© AUG 2026 | IRE Journals | Volume 10 Issue 2 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I2-1722452

Digital Transformation of Financial Risk Management: The Role of SAP Analytics and GRC Systems in Saudi Enterprises

RIZWAN
CIA, CISA, AAIA, CFRA, CMA
Senior Group Internal Audit Manager, Riyadh, Kingdom of Saudi Arabia

Abstract- ***Saudi Arabia's Vision 2030 agenda — through the Financial Sector Development Program, the National Transformation Program's digital-government mandate, and the Kingdom's broader economic diversification and privatization drive — is the direct catalyst pushing large enterprises to rebuild financial risk management on a digital foundation. This article examines how SAP Analytics (Analytics Cloud, embedded BI, and predictive modules) and SAP Governance, Risk and Compliance (GRC) applications are being combined to convert internal audit and risk functions from retrospective, sample-based reviewers into continuous-assurance partners aligned with that national agenda. Drawing on internal audit practice across diversified Saudi conglomerates spanning FMCG, QSR franchising, real estate, energy, and industrial distribution, the article proposes an integrated maturity framework that maps SAP Analytics and GRC capability against the IIA's Three Lines Model, COSO ERM (2017), and ISO 31000:2018, and against specific Vision 2030 programs. It further examines the alignment required with SAMA's Cyber Security and Business Continuity frameworks, ZATCA e-invoicing (Fatoora) controls, and the Saudi Data & AI Authority's (SDAIA) Personal Data Protection Law (PDPL). The article concludes with practical recommendations for internal audit functions seeking to move from periodic testing to embedded, analytics-driven risk monitoring while preserving independence and objectivity.***

Keywords: ***Digital transformation, financial risk management, SAP Analytics, GRC systems, internal audit, Saudi Arabia, Vision 2030, Financial Sector Development Program, ERP, continuous auditing, COSO ERM, SAMA, ZATCA, PDPL***

I. INTRODUCTION

Financial risk management in the Kingdom of Saudi Arabia is undergoing a structural shift. Enterprises that historically relied on periodic reconciliations, manual control checklists, and annual audit cycles are now operating inside an environment shaped by three simultaneous pressures: the economic diversification agenda of Vision 2030, an accelerating regulatory cadence from bodies such as the Saudi Central Bank (SAMA), the Zakat, Tax and Customs Authority (ZATCA), and the Saudi Data and Artificial Intelligence Authority (SDAIA), and a wave of Enterprise Resource Planning (ERP) modernization as legacy platforms such as Infor M3/Movex and JD Edwards are progressively replaced or supplemented by SAP S/4HANA.

Within this context, internal audit and risk functions face a dual mandate. First, they must provide assurance over financial reporting, treasury exposure, credit risk, and operational controls with a speed and granularity that manual sampling cannot achieve. Second, they must do so while regulators increasingly expect enterprises to demonstrate governance, risk, and compliance (GRC) maturity as a condition of market access, licensing, or financing. SAP Analytics and SAP GRC, deployed together, are emerging as the technical backbone that allows internal audit functions in Saudi enterprises to meet both mandates at once.

This article synthesizes practical experience gained auditing ERP-enabled financial processes across a portfolio of listed and private Saudi entities — spanning FMCG distribution, quick-service restaurant franchising, industrial equipment distribution, energy services, and residential real estate — to propose a structured view of how digital risk management is actually being implemented,

© AUG 2026 | IRE Journals | Volume 10 Issue 2 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I2-1722452

where it succeeds, and where it continues to fall short of its promise.

II. VISION 2030 AS THE STRATEGIC CATALYST

Saudi Arabia's Vision 2030 is not background context for this transformation — it is the direct driver of it. Three of the programs launched under Vision 2030 translate into concrete pressure on how Saudi enterprises manage financial risk, and each maps onto a specific capability that SAP Analytics and GRC systems are built to deliver.

2.1 Financial Sector Development Program (FSDP)

The FSDP's objectives — deepening capital markets, diversifying financing sources, and raising the sophistication of risk management in the private sector — place an implicit expectation on large enterprises to demonstrate institutional-grade risk governance, not just regulatory compliance. Audit committees increasingly benchmark internal control maturity against what the FSDP assumes a 'developed' financial sector participant looks like, which in practice means system-embedded controls and real-time risk visibility rather than manual, periodic review.

2.2 National Transformation Program (NTP) and Digital Government

The NTP's digital-government agenda has normalized system-to-system integration as the default mode of regulatory interaction — ZATCA's Fatoora e-invoicing platform and GOSI's digital services are direct examples. Enterprises whose internal financial systems remain manual or loosely integrated increasingly find themselves out of step with the interaction model regulators now expect, creating both compliance risk and competitive disadvantage relative to peers who have modernized.

2.3 Economic Diversification, Privatization, and Foreign Investment

As non-oil sectors — including the FMCG, QSR franchising, industrial distribution, and real estate sectors referenced throughout this article — take on a larger share of GDP under Vision 2030's diversification goals, and as privatization (per NCP, the National Center for Privatization) and inbound foreign investment increase, enterprises are subject to greater external due diligence, credit rating scrutiny, and cross-border reporting expectations. A digitally enabled, evidence-linked risk management architecture is what allows an enterprise to withstand that scrutiny efficiently rather than reconstructing assurance evidence manually each time it is requested.

Table 1 summarizes how each Vision 2030 program translates into a specific expectation of the internal audit and risk function, and the corresponding SAP Analytics / GRC capability that satisfies it.

Vision 2030 Program	Resulting Expectation on Financial Risk Management
Financial Sector Development Program (FSDP)	Institutional-grade, real-time risk governance rather than periodic manual review
National Transformation Program / Digital Government	System-to-system regulatory integration (e.g., ZATCA, GOSI) embedded in ERP and GRC
Economic diversification, privatization & FDI	Evidence-linked, audit-ready control environment that withstands external due diligence
Human Capability Development Program (HCDP)	Upskilling of finance, risk, and audit staff in ERP analytics and AI-assisted tools

© AUG 2026 | IRE Journals | Volume 10 Issue 2 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I2-1722452

III. THE CHANGING SHAPE OF FINANCIAL RISK IN SAUDI ENTERPRISES

Three categories of financial risk have grown materially more complex over the past three years for diversified Saudi groups.

3.1 Credit and Receivables Risk

Expected Credit Loss (ECL) modelling under IFRS 9 has moved from a year-end accounting exercise to a continuous monitoring requirement, particularly for entities with significant related-party or government-linked receivables, concentrated customer bases, or exposure to sectors experiencing project postponements. Internal audit functions increasingly find that ECL provisioning models built in spreadsheets outside the ERP are difficult to test, reconcile, and defend to audit committees, creating pressure to migrate ECL logic into governed, auditable analytics environments.

3.2 Treasury, Liquidity and Working Capital Risk

Fluctuating SAIBOR trends, extended payment cycles in industrial and QSR supply chains, and regulatory rent-control measures in the real estate sector have made working capital forecasting a board-level concern rather than a finance-department routine. Static month-end dashboards no longer satisfy audit committees that expect rolling, scenario-based visibility.

3.3 Regulatory and Fiscal Compliance Risk

ZATCA's phased e-invoicing (Fatoora) integration mandates system-level control over invoice generation, and non-compliance carries direct financial and licensing consequences. Similarly, evolving GOSI requirements, Nitaqat localization thresholds, and the National Cybersecurity Authority's Essential Cybersecurity Controls (ECC) all now intersect with financial systems in ways that were previously the domain of separate compliance teams. Fragmentation between finance, IT, and compliance functions is itself becoming a source of risk.

IV. SAP ANALYTICS AS AN ENABLER OF CONTINUOUS ASSURANCE

SAP Analytics Cloud (SAC), embedded BI within S/4HANA, and predictive scenario planning tools change the audit and risk equation in three practical ways.

- Granularity: analytics can operate at transaction level across the full population rather than a sample, surfacing exceptions such as duplicate payments, unusual journal entry timing, or credit note patterns that traditional sampling would likely miss.
- Timeliness: dashboards refreshed on operational data cycles allow risk indicators — ageing receivables, inventory excess and obsolescence, unapplied credits — to be monitored between audit cycles rather than discovered retrospectively.
- Explainability: when properly governed, SAP Analytics models retain a traceable link back to source transactions, which is critical for internal audit and external assurance providers who must be able to substantiate a finding back to underlying evidence rather than a black-box output.

In practice, the transition is rarely a single event. Enterprises migrating from legacy platforms typically run a period in which manually maintained process descriptions and control narratives lag the actual system configuration, meaning internal audit must explicitly re-validate control ownership and evidence trails post-migration rather than assuming legacy documentation remains accurate.

V. GRC SYSTEMS INTEGRATION

Where SAP Analytics addresses visibility, SAP GRC (Access Control, Process Control, and Risk Management modules) addresses the structural integrity of the control environment itself.

5.1 Access Control and Segregation of Duties

Segregation-of-duties (SoD) conflicts — for example, an individual able to both create a vendor master record and release payment to that vendor —

© AUG 2026 | IRE Journals | Volume 10 Issue 2 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I2-1722452

are a persistent finding in ERP environments that have grown organically through years of role assignment without periodic recertification. Automated SoD monitoring within GRC Access Control allows continuous conflict detection rather than the annual access review that many Saudi enterprises still rely on as their sole control.

5.2 Process Control and Continuous Monitoring

GRC Process Control allows control owners to formally attest to control performance on a defined cadence, with automated testing triggers for high-risk controls such as bank reconciliation completion, credit limit override approval, or manual journal entry authorization. This shifts internal audit's role from performing the control test itself toward validating the design and operating effectiveness of an automated monitoring layer — a materially more scalable model for a small audit team covering a multi-entity portfolio.

5.3 Risk Management and Enterprise Risk Register Integration

Linking the enterprise risk register — built on COSO ERM (2017) and ISO 31000:2018 principles — directly to GRC Risk Management allows risk owners to see real-time control performance data against the specific risks it is intended to mitigate, closing a gap that commonly exists between risk registers maintained in static presentation decks and the actual control environment they claim to describe.

VI. REGULATORY ALIGNMENT: THE SAUDI-SPECIFIC LAYER

A digital risk management architecture built for Saudi enterprises cannot be a direct copy of frameworks designed elsewhere. Four local regulatory reference points shape design choices.

Regulatory Reference	Practical Implication for SAP Analytics / GRC Design
SAMA Cyber Security & BCM Frameworks	Apply to financial institutions and, increasingly, to large corporates with banking-adjacent exposure; require demonstrable business continuity and disaster recovery testing over financial systems, not just policy documentation.
ZATCA Fatoora (E-Invoicing)	Requires system-level, tamper-evident invoice generation and real-time or near-real-time reporting integration; GRC controls must extend into the e-invoicing solution layer, not stop at the ERP boundary.
SDAIA Personal Data Protection Law (PDPL)	Governs how customer and employee data used in analytics models — including AI-assisted risk scoring — is collected, processed, and retained; analytics governance must document lawful basis and data minimization, particularly where predictive models use personal data.
CMA / Corporate Governance Regulations	For listed entities and their subsidiaries, board and audit committee reporting expectations increasingly assume the existence of automated control monitoring, raising the bar for what 'adequate' internal control evidence looks like.

The practical implication is that a GRC control library designed purely against COSO or ISO 31000 will under-specify the Saudi enterprise's actual regulatory exposure. Internal audit functions are increasingly building a hybrid control taxonomy that layers local regulatory requirements on top of the international framework rather than treating them as a separate compliance workstream.

VII. PROPOSED INTEGRATED MATURITY FRAMEWORK

Based on this practice base, a four-stage maturity model is proposed for internal audit functions assessing their own organization's digital risk management posture.

Maturity Stage	Characteristics Observed in Practice
Stage 1 — Fragmented	Spreadsheet-based ECL, SoD reviews performed annually via manual role extracts, no linkage between risk register and control testing evidence.
Stage 2 — Digitized	Core financial processes run in SAP, but analytics and GRC remain bolt-on tools used mainly for reporting rather than control monitoring.
Stage 3 — Integrated	GRC Access and Process Control embedded in the ERP; analytics dashboards used by control owners and audit committee, not only by internal audit.
Stage 4 — Predictive / Continuous	Predictive analytics flag emerging risk (e.g., receivables deterioration, control drift) ahead of financial impact; risk register dynamically reflects control performance data.

Most diversified Saudi enterprise groups observed in practice currently sit between Stage 2 and Stage 3: ERP-enabled but with GRC and analytics still substantially owned and interpreted by the internal audit function rather than embedded into first- and second-line ownership, which the IIA's Three Lines Model identifies as the more sustainable end-state.

VIII. IMPLEMENTATION CHALLENGES

- Legacy data quality: master data inherited from Movex, JD Edwards, or Yardi environments frequently requires substantial cleansing before it can support reliable predictive analytics, and this effort is regularly underestimated in migration project planning.
- Process ownership gaps: where SAP migration project teams disband after go-live, ongoing GRC rule maintenance (SoD rule books, control libraries) can lack a clear long-term owner, causing rule sets to degrade over time.
- Skills gap within the audit function: effective use of SAP Analytics and GRC requires internal auditors to develop working fluency in ERP data structures and analytics tooling — a capability set that traditional audit training programs have historically underweighted relative to control and compliance knowledge.
- Independence considerations: where internal audit has been closely involved in configuring GRC rules or analytics models, care must be taken to preserve the function's independence when subsequently auditing the same control environment, consistent with IIA Standards on objectivity.
- AI governance immaturity: as predictive and generative AI tools (including AI features embedded in SAP, Microsoft Copilot, and similar platforms) are introduced into risk analytics, most enterprises lack a formal AI governance framework addressing model risk, explainability, and PDPL-compliant data use — a gap regulators are expected to scrutinize more closely.

IX. RECOMMENDATIONS FOR THE INTERNAL AUDIT FUNCTION

- Establish a joint IT-Finance-Audit data governance charter before analytics build-out begins, so that master data ownership and quality standards are agreed rather than assumed.
- Position GRC Process Control ownership with first-line control owners, with internal audit retaining an independent testing and validation role rather than operating the monitoring tools directly.
- Embed local regulatory requirements (ZATCA, SAMA, SDAIA/PDPL, NCA ECC) explicitly into the GRC control taxonomy rather than managing them as a parallel compliance tracker.
- Build internal audit capability in ERP data analytics — through certifications such as CISA and AAIA and structured on-the-job exposure to SAP data structures — as a core competency rather than a specialist add-on.
- Introduce a formal AI governance review as a standing item in the internal audit plan wherever

predictive analytics or generative AI tools are used in financial risk processes.

X. CONCLUSION

Digital transformation is changing what 'adequate' financial risk management looks like in Saudi enterprises, and Vision 2030 is the reason the bar has moved. SAP Analytics and GRC systems provide the technical capability to move internal audit from a periodic, sample-based assurance model toward continuous, evidence-linked monitoring — but the technology alone does not deliver that outcome. Maturity depends on data governance discipline, clear control ownership beyond the audit function, explicit alignment with the Kingdom's regulatory architecture, and a deliberate investment in the audit function's own analytical capability, consistent with the Human Capability Development Program's expectations of the national workforce. Enterprises that treat SAP Analytics and GRC as an extension of the control environment, rather than a reporting layer sitting above it, are best positioned to meet both the assurance expectations of their audit committees and the broader ambition of Vision 2030: a financial sector and private-sector economy whose governance and risk management capability matches the scale of its diversification.

REFERENCES

[1] Kingdom of Saudi Arabia — Vision 2030, including the Financial Sector Development Program (FSDP), National Transformation Program (NTP), and Human Capability Development Program (HCDP).

[2] Institute of Internal Auditors (IIA) — International Professional Practices Framework (IPPF) and the Three Lines Model.

[3] Committee of Sponsoring Organizations of the Treadway Commission (COSO) — Enterprise Risk Management: Integrating with Strategy and Performance (2017).

[4] International Organization for Standardization — ISO 31000:2018, Risk Management Guidelines.

[5] International Financial Reporting Standards Foundation — IFRS 9 Financial Instruments; IFRS 15 Revenue from Contracts with Customers; IFRS 16 Leases.

[6] Saudi Central Bank (SAMA) — Cyber Security Framework and Business Continuity Management Framework.

[7] Zakat, Tax and Customs Authority (ZATCA) — E-Invoicing (Fatoora) Regulations and Implementation Resolution.

[8] Saudi Data and Artificial Intelligence Authority (SDAIA) — Personal Data Protection Law (PDPL) and Implementing Regulations.

[9] National Cybersecurity Authority (NCA) — Essential Cybersecurity Controls (ECC).

[10] Capital Market Authority (CMA) — Corporate Governance Regulations, Kingdom of Saudi Arabia.

[11] SAP SE — SAP Analytics Cloud and SAP Governance, Risk and Compliance (GRC) product documentation.