Sepio Compliance Guide:

NBC's Technology Risk Management Guidelines

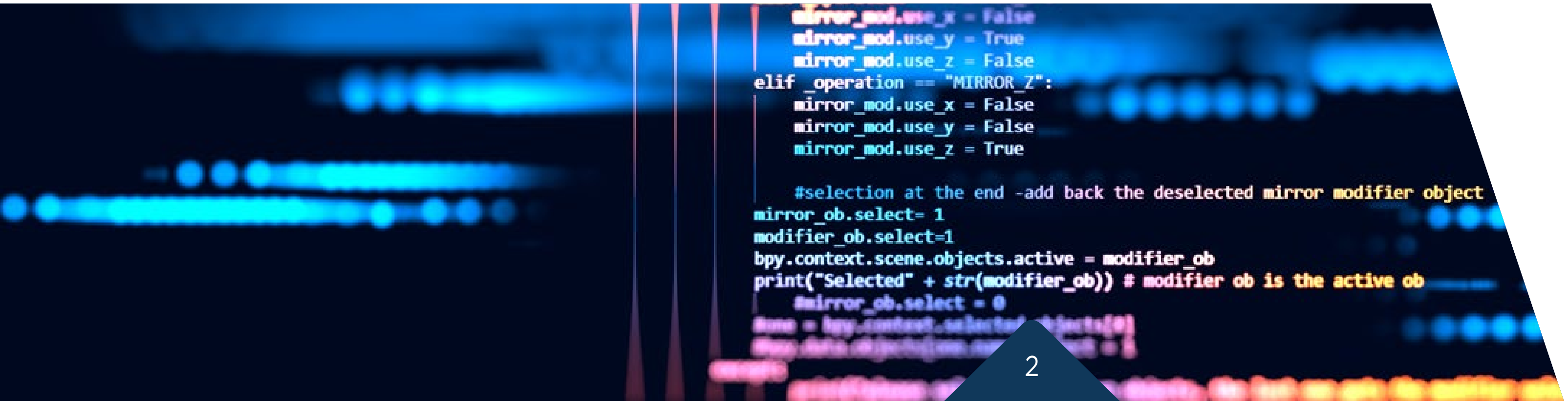
Introduction:

With Banking and Financial Institutions (BFIs) increasingly using technology to support various business processes, the National Bank of Cambodia (NBC) has established guidelines to help BFIs create a secure technology ecosystem. Implementation of these recommendations needs to be risk based following the stipulations outlined in the guidelines.

This guide outlines how to use Sepio's asset visibility, control, and continuous monitoring capabilities to meet the NBC requirements for BFIs organizations. It details the alignment with relevant controls, while offering practical steps to enhance compliance and strengthen your organization's security posture, ensuring proper cyber hygiene controls are in place across all assets in your organization.

	CATEGORY	HOW SEPIO HELPS
1. Information Technology Governance	**1.1. IT Governance Structure**	Sepio supports strong IT governance by providing **real-time visibility and control over hardware assets.** This aligns with governance policies requiring **asset monitoring, risk management, and compliance reporting.**
	1.2. Risk-Based IT Strategy	• Sepio's **trafficless asset discovery** ensures that no unauthorized devices infiltrate the IT environment, reducing governance risks related to hardware-based attacks. • **Integration with security frameworks** enables organizations to maintain adherence to regulatory requirements.

	CATEGORY	HOW SEPIO HELPS
2. IT Governance Policy and Procedures	**2.1. IT Policy, Standards, and Procedures**	Sepio contributes to **effective IT governance** by: • Providing **accurate, real-time asset inventories** that support risk-based IT policies. • Enforcing **hardware-related compliance standards** by ensuring that only authorized devices are connected to the network.



```
    mirror_mod.use_x = False
    mirror_mod.use_y = True
    mirror_mod.use_z = False
elif _operation == "MIRROR_Z":
    mirror_mod.use_x = False
    mirror_mod.use_y = False
    mirror_mod.use_z = True

    #selection at the end -add back the deselected mirror modifier object
mirror_ob.select= 1
modifier_ob.select=1
bpy.context.scene.objects.active = modifier_ob
print("Selected" + str(modifier_ob)) # modifier ob is the active ob
    #mirror_ob.select = 0
```

	CATEGORY	HOW SEPIO HELPS
3. Information Security Policy and Procedures	**3.1. Cyber Security Essentials**	**3.1.1. Access Control** Sepio enhances access control by: • **Preventing rogue device connections** by continuously verifying the authenticity of connected hardware. • Supporting **tag-based access control (TBAC)** by restricting access to predefined trusted devices. • Detecting unauthorized hardware even if it is **disguised with spoofed credentials or MAC addresses.**
		3.1.2. Network Security • Unlike traditional network traffic monitoring, Sepio trafficless approach secures the IT infrastructure by monitoring physical layer connectivity. • Detects man-in-the-middle (MITM) attacks, black-box attacks, and rogue devices. • Supports zero-trust hardware access by enforcing strict hardware validation before allowing network communication.
		3.1.3. Remote Access • Identifies unauthorized **USB and peripheral devices** that could be used to access internal resources remotely. • Prevents **hardware-based insider threats** by enforcing policies on externally connected devices.

	CATEGORY	HOW SEPIO HELPS
		3.1.4. Patch Management • Provides insights into network infrastructure **firmware versions** and vulnerabilities to support **timely patching.**
		3.1.5. Cryptographic Controls • Supports **hardware verification** by ensuring encryption modules exists where required and that they are **not tampered with.**
		3.1.6. Vulnerability Assessment Sepio supports vulnerability assessment by: • Identifying **known-to-vulnerable hardware** and providing immediate alerts. • Integrating with **threat intelligence feeds** to detect high-risk devices. • Enabling **risk scoring** for hardware assets.
		3.1.7. Physical and Environmental Security Sepio strengthens physical security by: • Pinpointing **hardware locations** (e.g., edge port, USB port, PCI slot). • Enabling **geofencing policies** (through tags and attributes) that restrict device usage to approved locations. • Detecting **unauthorized physical access attempts** through unexpected hardware presence.

	CATEGORY	HOW SEPIO HELPS
		3.1.8. User Training and Awareness • Sepio helps security teams **educate employees** about hardware threats by demonstrating **real-world attack scenarios.** • Provides **visual dashboards** to illustrate hardware security risks and compliance status.
		3.1.9. System and Application Security Controls Sepio enhances system security by: • Preventing **hardware-based exploits** (e.g., wifi keyloggers, cloning attacks). • Enforcing **device policies** to limit unauthorized connections. • Detecting **hidden, rogue devices** that evade traditional endpoint security tools.
		3.1.10. Data Security • Prevents **data exfiltration via unauthorized peripherals**. • Identifies **malicious implants or covert data-stealing devices.**
		3.1.11. Wireless Security Sepio helps mitigate **wireless threats** by: • Detecting known to be vulnerable **RF-based devices (i.e., Unifying receivers).** • Identifying **fake access points** or rogue network adapters.

	CATEGORY	HOW SEPIO HELPS
		3.1.12. Supplier Relationships • Ensures **third-party hardware compliance** by validating supplier-provided devices. • Supports **supply chain security** by detecting unauthorized device modifications.

	CATEGORY	HOW SEPIO HELPS
## 4. IT Services Outsourcing		Sepio ensures security in outsourced IT environments by: • **Monitoring third-party hardware activity** to prevent hidden threats. • Providing **automated asset reports** to track compliance of external vendors.

	CATEGORY	HOW SEPIO HELPS
## 5. Information Security Audit		Sepio simplifies security audits by: • Automating as**set discovery and classification**. • Maintaining **historical hardware usage logs** for forensic investigations. • Providing **compliance dashboards** for regulators and auditors.

	CATEGORY	HOW SEPIO HELPS
6. Payment Card Security		Sepio enhances payment security by: • Detecting **rogue devices (i.e., BlackBox)** at ATMs and kiosks. • Identifying **unauthorized payment terminal modifications.** • Preventing **hardware tampering in point-of-sale (POS) systems.**

	CATEGORY	HOW SEPIO HELPS
7. Business Continuity Planning (BCP)		Sepio supports BCP by: • Detecting **hardware availability failures before they impact critical operations.**

	CATEGORY	HOW SEPIO HELPS
8. Audit Trails and Incident Management		Sepio strengthens audit and forensic capabilities by: • Recording **all device connection events** for compliance tracking. • **Triggering alerts on unauthorized asset changes.** • Providing **evidence for security investigations.**

Key Takeaways for Compliance

1. **Continuous Visibility**
   - Achieving a robust cyber security posture requires non-stop discovery and profiling, ensuring that all devices are accurately tracked.
2. **Automated Integration**
   - Manual processes cannot scale for large BFIs entities. Integrations and automations with procurement systems, NAC solutions, and endpoint management are critical.
3. **Lifecycle Enforcement**
   - From procurement to decommissioning, each stage of an asset's lifecycle must be governed by security policies that are monitored and enforced by solutions like Sepio.
4. **Risk-Driven Remediation**
   - Detailed hardware context (ownership, risk level, compliance status) enables targeted remediation strategies that minimize operational disruptions while maintaining security.
5. **Audit and Reporting**
   - Regularly review comprehensive logs and metrics (e.g., devices not in ITAM, NAC enrollment gaps) to identify vulnerabilities, demonstrate compliance, and drive continuous improvement.

Conclusion

By leveraging Sepio's **real-time asset visibility, automated discovery, detailed hardware AssetDNA**, and seamless integrations, medium and large BFIs can meet the NBCs practice requirements for cybersecurity.

Adopting these practices not only strengthens cybersecurity defences but also **ensures alignment with other global standards** (i.e., DORA), ultimately **protecting data and critical systems** from unauthorized access and cyber threats.