Securing Modern ERP

Cyber Risk in ERP Transformation

September 2, 2026

forvis mazars

YOUR SPEAKER

Ben Sady

Principal — cybersecurity, IT risk, controls, privacy, and regulatory compliance

What I do

- Lead ERP security, risk assessment, control design, and compliance initiatives
- Advise on cybersecurity, IT risk, controls, privacy, and regulatory compliance
- Help finance, audit, IT, and business leaders translate cyber risk into action

How I work

“My work sits at the intersection of technology, risk, controls, and the business, particularly where organizations are making major changes and need the control environment to keep pace.”

WHERE THIS COMES FROM

What I used to believe — and what changed

Based on my experience with ERP programs, earlier decisions about security and controls can support better program outcomes.

The old way — security only as a gate

- Security joined the program at user acceptance testing
- Controls were documented after the configuration was frozen
- Risk was a project checklist item, not a business responsibility
- Go-live was treated as the finish line
- Security findings became post-go-live remediation projects

What changed — security as a design requirement

- Security requirements enter at design, beside process and data
- Controls are built into the configuration, not bolted on after
- Ownership is named before go-live and survives it
- Go-live is the start of the run state, not the end of the work
- Evidence is produced by the system, not assembled for the auditor

The programs that went well did not have more controls. They decided earlier.

LEARNING OBJECTIVES

What you will take away

Three objectives frame the session.

01

Understand the risk shift

Explain how ERP modernization introduces cyber risk across cloud, integrations, identity, and data.

02

Spot the breakdowns

Identify where controls commonly break down before, during, and after go-live.

03

Apply what works

Apply practical approaches to strengthen ERP security, controls, and governance.

Everything that follows maps back to these three.

Section 01

The promise

ERP modernization is positioned as a path to greater efficiency, reporting, automation, and scalability.

WHY NOW

Why this topic matters now

In many organizations, cyber risk extends beyond the IT layer and can affect financial reporting, continuity, privacy, compliance, and audit readiness.

Legacy ERP — a closed system

- Largely on-premises and self-contained
- Change was slow and infrequent
- Access and controls lived inside one boundary
- Interfaces were often fewer and more centralized

Modern ERP — a connected ecosystem

- Cloud and SaaS delivery with shared responsibility
- Integrations across HR, CRM, finance, procurement, and data platforms
- Identity, workflow, and API dependent
- Continuous vendor-driven change

The system got more capable. The control environment has to keep up.

THE PROMISE

The promise of modern ERP

A future state leadership may expect, with benefits that can change what the organization depends on.

01

Standardize

- Consistent processes and a common operating model across entities and functions.
- Faster, more reliable reporting and better decision support.

02

Automate

- Manual workflows, approvals, and reconciliations move into the system.
- Controls can be enforced by design rather than by reminder.

03

Scale and connect

- Greater resilience and access to new capabilities.
- Connectivity across finance, HR, procurement, operations, customers, and partners.

Every benefit also deepens dependence on access, data, integrations, cloud services, automation, and rapid change.

Section 02

The complications

The same modernization that creates value can introduce new risk through cloud, integrations, access, data, AI, and rapid change.

THE 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, integrations are in test.

Excessive access

Privileged access is broader than expected

Incomplete SoD

Rules were never tuned to the business

Unrated integrations

Third-party interfaces not risk-rated

Inconsistent logging

Events captured, exceptions unreviewed

Scattered evidence

Approvals live in email and spreadsheets

The ERP project was progressing. The cyber and controls operating model had not kept pace.

LEARNING OBJECTIVE 1

How ERP modernization changes the risk profile

Modern ERP does not remove control risk. It changes where the risk lives.

01

Cloud adoption

Responsibility splits across the organization, cloud provider, ERP vendor, MSP, and internal teams.

02

Expanding integrations

Dependency grows on APIs, third-party platforms, data flows, and interface controls.

03

Rapid change

Pressure on approvals, testing, emergency changes, and release governance.

04

Automation and workflow

Good configuration strengthens control; flawed configuration automates bad decisions.

05

Embedded AI

Sensitive-data exposure, unreliable output, vendor dependency, and unclear human oversight.

06

Data centralization

Greater impact from unauthorized access, leakage, privacy failure, and reporting error.

THE RISK EQUATION

The ERP cyber risk equation

A quick diagnostic for any 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 faster
- More vendors support the environment
- More controls depend on configuration and workflow

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

LEARNING OBJECTIVE 2

Where controls commonly break down

Controls rarely fail because nobody cared. They fail because ownership, evidence, and monitoring were never designed in.

Role design

Built for implementation speed, not least privilege

Segregation of duties

Rules incomplete or never tuned to the business

Joiner, mover, leaver

Disconnected from ERP role assignment

Change evidence

Approvals exist, but evidence is inconsistent

Emergency changes

Poorly controlled and rarely reviewed after the fact

Interfaces

Treated as technical tasks rather than control points

Log review

Logging enabled, meaningful exceptions unreviewed

Ownership

Unclear once the project team stands down

RISK AREA 01

Access and identity management

A frequently encountered ERP risk area.

01

Access and 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 is not enough if roles are overbuilt or poorly governed.
- Segregation of duties must be business-relevant, not a generic ruleset.
- Privileged access should be limited, monitored, approved, and recertified.

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.

RISK AREA 02

Change, release, and configuration

SaaS delivery does not mean change management is handled for you.

02

Change and release

Configuration, vendor updates, customizations, integrations, workflows, and reporting change constantly

Where risk shows up

- A false sense that the vendor owns change management
- Configuration changes made outside formal approval
- Testing evidence that cannot be reproduced
- Emergency changes without after-the-fact review
- Release impact assessed late or not at all

Efficient ways to manage

- ITSM workflow for approvals, testing evidence, and release documentation
- DevSecOps practices for custom code, integrations, and extensions
- Automated monitoring of configuration changes
- Standardized release calendars and change risk scoring
- Production support automation for incidents and escalations

RISK AREA 03

Integrations, APIs, and third parties

Modern ERP rarely operates alone — interfaces carry sensitive data and trigger financial transactions.

03

Integrations and APIs

HRIS, CRM, banking, procurement, payroll, reporting, data platforms, and third parties

Where risk shows up

- Interfaces that move sensitive data, trigger payments, or update master data
- APIs without clear security, monitoring, or ownership
- Custom portals, extensions, and externally exposed interfaces
- Interface failures that go unreconciled

Efficient ways to manage

- API security tools and gateway monitoring
- Vulnerability scanning, penetration testing, API testing, and secure code review based on exposure
- Third-party risk platforms and vendor due diligence
- Data flow inventory and integration risk assessment
- Interface dashboards with exception reporting and reconciliation

RISK AREA 04

Data protection and privacy

ERP can hold highly sensitive organizational data, and new modules, cloud migrations, and reporting capabilities can introduce additional exposure.

04

Data protection and privacy

Employee, customer, vendor, financial, tax, banking, and payroll data

Where risk shows up

- ERP holds employee, customer, vendor, financial, tax, banking, and payroll data
- Cloud ERP raises new residency, retention, encryption, masking, and access questions
- Data migration exposes legacy data quality and privacy issues
- Reporting and analytics layers create downstream exposure

Efficient ways to manage

- Data classification and discovery tools
- DLP and data loss monitoring
- Encryption and key management governance
- Retention and archival automation
- Privacy impact assessments for new modules and integrations
- Masking or tokenization in non-production environments

RISK AREA 05

Operations, monitoring, and resilience

ERP security is not finished at go-live — monitoring should focus on meaningful risk, not on collecting logs.

05

Operations and resilience

Jobs, logs, incidents, backups, and vendor updates — the run-state disciplines that keep ERP secure and available.

What the operating model needs

- Job monitoring and batch failure follow-up
- Logging with real exception review
- Incident response tuned to ERP scenarios
- Backup and restore validation
- Vendor update evaluation and operational support

Efficient ways to manage

- SIEM integration for ERP security events
- ERP-native monitoring dashboards
- Automated job monitoring and alerting
- Production support automation for incident routing and escalation
- Continuous control monitoring for high-risk activity
- KPI and KRI dashboards for leadership and control owners

THE CHALLENGE

These are your challenges

This section highlights six challenges commonly observed in ERP programs.

01

Access outpaces governance

Roles are built for go-live speed; segregation of duties, privileged access, and recertification catch up later, if at all.

02

Change moves faster than approval

Vendor releases and configuration changes arrive continuously, while approval and testing evidence lag behind.

03

Integrations carry unowned risk

Interfaces move sensitive data and trigger transactions with no risk rating and no named owner.

04

Data exposure widens quietly

Every module, migration, and report extends the reach of employee, customer, financial, and payroll data.

05

Monitoring collects, nobody reviews

Logs and alerts exist; exception review, incident response, and follow-up do not.

06

Ownership dissolves at go-live

The project team stands down and the control environment is left without a permanent home.

Section 03

The response

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

THE CENTRAL IDEA

The one decision that can make everything else easier

Addressing risks during design may help reduce findings and remediation effort after go-live.

Treat ERP security as a design requirement with named owners and evidence — not as a checkpoint before go-live.

Make that one shift and access, change, integrations, data, and monitoring stop being five separate fights. They become outputs of how the program is already being run.

01

Decide upstream

Security requirements are set alongside the process and data design, so controls are configured from the start rather than retrofitted afterward.

02

The rest follows

Access, change, integration, data, and monitoring controls inherit the same owners, cadence, and evidence model instead of each being solved separately.

03

The cost curve flips

Findings are prevented during design instead of remediated after go-live, when they are slowest and most expensive to fix.

THE FRAMEWORK

The ERP risk domains to organize around

Modern ERP sits at the center; nine domains organize the work around it.

- Governance and oversight
- Access and identity
- Change and release
- IT and cloud operations
- Application and workflow controls

Modern ERP

AI and automation governance cuts across every domain.

- Data protection and privacy
- Integration and API security
- Monitoring and continuous improvement
- AI and automation governance

GOVERNANCE AND OWNERSHIP

What good governance looks like

Ownership, decisions, and evidence that outlast the project.

01

Ownership

- Clear, documented ownership for ERP security, controls, data, integrations, and operations.
- Defined responsibilities across IT, finance, security, compliance, internal audit, and process owners.

02

Decisions

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

03

Evidence

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

Governance forums should continue after implementation, not disband at go-live.

EFFICIENT MANAGEMENT MODEL

Move from manual control to managed risk

The goal is not more manual controls. It is a manageable operating model supported by the right tools.

Need	Efficient enabler
Risk visibility	GRC platform, ERP risk register, control dashboards
Access governance	IAM and IGA, SoD tools, PAM, MFA
Change control	ITSM workflow, automated approvals, release tracking
Integration risk	API monitoring, third-party risk tools, interface inventories
Data protection	DLP, data discovery, encryption, privacy workflow tools
Operating support	Production support automation, ticketing, alerting
Continuous assurance	Continuous control monitoring, exception dashboards, audit evidence repositories

Technology does not replace governance, but it can make governance sustainable.

How GRC platforms help

A centralized platform can help connect risks, controls, owners, evidence, and remediation.

01

One system of record

- Centralize risks, controls, owners, evidence, issues, and remediation plans.

02

Connected context

- Link ERP risks to controls, policies, business processes, systems, and compliance obligations.

03

Testing and audit readiness

- Support control testing, certifications, issue tracking, and management reporting.
- Improve audit readiness by reducing reliance on scattered spreadsheets and email.

In practice: A GRC platform can connect an ERP access risk to its control, control owner, quarterly review evidence, testing status, deficiency, and remediation plan.

How IAM and access tools help

Tactical efficiency where ERP risk moves fastest

01

Grant and revoke

- Automate provisioning and de-provisioning.
- Enforce approval workflows for high-risk roles.

02

Certify and detect

- Support periodic access certifications.
- Identify segregation of duties conflicts and excessive access.

03

Evidence the workflow

- Improve traceability from request to approval to access granted.

In practice: Instead of exporting user lists and emailing managers, access reviews are routed, tracked, escalated, and evidenced through an IAM or IGA workflow.

SECURITY ENABLER: CONTINUOUS MONITORING AND DETECTION

How monitoring and automation help

Close the loop between operations, security, compliance, and audit.

01

Monitor

- Privileged activity and failed logins
- Unusual transactions and interface failures
- Batch jobs and configuration changes

02

Automate

- Alerts routed to the right support team
- Job failure alerts tied to incident tickets
- Escalation when exceptions age

03

Review

- Dashboards for unresolved exceptions and recurring issues
- Exception review for manual journal entries, vendor master changes, and payment changes
- Alerts for dormant privileged accounts

Monitor, automate, review: detection is the loop that keeps operations, security, compliance, and audit aligned.

How assessments and documentation help

What an independent assessment, a control matrix, and a security plan do that tooling alone cannot.

01

Security assessments

- Independently test ERP security design, configuration, access, and integrations.
- Scope application, API, and penetration testing based on the organization's identified exposure.

02

IT risk and control matrix

- Build or refresh the ERP RCM linking risks, controls, owners, frequency, and evidence.
- Validate control design before go-live and operating effectiveness after.

03

System security plan

- Document the ERP security architecture, responsibilities, and control environment in a maintained reference that can support leadership, audit, and regulatory discussions.

In practice: A security assessment identifies the gap, the risk and control matrix assigns the owner and the evidence, and the system security plan keeps both current as the ERP environment changes.

CONTINUOUS MANAGEMENT

Where to focus before go-live vs. after go-live

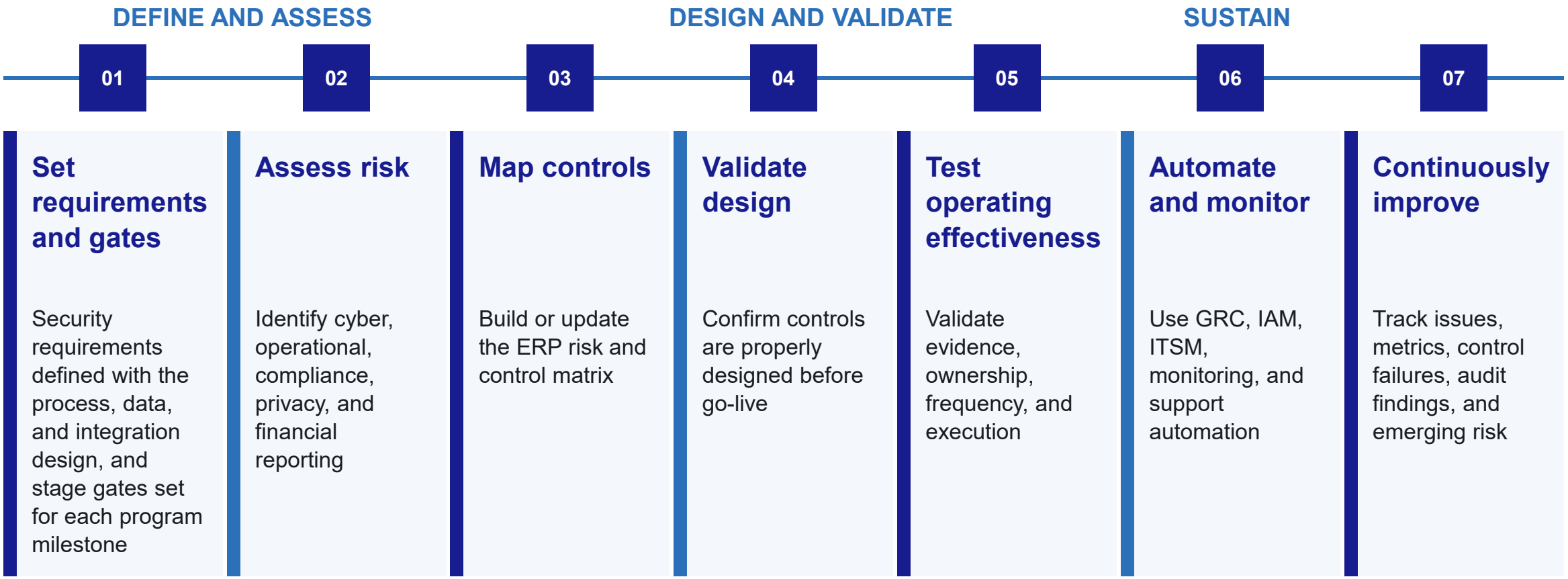
Addressing ERP risk before go-live can reduce later remediation needs, while sustained control activities remain important after go-live

Before go-live	After go-live
Security design	Access recertification
Role design and segregation of duties	Continuous monitoring
Integration inventory	Incident and exception management
Data migration risk	Control testing
Application, API, and penetration testing	Retesting after material changes and remediation
Change governance	Production support metrics
Control matrix	Audit evidence and remediation
Logging requirements	Governance cadence

LEARNING OBJECTIVE 3

Building an ERP security and controls roadmap

A practical sequence organizations can adapt to their ERP programs.



BRINGING IT ALL TOGETHER

Four things that make this real

An effective response may require more than a tool purchase.

01	**Build security into change management**	• Set security requirements during design, establish stage gates for each milestone, and define formal criteria for activities before and after go-live.
02	**System security plan**	• One maintained reference for the ERP security architecture, responsibilities, and control environment that leadership, auditors, and regulators all work from.
03	**IT risk and control matrix**	• Risks mapped to controls with named owners, frequency, and evidence, so accountability is explicit, testable, and survives the project team.
04	**Independent security assessments**	• Objective validation of control design before go-live and operating effectiveness after, including application, API, and penetration testing scoped to real exposure.

In practice: Requirements and stage gates keep security in the build, the security plan holds the design, the control matrix assigns owners and evidence, and independent assessment provides evaluation of the design and operation of controls — before go-live and after every material change.

KEY TAKEAWAYS

Practical takeaways

What to carry back into your ERP program.

01

The risk changed

- ERP modernization did not remove control risk. It moved it into cloud, identity, integrations, data, and continuous change.
- Embedded AI belongs inside the same ERP risk framework, not beside it.

02

The failure pattern

- Controls may break down when ownership, evidence, and monitoring are not sufficiently incorporated into the design.
- If unaddressed before go-live, these issues can persist into operations.

03

The answer

- Build security into change management — requirements at design, stage gates at each milestone, criteria before and after go-live.
- A security plan, a risk and control matrix, and independent assessment keep it true as the environment changes.

Security is not a phase of the ERP program. It is a requirement of the design, and it can help support a more manageable post-go-live environment.

IN CLOSING

Secure the transformation, not just the system

Decisions made during design can significantly influence the control environment at go-live.

Write it down, assign it, gate it, and prove it.

Organizations may be better positioned when they treat cybersecurity and controls as design requirements and ongoing disciplines.

01

Set the requirements now

Put security requirements and stage gates into the program plan this quarter — defined at design, tested at each milestone, and cleared before go-live.

02

Name the owners and the evidence

Build the risk and control matrix so access, change, integrations, data, and monitoring each have an accountable owner, a frequency, and evidence that survives the project team.

03

Evaluate it independently

Validate control design before go-live and operating effectiveness after, and keep the security plan current as the environment changes.

Contact >> Reach out with questions, to learn more, or schedule a meeting

Forvis Mazars

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