Information Security

In 2025, Bank Albilad reinforced its commitment to maintaining the highest level of trust and operational resilience by shifting its security posture from reactive to a fully, risk-driven and proactive model, leveraging cyber threat intelligence analytics.

This strategic pivot enhanced governance and complete alignment with regulatory requirements, ensuring stronger uninterrupted business continuity.

2025 Highlights

100% incident resolution within SLA; incident performance remained stable.

Enhanced security architecture review effectiveness, significantly reducing high-risk findings across critical systems.

100% completion of all scheduled security awareness programs for employees and customers.

100% compliant, zero critical findings in Open Banking API security assessments.

PCI DSS v4.0 certified; fully aligned with SAMA CSF and NCA requirements.

Strategic Shift and Performance Excellence

The Bank's strategic execution focused on measurable improvements in control effectiveness. Key initiatives included:

Proactive Defense

Strengthening the security posture through real-time detection enhancements (SOC maturity, Thread Detection, and SIEM upgrades), coupled with increased automation and intelligence-led monitoring.

Regulatory Compliance

The Bank achieved full alignment with SAMA CSF and NCA standards and completed its PCI DSS v4.0 certification. Continuous SAMA readiness tracking was maintained to achieve the highest level of compliance.

Operational Resilience

Incident performance remained highly stable, achieving a 100% resolution rate for all incidents detected within service level agreements (SLAs).

In 2025, Bank Albilad significantly strengthened its third-party cybersecurity governance, risk, and compliance assessment by embedding continuous due diligence. This proactive approach extends the Bank's security perimeter and enhances overall system resilience.

Governance, Risk, and Innovation (GRC)

The Bank continuously strengthens its governance structures to ensure secure and compliant operations, particularly in dynamic areas such as Open Banking and cloud environments.

Secure Architecture

Enhancing secure architecture vertical, which strengthened design governance and resulted in reduction in high-risk issues. This also improved compliance by integrating architecture reviews across all major systems.

API Security and Open Banking

Following SAMA's enhanced Open Banking standards, the Bank assessed and tested API security controls across its Open Banking APIs and API gateway. Vulnerability scans, penetration tests, and continuous monitoring confirmed 100% compliance and zero critical findings, ensuring secure, resilient, and regulator-trusted Open Banking operations.

Red Teaming and Resilience

The Bank advanced its crisis simulation and red-team programs and prioritized strengthening cyber resilience by expanding cloud security governance and reinforcing data security controls in line with evolving SAMA and NCA regulations.

Security Culture and Customer Focus

The Bank recognizes that security is a collective responsibility and actively engages both employees and customers in building a strong security culture.

Awareness Programs

The Bank achieved a 100% completion rate for all scheduled security awareness programs delivered to both employees and customers. These programs included email campaigns, intranet posts, workshops, and external customer-focused security advisories.

Customer-Driven Security

Customer feedback directly shaped several security protocol enhancements aimed at balancing strong protection with seamless digital experiences. These improvements included:

- Simplified Multi-Factor Authentication (MFA) flow, incorporating trusted devices and biometric options.
- Reducing session time-out friction while maintaining security.
- Improving the user interface for security alerts to ensure better customer understanding.
- Communication and awareness initiatives for customers across digital channels.