

Operationalizing AI Governance Through the Use Case Lifecycle

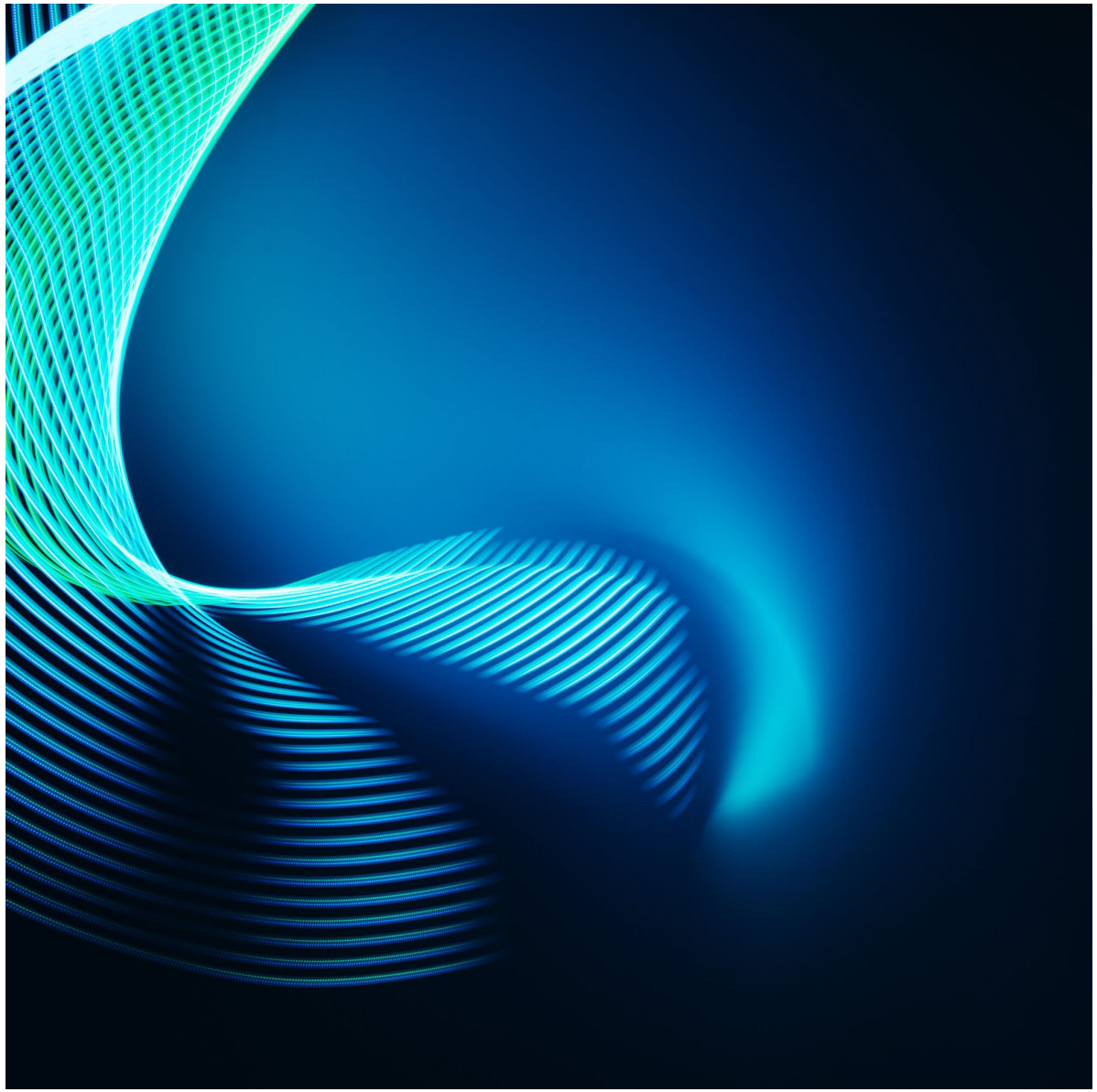
Intake | Risk Rating | Governance Intensity | Monitoring

2026 Financial Institutions Virtual Symposium

forvis mazars

Agenda

1. The Use Case Lifecycle
2. Intake and Initial Assessment
3. Use Case Risk Rating
4. Governance Intensity
5. Monitoring and Reassessment



© 2026 Forvis Mazars, LLP. All rights reserved.

The Governance Foundation Still Holds

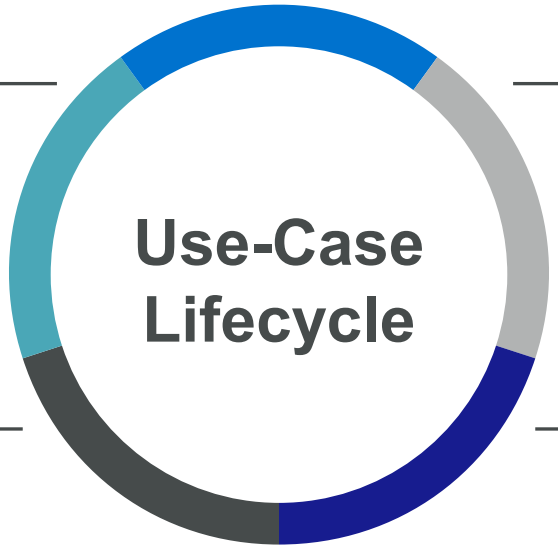
Use case management connects the pieces institutions have already been building. Policies and oversight remain foundational, and the lifecycle applies them to an actual use.

Policy

Permitted, restricted, and prohibited uses

Risk & control frameworks

MRM, compliance, privacy, cyber, third-party, data, and operational risk



Roles & decisions

Who owns, reviews, approves, challenges, and escalates

Training

Approved tools, data handling, human review, and escalation

Inventory

Visibility into platforms, material uses, models, owners, and status

© 2026 Forvis Mazars, LLP. All rights reserved.

The Operating Question Has Changed

The challenge is moving beyond just the framework to making repeatable decisions.

What institutions have built

- Policy and acceptable use standards
- Governance committees and roles
- AI, application, and model inventories
- Training and approved technology
- Existing risk and control functions

What institutions now need to operate

- A usable front door to route decisions
- Consistent use case risk rating
- Clear routing and decision rights
- Evidence requirements by risk
- Monitoring and reassessment triggers

The lifecycle provides the connective tissue from idea through reassessment or retirement.

© 2026 Forvis Mazars, LLP. All rights reserved.

01

The Use Case Lifecycle

A common process with risk-based depth at each stage



The Use Case Lifecycle Is the Organizing Framework

A use case is managed through a sequence of decisions from idea to retirement.



Identify	Find business friction, vendor-embedded capabilities, employee uses, and changes to existing systems.
Assess and approve	Capture purpose, data, reliance, consequences, ownership, and controls; route to the appropriate reviewers.
Operate and reassess	Monitor the failure modes and outcomes that matter; reopen prior decisions when the use, technology, or reliance changes.

© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

Define the Unit of Governance Before Building the Inventory

The platform, capability, business use, and individual prompt are not the same object.

Platform	**Enterprise Copilot, vendor application, internal solution**	Technology ownership, vendor, security, access, data boundaries
Capability	**Search, summarize, extract, classify, predict, recommend, act**	What the system can do and what controls constrain it
Material Use Case	**Complaint routing, complaint categorization, credit recommendation**	Business purpose, users, affected parties, reliance, consequence
Routine User Activity	**A draft email, meeting notes, or one-off prompt**	Generally governed through platform standards and acceptable-use rules

Inventory material business uses separately when purpose, data, reliance, affected parties, or control requirements differ.

© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

Connected Inventories, Different Control Questions

One intake can create or update multiple linked records.

Application

What technology is deployed?

- Owner
- Vendor
- Architecture
- Access
- Resilience
- Lifecycle

AI Use Case

How is AI used in the business?

- Purpose
- Users
- Affected Parties
- Data
- Autonomy
- Controls
- Status

Model

Does the use meet the model definition?

- Methodology
- Outputs
- Material Reliance
- Tier
- Validation
- Monitoring

Common identifier and documented classification decision

© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

AI Governance and MRM Answer Different Questions

Use one intake, then make separate AI risk and model determinations.

AI Governance

Is AI present, and how is the capability being used?

Applies to approved platforms, embedded vendor features, configured use cases, and higher-risk workflows.

Examples

- Enterprise assistant
- Policy search
- Complaint classification
- Autonomous workflow

Both

Is the use AI-enabled and also a model under bank policy?

AI governance addresses use, data, autonomy, responsible use, and lifecycle. MRM addresses model risk, tiering, validation, and performance.

Examples

- ML fraud score
- AI credit recommendation
- BSA alert prioritization model

Model Risk Management

Does the methodology meet the model definition and create material model risk?

Applies to traditional and AI-enabled models based on the bank's definition, materiality, complexity, and reliance.

Examples

- CECL
- ALM
- Stress testing
- Credit scorecard without AI

© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

A Decision-Ready Inventory Record

The record should tell one connected story across all eight fields.

Purpose & Scope
Business problem, workflow, outcome, prohibited uses

Ownership & Users
Accountable owner, operators, reviewers, affected parties

Technology, Permissions & Vendor
Platform, provider, model, integrations, connected tools, permitted actions

Lifecycle Status
Idea, pilot, production, restricted, suspended, retired

Material Use Case

Data & Access
Sources, classification, lineage, retention, permissions

Risk & Classification
Risk tier, model determination, applicable domains

Controls, Continuity & Evidence
Human review, testing, limitations, fallback, suspension, recovery

Output & Reliance
What is produced, who acts, downstream systems

The record should support classification, approval, related inventories, monitoring, change decisions, and reporting.

© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

02

Intake and Initial Assessment

One front door, common facts, and risk-based routing



One Front Door, Multiple Review Paths

Collect common information once and engage specialists based on the use.



Submit

Purpose, process, tool, users, data

Screen

AI status, prohibited use, platform approval

Classify

Model determination and applicable risk domains

Risk Rate

Impact, data, influence, autonomy, oversight

Route

Standard, structured, enhanced, or full MRM

Decide

Approve, condition, pilot, restrict, remediate, reject

Example risk functions that should plug into the process:

- MRM
- Compliance
- Fair Lending
- Privacy
- Cyber
- Third-Party
- Data
- Operational Risk

© 2026 Forvis Mazars, LLP. All rights reserved.

03

Use Case Risk Rating

Rate the configured use, then use hard-stop factors and judgment to confirm the result



A Defensible Rating Separates Inherent Risk From Control Effectiveness

Controls should not erase the consequence of failure.

Inherent Risk

- Purpose, affected parties, and permitted use
- Decision influence, transfer of agency, and autonomy
- Data sensitivity, access, and permission scope
- Customer, financial, regulatory, and operational consequence
- Reversibility and ability to contain or remediate
- Complexity, traceability, and detectability

Control Effectiveness

- Qualified human review
- Testing and acceptance criteria
- Access, action limits, logging, fallback, and suspension
- Data and source controls
- Change, incident, and monitoring design

Residual Risk

- Final Tier
- Approval conditions
- Governance intensity

A control may reduce risk when its design and operating effectiveness are adequately supported.

© 2026 Forvis Mazars, LLP. All rights reserved.

Risk Domains Provide a More Complete View

The domains below are representative. Risk domains may vary based on risk categorization and existing taxonomies.

Customer & Consumer

Direct communication, eligibility, pricing, terms, service, complaint handling

Regulatory & Legal

Regulated process, disclosures, records, fair lending, BSA/AML, privacy, IP

Financial & Reporting

Loss, reserve, valuation, reporting, capital, liquidity, revenue, cost

Operational Resilience & Containment

Criticality, framework, containment, suspension, recovery

Data & Privacy

Sensitivity, provenance, quality, scope, access, retention, cross-border use

Influence, Agency & Autonomy

Decision influence, action authority, tool and account permissions, autonomous operating scope

Model & Output Risk

Methodology, accuracy, grounding, explainability, uncertainty, drift, misuse

Third-Party & Change

Provider dependency, model or configuration changes, concentration, exit

Hard-stop factors should elevate review even when the aggregate score appears moderate.

© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

Risk Rating Matrix: Tier Definitions and Decision Rules

The output should explain the rating. Depending on your organization, Tier 1 could be considered high or low.

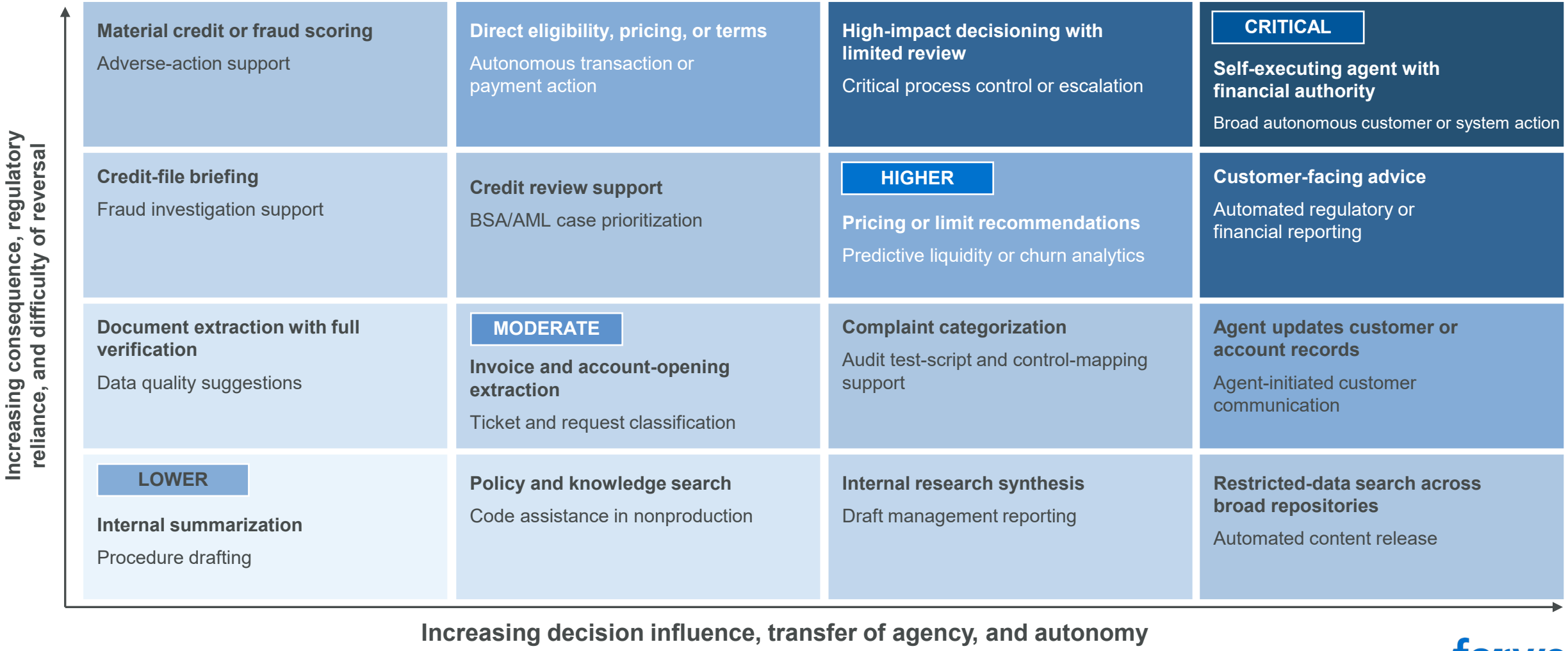
Lower	Assistive internal use; limited consequence; errors are readily detectable and reversible.	Platform or use record as defined; business approval; baseline security, data, vendor, and acceptable-use controls.
Moderate	Supports a regulated or material workflow; classification or recommendation can affect routing, timing, or quality.	Use-case record; domain review; structured testing; approval conditions; defined metrics and periodic review.
Higher	Material influence on customer, financial, compliance, credit, fraud, BSA/AML, or critical operational outcomes.	Enhanced multidisciplinary review; independent challenge as applicable; formal thresholds, change control, and reporting.
Critical	Direct decisioning or action with material consequence, limited reversibility, high autonomy, or critical reliance.	Senior or committee decision; full MRM when applicable; validation or equivalent independent review; continuous or high-frequency oversight.

© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

Directional Use-Case Risk Matrix

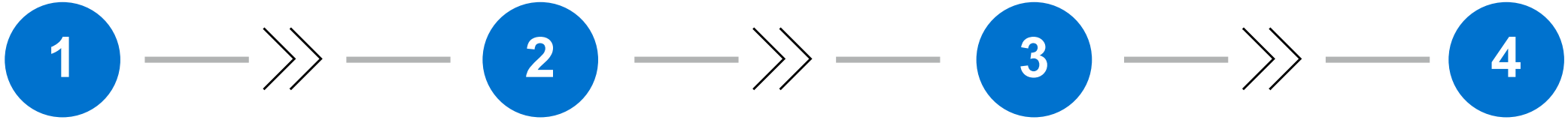
Use consequence and decision influence to establish a starting point, then apply domain scoring and hard stops.



© 2026 Forvis Mazars, LLP. All rights reserved.

How to Use the Directional Matrix

The matrix sets the starting tier, and a detailed assessment confirms or adjusts it.



Locate the Use

Place the configured use based on consequence and the degree of influence or autonomy.

Test Escalation Factors

Test customer impact, restricted data, regulatory reliance, criticality, permission scope, reversibility, and autonomous action

Assess Controls

Evaluate whether human review, testing, access, source, logging, fallback, and change controls are effective.

Confirm Residual Tier

Document the final tier, rationale, approval conditions, governance path, and monitoring obligations.

The matrix supports discussion and consistency; it does not replace written rationale or domain expertise.

© 2026 Forvis Mazars, LLP. All rights reserved.

04

Governance Intensity

Translate the risk tier into review, evidence, testing, and monitoring requirements



Risk Rating Determines Governance Intensity

The rating is useful only when it changes the required response.

LOWER	Standard path	• Named Owner • Approved Platform • Intended Use	• Permitted Data • Baseline Testing	• Incident & Change Reporting
MODERATE	Structured path	• Use-case Assessment • Domain Review	• Representative Scenario Testing	• Defined Human Review & Escalation • Periodic Monitoring
HIGHER	Enhanced path	• Multidisciplinary Review • Independent Challenge as Applicable	• Defined Limits & Permissions • Formal Thresholds & Escalation	• Enhanced Change Control • Formal Monitoring & Reporting
CRITICAL	Heightened path	• Senior Approval & Risk Acceptance • Restricted Deployment / Strong Conditions	• Full MRM When Applicable • Validation or Equivalent Independent Review • Action & Permission Limits	• Containment, Suspension & Fallback • Frequent / Real-Time Oversight

Higher risk should produce stronger evidence and clearer decision rights.

© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

Three Banking Uses Show How the Path Changes

The process remains recognizable while the participants and evidence expand.

Internal Policy Assistant

Illustrative Tier:
LOWER/MODERATE

REVIEWERS

Business + technology + security/privacy

TEST EVIDENCE

Known-answer, no-answer, source accuracy, permissions, prompt-injection, abstention

PRODUCTION FOCUS

Content freshness, unsupported answers, access incidents, vendor changes

Complaint Categorization

Illustrative Tier:
MODERATE/HIGHER

REVIEWERS

Business + compliance + privacy + technology

TEST EVIDENCE

Historical holdout, category accuracy, missed escalation, human-review effectiveness

PRODUCTION FOCUS

Accuracy by category, override patterns, backlog, missed regulatory complaints

Credit Review Assistant

Illustrative Tier:
HIGHER

REVIEWERS

Credit + risk + data + technology + compliance + MRM, as applicable

TEST EVIDENCE

Accuracy, missing-info tests, exception and edge-case review, source traceability, repeated-run consistency, analyst challenge

PRODUCTION FOCUS

Analyst corrections, missing-document rates, false-positive flags, quality-review findings, override patterns

© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

05

Monitoring and Reassessment

Monitor the failure modes that matter and reopen the decision when the use changes



Inventory, Oversight, and Monitoring Are Different

Only consequential uses need model-style performance monitoring.

INVENTORY	Know It Exists	• Owner • Purpose • Users	• Technology • Data • Status	• Tier • Approvals
OVERSIGHT	Confirm It Remains Appropriate	• Attestation • Permitted Use • Access	• Vendor & Configuration Changes	• Incidents • Continued Value
MONITORING	Evaluate Performance & Risk	• Accuracy • Unsupported Output • Overrides	• Missed Events • Outcomes • Thresholds	• Drift • Complaints

Routine productivity uses may be governed at the platform level;
material use cases require metrics tied to their own failure modes.

© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

Lifecycle Triggers Reopen the Assessment

The original rating and approval conditions can become stale.

Scope

New business unit, geography, product, user population, or customer-facing deployment

Data

New source, higher sensitivity, broader retrieval, changed lineage, or quality degradation

Reliance

Output moves from convenience to recommendation, decision, control, or regulatory evidence

Agency & Autonomy

Broader authority, permissions, connected tools, longer operation without a meaningful checkpoint

Technology & Configuration

Vendor, model, prompt, RAG corpus, tool, integration, permission, threshold, or material feature change

Performance & Control Effectiveness

Threshold breach, incident, complaint, drift, new failure mode, ineffective human review, or containment failure

Trigger → reassess inherent risk and controls → confirm tier → update approvals, inventory, testing, monitoring, and contingency.

© 2026 Forvis Mazars, LLP. All rights reserved.

End-to-End Example: Complaint Intake, Categorization, and Routing

A broadly applicable financial services use with clear customer, compliance, and operating consequences.



Identify

Complaint teams face inconsistent categorization, manual routing, and deadline pressure.

Intake

Complaint text, channel, product, customer data, categories, deadlines, and escalation rules.

Risk Rate

Moderate to higher depending on whether the output only suggests a category or drives routing, suppression, or reporting.

Approve

Complaint management, compliance, privacy, technology, security, and MRM determination as applicable.

Deploy

Pilot on historical complaints; require trained review and preserve source text, rationale, and override.

Monitor

Accuracy by category, missed high-severity complaints, overrides, routing time, backlog, and reporting exceptions.

Reassess

New products, new jurisdictions, different categories, reduced review, vendor/model change, or missed escalation.

The same use can move from moderate to higher risk when it begins to drive escalation, regulatory reporting, or customer treatment.

© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

A Practical Implementation Sequence

Pilot the lifecycle before making it the enterprise standard.

01 Set the Boundary

Define platform, capability, material use case, and routine activity.

02 Create One Intake

Collect common facts and connect model and domain determinations.

03 Calibrate the Matrix

Score 15–25 known uses; adjust definitions, weights, thresholds, and hard stops.

04 Map Governance Intensity

Specify evidence, approvals, testing, monitoring, and change triggers by tier.

05 Pilot Contrasting Uses

Run one lower-, one moderate-, and one higher-risk use through the process.

06 Measure & Refine

Track cycle time, rework, routing accuracy, exceptions, decisions, user experience, and portfolio exposure.

Start small enough to learn, but varied enough to expose inconsistent scoring, duplicate review, and impractical evidence requirements.

© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

Policies establish expectations.

Governance establishes accountability.

The use case lifecycle helps turn both into a repeatable decision-making process.

IDENTIFY | INTAKE | RISK RATE | APPROVE | DEPLOY | MONITOR | REASSESS

Rate the use. Scale the response.
Reopen the decision when the use changes.

forvis mazars