BeyondTrust

This guideline is largely based on the recommendations detailed in the Cyber Resilience Oversight Expectations (CROE) for Financial Market Infrastructures issued by the European Central Bank in December 2018.

Mapping BeyondTrust Capabilities to the Bank of Mauritius's Guideline on Cyber and Technology Risk Management

TABLE OF CONTENTS

Overview

The Bank of Mauritius (referred to in this document as "the Bank") fully supports the digital transformation of the financial sector worldwide that was accelerated during the pandemic. It also acknowledges the related increase in the threat landscape and the potential spillover effects on financial stability.

The Bank's **Guideline on Cyber and Technology Risk Management**, published in May 2023, outlines the **minimum requirements** in which banks and payment service providers are expected to implement cyber and technology risk management measures. The primary goal of this guidance is to ensure that cyber risks are well understood and managed appropriately within financial organizations operating in Mauritius. This guideline is largely based on the recommendations detailed in the *Cyber Resilience Oversight Expectations (CROE) for Financial Market Infrastructures* issued by the European Central Bank in December 2018.

As outlined in the document, and in addition to current minimum requirements, banks and financial service providers will also need to consider the implementation of encouraged measures set out in the guideline.

This also includes standards in relevant international guidance documents, including but not limited to:

- The National Institute of Standards and Technology (NIST) Cybersecurity Framework
- The Control Objectives for Information and Related Technologies (COBIT) by ISACA
- Other relevant ISO information security standards and additional best practices

In response to this guidance, this paper has been prepared so that banks and financial service providers operating in Mauritius can quickly understand how BeyondTrust Privileged Access Management (PAM) solutions map into requirements set forth in the Bank of Mauritius's Guideline on Cyber and Technology Risk Management. IT and security administrators within these organizations may use this paper to gain a clearer understanding of the requirements set forth in the 2023 Guideline and to learn how to use BeyondTrust solutions and their capabilities to comply with them.

The Bank's Guideline have been constructed around a ten-part framework. Each of these ten sections outlines specific requirements and recommendations as they relate to various cybersecurity components, such as threat response, governance, and training.

The 10 Sections the Bank's Guideline Include:

1. Governance
2. Identification of Cyber and Technology Risks
3. Protection
4. Detection
5. Response and Recovery
6. Assurance and Testing
7. Situational Awareness
8. Learning and Evolving
9. Reporting Requirements
10. Transitional Arrangements

Each section contains detailed sub-sections, illustrating substantial requirements ranging from specific cybersecurity architectures to personnel policies. In the remainder of this paper, we will map only the sections and sub-sections where BeyondTrust's PAM solutions can help financial institutions comply with the Bank of Mauritius's Guideline on Cyber and Technology Risk Management.

BeyondTrust Solutions & The Bank's Guideline

BeyondTrust is a global Privileged Access Management leader, offering privilege and identity management solutions that go beyond traditional preventative privilege management. Capabilities like real-time threat detection, secure remote access to anywhere, and proactive privilege recommendations make our solutions a top choice by financial and banking organizations across the world. Our solutions allow organizations to maintain security and demonstrate compliance.

Several BeyondTrust solutions meet the criteria and capabilities requested by the Bank of Mauritius's Guideline on Cyber and Technology Risk Management. BeyondTrust capabilities address 36 recommendations across several sub-sections, most prominently in sections **II: Identification of Cyber and Technology Risks** and **III: Protection.**

The following section directly maps these solutions to the Bank's guideline, sub-section by sub-section.

Mapping to Guideline Controls

As excerpted from the Bank of Mauritius's **Guideline on Cyber and Technology Risk Management**, below are several specific points and sub-sections that can be directly addressed or satisfied by BeyondTrust solutions.

PART II – IDENTIFICATION OF CYBER AND TECHNOLOGY RISKS

Guideline Section	Sub-section	Description of Guideline	Supported by Password Safe	Supported by Privileged Remote Access	Supported by Privilege Management for Windows/ Mac	Supported by Privilege Management for Unix/ Linux
20: "A financial institution shall..."	(ii)	Ensure that all functions, roles, processes, assets (including those involving third-party service providers) and any other data, device(s), component(s) or connection point(s) of the network system are duly identified, classified and documented.	•	•		
	(iv)	Maintain an inventory of all individual and system accounts (including privileged and remote access accounts), cyber/ technology services, key roles, processes, information assets, third-party service providers and interconnections together with criticality rating.	•	•		
	(ix)	Comprehensively document all individual and system accounts, including privileged and remote access accounts, so that it can track all access rights to its information assets.	•	•		
22: "A financial institution is encouraged to..."	(ii)	Implement automated tools (such as a centralized identity and access management tool) to support the identification and classification of roles, user profiles and individual and system credentials.	•	•		

PART III – PROTECTION

Control Implementation & Design

Guideline Section	Sub-section	Description of Guideline	Supported by Password Safe	Supported by Privileged Remote Access	Supported by Privilege Management for Windows/ Mac	Supported by Privilege Management for Unix/ Linux
23: "A financial institution shall..."	(i)	Put in place a robust and effective set of security controls that will enable it to fulfil its security objectives, which should include ensuring the confidentiality, integrity and availability of information stored in its information systems.	•	•	•	•
	(ii)	Develop security controls to address all aspects of security, including logical, physical, people and third-party security. The controls should be commensurate to the cyber and technology risks faced by the financial institution and should be consistent with its business goals and risk appetite.	•	•	•	•

Network & Infrastructure Management

Guideline Section	Sub-section	Description of Guideline	Supported by Password Safe	Supported by Privileged Remote Access	Supported by Privilege Management for Windows/ Mac	Supported by Privilege Management for Unix/ Linux
24: "A financial institution shall..."	(i)	Set up a secure boundary to protect its network infrastructure through the use of technologies such as, inter alia, a router, firewall or virtual private network. The boundary should distinguish trusted and untrusted areas based on risk profile and criticality of information assets stored within each zone. Reasonable access criteria should be applied within and between each security zone using the concept of least privilege.	•	•		
	(ii)	Implement network segmentation in accordance with the sensitivity of the systems.		•		
	(iii)	Define baseline systems and security requirements for information systems and system components including devices used for remotely accessing the financial institution network in order to facilitate configuration and security reinforcement of such systems and components.		•		
	(iv)	Use secured network protocols (shell protocols and transport layer security protocols or equivalent) to ensure confidentiality and integrity of information shared on and through the network including remote connections.	•	•		
	(vii)	Ensure that there are procedures to limit, lock and terminate system and remote sessions after a predefined period of inactivity and when predefined conditions (including unsuccessful attempts) are met.	•	•		

Guideline Section	Sub-section	Description of Guideline	Supported by Password Safe	Supported by Privileged Remote Access	Supported by Privilege Management for Windows/ Mac	Supported by Privilege Management for Unix/ Linux
24: "A financial institution shall..."	(ix)	Implement technical measures to prevent the execution of unauthorized code on institution-owned or managed devices, network infrastructure and system components.			•	•
	(x)	Ensure that changes to system configurations are strictly controlled and monitored and that programs that can alter or override system configuration are restricted. This should also be applicable to remote connections.	•	•	•	•
	(xi)	Implement technologies and solutions to detect and block actual and attempted attacks or intrusions. This may include intrusion detection or prevention systems, endpoint security solutions (e.g., antivirus, a firewall, or a host intrusion detection system (HIDS) or host intrusion prevention system (HIPS)) or any other relevant solutions (e.g., an access gateway or a jump box), including on devices and in environments used for remote connections.	•	•	•	•
	(xv)	Ensure that users are prevented from installing unauthorized applications.			•	•

Logical Security Management

Guideline Section	Sub-section	Description of Guideline	Supported by Password Safe	Supported by Privileged Remote Access	Supported by Privilege Management for Windows/ Mac	Supported by Privilege Management for Unix/ Linux
25: "A financial institution shall..."	(i)	Identify and restrict logical access to its system resources to the minimum required for legitimate and approved work activities, according to the principle of need to know and least privilege.	•	•	•	•
	(ii)	Establish policies, protocols, and controls for access privileges and how they should be managed. The access privileges should be promptly revoked or adjusted upon change in employment status of employees and should be reviewed at least annually.	•	•	•	•
	(iii)	Establish strong security standards to deploy Application Programming Interfaces (APIs) which should as a minimum include:				
	a.	Measure to protect API keys of access tokens by implementing a comprehensive key management lifecycle that incorporates key generation, usage, storage, rotation, and eventual retirement.	•			
	(iv)	Establish dual control for access to critical systems, services, infrastructure and other assets.	•	•		
	(v)	Regularly review access to the information system to detect any unnecessary access or rights.	•		•	•
	(iv)	Ensure that unauthorized access to systems is blocked.	•	•		

Guideline Section	Sub-section	Description of Guideline	Supported by Password Safe	Supported by Privileged Remote Access	Supported by Privilege Management for Windows/ Mac	Supported by Privilege Management for Unix/ Linux
25: "A financial institution shall..."	(vii)	Ensure that there is limited and controlled access (logical, and/or remote access) to critical systems, services, infrastructures and other assets and that same are duly monitored logged with relevant audit trail.	•	•	•	•
	(viii)	Regularly review all access privileges according to defined procedures.			•	•
	(ix)	Regularly review all access privileges according to defined procedures.	•	•		
	(x)	Establish procedures for allocating privileged access which should also include delegated access on an on-demand or event-by-event basis for specific administrative activities as defined by the bank. The use of service accounts for administrative purposes should be tightly regulated and monitored. User and administrator accounts should be nominative and identifiable.	•	•		
	(xi)	Ensure that appropriate logs are maintained to identify access and activities by privileged users and users having access to critical systems, services, infrastructures and other assets or functions and any other systems, functions or applications as determined by the financial institution based on its risk assessments.	•	•		

Guideline Section	Sub-section	Description of Guideline	Supported by Password Safe	Supported by Privileged Remote Access	Supported by Privilege Management for Windows/ Mac	Supported by Privilege Management for Unix/ Linux
25: "A financial institution shall..."	(xii)	[Ensure] all privileged access or access to critical systems, services, infrastructures and other assets, functions or applications is monitored to detect anomalous behavior.	•	•		
	(xiv)	Implement controls to prevent unauthorized privilege escalation.			•	•
	(xv)	Develop capabilities, such as people, processes, and technology, to track privileged users' actions and access to sensitive systems in order to detect and prevent anomalous behavior and alert necessary personnel.	•	•	•	•
	(xx)	Establish credential requirements which among others take into consideration the risk level (e.g., multi-factor authentication for higher risk access).	•	•		
	(xxi)	Ensure that multi-factor authentication for employees and authorized third-parties is implemented for the following:				
	a.	All administrative accounts for critical operating systems, databases, applications, security appliances or network devices;	•	•		
	b.	All accounts for critical systems, services, infrastructures and other assets/applications which directly allow access to customer information through the internet (e.g. web-based applications, etc); and	•	•		
	c.	All instances of remote access which allows users connect to the network system of the financial institution.		•		

Guideline Section	Sub-section	Description of Guideline	Supported by Password Safe	Supported by Privileged Remote Access	Supported by Privilege Management for Windows/ Mac	Supported by Privilege Management for Unix/ Linux
27: "A financial institution shall..."	(i)	Automate the administration of information system access accounts to, inter alia, disable and/or delete disabled, temporary and emergency accounts after a predetermined period of time and to detect unauthorized access.	•			
	(iv)	Make use of one-time password for critical applications.	•			

Conclusion: BeyondTrust Satisfies Key Guideline Requirements

As outlined, BeyondTrust solutions provide many of the technological and risk management capabilities directly requested or recommended according to the Bank's guidance. Solutions **Password Safe** and **Privileged Remote Access** satisfy a substantial amount of the listed sub-section requirements – including points that might otherwise be difficult to comply with when using alternative or proprietary solutions. Additionally, **Privilege Management for Windows/Mac** and **Privilege Management for Unix/Linux** also satisfy a high number of requirements listed in the Bank's Guideline for Cyber and Technology Risk Management.

Password Safe enables organizations to manage privileged passwords, accounts, credentials, secrets, and sessions for all people and machines on their network. Password Safe also secures the passwords used for employee business applications, protecting the identity security of non-privileged human accounts for the entire organization. This ensures complete control and security over privileged account credentials and accounts, and logs and monitors all privileged activity and session for compliance and forensic review – a vital set of requirements outlined in the Bank of Mauritius's guideline.

Automated discovery, onboarding, a rotation of privileged passwords, secrets, and SSH keys further secures sensitive accounts from abuse or compromise. Within financial services, banking, or payment organizations, this level of privileged account security is desired by a wide array of international, national, and industry guidelines – including many key sub-sections specified by the Bank of Mauritius in the reference document.

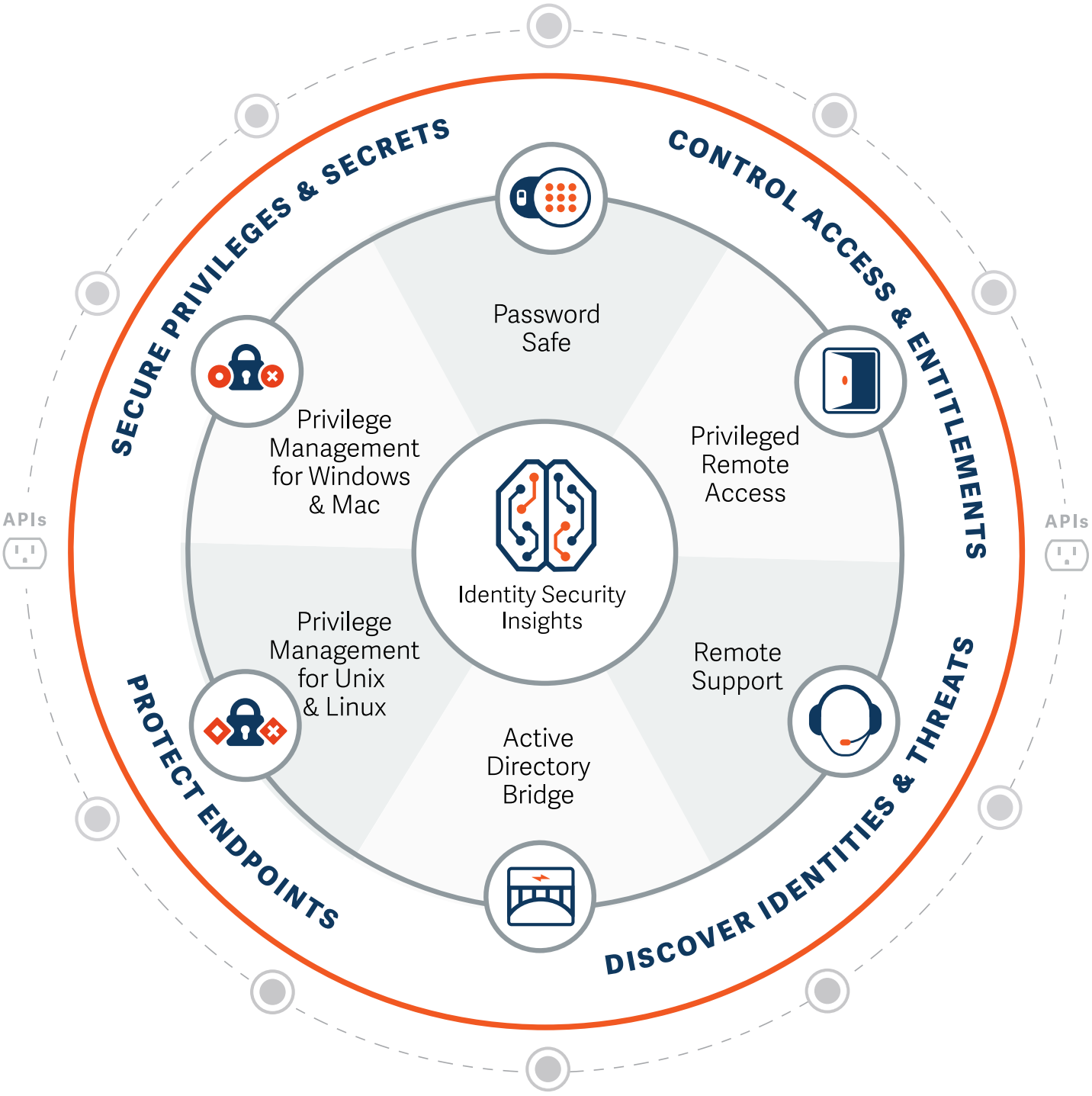
Privileged Remote Access is a solution designed to deliver simple, secure access for employees, third parties, and vendors anywhere in the world without the use of VPNs or known credentials. Additionally, this solution enables cloud engineers, DevOps teams, and other designated roles to connect to cloud infrastructure with secure connectivity, authentication, and auditability without introducing burdensome procedures.

As it relates to the Bank's Guideline for Cyber and Technology Risk Management, Privileged Remote Access also satisfies a number of vital requirements – particularly the sub-sections discussing secure remote access, infrastructure access, and remote session management controls. Privileged Remote Access's secure access capabilities enable least privilege, just-in-time access, and detail audit trails, forensics, and analytics – all available in real-time or post-session.

Privilege Management for Windows/Mac maps to a significant number of sub-section requirements across the reference document. Designed to remove local admin rights, enforce least privilege dynamically, and prevent malware deployment, this satisfies many of the requirements listed around privilege escalation, application execution, and attack surfaces. Privilege Management for Windows/Mac enforces tight and specified control over what application, programs, or navigation choices users are able to make – substantially reducing the vulnerability window.

Privilege Management for Unix/Linux applies root-level, fine-grained controls over privileges, enforcing elevation rules, tracking unauthorized activity, and maintaining real-time session monitoring across infrastructure. This prevents unauthorized code, scripts, or users from activating across Unix and Linux systems – a major requirement laid forth in the Bank of Mauritius's requirements. Additionally, Privilege Management for Unix/Linux enforces strict application and remote system controls, complete with tracking and monitoring – another highly sought requirement in the reference document.

The Complete BeyondTrust Platform



Password Safe

Manage privileged passwords, accounts, credentials, secrets, and sessions for people and machines, ensuring complete control and security — all while enabling zero trust.

Privileged Remote Access

Extend privileged access security best practices beyond the perimeter by granularly controlling, managing, and auditing remote privileged access for employees, vendors, developers, and cloud ops engineers.

Remote Support

Supercharge your service desk with secure access and support for any device, any system, from anywhere – including Windows, macOS, Linux, Android, & iOS.

Privilege Management for Unix & Linux

Achieve compliance, establish least privilege and zero trust, and prevent and minimize security breaches—without hurting productivity.

Privilege Management for Windows & Mac

Remove local admin rights, enforce least privilege dynamically across Windows and macOS, prevent malware and phishing attacks, and control applications without compromising productivity.

Identity Security Insights

Gain a centralized view of identities, accounts, entitlements, and privileged access across your IT estate and detect threats resulting from compromised identities and privileged access misuse.