Findings Summary on Michu Application Audit

No	Findings	Criteria and Impact	Recommendations
1. Third-Party Dependency and Absence of Internal Technical Support Team			
1.1	There is no internal technical team assigned to manage the Michu system, such as: • All application-level activities including bug fixes, patching, deployments, and monitoring are handled solely by Kifiya. • Internal IT and Digital Channel staff do not have administrative credentials or technical documentation. • SLA includes NDA terms but lacks clauses requiring internal capability development or technical handover.	**Criteria:** **Requirements for Information Technology (IT) Management of Banks Directive No. SBB/83/2022:** **4.6.** To ensure proper implementation of IT related initiatives and projects, a bank shall develop and follow effective project and IT vendor management framework. **7.2.** The IT risk management strategies, plans, policies, procedures and standards indicated under sub-article 7.1 hereinabove shall at least cover: viii) IT vendor and third-party service provider management; **IS Policy:** **10.6.3.** The Bank shall ensure that all third-party providers' services are properly identified and that the technical and organizational interfaces with suppliers are documented. **10.6.7.** The Bank shall put in place mechanisms to prevent vendor lock-in a situation where the Bank cannot easily change service or product	Establish an internal Michu technical team with access rights, clear responsibilities, and training plans. Incorporate support escalation procedures in the SLA, where internal teams manage Level 1 and 2 support, and Kifiya is involved only at Level 3.

		providers due to contractual and/or technical complexities. **10.8.5.** The Bank shall define and implement Service Levels Agreements (SLAs) that shall be measurable and have associated performance targets. **Cause:** ▪ Lack of structured handover planning or system knowledge transfer from Kifiya to internal staff. ▪ SLAs were created without ensuring operational sustainability beyond vendor support. **Impact:** ▪ Creates a single point of failure with no in-house fallback capability. ▪ Inability to maintain continuity or escalate incidents internally. ▪ Potential compliance risk due to full external control of a critical financial platform.	
2. Internal Audit Scope Limitation and Lack of Oversight on Kifiya			
2.1.	There is no visibility or control over Kifiya's internal processes or development practices, such as:	**Criteria:** **IS Policy:** **10.8.5.** The Bank shall define and implement Service Levels Agreements	Amend the SLA to include clear audit and reporting rights. Establish a third-party assurance framework that requires regular

Findings Summary on Michu Application Audit

	• Internal Audit is not granted access to review platform logs, backend databases, code repositories, or security configurations. • No contractual right is defined in the SLA for audit or inspection of third-party systems.	(SLAs) that shall be measurable and have associated performance targets. **10.8.6.** IS process shall define and implement Operation Level Agreements (OLAs) as aligned with the SLAs entered with other Bank organs. **Cause:** ▪ SLA lacks provisions on internal or third-party audit rights. ▪ Governance structure does not integrate Risk, Audit, or Compliance into the vendor lifecycle. **Impact:** ▪ Significant assurance gap over security, integrity, and reliability of a high-risk platform. ▪ Difficulty in verifying access controls, incident management, or compliance status.	reporting from vendors and grants Internal Audit limited access to system controls, metrics, and incident logs.
3. Infrastructure Ownership Without Operational Control			
3.1.	The bank owns the servers and network environment, but Kifiya controls the system remotely, such as:[I think depends on the agreement b/n the parties]	**Criteria:** **IS Policy:** **10.1.4.** The Bank shall develop and implement information security controls to safeguard IS assets	Establish shared administrative access and implement access monitoring. Define clear ownership and control rules in the SLA, ensuring internal

Findings Summary on Michu Application Audit

	• Remote access by Kifiya personnel is not logged or monitored. • Bank IT staff cannot perform any platform-level administration, including access control, database backup, or system recovery. • No records exist of configuration settings, change history, or platform audit logs within internal systems.	against an authorized access, data breaches and cyber threats. **10.11.5.** The Bank shall promote a culture of accountability, transparency and ownership within IS process. **10.8.5.** The Bank shall define and implement Service Levels Agreements (SLAs) that shall be measurable and have associated performance targets. **10.8.6.** IS process shall define and implement Operation Level Agreements (OLAs) as aligned with the SLAs entered with other Bank organs. **Cause:** ▪ Ownership of infrastructure was not matched with system-level control. ▪ No policies established to ensure internal visibility and technical boundaries. **Impact:** ▪ High risk of unauthorized changes or misconfigurations. ▪ Loss of accountability and inability to investigate or respond to technical issues. ▪ Security risks due to unmanaged access from third-party personnel.	personnel can monitor, configure, and maintain the system.

Findings Summary on Michu Application Audit

4. Lack of Role Segregation and Escalation Procedures			
4.1.	There is no clearly defined support model or escalation flow, such as: • All support tickets regardless of severity are directly handled by Kifiya. • Internal staff have no formal involvement in issue diagnosis or resolution. • SLA lacks a RACI matrix (Responsible, Accountable, Consulted, Informed) for support tasks.	**Criteria:** **IS Policy:** **10.1.4.** The Bank shall develop and implement information security controls to safeguard IS assets against an authorized access, data breaches and cyber threats. **10.5.7.** The Bank shall implement segregation of roles and responsibilities within IS process to avoid conflicts of interest and prevent the possibility for a single individual to subvert the Bank's critical IS assets. **10.8.5.** The Bank shall define and implement Service Levels Agreements (SLAs) that shall be measurable and have associated performance targets. **10.8.6.** IS process shall define and implement Operation Level Agreements (OLAs) as aligned with the SLAs entered with other Bank organs. **Cause:** ▪ No collaborative support design between the bank and the vendor. ▪ SLA focuses on service uptime, not operational governance. **Impact:**	Redesign support workflows with tiered escalation levels, assigning internal teams to Levels 1–2 and reserving Level 3 for Kifiya. Document role segregation in both the SLA and internal SOPs.

		▪ Increased risk of unauthorized or unsanctioned actions by vendor staff. ▪ No ability to enforce escalation timelines or ensure proper accountability. ▪ Delayed resolution or misalignment between business needs and technical response.	
5. Data Security and Customer Protection Risks			
5.1.	There are no enforced data protection controls in the vendor-managed environment, such as: • No data masking or minimization on exposed APIs and database queries. • No encryption policy applied to data at rest or in transit. • Internal teams cannot review or control access logs, session records, or error logs. • No endpoint protection, DLP, or	**Criteria:** **Requirements for Information Technology (IT) Management of Banks Directive No. SBB/83/2022:** **7.2.** The IT risk management strategies, plans, policies, procedures and standards indicated under sub-article 7.1 hereinabove shall at least cover: ix) customer data privacy; **IS Policy:** **10.11.8.** The Bank shall ensure confidentiality of information including privacy protection in line with compliance, legal and regulatory requirements. **10.6.6.** The Bank shall ensure that contact with third party comply with	Update the SLA to require data encryption, masking, and minimization. Enforce shared security responsibility, requiring Kifiya to comply with the bank's data protection policy and provide periodic assurance reports.

	SIEM coverage extended to Kifiya activity.	business, legal, regulatory and information security requirements. **10.8.5.** The Bank shall define and implement Service Levels Agreements (SLAs) that shall be measurable and have associated performance targets. **Cause:** ▪ The bank's information security standards are not extended to vendor-managed environments. ▪ Lack of data governance enforcement in third-party agreements. **Impact:** ▪ Customer data exposure risk due to inadequate vendor controls. ▪ Potential breach of national data protection and cybersecurity regulations. ▪ Severe reputational damage and loss of trust in case of incident.	
6. Governance and Risk Management Gaps in Fintech Partnerships			
6.1.	The bank lacks a formal governance framework to manage fintech partnerships and third-party risks effectively, such as:	**Criteria:** **Requirements for Information Technology (IT) Management of Banks Directive No. SBB/83/2022:** **4.6.** To ensure proper implementation of IT related initiatives and projects, a	▪ Establish a third-party risk management policy with input from all key functions. ▪ Maintain a live vendor risk register

Findings Summary on Michu Application Audit

	• No vendor risk register exists to assess exposure across vendors. • SLAs are not reviewed regularly by legal, risk, or IT security teams. • There is no committee or working group overseeing performance, compliance, or continuity of fintech providers.	bank shall develop and follow effective project and IT vendor management framework. **7.2.** The IT risk management strategies, plans, policies, procedures and standards indicated under sub-article 7.1 hereinabove shall at least cover: viii) IT vendor and third-party service provider management; **IS Policy:** **10.12.2.** The Bank shall establish and implement a governance framework for IS program and project management. **Cause:** ▪ Absence of a third-party governance framework aligned with industry standards. ▪ Lack of integration between Legal, Risk, Audit, and IT in vendor lifecycle processes. **Impact:** ▪ Missed opportunities to detect early vendor risk signals. ▪ Inability to proactively manage compliance and performance risks.	and perform periodic performance, compliance, and security reviews. ▪ Create a Vendor Management Governance Committee to oversee all fintech-related partnerships.

Findings Summary on Michu Application Audit

		▪ Strategic risk of system failure or reputational harm due to vendor oversight failure. ▪ Increases risk of undocumented and unresolved security or availability incidents.	
7. Limited Control Over Platform Architecture and System Updates			
7.1.	Architecture design and system updates are initiated and deployed by the third-party provider, **such as**: • The bank does not participate in platform architectural decisions (e.g., middleware stack, integration methods, security design). • New releases and patches are applied by Kifiya without formal bank-side change control board (CCB) approval. • Internal IT teams do not have	**Criteria:** **IS Policy:** **10.6.3.** The Bank shall ensure that all third-party providers' services are properly identified and that the technical and organizational interfaces with suppliers are documented. **10.10.11.** Changes to any component of the data centre and Infrastructure that is designated as a critical infrastructure shall be subject to the IS change management procedure. [remember that the governing rules are the agreement how ever it cannot contradict with banks policy unless there is exceptions this will works for other] **Cause:** ▪ The system was developed and is maintained entirely by Kifiya under a vendor-locked model.	▪ Include architecture ownership and co-governance clauses in the SLA, requiring prior approval for changes to core technical components. ▪ Mandate release notes, documentation, and version control access to internal IT teams. ▪ Establish a joint architecture review board with representation from both Kifiya and the bank to oversee technology direction, platform scalability, and

Findings Summary on Michu Application Audit

	visibility into underlying code changes or roadmap items for enhancements. • There is no internal documentation or version control repository accessible to the bank.	▪ The SLA lacks clauses requiring architectural transparency or change governance. ▪ There is no strategic technology ownership framework that mandates internal review or co-decision on critical changes. **Impact:** ▪ The bank is exposed to technical lock-in, with no ability to transition the system or vendors in case of performance or security concerns. ▪ Updates may introduce untested or non-compliant features, increasing operational and regulatory risk. ▪ Absence of architectural awareness impairs strategic planning, scalability, and integration capability with other bank platforms.	integration roadmap.