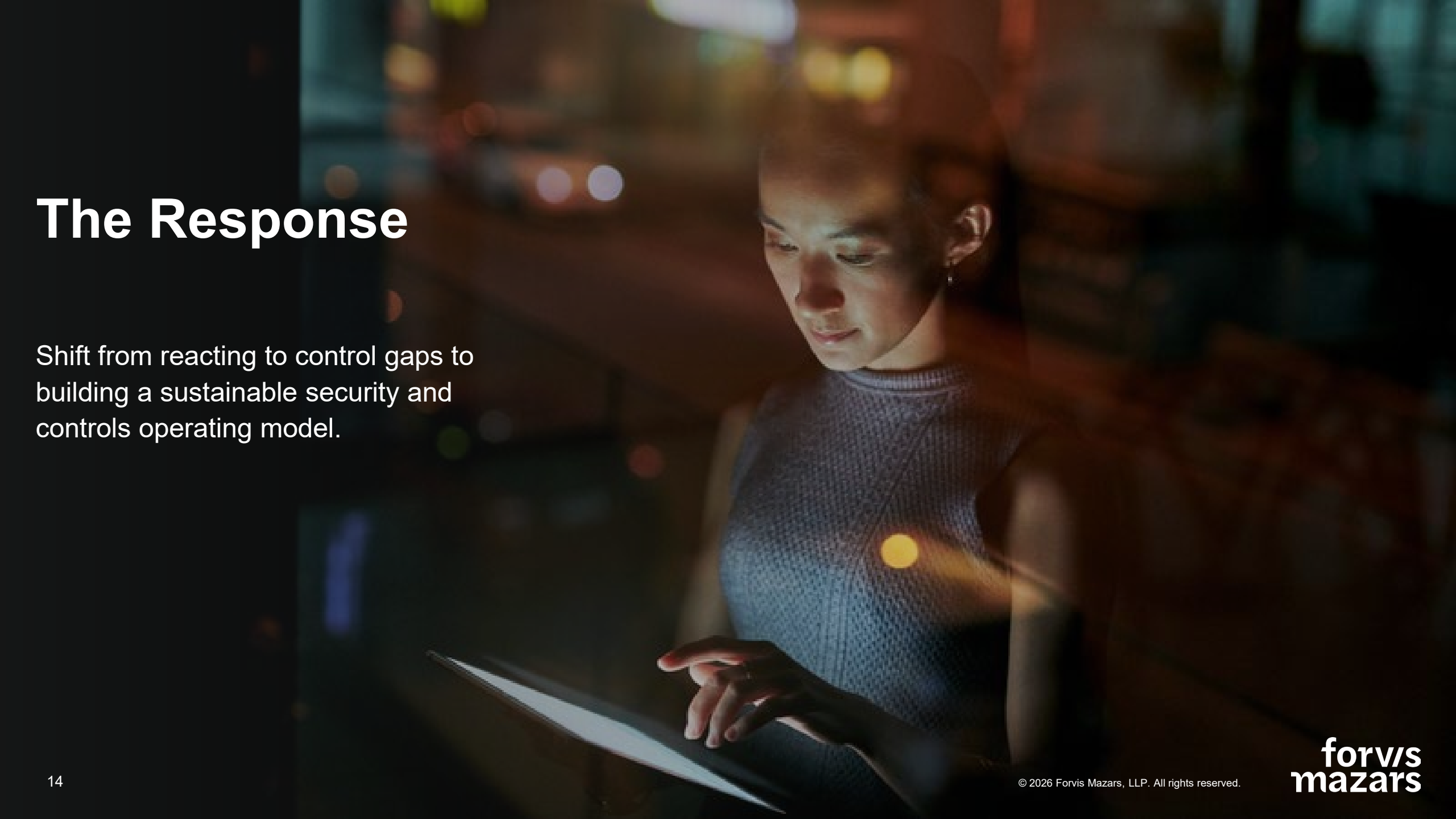
- Build cloud-native roles from privileges and duties, not a lift-and-shift
- Set shared currencies, calendars, and address books consistently
- Validate access and controls in conference room pilots before cutover
- Freeze legacy entry, run a final delta load, then reroute identity and APIs

© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

The Response

Shift from reacting to control gaps to building a sustainable security and controls operating model.



© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

Strengthening Security
Securing the Surface as It Expands

If you only change one thing about how your ERP program treats security, change this.

Every new connection, identity, and data flow should arrive with an owner and a control, so the surface is secured as it expands rather than after.

1. **Inventory the Surface**: You cannot protect what was never mapped, so keep a live view of every tenant, integration, identity, privileged role, and data flow
2. **Control Every New Entry Point**: Assign each new connection, identity, and data flow a named owner, a least-privilege access model, and appropriate monitoring
3. **Assume It Keeps Growing**: Vendor releases, new integrations, and AI agents widen the surface continuously, so assessment and monitoring run on a cadence rather than as a go-live gate



Secure the surface as it grows, and access, change, integrations, data, and monitoring stop being five separate problems.

© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

The Framework
ERP Risk Domains to Organize Around

- Governance & Oversight
- Access & Identity
- Change & Release
- IT & Cloud Operations
- Application & Workflow Controls

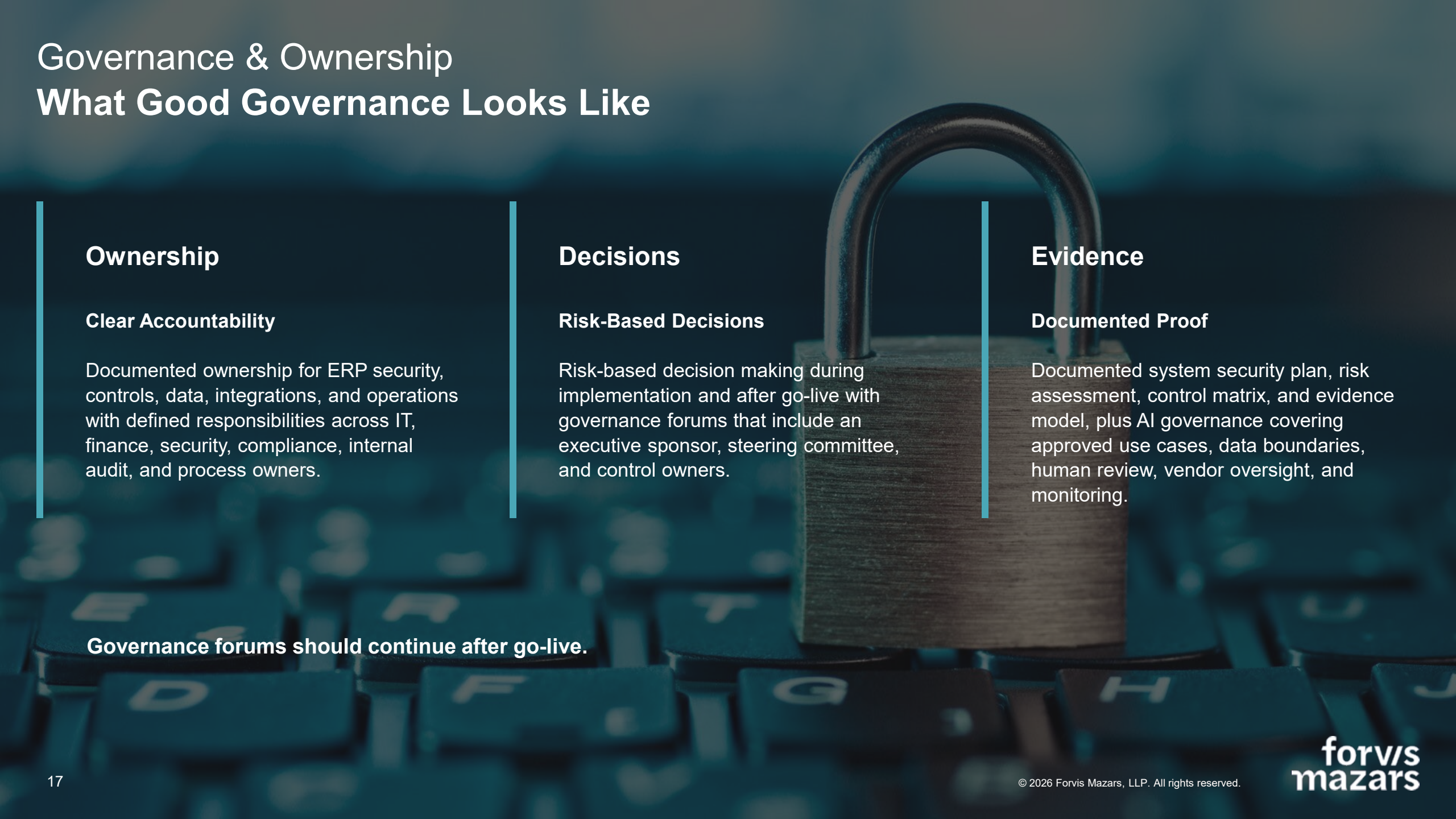
Modern ERP

AI and automation governance cut across each domain.

- Data Protection & Privacy
- Integration & API Security
- Monitoring & Continuous Improvement
- AI & Automation Governance

© 2026 Forvis Mazars, LLP. All rights reserved.

Governance & Ownership
What Good Governance Looks Like



Ownership

Clear Accountability

Documented ownership for ERP security, controls, data, integrations, and operations with defined responsibilities across IT, finance, security, compliance, internal audit, and process owners.

Decisions

Risk-Based Decisions

Risk-based decision making during implementation and after go-live with governance forums that include an executive sponsor, steering committee, and control owners.

Evidence

Documented Proof

Documented system security plan, risk assessment, control matrix, and evidence model, plus AI governance covering approved use cases, data boundaries, human review, vendor oversight, and monitoring.

Governance forums should continue after go-live.

© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

ERP Cyber Risk
Where to Focus Before & After Go-Live

The ideal time to address ERP risk is before go-live. Value comes from maintaining controls after.

Before Go-Live

- Security design
- Role design and segregation of duties
- Integration inventory
- Data migration risk
- Application, API, and penetration testing
- Change governance
- Control matrix
- Logging requirements
- Security tooling plan (IAM, PAM, SSPM)

After Go-Live

- User access reviews
- Continuous monitoring
- Incident and exception management
- Control testing
- Retesting after material changes and remediation
- Production support metrics
- Audit evidence and remediation
- Governance cadence
- Posture monitoring and privileged access review

© 2026 Forvis Mazars, LLP. All rights reserved.

Building an ERP Security & Controls Roadmap

Define & Assess

01 Set Requirements

Security requirements defined with the process, data, and integration design

02 Assess Risk

Identify cyber, operational, compliance, privacy, and financial reporting risks

Design & Validate

03 Map Controls

Build or update the ERP risk and control matrix, naming the tooling that enforces each control, such as IAM, PAM, SSPM, and GRC

04 Validate Design

Confirm controls are properly designed before go-live

05 Test Operating Effectiveness

Validate evidence, ownership, frequency, and execution

Sustain

06 Automate & Monitor

Use GRC, IAM, IT service management, monitoring, and support automation

07 Continuously Improve

Track issues, metrics, control failures, audit findings, and emerging risks

© 2026 Forvis Mazars, LLP. All rights reserved.

ERP Security & Controls Roadmap
Four Critical Disciplines

Build Security Into Change Management

Set security requirements at design, hold stage gates at each milestone, and apply formal criteria before and after go-live.

Maintain a System Security Plan

Keep one reference for ERP security architecture, responsibilities, and controls that leadership, auditors, and regulators can work from.

Map Risks to Controls & Owners

Tie each risk to a control with a named owner, frequency, and evidence so accountability can outlast the implementation project team.

Validate Independently

Confirm control design before go-live and operating effectiveness after, including application, API, and penetration testing scoped to exposure.

© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

Key Takeaways

Recognize the risks, close the gaps, and secure the surface as ERP evolves.

Mission-Critical Core

- ERP sits at the center of finance, operations, supply chain, and reporting
- A breach or control failure can create enterprise-wide operational, financial, and data exposure

Expanding Attack Surface

- Cloud platforms, integrations, and high-value data flows widen the ERP attack surface
- Defenses have to sit inside ERP, not just around it

Securing the Surface

- Governed access, controlled change, and monitored integrations close the ways in
- Ownership, evidence, security tools, and continuous monitoring keep them closed as the system evolves
- Anchored by a system security plan, an IT risk and control matrix, and independent security assessments

© 2026 Forvis Mazars, LLP. All rights reserved.



IT Risk & Compliance

Questions?

© 2026 Forvis Mazars, LLP. All rights reserved.

Thank you for joining our

2026 Cybersecurity Virtual Symposium

Looking for more?

Don’t Miss **AI in SOC Examinations: Automation & Audit Judgment**

Tuesday, October 27, 2–3 p.m. ET

© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

Contact

Forvis Mazars

Ben Sady
Principal, IT Risk & Compliance
P: 804.474.1267
ben.sady@us.forvismazars.com

Martin van de Pol
Principal, Business Technology Services
P: 615.973.8292
martin.vandepol@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.