(MIJ) 2025, Vol. No. 11 No 2 (Special Issue) **e-ISSN: 2454-924X; p-ISSN: 2454-8103**

From Automation to Accountability: Compliance Strategies for AI-Driven SAP Finance Systems

Srikanth Ganji
SAP Solution Architect
Technology Hub Inc., USA

[1]*Received: 29/08/2025; Accepted: 08/10/2025; Published: 12/10/2025*

Abstract

AI now automates core SAP finance workflows—from journal entry classification and reconciliations to anomaly detection—raising new obligations for evidence, explainability, and control assurance. This paper proposes a risk-based compliance blueprint that operationalizes accountability across the SAP stack. The approach aligns model governance and IT general controls with recognized guidance (e.g., NIST AI RMF "Govern–Map–Measure–Manage" and ISO/IEC 23894 AI risk management), translating them into SAP-specific control objectives for data lineage, model lifecycle management, human-in-the-loop checkpoints, and audit-ready logging.

We outline a layered control model: (1) Data & lineage—traceable sourcing, quality thresholds, and retention mapped to financial reporting assertions; (2) Model lifecycle—peer-reviewed development standards, bias/robustness testing, and signed release gates; (3) Explainability—use of XAI artifacts (e.g., SHAP-based feature attributions) as durable audit evidence for decisions affecting credit, provisioning, or revenue recognition; (4) Access & SoD—bot identities in SAP GRC with rulebooks that treat algorithms as privileged users; (5) Continuous control monitoring—controls-as-code for drift, data shifts, and policy breakpoints feeding SAP Process Control/Audit Management dashboards.

To handle cross-jurisdictional obligations, the blueprint maps control tests to regulatory expectations emerging for AI in financial services (documentation, transparency, human oversight), emphasizing risk registers and conformity assessment artifacts that can be reused across audits. Results include improved control effectiveness, faster walkthroughs/substantive testing, and defensible traceability from transaction to model output. The paper concluded with an implementation roadmap for SAP S/4HANA and BTP services, highlighting quick wins (central model registry, decision logs) and maturity targets (automated drift remediation) to move organizations from automation to demonstrable accountability.

Keywords: *Artificial Intelligence governance; Internal control; Explainable AI; SAP; SAP HANA*

1. Introduction

Enterprise finance has evolved from simple "bots that click" to AI that is embedded and can learn from actual operational statistics, and can make higher-order decisions, all within SAP S/4HANA. A common example already live in numerous firms is the ML-assisted matching of receivables: the system will propose clearings and residual items from bank statements and remittance advice, which minimizes manual clean-up and advances straight-through processing. Presented through SAP's Machine Learning–enabled Cash Application and underpinned by model-ops on SAP Business Technology Platform (BTP), this is a more profound shift: assurance and evidence, as well as transaction processing, are occurring inside the ERP itself.

This shift elevates the expectations of accountability. "Black-box" automation must become auditable automation - for control owners, internal/external auditors, and regulators. In Sarbanes-Oxley environments, management is required to attest to the effectiveness of ICFR, and auditors express an opinion under PCAOB AS 2201. Thus, any AI that affects journal entries, reconciliations, or disclosures will be scrutinized. In practice, that means having traceable

[1] *How to cite the article:* Ganji S (2025); From Automation to Accountability: Compliance Strategies for AI-Driven SAP Finance Systems; Vol 11 No. 2 (Special Issue); 163-170

data lineage, durable decision logs, and repeatable tests, linking model behavior to assertions in the financial statements and the control objectives that auditors are tasked to evaluate.

Expectations to manage model-risk influences this agenda as well. The U.S. Federal Reserve's SR 11-7 - which is used beyond only banking - provides the critical components: robust development and integration, independent validation, and ongoing monitoring with rigorous governance. When routines such as classification, anomaly detection, forecasting, or matching are running under the SAP finance workflows, the governance should be treated as a model and not as a distinguishing characteristic. This will call for controls on the training data and feature engineering, documented thresholds for performance, active drift detection, and challenger versus champion approaches - with documented evidence to test and re-perform.

At last, broader AI governance frameworks assist to translate risk concepts into daily practices. The NIST AI RMF 1.0 introduces a straightforward rhythm - Govern, Map, Measure, Manage - that seamlessly aligns with SAP landscapes: establish policies and assign roles; map use cases, context, and risk; measurement through testing and metrics; and manage through mitigations and continuous monitoring.

Aligning SAP GRC capabilities (Process Control, Access Control, Audit Management) and BTP's AI operations (SAP AI Core and AI Launchpad) to this cycle enables a defensible chain of custody from source data to model artifact to journal impact.

In Europe and for multinational groups, the EU Artificial Intelligence Act adds prescriptive obligations for high-risk AI systems, including risk management, data and data-governance controls, transparency to users, human oversight, and accuracy/robustness requirements. Although core financial accounting uses are not automatically classified as high-risk, many finance-adjacent AI use cases (e.g., creditworthiness assessment in shared-services or captive finance units) can be, and general-purpose model obligations are tightening. Consequently, SAP finance leaders benefit from designing control evidence and documentation (risk registers, technical documentation, testing records, human-in-the-loop checkpoints) that can be reused across audits and regulatory reviews.

This paper addresses that need by proposing a practical compliance blueprint for AI-driven SAP finance systems. We articulate an SAP-specific reference architecture in which AI services are operated through SAP AI Core and orchestrated via SAP AI Launchpad, with model inventories, metrics, and release gates forming the backbone of accountability. At the control layer, **SAP Process Control** keeps a constant eye on key risks—spotting data-quality breaks, segregation-of-duties (SoD) issues (including those involving bot or service accounts), and any breaches of defined drift limits. **SAP Access Control** governs privileged and emergency ("firefighter") access, while **SAP Audit Management** organizes the workpapers, evidence, and issue logs. Used together, these tools don't just speed up automation—they create a clear, end-to-end audit trail that holds up to ICFR testing and the next wave of AI oversight.

To make this real, the paper lays out a step-by-step roadmap and a testable control catalog that turn AI governance principles into tangible SAP configurations, logs, and artifacts. We treat explainability—like the local rationale behind a match decision—as evidence to be retained, apply SR 11-7–style validation and ongoing monitoring, and align the overall control set to NIST AI RMF 1.0 and the EU AI Act. The result is AI that's not only effective, but defensible. Following this approach moves an organization from "automation that works" to "automation that can be defended," making AI a driver of both efficiency and audit confidence.

2. SAP Reference Architecture for Accountable AI in Finance

Business layer: S/4HANA Finance (e.g., Accounts Receivable, Bank Communication), SAP Cash Application ML for receivables matching.

Control layer: SAP Process Control for continuous controls monitoring (CCM) and automated testing; SAP Audit Management for evidence, workpapers, and issues; SAP Access Control (ARA, EAM, BRM) for SoD and critical access.

Model ops layer (BTP): SAP AI Core executes/operates AI assets; SAP AI Launchpad centralizes AI lifecycle, logs/metrics, and model comparison—key for traceability.

3. Compliance Blueprint: From Automation to Accountability

3.1 Data & Lineage

Define source-to-posting lineage for training, inference, and journal impacts; enforce data quality thresholds; retain datasets, features, and inference logs per record-retention policy. Map to NIST AI RMF "Map/Measure" and ISO/IEC 23894 risk process.

3.2 Model Lifecycle Controls (Development–Validation–Release)

Adopt SR 11-7 practices: documented requirements, training/validation splits, performance thresholds, stability tests, drift monitoring, back-testing, and independent validation. Gate releases in AI Launchpad; archive artifacts and metrics.

3.3 Explainability as Audit Evidence

Use model-agnostic explainability for material decisions (credit approvals, provisioning, revenue-impact postings). LIME and SHAP are widely cited techniques; store global and local explanations alongside decisions for repeatable audits.

3.4 Identity, Access, and SoD (Bots Included)

Treat AI services and RPA/bot IDs as users subject to SoD, critical access, and elevated access governance in SAP Access Control—with periodic User Access Reviews and detective reports (ARA).

3.5 Continuous Controls Monitoring and Audit Trail

Configure SAP Process Control monitoring jobs for data quality breakpoints, SoD violations, and model drift alerts; funnel evidence and exceptions to SAP Audit Management for end-to-end traceability.

4. Control Catalog

Table 1 — AI lifecycle risks → control objectives → audit evidence → SAP/BTP enablers

Risk theme	Control objective	Typical evidence	SAP/BTP enablers
Data lineage/quality	Traceable sourcing; defined acceptance thresholds	Source-to-target mappings; quality dashboards; rejected-record logs	SAP Process Control CCM jobs; S/4HANA data quality checks (SAP Help Portal)
Model development	Documented requirements; reproducible training	Versioned code/data; training configs; metrics	SAP AI Core runs; AI Launchpad model registry & metrics (SAP Help Portal)
Validation & release	Independent validation and release gates	Validation report; sign-off; release ticket	SR 11-7 validation artifacts; AI Launchpad release workflow (Federal Reserve)
Explainability	Decision rationale recorded	Global & local explanations; challenger/ champion comparisons	SHAP/LIME artifacts linked to postings; AI Launchpad comparisons (ACM Digital Library)
Access & SoD	Least privilege; monitored emergency access	ARA SoD reports; UAR approvals; EAM logs	SAP Access Control (ARA/EAM) (SAP Help Portal)

Risk theme	**Control objective**	**Typical evidence**	**SAP/BTP enablers**
Monitoring & audit	Continuous monitoring; evidence retention	CCM results; issues; action plans; audit workpapers	SAP Process Control & Audit Management (SAP Help Portal)

Table 2 — Mapping EU AI Act obligations to SAP/BTP control tests (illustrative)

EU AI Act obligation (examples)	**What to test**	**How to evidence in SAP/BTP**
Risk management system (e.g., Art. 9)	Risk register includes data, model, and operational risks	Risk log in Process Control with mapped tests & owners; release gates captured in AI Launchpad (EUR-Lex)
Data & data governance (Art. 10)	Dataset quality, representativeness, bias checks	Data-quality CCM; validation notebooks and metrics stored with model version in AI Launchpad (EUR-Lex)
Transparency & information to users (Art. 13)	Decision impact notices, human-in-the-loop checkpoints	Posting screens/workflows that display rationale and require approvals; explanation artifacts attached to document flow (EUR-Lex)
Human oversight (Art. 14)	Manual override and escalation paths	SAP Workflow approvals; emergency access via EAM with post-facto review (SAP Help Portal)
Accuracy/robustness/cybersecurity (Art. 15)	Drift/accuracy thresholds; model rollback	AI Launchpad metrics alerts; change logs; rollback plan with transport evidence (SAP Help Portal)

Table 3 — Key metrics for "accountability" in AI-enabled finance

Metric	**Definition**	**Target/Alert**
Post-go-live model accuracy	% correct matches (e.g., cash application) vs. baseline	≥ agreed SLA; alert if −5% vs. baseline for 7 days
Data quality breach rate	% inference requests failing quality checks	≤ 1% per period; alert if trend ↑ 3 periods
SoD violations involving bot IDs	# of active violations & mean time to remediate	0 open critical > 7 days
Explainability coverage	% of AI-impacted postings with stored local explanations	100% for material decisions
Validation freshness	Days since last independent validation	≤ 365 days; alert at 300 days

5. Implementation Roadmap

Days 0–30 (Foundations). Stand up AI inventory and risk register (align to NIST "Map"); enroll all bot and service accounts in SAP Access Control; configure baseline CCM jobs in SAP Process Control; position AI Launchpad as the model registry of record. (NIST)
Days 31–60 (Controls-as-Code). Automate data quality tests and drift monitors; wire explanation exports (LIME/SHAP) into document attachments; enable UAR cadence; publish validation template aligned to SR 11-7.
Days 61–90 (Assurance-ready). Dry-run an internal audit using SAP Audit Management; finalize evidence retention schedules; complete EU AI Act obligation mapping and control tests; set KRIs (Table 3).

6. Case Vignette

A global manufacturer deploys SAP Cash Application for AR matching. Controls include (a) lineage for bank statements, remittance advice, and open item data; (b) AI Launchpad-tracked versions and metrics; (c) LIME/SHAP explanations stored with high-value offsets; (d) bot IDs governed via ARA SoD; and (e) CCM alerts on drift and quality breaches routed to Audit Management. Result: faster reconciliations with audit-ready evidence for every automated match and override.

7. Internal Audit Test Plan

Scope & objectives. Internal Audit (IA) will evaluate the design and operating effectiveness of controls governing AI-enabled finance processes in SAP (e.g., cash application, anomaly detection in journal entries) and the supporting model-operations stack on SAP BTP. The work is aligned to ICFR requirements (PCAOB **AS 2201**), supervisory guidance on model risk (Fed/OCC **SR 11-7**), the **NIST AI RMF 1.0** (Govern–Map–Measure–Manage), and—where relevant—obligations in the **EU AI Act** for risk management, data governance, transparency, human oversight, and robustness.

7.1 Planning & risk assessment

- **Understand the landscape.** Obtain a current inventory of AI use cases, models, and bot/service accounts; map process flows in S/4HANA (e.g., SAP Cash Application) and identify control points (approvals, overrides, postings).
- **Set audit criteria.** Anchor testing criteria to AS 2201 control assertions, SR 11-7 model lifecycle expectations, and NIST AI RMF functions. Document applicable EU AI Act articles if the use case is potentially "high-risk."
- **Define population & sampling.** Define populations of AI-affected transactions (e.g., automated matches, recommendations accepted/rejected), model versions, and access events (ARA/EAM). Use risk-based sampling emphasizing high-value postings and periods of model change.

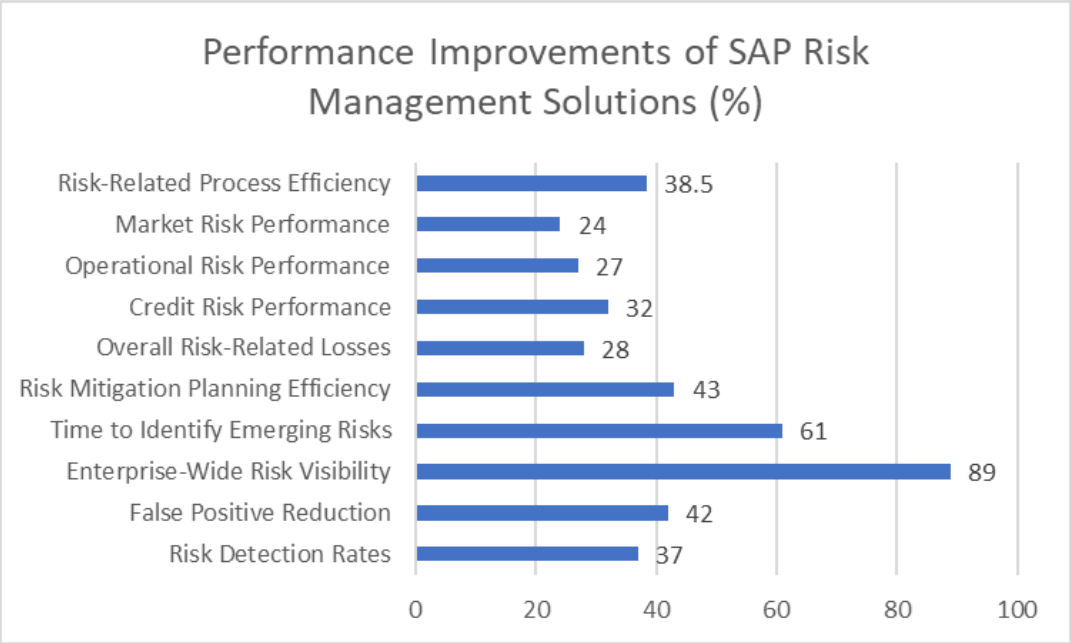

Figure 1 Performance Improvements After Implementing SAP Risk Management Solutions

7.2 Design-effectiveness procedures

- **Governance & policies.** Verify policies mapping NIST AI RMF and—if applicable—the AI Act—to concrete SAP/BTP controls (Process Control CCM jobs, Access Control ARA/EAM rules, AI Launchpad release gates). Inspect RACI and escalation paths for human oversight.
- **Model lifecycle design.** Inspect the documented process for model registration, metrics, comparison/rollback, and audit logging in **SAP AI Launchpad/SAP BTP**; confirm that logging/metrics are enabled and retained.
- **Access & SoD for bots.** Assess rulebooks in **Access Risk Analysis (ARA)** to ensure bot/service accounts are included; confirm **Emergency Access Management (EAM)** configuration for privileged, time-bound access with after-the-fact review
- **Continuous monitoring design.** Review **SAP Process Control** CCM configuration for data-quality thresholds, SoD scans, and model-drift alerts; verify integration to Audit Management for issue workflow.

7.3 Operating-effectiveness procedures

- **Walkthroughs (end-to-end).** Trace a sample of AI-affected postings from source data → inference → approval/override → GL impact. Reperform the decision with stored model version and parameters; confirm evidence (decision log, explanation if used) is durable and tamper-evident in workpapers.
- **Model validation & monitoring.** For each in-scope model, test: (i) approval of the current version; (ii) presence of training/validation metrics; (iii) alerts for drift and accuracy thresholds; (iv) challenger/champion comparisons where applicable. Verify IA can view metrics and model comparisons in AI Launchpad.
- **Access control testing.** Run **ARA** user- and role-level risk reports covering bot IDs; inspect mitigations and **UAR** evidence. For EAM, sample Firefighter sessions, confirm ticket reference and post-facto review/closure within SLA.
- **Continuous controls monitoring evidence.** Inspect most recent CCM jobs (success/failure), exception queues, and action plans; verify closure is recorded in **SAP Audit Management** with owner, root cause, and target date.

- **BTP audit logs.** Retrieve relevant BTP **Audit Log** events (model deployment, metric write, role changes) via the Audit Log Viewer/API and reconcile to change tickets/releases.

7.4 Evidence requests

- Model registry extract; version history; training/validation artifacts; metrics and thresholds; drift alerts; rollback records.
- Process Control job definitions, schedules, and last-run results; exception lists; remediation tracking.
- ARA SoD ruleset, mitigations, dashboards; EAM firefighter logbooks and approvals.
- BTP audit log exports for the audited period (subaccount scope).

7.5 Test attributes & rating guidance

- **Design**: policy-to-control mapping complete; roles and oversight clear; logging/retention defined.
- **Operation**: control executed on schedule; evidence complete (who/what/when); exceptions detected and remediated timely; monitoring closed-loop.
- **Rating**: Effective / Partially effective (minor gaps) / Ineffective (material gaps impacting ICFR conclusions). Tie conclusions to AS 2201 deficiency taxonomy.

7.6 Reporting & follow-up

- **Issue classification.** Classify findings by control family (data/lineage, model lifecycle, explainability, access/SoD, monitoring/logging). Map each to NIST AI RMF and, where applicable, EU AI Act articles to streamline regulatory reuse.
- **Remediation verification.** For medium/high findings, validate design updates (e.g., enabling Launchpad metrics tabs, tightening ARA rules, activating new CCM jobs) and re-test operation after one full cycle.

8. Conclusion

Artificial intelligence now holds an essential position in SAP Finance: it recommends matches, identifies exceptions, and once approved, posts journal entries. That integrity must be supported by bona fide accountability. By leveraging SAP GRC and BTP tooling with established assurance frameworks—AS 2201 for ICFR, SR 11-7 for model risk—as well as the NIST AI RMF 1.0 and the EU AI Act, organizations can develop a transparent chain-of-custody from data → model → posting. The return is a much faster close while maintaining defensibility in audits and against the regulators.

In practical, accountability shows up when four elements are present and demonstrated:

1. **Clear governance**—owners, policies, and human-in-the-loop checkpoints;
2. **Controlled model lifecycle**—registered versions, performance metrics, drift rules, and rollback paths;
3. **Tight access discipline**—ARA SoD coverage for bot/service IDs and EAM for emergencies;
4. **Continuous monitoring with durable logs**—Process Control CCM, Audit Management workpapers, and BTP audit logs.

Together, these turn automation from a “black box” into an auditable system of record.

Looking ahead, assurance will broaden as teams adopt **generative AI** on SAP BTP (e.g., prompt registries and Generative AI Hub) to support finance analytics and documentation. The same blueprint applies: register and govern models and prompts, capture lineage and metrics, restrict and monitor privileged use, and retain explanations and logs as audit evidence—so AI delivers both speed **and** trust.

The same blueprint applies: register prompts and models, capture metrics and lineage, restrict and monitor privileged access, and integrate events into BTP and Audit Management logs for reuse across audits. Embedding these practices early reduces future retrofit costs and avoids fragmented evidencing.

The message is simple: **automation without accountability is a control weakness; automation with accountability is a competitive advantage.** By institutionalizing the test plan above and hard-wiring logs, metrics, and approvals into day-to-day SAP operations, organizations accelerate financial throughput while improving assurance quality. That dual win—speed with trust—is the hallmark of mature, AI-enabled finance.

References

Board of Governors of the Federal Reserve System & Office of the Comptroller of the Currency. (2011). *SR 11-7: Supervisory guidance on model risk management*. https://www.federalreserve.gov/supervisionreg/srletters/sr1107.htm

de Lange, P. E., Melsom, B., Vennerød, C. B., & Westgaard, S. (2022). Explainable AI for credit assessment in banks. *Journal of Risk and Financial Management, 15*(12), 556. https://doi.org/10.3390/jrfm15120556

European Union. (2024, July 12). Regulation (EU) 2024/1689 of the European Parliament and of the Council on artificial intelligence. *Official Journal of the European Union, L*. http://data.europa.eu/eli/reg/2024/1689/oj

International Organization for Standardization. (2022). *Information technology — Governance of IT — Governance implications of the use of artificial intelligence by organizations* (ISO/IEC 38507:2022).

International Organization for Standardization. (2023). *Artificial intelligence — Guidance on risk management* (ISO/IEC 23894:2023). https://www.iso.org/standard/77304.html

Lundberg, S. M., & Lee, S.-I. (2017). A unified approach to interpreting model predictions. In I. Guyon, U. V. Luxburg, S. Bengio, H. Wallach, R. Fergus, S. Vishwanathan, & R. Garnett (Eds.), *Advances in Neural Information Processing Systems 30* (NeurIPS 2017). https://proceedings.neurips.cc/paper_files/paper/2017/file/8a20a8621978632d76c43dfd28b67767-Paper.pdf

National Institute of Standards and Technology. (2023). *Artificial intelligence risk management framework (AI RMF 1.0)* (NIST AI 100-1). https://doi.org/10.6028/NIST.AI.100-1

Ribeiro, M. T., Singh, S., & Guestrin, C. (2016). "Why should I trust you?": Explaining the predictions of any classifier. *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, 1135–1144. https://doi.org/10.1145/2939672.2939778

SAP. (n.d.-a). *SAP access control*. Retrieved October 24, 2024, from https://learning.sap.com/learning-journeys/exploring-the-fundamentals-of-sap-system-security/describing-sap-access-control

SAP. (n.d.-b). *SAP AI Launchpad*. Retrieved October 24, 2024, from https://learning.sap.com/learning-journeys/learning-how-to-use-the-sap-ai-core-service-on-sap-business-technology-platform/configuring-sap-ai-core-and-sap-ai-launchpad_a51c5214-d9ab-4f22-bc81-b683d09697fc

SAP. (n.d.-c). *Machine learning based cash application*. Retrieved October 24, 2024, from https://www.sap.com/products/financial-management/cash-application.html

SAP. (n.d.-d). *SAP audit management*. Retrieved October 24, 2024, from https://www.sap.com/products/audit-management.html

SAP. (n.d.-e). *SAP process control*. Retrieved October 24, 2024, from https://www.sap.com/products/process-control.html