RM | REZA MONSHIZADEH
AI · TECHNOLOGY · GOVERNANCE

BOARD BRIEFING REPORT
EUROPEAN BANKING & FINANCIAL MARKETS

We Have a Policy, a Standard and a Certificate — What Do They Prove?

A Board Briefing Report on AI governance architecture — EU AI Act, ISO/IEC 42001, NIST AI RMF, testing and evidence.

Reza Monshizadeh · Monshizadeh.com · 7 min read

01 SITUATION

Each is called the framework. None of them answers the same question.

ASSUME THE FOLLOWING

Management presents the board with:

- an AI policy aligned to the EU AI Act,
- an ISO/IEC 42001 certification programme,
- a risk methodology based on the NIST AI Risk Management Framework,
- and a technical testing process.

> A certificate does not replace a regulatory crosswalk.

> A risk assessment does not establish that a control works.

> A test result does not prove that the correct legal obligations were identified.

THE BOARD ASK

Can management demonstrate how legal obligations, organisational governance, risk decisions and system testing connect in one traceable operating model?

02 MANAGEMENT SUMMARY

Three points to orient the board.

01

A complete framework has four connected layers

Law defines obligations. The management system makes governance repeatable. The risk method structures judgement. Testing and evidence show how systems and controls perform. Complementary — not interchangeable.

02

A certificate is not a crosswalk

ISO/IEC 42001 can provide a certifiable AI management system — it does not automatically establish EU AI Act compliance. **EN 18286** was developed specifically for the AI Act's quality-management requirement.

03

Expect a framework stack, not one label

The required proof is a traceable line from obligation to control, test, owner and retained evidence — one governed architecture covering the full AI population and lifecycle.

An institution can buy a certificate. It cannot buy the crosswalk.

03 ANSWER QUALITY CALIBRATION

The RAG status calibrates the quality of the answer. It does not judge the institution.

DIMENSION	GREEN	AMBER	RED
Inventory	One governed and reconciled AI population	Inventory exists, but some third-party or embedded AI remains outside it	*"We know where our AI is."*
Legal mapping	Requirement-to-control crosswalk by use case	Legal map exists but is not connected to controls	*"We are aligned with the AI Act."*
Certification scope	Scope, exclusions and organisational boundaries are explicit	Certificate exists, but its scope is not reconciled to the AI inventory	*"We are pursuing ISO certification."*
Risk method	Classification determines the governance route	Risk scores exist, but do not change requirements or approvals	*"We follow the NIST framework."*
Testing	Acceptance thresholds are tied to intended use	Testing is performed but detached from the use case or decision	*"The vendor has tested the model."*
Accountability	A named owner holds authority to approve, stop and escalate	Committees are involved, but personal authority is unclear	*"It goes through the AI committee."*
Third parties	Evidence, change duties and assurance rights are defined	Contract language exists, but operational evidence is incomplete	*"That is the provider's responsibility."*
Board reporting	Effectiveness, exceptions and decisions are reported	Delivery status is reported, but control effectiveness is not visible	*"The programme is on track."*

GREEN is not a certificate. GREEN is a traceable line from obligation to evidence.

04 THE FRAMEWORK STACK

Four layers. Four different questions. One operating model.

01 LEGAL FRAMEWORK

What must the organisation do?

EU AI Act, GDPR, DORA, financial-sector regulation and applicable product, employment and consumer-protection requirements.

DOES NOT PROVE
That the obligations have been translated into operating controls.

02 MANAGEMENT SYSTEM

Who governs AI, through which responsibilities and processes?

ISO/IEC 42001, ISO/IEC 38507 and, for the AI Act quality-management requirement, EN 18286.

DOES NOT PROVE
That each AI system is correctly classified, legally compliant or technically trustworthy.

03 RISK METHOD

How are AI risks identified, evaluated, accepted and treated?

NIST AI RMF, ISO/IEC 23894, model-risk methodologies and enterprise risk-classification processes.

DOES NOT PROVE
That the selected controls operate effectively.

04 TESTING & EVIDENCE

What demonstrates that the system and its controls perform as claimed?

AI Verify, impact assessments, validation, robustness and security testing, control testing and independent assurance.

DOES NOT PROVE
That every applicable obligation has been identified and assigned.

Each layer answers a different question. None of them answers the next one.

05 WHO SHOULD ANSWER

One integrated management response — led by the executive accountable for enterprise AI, technology or data, together with the executive responsible for risk or compliance.

REQUIRED CONTRIBUTORS

- Business Ownership
- Legal
- Compliance
- Risk
- Model Risk
- Technology
- Data
- Cybersecurity
- Data Protection
- Third-Party Risk
- Procurement
- Internal Audit

ACCOUNTABILITY NOTE

Committee membership is not the same as personal accountability. The named owner must hold the authority to approve, restrict, suspend or escalate the relevant AI use.

INTERNAL AUDIT

Internal Audit may assess design and operating effectiveness. It should not become the owner of first-line AI governance.

06 EVIDENCE THE BOARD SHOULD REQUEST

Ten artefacts that make the architecture verifiable.

01 **Enterprise AI Inventory**
One governed population covering internally developed, purchased, embedded and third-party AI.

02 **Framework Architecture Map**
The relationship between law, management systems, risk methods, testing and assurance.

03 **Regulatory Crosswalk**
Applicable requirements connected to policies, controls, owners, tests and evidence.

04 **Accountability & Decision Rights**
Approval, residual-risk acceptance, intervention, suspension and escalation authority.

05 **Classification Methodology**
Legal classification, materiality, customer impact, operational criticality and reversibility.

06 **Lifecycle Control Map**
Requirements from initiation and procurement through deployment, change and retirement.

07 **Impact & Risk Assessment**
A completed assessment for one consequential use case.

08 **Test & Validation Record**
Test objectives, methods, acceptance thresholds, exceptions and approval.

09 **Certification Scope Statement**
Covered entities, processes, systems, exclusions and certification boundaries.

10 **Board Reporting Pack**
Risk exposure, exceptions, incidents, material changes, overdue actions and decisions required.

One use case should be traceable from legal classification to current operating status — **without changing populations, definitions or owners between documents.**

07 GOVERNANCE CHECK

WARNING SIGNALS

These answers may sound reassuring in a board meeting. They are not yet decision-grade.

- ⚠ *“We follow the NIST framework.”*
- ⚠ *“We are aligned with the AI Act.”*
- ⚠ *“We are pursuing ISO certification.”*
- ⚠ *“The vendor has tested the model.”*
- ⚠ *“A person approves the output.”*
- ⚠ *“That is covered by the AI policy.”*
- ⚠ *“It is only an internal tool.”*
- ⚠ *“The framework is being rolled out.”*

None of these statements is necessarily wrong. **They are simply not sufficient evidence for board-level reliance.**

08 PATH TO GREEN

Six conditions for one governed architecture.

01 Architecture Named
The four layers are defined and used consistently.

02 Crosswalk Built
Obligations connect to controls, owners, tests and evidence.

03 Classification Drives the Route
Materiality and legal status determine governance intensity.

04 Evidence Standard Defined
Required records are specified before production approval.

05 Third Parties Included
External models, data, tools and infrastructure remain inside the governance perimeter.

06 Effectiveness Monitored
Reporting shows control operation, exceptions and decisions — not only programme completion.

SUGGESTED NEXT QUESTION

Take one AI system that can materially affect a customer, employee, transaction or critical process — can management show, in one evidence chain, the applicable law, accountable owner, approved risk decision, operating controls, test results, human intervention route, third-party dependencies and current production status?

EXECUTIVE QUESTIONS FOR EUROPEAN BANKING & FINANCIAL MARKETS

An institution can buy a certificate. It cannot buy the crosswalk.

The board should not ask which framework the organisation follows. It should ask whether one consequential AI use can be traced from obligation to operating evidence.

SELECTED SOURCES

Regulation (EU) 2024/1689 — Artificial Intelligence Act.

Regulation (EU) 2026/1744 — Digital Omnibus on AI.

CEN-CENELEC — EN 18286: Quality Management for EU AI Act Purposes.

ISO/IEC 42001:2023 — AI Management Systems.

ISO/IEC 42006:2025 — Certification of AI Management Systems.

NIST — AI Risk Management Framework & Generative AI Profile.

AI Verify Foundation — Testing Framework.

EBA — AI Act Implications for Banking and Payments.

Reza Monshizadeh · Senior Technology Executive · Frankfurt