الغزاوي ومشاركوه
AlGhazzawi & Partners

CLOUD & OUTSOURCING FOR THE FINANCIAL SECTOR

The financial sector in Saudi Arabia is undergoing rapid digital transformation. Banks, FinTech companies, financial service providers, and capital market participants are increasingly relying on cloud infrastructure and outsourcing partnerships to improve performance, scale operations, reduce costs, and accelerate innovation. These models support faster delivery of digital products and services and align with Vision 2030's financial sector development objectives.

Introduction

However, greater reliance on third-party technology brings significant legal, operational, cybersecurity, and regulatory implications. Financial institutions remain responsible for the resilience, security, and compliance of their cloud and outsourcing environments, particularly under the requirements of the Saudi Central Bank (SAMA), the Capital Market Authority (CMA), the Communications, Space and Technology Commission (CST), and the Personal Data Protection Law (PDPL).

This is especially important as cloud adoption expands across Saudi Arabia's capital markets ecosystem. Brokerage firms, investment managers, securities platforms, and trading applications rely heavily on cloud infrastructure, outsourced technology providers, and data-driven operations. Effective oversight of these arrangements is therefore essential for protecting customer and investor information, maintaining service continuity, supporting regulatory compliance, and preserving market integrity and public confidence.

Why Outsourcing & Cloud Compliance Matters

As financial institutions adopt cloud technology and outsourcing models to enhance efficiency and innovation, they simultaneously increase their exposure to third-party risk, cybersecurity threats, and regulatory scrutiny. While external partners can strengthen performance and accelerate digital transformation, they also create dependencies that must be governed carefully.

Regulators in Saudi Arabia, including SAMA, CMA, CST, and The Saudi Data & AI Authority (SDAIA) emphasize that when financial services rely on cloud or outsourced operations, the organization remains legally and operationally responsible, even if another provider is performing the function.

This means that

- Accountability cannot be transferred to vendors or technology providers.
- Data protection, privacy, and security obligations remain with the institution.
- Service continuity and system reliability must be guaranteed regardless of provider issues.
- Failure to control vendor risk directly exposes the organization to penalties, downtime, and reputational harm.

In a sector where trust and stability are critical, weak control of outsourcing arrangements can lead to:

- Breaches affecting customer confidence.
- Regulatory violations and compliance penalties.
- Service disruption impacting financial operations.
- Public loss of confidence and long-term brand damage.
- Increased exposure to financial crimes, including money laundering, fraud, or embezzlement.

Key Contract Areas to Review

To effectively manage outsourcing and cloud risk, financial institutions must ensure that their contracts clearly define responsibilities, obligations, and legal protections. Many vulnerabilities arise not from technology failure, but from unclear or outdated contractual terms that fail to address regulatory and operational realities.

Below are the critical contract components that must be reviewed and strengthened before entering or renewing vendor agreements:

- **Data Protection & PDPL Compliance for Cloud Services in KSA:**
  Contracts must specify how personal and sensitive data is collected, stored, processed, shared, and deleted, while also supporting compliance with PDPL data subject rights, including access and correction requests, and ensuring vendor cooperation in responding to such requests within applicable regulatory timeframes.
- **Breach Notification & Incident Response Proceduress:**
  Vendors must be obligated to report cybersecurity or data incidents within clearly defined timeframes and cooperate in investigation, communication, and remediation efforts.
- **Security Controls, Standards & Audit Rights:**
  Contracts should document minimum security requirements, technical controls, testing expectations, and the client's right to audit, monitor, and verify compliance performance.
- **Service Level Agreements (SLAs) & Performance Guarantees:**
  Clear metrics for availability, uptime, recovery, support hours, and penalties for service failure protect operations from disruption and unpredictable downtime.
- **Liability, Indemnity & Financial Responsibility:**
  Contracts should define financial responsibility for failures, negligence, breaches, and non-compliance. Without this protection, the institution absorbs full risk.
- **Data Localization, Access, and Cross-Border Transfer PDPL Rules:**
  Specify where data is hosted, who has access, and under what legal framework data can move outside Saudi Arabia, especially under PDPL and data sovereignty rules.
- **Exit Strategy & Vendor Transition:**
  Define how data will be returned or safely destroyed and how continuity will be maintained if the contract ends, the vendor fails, or migration becomes necessary.
- **Subcontracting & Downstream Vendor Transparency:**
  Ensure visibility and approval rights over additional third parties involved in service delivery.

Risks of Avoiding Review

Failing to review and update cloud and outsourcing contracts exposes financial institutions to serious vulnerabilities. Many risks arise not from technology failure itself, but from unclear contractual obligations, weak governance, and a lack of accountability. In a highly regulated industry, these gaps can quickly escalate into operational disruption and legal consequences.

Key Risks Include:

- **Cybersecurity Breaches & Data Exposure:**
  Without strong contractual controls, organizations may lack visibility into how data is protected, who can access it, and how incidents are handled. A breach involving financial or personal data can result in significant legal, regulatory, and reputational impact.
- **Regulatory Non-Compliance:**
  Failure to align with PDPL, SAMA, CST, and cybersecurity frameworks due to weak vendor oversight can result in penalties, restrictions, or forced service suspension.

- **Service Outages & Operational Disruption:**
  Weak or missing SLAs can leave institutions without recourse if systems fail, services go offline, or performance degrades, directly impacting customers and revenue.

- **Reputational Damage & Loss of Customer Confidence:**
  In financial services, reputation is one of the most valuable assets. Public incidents linked to third-party failures undermine brand credibility and long-term customer trust.

- **Financial Loss from Contract Gaps:**
  If liability and indemnity clauses are unclear or limited, institutions may carry full responsibility for costs, penalties, and remediation, even when a vendor fails.

Strategic Imperatives for 2026

To build resilience and prepare for the next wave of digital growth, financial institutions must focus on:

- Annual contract & vendor governance audits.
- Vendor risk assessment and framework monitoring.
- Cyber incident response testing & continuity planning.
- Aligned governance between legal, risk & IT.
- Clear migration and exit strategies.
- Full alignment with SAMA, CMA, PDPL, CST, and applicable cybersecurity standards.

Conclusion

Cloud and outsourcing arrangements are now essential to the growth of financial institutions and capital market participants in Saudi Arabia. However, their value depends on strong contracts, effective vendor oversight, and clear alignment with SAMA, CMA, PDPL, CST, and applicable cybersecurity requirements.

As reliance on cloud services, trading platforms, and outsourced technology providers increases, institutions must ensure that customer and investor data protection, service continuity, breach response, audit rights, and exit arrangements are properly addressed.

Institutions that review and strengthen these arrangements early will be better positioned to reduce legal, operational, cybersecurity, and regulatory risks, while building long-term resilience, trust, and market confidence. Are your cloud and outsourcing contracts truly protecting your organization, your customers, your investors, and your reputation?

Reach out to AlGhazzawi & Partners to conduct a comprehensive review of your cloud and outsourcing agreements and ensure your institution is fully prepared for 2026.