



ARCON | Privileged Access Management helps to comply with the National Bank of Cambodia – Technology Risk Management Guidelines

Table of Content

1. Overview
2. What is Technology Risk Management Guidelines issued by National Bank of Cambodia?
3. Who should comply with Technology Risk Management Guidelines issued by National Bank of Cambodia?
4. ARCON – A one-stop solution to comply with NBC's Technology Risk Management Guidelines
5. NBC's Technology Risk Management Compliance Mapping Checklist
6. Conclusion

Overview

Cambodia is one of the fastest growing economies in the Asia Pacific region. A recent press release (January 2024) by IMF (International Monetary Board) Executive Board showed that the country clocked a GDP growth of 5.2% in 2022-2023. This is because of development in multiple sectors spread across the country including the banking and financial sectors.

However, simultaneously with economic growth, technological risks come. Cambodia faces cybersecurity challenges against the backdrop of growing IT infrastructure, especially in the BFIs (Banking and Financial Institutions). The BFIs in the country are susceptible to cyber threats such as phishing attacks, malware infections, ransomware, and insider threats. It leads to financial losses, data breaches, and reputational damage for banks and their customers.

Cambodian banks have been investing in cybersecurity measures to protect their systems, networks, and customer data. This includes deploying firewalls, intrusion detection systems, encryption technologies, and security awareness training for employees. These banking organizations collaborate with industry associations, government agencies, and international organizations to share information and best practices on cybersecurity. This collaboration helps improve the collective cyber resilience of the banking sector.

Banks in Cambodia also focus on managing cybersecurity risks associated with third-party service providers, such as cloud service providers, payment processors, and vendors. This involves assessing the cybersecurity posture of third parties and implementing contractual obligations for security controls.

What is Technology Risk Management Guidelines issued by National Bank of Cambodia?

The National Bank of Cambodia (NBC) is the central bank responsible for regulating and supervising banks in Cambodia. NBC has issued regulatory guidelines to enhance cybersecurity in the banking sector, including requirements for banks to implement robust cybersecurity measures and report cybersecurity incidents.

The guidelines are primarily expected to enhance the safety, security, and efficiency of banking IT operations, that can benefit the organizations and their customers. However, the progress of implementing these guidelines must be monitored by the cyber department and top management regularly, and a review of the implementation status of the guidelines may be put to the Board every year.

The guidelines denote a thorough list of acronyms that typically cover various aspects of technology risk management. They are -

- Information Security
- Financial Security
- IT Governance
- Third-party Risk Management
- Data Privacy & Data Integrity
- Compliance and Reporting

The implementation of NBC's Technology Risk Management guidelines cannot be static. Banking organizations need to pro-actively create/fine-tune/modify their policies, procedures and technologies based on new developments and emerging concerns. NBC reviews the progress of implementing these guidelines and examines the comprehensiveness and efficacy of them. NBC also validates whether they are commensurate with the nature and scope of operations.

Who should comply with Technology Risk Management Guidelines issued by National Bank of Cambodia?

The Technology Risk Management guidelines provide robust security measures to reinforce the overall financial network within Cambodia. It is extremely crucial to understand the types of organizations who must comply with this framework. It includes:

- All banks that are functioning in Cambodia
- Insurance and/or reinsurance companies established and operational in Cambodia
- Financial service providers who offer its services in Cambodia
- Credit bureaus active in Cambodia
- Financial market infrastructural entities (e.g., securities registries, stock exchanges, clearing houses)

In this regard, the banking industry is required to adhere to all areas, or domains, of this framework, covering various requirements such as application security, access control, infrastructure security, etc. Other organizations, depending on their function and risk exposure, may be required to comply with the selected domains. NBC's Technology Risk Management guidelines ensure that the banking organizations are prepared to address any cyber threats.

ARCON Privileged Access Management – a comprehensive solution to comply with NBC's Technology Risk Management Guidelines

Every organization is supposed to follow IT security regulations to enforce data privacy, integrity, and security. Complying with regulatory mandates becomes extremely easy if an organization can build a security baseline with an advanced IT security posture as applicable. It enables an organization to take control of the users to comply with the access control requirements and remain consistent with the regulatory standards. Towards this end, Privileged Access Management plays crucial roles.

Identity management has been at the core of technology usage considering that there are now hundreds of applications and systems that one uses in their day-to-day operations, and this gets further complex with the interconnected technologies talking to each other. While identity management is an issue, there are even more complex issues surrounding Privilege Identity Management. Privileged identities hold the keys to the applications and systems and have access to the heart of the various technologies.

ARCON | PAM is a Privilege Access Management Solution designed to address the challenges of privileged identities and provides an added layer of security to help build in controls that ensure access only on a "need to know" and "need to do" basis. The PAM solution has several components; however, the major components are Access Multifactor Authentication, Single Sign-On, Password Management, Access Control, and Session Monitoring. ARCON enables IT security professionals to form impregnable perimeter security around IT systems, endpoints, and data whilst enabling them to develop a comprehensive Governance, Risks, and Compliance (GRC) framework.

Built on three founding pillars: Predict, Protect, and Prevent, ARCON offers a robust stack of solutions to build 'proactive' cybersecurity posture against 'reactive' stance and mitigate looming insider, third-party, and advanced cyber threats in real-time. The solutions include:



Privileged Access Management: ARCON | Privileged Access Management (PAM) solution offers best-in-class access control features and functionalities to safeguard critical systems from insider and third-party threats. An enterprise-class Unified Governing Platform offers the deepest level of granular controls and just-in-time privileged access to systems to ensure rule and role-based access to target systems.


Endpoint Privilege Management: ARCON | Endpoint Privilege Management (EPM) is a robust solution that enables IT security and risk management teams to protect endpoints from malicious end-users. Being an AI/ ML empowered solution, it enforces the least privileged principle and ensures just-in-time access to the business-critical applications - keeping customers' and business data safe and secure.


Cloud Governance: ARCON | Cloud Governance offers complete visibility over end-user access rights and gains total control over the insights of complex cloud infrastructure.



NBC's Technology Risk Management Compliance Mapping Checklist


Here is an elucidation of the relevant areas of NBC's Technology Risk Management guidelines explained in the table below and how different ARCON solutions help SRM (Security & Risk Management) teams to comply with these mandates.


Policy Number and Description	Compliance with the Mandate?	ARCON solution Offering
<p>3.1.1 Access Control (c): The access control matrix should be supported by formal procedures and defined responsibilities. A formal user registration, de-registration and provisioning process must be implemented to enable access rights assignment. Asset owners should review users' access rights at regular intervals.</p>		<p>ARCON PAM helps organizations to build strong mechanisms to manage people, -process and policy. Access to systems is supported by One Admin Console, which ensures every PAM transaction happens through a centralized engine with stringent granular controls. Furthermore, thanks to its comprehensibility, ARCON ensures complete life-cycle management of privileged identities. Right from on-boarding user to PAM systems and auto-mapping user roles and responsibilities to target applications and systems along with intuitive workflow matrix, ARCON PAM offers Identity Governance as well which allows security and risk management leaders, provisioning and de-provisioning, certification and re-certification of users' and their corresponding access to systems.</p>
<p>3.1.1 Access Control (d):</p> <ul style="list-style-type: none"> Implementation of role-based access control designed to ensure effective segregation of duties 		<p>ARCON PAM provides adequate safeguards to protect end-users and control their privileged access with Role-Based Access Control (RBAC). The solution not just ensures that the principle of least privilege is implemented, but also each user's access to target devices happens in a controlled environment.</p>

<ul style="list-style-type: none"> ▪ Changing default usernames and/or passwords of systems and prohibiting sharing of user IDs and passwords of generic accounts ▪ Modification of access rights whenever there is a change in role or responsibility and removal of access rights on cessation of employment/contract ▪ Periodic reconciliation of user IDs in a system and actual users required to have access and deletion of any unnecessary IDs, if any ▪ Auditing, logging and monitoring of access to IT assets by all users ▪ Considering de-activating user IDs of users of critical applications who are on prolonged leave 		<p>ARCON PAM’s password vaulting feature ensures that privileged credentials are stored and managed in a highly secure environment by providing a secure and single point of control. It allows organizations to enforce password policies such as password expiration, complexity and rules to ensure that passwords are rotated and randomized regularly and meet the organization's security standards.</p> <p>During situations when IT administrators need to modify end-user role, ARCON PAM offers “Modify User Role” feature. This is extremely useful when -</p> <ul style="list-style-type: none"> ▪ Two different user roles need to be interchanged ▪ Any additional roles to be added to the set of roles to an existing end-user ▪ A single user with two user roles needs to be generated <p>ARCON PAM offers Identity Governance (IG) that assists banking organizations to ensure that the right people have the right level of access to the right resources at the right time and mitigate risks. IG includes the entire identity lifecycle, including identity creation, management, and deletion whenever required. As a result, any dormant account is identified, detected and removed before any misuse happens.</p> <p>ARCON PAM offers real-time session monitoring of privileged identities that helps to detect and respond to security threats quickly and effectively. It includes real-time alerts for suspicious activity, enabling security teams to respond to potential threats quickly by freezing or terminating the session. This feature adds an extra layer of security to privileged accounts and secures confidential data assets.</p>
<p>3.1.1 Access Control (h): Personnel with elevated system access entitlements should be closely supervised with all their systems activities logged in, as they have inside knowledge and the resources to circumvent systems controls and security procedures. Some of the control and security practices enumerated below need to be considered:</p>		<p>ARCON PAM provides granular level access control to the users based on their defined roles, responsibilities, and tasks. It enables organizations to define and enforce precise access policies for privileged users, reducing the risk of unauthorized access and misuse of sensitive systems and data.</p> <p>ARCON PAM offers multi-factor authentication (MFA) that acts as a strategic entry point for system-based users. It ensures a robust user authentication mechanism to prevent unauthorized and suspicious access – both for on-prem and remote users (i)</p>

<ul style="list-style-type: none"> I. Implementing two-factor authentication for privileged users Instituting strong controls over remote access by privileged users II. Restricting the number of privileged users III. Granting privileged access on a ‘need-to-have’ or ‘need-to-do’ basis IV. Maintaining audit logging of system activities performed by privileged users V. Ensuring that privileged users do not have access to systems logs in which their activities are being captured VI. Conducting regular audit or management review of the logs Prohibiting sharing of privileged IDs and their access codes VII. Disallowing vendors and contractors from gaining privileged access to systems without close supervision and monitoring 		<p>With granular level access control, banking organizations can limit privileged users' access to only those systems, applications, and data that they need to perform their jobs. It helps to create policies that restrict users from performing tasks deviating from their roles on a specific system or application. (ii)</p> <p>ARCON offers a very robust Access Control module that ensures the deepest level of granular controls. It includes:</p> <ol style="list-style-type: none"> 1. Fine-grained access control: Admins can control exactly which users have access to which services and resources 2. Process and Command Restriction: Admins can restrict or elevate specific processes or commands that can be executed 3. Critical Command Approval: Privileged user requires that certain commands be approved by the admin before they can be executed 4. Reporting: Admins can generate reports on the privileged user activities and access control events <p>Fine-grained access control of ARCON PAM enables organizations to manage privileged access more effectively and reduce the risk of insider threats and cyberattacks. (v) & (vii)</p> <p>ARCON PAM helps in audits trails of every privileged session by providing customized and detailed analytics of every privileged access to target systems. Based on the reports, IT administrators identify suspicious users and prohibit them from doing their activities. (vi)</p>
<p>3.1.3 Remote Access:</p> <p>Remote access to BFIs provides an attacker with the opportunity to manipulate and subvert the BFIs’ systems from outside the physical security perimeter. Management should establish policies restricting remote access and be aware of all remote-access devices attached to their systems. These devices should be strictly controlled.</p>		<p>ARCON PAM offers Global Remote Access (GRA) that automates IT processes and controls users to remotely access and manage unattended devices such as servers, desktops, and laptops without the need for any approvals but in a secure manner. It allows secure authentication for convenient resource access, and it also allows IT teams to create and manage remote access support tickets. An authorized administrator can grant or deny user’s requests for elevated access privileges.</p>

		<p>GRA enables users to securely transfer files between remote devices without relying on third-party service providers. With Secure File Transfer, users can easily and securely transfer files such as documents, images, videos, and others between remote devices through an encrypted connection.</p>
<p>3.1.3 Remote Access (g): Maintain logs for remote access communications. Logs should include the date, time, user, user location, duration, and purpose for all remote access including all activities carried out through remote access.</p>		<p>ARCON's Global Remote Access (GRA) strengthens the security posture and reduces the attack vector by generating detailed reports of every remote session regularly. The reports allow administrators to monitor and audit key resource access details including date, time, user details, user location, logging duration and more. This aids in the prevention of unauthorized access, malicious activities, and strong defense against IT threats.</p>
<p>3.1.10 Data Security: Concerns over the need to better control and protect sensitive information have given rise to a new set of solutions aimed at increasing an enterprise's ability to protect its information assets. These solutions vary in their capabilities and methodologies, but collectively they have been placed in a category known as data leak prevention (DLP). BFI may consider such solutions, if required, after assessing their potential to improve data security.</p> <p>DLP solutions provide a comprehensive approach covering people, processes, and systems that identify, monitor, and protect data in use (e.g., endpoint actions), data in motion (e.g., network actions), and data at rest (e.g., data storage) through deep content inspection and with a centralized management framework. Most DLP solutions include a suite of technologies that facilitate three key objectives:</p>		<p>ARCON's Endpoint Privilege Management (EPM) solution enables IT security and risk management teams to protect endpoints from malicious end-users.</p> <p>Endpoints in an enterprise IT environment can be compromised if the end-users can easily target confidential information using any removable storage device. ARCON EPM's Data Loss Prevention (DLP) mechanism helps IT administrators to mitigate security vulnerabilities by restricting endpoints such as pen drives, external hard drives, mobile devices or even mobile Bluetooth connections and Bluetooth transfers. This USB restriction feature prevents copying of any sort of information/file/folder from the endpoint to USB and vice versa.</p> <p>Another key functionality of ARCON EPM is data contextualization. As BFIs of all shapes and sizes generate a huge volume of data every day, IT security pros require a mechanism through which actionable insights can be generated to make well-informed decisions. Data Intellect, a critical component of EPM, builds a ring-fence around data and provides a contextual security layer around the data.</p> <p>ARCON EPM also offers File Integrity Monitoring (FIM) that can track unauthorized file changes on user devices in real time and processes, track unauthorized changes. It</p>

<ul style="list-style-type: none"> I. Locate and catalogue sensitive information stored throughout the enterprise Monitor and control the movement of sensitive information across enterprise networks and II. Monitor and control the movement of sensitive information on end-user systems. 		<p>helps to keep a thorough track of file history and roll back changes if needed. This level of data governance and lifecycle management is unusual in any traditional EPM product. Hence, FIM is sought and admired by SRM leaders of BFIs, especially where there is continuous data flow.</p>
<p>3.4 Audit Trails</p> <p>Audit and security logs are useful information which facilitates investigations and trouble shooting.</p> <ul style="list-style-type: none"> a) Ensure that records of user access are uniquely identified and logged for audit and review purposes. b) Have accountability and identification of unauthorized access is documented. c) Enable audit logging of system activities performed by privileged users. d) Protect against unauthorized changes to log information by using appropriate logging facility. e) Ensure appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security. 		<p>To meet this regulatory requirement of NBC, enterprises need to generate and maintain comprehensive audit trails for every privileged session seamlessly.</p> <p>ARCON PAM's robust reporting engine makes SRM team audit-ready by providing customized and detailed analytics of every privileged access to target systems. It helps them to make better IT privileged user decision making. The solution enables the auditors to assess the organization's regulatory compliance status at any given time.</p> <p>ARCON PAM proactively secures all databases and applications as every command/query executed by end-users is captured for a security assessment. This way, the Security and Risk Assessment team seamlessly manages the lifecycle of privileged accounts as every activity performed by privileged users is captured in both video and text format.</p>

<p>3.6.3 Cloud Computing (e): Third-party access to sensitive information creates a risk of compromise to confidential information. It is necessary to ensure the protection of intellectual property (IP), trade secrets and confidential customer information hosted on the cloud.</p>		<p>ARCON Cloud Governance offers holistic risk management against third-party threats. The in-built AI and ML capabilities enable administrators to analyze and categorize permission usage, detect shadow administrative rights and overprivileged permissions, and generate risk scores for further action (restrictive measures).</p> <p>This solution offers a dynamic access control policy where privileged rights can be revoked automatically or on-demand after the completion of tasks.</p>
---	---	---

Conclusion

ARCON | Privileged Access Management, ARCON | Endpoint Security Management and ARCON | Cloud Governance solutions enable SRM leaders to -

- Comply with NBC's Technology Risk Management guidelines
- Mitigate the chances of data breach incidents and password abuse
- Build a stringent rule and role-based access control framework
- Ensure robust identity and access management posture
- To analyze and categorize access permissions and restrictions
- Strengthen data loss prevention (DLP) measures

about ARCON

ARCON is a leading Information Risk Management solutions provider specializing in Privileged Access Management and Continuous Risk Assessment solutions.

ARCON Privileged Access Management (PAM) is a leading global product and a robust solution that mitigates risks arising out of privilege identity and access management.

Connect with us    

All rights reserved by ARCON

This document or any part of the document may not be reproduced, distributed or published in any form without the written consent of the copyright owner under any circumstances. Any kind of infringement in the owner's exclusive rights will be considered unlawful and might be subject to penalties.