



>>> Learn how BeyondTrust Privileged Access Management (PAM) solutions map to requirements set forth in the Central Bank of Egypt's Financial Cybersecurity Framework.

Mapping BeyondTrust Capabilities

to the **Egypt Financial Cybersecurity Framework**





TABLE OF CONTENTS

Overview

Authority

Roles

Methodology

Functions

Structure

How Beyondtrust Solutions Can Help?

Controls Chart

Cyber Risk Management

Inside Threat

Objective

Scope

Technology Capabilities

Flexible Deployment Options

Cyber Technology and Operations Capabilities

Identity and Access Management

Objective

Scope

Technology Capabilities

Endpoint Security

Objective

Scope

Technology Capabilities

Network Security

Objective

Scope

Technology Capabilities

Digital Channels

Objective

Scope

Technology Capabilities

Outsourcing and Vendor Management

Third-Party and Vendor Management

Objective

Scope

Technology Capabilities

Cloud Security

Objective

Scope

Technology Capabilities

Additional Resources

Overview

This guide has been prepared so that IT and security administrators can quickly learn how BeyondTrust Privileged Access Management (PAM) solutions map to requirements set forth in the Central Bank of Egypt's Financial Cybersecurity Framework.

The Central Bank of Egypt (referred to in this document as "The Authority" or "CBE") established the Financial Cybersecurity Framework as a starting point to bolster the cybersecurity posture and cybersecurity resilience for the financial sector of Egypt.

This framework incorporates several cybersecurity best practices and controls to be incorporated into financial sector cybersecurity programs. These best practices are based on the following core industry-accepted publications:

- NIST Cybersecurity Framework
- NIST SP 800-53, Revision 5
- PCI/DSS 3.2.1
- ISO 27001:2013
- CIS Controls



Authority

This framework is established relevant to Egyptian Laws and regulations under the legal standing of the CBE, as codified by Law No. 194 for 2020, in reference to the financial sector alongside other laws such as Egypt Law for Information Technology Crimes, Egypt Anti-Money Laundering by Law No. 80 for 2002, and its amendment.

Specific guidance issued by the Central Bank of Egypt on several topics directly addresses these laws and are covered by elements within this framework. As such, this framework must be broadly understood as the official guidance of the CBE as it relates to cybersecurity, technology, and risk management.

This framework is not intended to replace or overwrite any CBE regulations and is not considered as an approval license for new services; all banking and Financial Institutions working under Central Bank of Egypt supervision should follow the announced CBE regulations and follow the standard process for license approvals.

Roles

The Central Bank of Egypt, under legal authority, establishes strategic technical and policy standards and associated compliance requirements for regulated financial institutions to follow. Financial institutions operating within CBE areas of jurisdiction under Egyptian law must evaluate their cybersecurity posture against this framework using applicable assessment mechanisms, as provided by the CBE.

Methodology

The CBE has developed this cybersecurity framework to cover all controls based on different standards (NIST framework, ISO 27001/27002, CIS controls, PCI-DSS) by connecting three main pillars (people, process, technology) with five key functions and 23 domains (Figure 1).

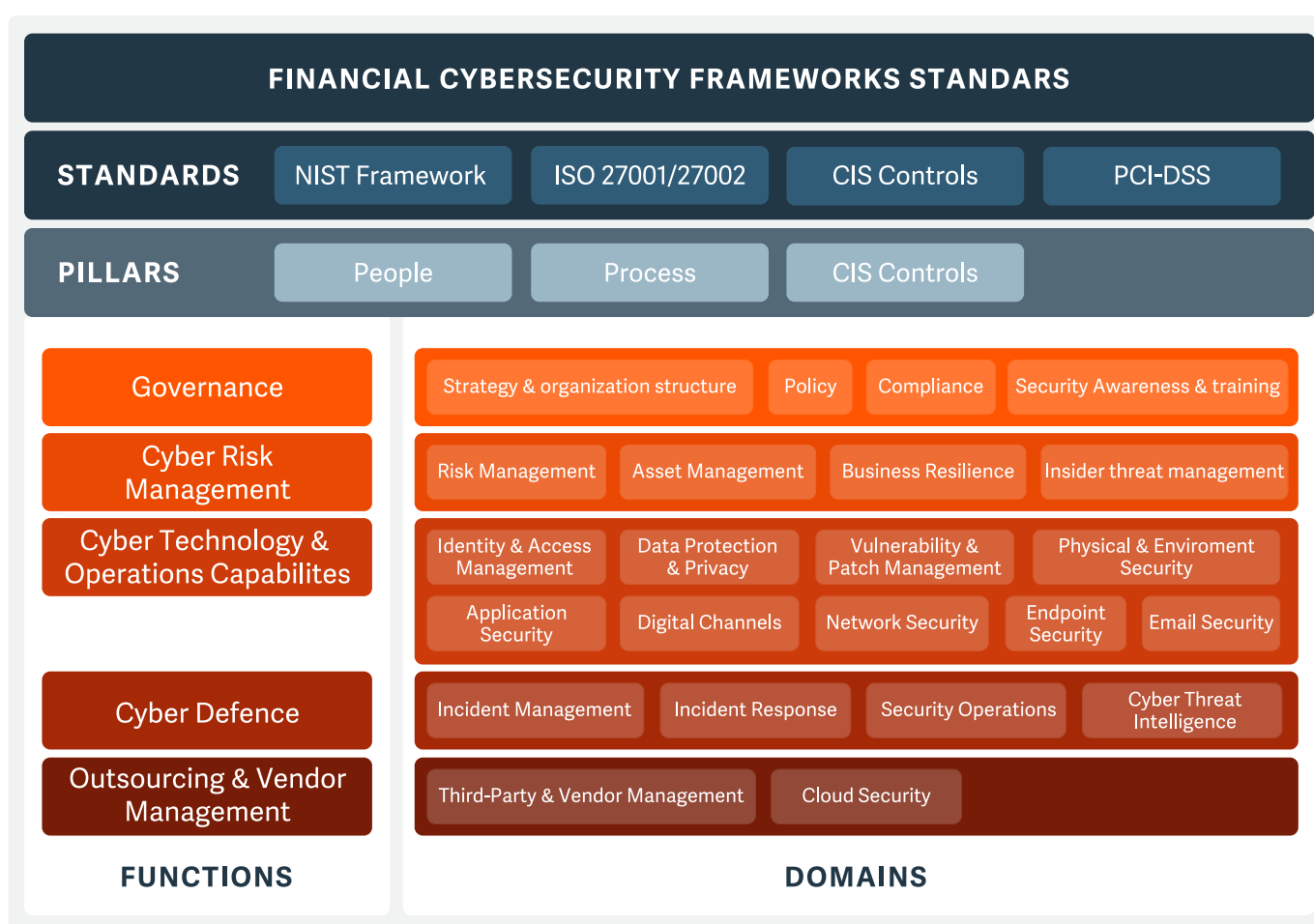


Figure 1: Functions and Domains

Disclaimer: The color mapping for referencing is the same between figure 1, 2 and 3

Functions

The overarching functions are organized as follows:

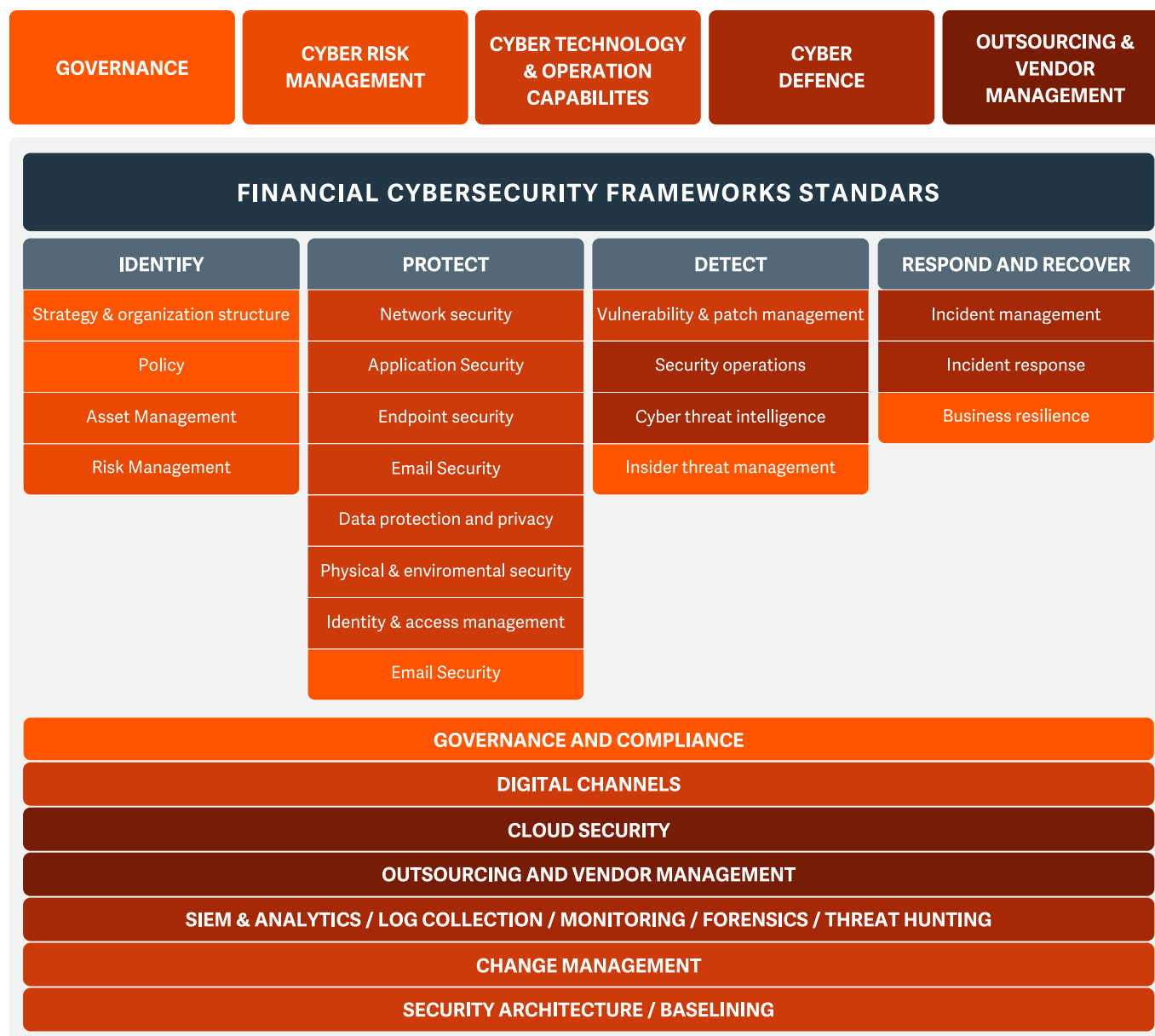


Figure 2: Framework Core functions mapped to NIST

The functions are organized for simplicity and logical division



Structure

Each domain is structured similarly to the following sections throughout the framework:

Subsection	Description
Objective	Identifies the objective for the domain and the threats that the associated controls aim to mitigate
Scope	Defines the overall scope of the domain to provide context, boundaries, and limitations
People	Highlights specific knowledge, competencies, and considerations for the individuals working in the domain
Process	Specifies policy-driven, process-based security controls that must be considered and implemented within the domain
Architecture Standards	Specifies the architecture and design standards that must be considered and implemented within the domain (where applicable)
Technology Capabilities	Details technology-based security controls and technical capabilities that must be considered and implemented within the domain
Control Baseline	Provides baseline controls from CIS that simplify the controls in v8
Governing Standards	Cross-referenced table of controls associated with the core publications and any additional relevant domain-specific documentation



How BeyondTrust Solutions Can Help?

BeyondTrust capabilities address 14 individual controls across 3 of the 5 main domains within the **CBE Financial Cybersecurity Framework**.

Listed below are the BeyondTrust solutions that map to the CBE Financial Cybersecurity Framework and related policy requirements.

- **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 limiting productivity.
- **Privilege Management for Windows and 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, and privileged access across your IT estate while leveraging threat intelligence recommendations to improve your identity security posture.



The tables on the following page will highlight the primary applicable CBE Financial Cybersecurity Framework requirements that are addressed by capabilities within BeyondTrust solutions. This is not an exhaustive list but includes the most relevant features for supporting the requirements of the CBE Financial Cybersecurity Framework.

Controls Chart

Outlined Below are specific controls that can be addressed by BeyondTrust solutions, to significantly reduce the risk related to identity-based risks.

Cyber Risk Management

Cyber Risk Management serves to align business operations and risk exposure to appropriate levels by implementing controls designed to mitigate against risks. This process begins by identifying and classifying business critical processes, assets, and risks, and then monitoring, managing, transferring, mitigating, or accepting risk.

Insider Threat

Objective

Insider Threat Management aims to safeguard intellectual property, prevent financial theft and fraud, protect brand reputation, and ensure the safety of personnel from employees or contractors misusing their access to the organization's systems or workspace. Insider threats pose significant counterintelligence and counterespionage risks because, unlike external threats, insiders possess knowledge of, and access to, the organization's security practices, data, and systems. This provides ample opportunity to misuse existing access or enable access to unauthorized individuals remotely.



Scope

Insider Threat Management focuses on monitoring authorized individuals, such as employees and contractors, to proactively identify, understand, and address risky or unintended behaviors. Insider Threat Management also applies to third parties such as subcontractors, consultants, partners, and customers with authorization to access organizational assets. Mitigating the risk posed from an insider threat takes a holistic and tailored approach that accounts for both legal and human resource sensitivities.

Technology Capabilities

Section	Reference # of the security control	Security Control Area	Reference # of the security control sub-area	Security Control sub-area	Control Reference	Control	Password Safe	Privileged Remote Access	Privilege Management (Unix, Linux, Windows, Mac)
Security governance & security processes	2.4	Insider Threat Management	2.4.5	Advanced Forensics	2.4.5.b	Tool(s) deployed to collect and preserve sources of potential evidence to support for legal or human resource efforts associated with insider threats. Tool(s) should be capable of all functionalities identified in Section 3.2 Incident Response.	•	•	•



Cyber Technology And Operations Capabilities

Cyber Technology and Operations Capabilities aims to prevent attempts by adversaries to successfully compromise an organization's network. Cyber Technology and Operations Capabilities largely focuses on security architecture, configuration baselines, and systems hardening.

Identity and Access Management

Objective

Identity and Access Management (IAM) aims to provision or revoke access for users and systems to operate on the organization's enterprise. A secondary purpose of IAM is to ensure users are only granted minimal levels of access, as is needed to perform core job functions. This is applied with different requirements based on whether the person requiring access is a combination of typical user, privileged user, employee, contractor, or customer.

Scope

AM is a foundational component across all elements within Cyber Technology and Operations Capabilities. Enhancing IAM security is one of the most fundamental steps that must be prioritized and resourced as cyber attackers often leverage authentication bypass techniques and use stolen credentials and privilege escalation when breaching a system.

Enhancing IAM security can prevent the following common threats:

- Unauthorized access
- Unauthorized modification
- Credential theft
- Social engineering
- Phishing
- Privilege escalation
- Brute force
- Password spray
- Credential dumping

Identity and Access Management applies to users, data, applications, and endpoints, and should emphasize all components of the access management lifecycle to include:

- Provisioning
- Token Management
- Entitlement Management
- Privilege Auditing
- Credential Vaulting
- Privileged Access Management

Note that organization specific systems have more specific IAM requirements identified and described in Section 4.8 Digital Channels.



Figure 15: Identity and Access Management Architecture Example



Technology Capabilities

Section	Reference # of the security control	Security Control Area	Reference # of the security control sub-area	Security Control sub-area	Control Reference	Control	Password Safe	Privileged Remote Access	Privilege Management (Unix, Linux, Windows, Mac)
Cyber technology and Operations capabilities	4.1	Identity and Access Management	4.1.5	Identity & Privileged Access Management Tools	4.1.5c	Tool(s) deployed provide heightened visibility and security when exercising identity and privileged access. The system should be capable of the following: • Credential management • Entitlement provisioning • Multi-factor authentication • Geographic requirements • Posture check • Virtualized infrastructure • Time restrictions • Enhanced alerting • Behavior analytic	•	•	•
				Session Recording	4.1.5.d	Tool(s) deployed record all activity associated with high-risk, highly sensitive, or privileged activity. The recording is maintained in an immutable format and is reviewed by outside auditors on a regular basis at least annually.	•	•	•
				Password Vaulting	4.1.5.e	Tool(s) deployed to store and manage access to passwords across the organization. This is leveraged to randomize local passwords to prevent re-use across multiple systems. System is tightly controlled and integrated into the SIEM.	•	•	



Section	Reference # of the security control	Security Control Area	Reference # of the security control sub-area	Security Control sub-area	Control Reference	Control	Password Safe	Privileged Remote Access	Privilege Management (Unix, Linux, Windows, Mac)
Cyber technology and Operations capabilities	4.1	Identity and Access Management	4.1.5	Service Account Management	4.1.5.f	System is employed to manage service accounts in use by services and applications or database connections to ensure regular password rotation to comply with password-aging requirements. This system ensures that passwords are not stored or managed within application source code or configuration files.	•		
				Centralized Access Management	4.1.5.g	System(s) federate access across the organization to eliminate local accounts and shared credentials. This is important when managing infrastructure and network devices where traditional federated services such as AD and LDAP may not be natively supported.	•	•	•

Endpoint Security

Objective

Endpoint Security aims to protect servers, desktops, and workstations that employees, third parties, and contractors use to connect to the organization's network.

Implementing Endpoint Security using comprehensive standards and technical controls can prevent:

- Malware infections
- Command and Control activity
- Data exfiltration
- Ransomware/Data destruction
- Privilege escalation
- Lateral movement



Scope

Endpoints can be physical or virtual including servers, databases, desktops, workstations, mobile devices, automated teller machines, and point-of-sale (POS) systems. The endpoint location and function assist in deciding the required level of security controls needed and should account for common and unique risks posed by on-premises, off-premises, cloud, third-party, and telework devices.

Technology Capabilities

Section	Reference # of the security control	Security Control Area	Reference # of the security control sub-area	Security Control sub-area	Control Reference	Control	Password Safe	Privileged Remote Access	Privilege Management (Unix, Linux, Windows, Mac)
Cyber technology and Operations capabilities	4.6	Endpoint Security	4.6.5	Application Control/ Allow-Listing	4.6.5.l	Tool(s) deployed provide administrators the ability to restrict applications on the endpoint to run only those explicitly permitted. The software is integrated into a central console and reporting system for analysis, correlation, and alerting as described in Section 3.3 Security Operations.			•
				Database activity monitoring	4.6.5.r	Tool(s) supports the ability to identify and report on fraudulent, illegal, or other undesirable behaviors on critical databases, with minimal impact on user operations and productivity.	•	•	

Network Security

Objective

Network Security aims to protect data and information in transit, ensure proper network visibility, limit network access to only authorized endpoints, and take corrective actions on malicious activity discovered.



Implementing comprehensive network security standards and technical controls can prevent the following threats:

- Unauthorized access
- Network reconnaissance
- Malware infections
- Data exfiltration
- Command and Control activity

Scope

The network is the underpinning foundation that enables access to, from, and through endpoints, clouds, and applications, regardless of geographic location. Network Security focuses on the logical structure, policies, processes, and technologies to protect data in transit and remote connectivity to physical or virtual systems.

Technology Capabilities

Section	Reference # of the security control	Security Control Area	Reference # of the security control sub-area	Security Control sub-area	Control Reference	Control	Password Safe	Privileged Remote Access	Privilege Management (Unix, Linux, Windows, Mac)
Cyber technology and Operations capabilities	4.7	Network Security	4.7.6	Jump Host	4.7.6.b	System(s) employed to regulate access to sensitive and critical systems by serving as a hardened, single ingress point. The jump host should be designed to perform administrative and privileged tasks. Jump host activity is integrated into a central console and reporting system for analysis, correlation, and alerting as described in Section 3.3 Security Operations.	•	•	



Section	Reference # of the security control	Security Control Area	Reference # of the security control sub-area	Security Control sub-area	Control Reference	Control	Password Safe	Privileged Remote Access	Privilege Management (Unix, Linux, Windows, Mac)
Cyber technology and Operations capabilities	4.7	Network Security	4.7.6	Secure Privileged Access	4.7.6.d	Tool(s) deployed to regulate access for administrative and management network functions. Network devices must support centralized, privileged authentication such as TACACS or RADIUS. Privileged access activity is integrated into a central console and reporting system for analysis, correlation, and alerting as described in Section 3.3 Security Operations.		•	
			4.7.6	Virtual Private network	4.7.6.t	Tool(s) that extends a private network across a public network and enables users to send and receive data across shared or public networks by using several types of VPN. Host-to-Site: This may be used for teleworkers who need access to the private networks and allow the teleworkers to access important assets without exposing them to the public internet. NOTE: No Site-to-Site VPN capability		•	



Digital Channels

Objective

The goal of **Digital Channels** is to align with industry-specific security concerns and technology with components outlined by this cybersecurity framework, Egypt's FinTech and Innovation Strategy, the National Vision 2030, and CBE regulations for mobile payments and internet banking. Digital Channels supports the security controls needed to protect against threats, including those listed below. These controls are also designed to align with modern and emerging technology as society shifts towards a digital and predominantly cashless economy.

Named financial threats include:

- Abuse
- Fraud
- Financial theft
- Identity theft
- Money laundering
- Terror financing
- Legal compliance

Scope

Digital Channels spans both consumer financial technology as well as bank-specific backend processing. Designed to integrate with organizational, national, and international systems, these include but are not limited to:

- Payment processing systems
- Clearing systems
- Settlement systems
- Trading platforms
- Micro-Finance applications
- Mobile wallets
- Point-of-sale systems
- Bill payment platforms
- Automated financial kiosks



Section	Reference # of the security control	Security Control Area	Reference # of the security control sub-area	Security Control sub-area	Control Reference	Control	Password Safe	Privileged Remote Access	Privilege Management (Unix, Linux, Windows, Mac)
Cyber technology and Operations capabilities	4.8	Digital Channels	4.8.5	Privileged Access Management	4.8.5.e	Tool(s) deployed to provide heightened visibility and security when exercising privileged access.	•	•	

Outsourcing And Vendor Management

Third-Party and Vendor Management

Objective

Identity and Access Management (IAM) aims to provision or revoke access for users and systems to operate on the organization's enterprise. A secondary purpose of IAM is to ensure users are only granted minimal levels of access, as is needed to perform core job functions. This is applied with different requirements based on whether the person requiring access is a combination of typical user, privileged user, employee, contractor, or customer.

Scope

Third-Party and Vendor Management covers services ranging from technical support—including IT help desks and cybersecurity infrastructure management—to foundational facility operations such as electricians, air conditioning mechanics, or custodial services. Each vendor relationship must be considered independently, as the vendor's level of access to physical premises and IT systems will vary.



Technology Capabilities

Although no specific technology-based controls are included in the official report, BeyondTrust's Privileged Access Management platform enables you to secure, manage, and audit external vendors and contractors' privileged access without using a VPN. Eliminate "all or nothing" remote access for vendors or privileged insiders with granular, role-based access to specific systems. BeyondTrust also simplifies access processes by providing one tool built to facilitate all unattended access for remote systems and endpoints.

Third-Party and Vendor Management

Objective

Cloud Security aims to address the unique risks posed by using Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), or Software-as-a-Service (SaaS) cloud computing offerings. While cloud computing technologies may be viewed by some as novel, they are derivative of many legacy technologies. By shifting the ownership of on-premises servers and hosting services to off-premises, third-party vendors and organizations may be utilizing infrastructure that does not reside within Egyptian jurisdiction.

Therefore, Cloud Security addresses the following threats:

- Unauthorized access
- Data privacy
- Lateral movement between and within cloud tenants
- Virtualization vulnerabilities
- Expansive attack surface



Scope

Cloud Security encompasses virtualized infrastructure, platform, or software services by a cloud service provider (CSP). This domain covers private or multi-tenant clouds and does not differentiate the level of implementation from Infrastructure to Platform to Software. Cloud Security builds upon existing best practices and security controls already addressed by endpoint, application, network, third-party, and vendor domains.

The cloud security controls defined within this section are to be considered the minimum proposed security controls to be followed and will become CBE cloud regulations.

Technology Capabilities

Section	Reference # of the security control	Security Control Area	Reference # of the security control sub-area	Security Control sub-area	Control Reference	Control	Password Safe	Privileged Remote Access	Privilege Management (Unix, Linux, Windows, Mac)
Cyber technology and Operations capabilities	5.2	Cloud Security	5.2.2	Cloud Security Posture Management (CSPM)	5.2.5.b	A tool used to continuously monitor and identify risks from intentional or unintentional misconfigurations within a cloud environment.			
				Privileged Access Management	5.2.5.h	A tool is deployed to provide heightened visibility and security when exercising privileged access.	•	•	



Additional Resources

FREE TOOL

Privileged Access Discovery Application: Utilize the most powerful free tool available to scan your environment and pinpoint overprivileged accounts, service accounts, unused accounts, privileged credentials, remote access tools, and more.

TAKE THE TEST

Need a VPN Alternative? Take the Remote Access Test: Learn if your team has the appropriate secure remote access tools in place to handle the large volume of users who are connecting remotely into your network.

WHITEPAPER

Cybersecurity Survival Guide: Access the tips and strategies that can help you steer clear of the landmines in the cybersecurity landscape.

VIDEO

Intelligent Identity and Access Security: Watch the overview video to learn how our unique platform approach leaves no privilege left unmanaged.

REPORT

10th Microsoft Vulnerabilities Report 2023: See into the past, present, and future of the vulnerability landscape.

ABOUT BEYONDTRUST

BeyondTrust is the worldwide leader in intelligent identity and access security, empowering organizations to protect identities, stop threats, and deliver dynamic access to empower and secure a work-from-anywhere world. Our integrated products and platform offer the industry's most advanced privileged access management (PAM) solution, enabling organizations to quickly shrink their attack surface across traditional, cloud and hybrid environments.

With a heritage of innovation and a staunch commitment to customers, BeyondTrust solutions are easy to deploy, manage, and scale as businesses evolve. We are trusted by 20,000 customers, including 75 of the Fortune 100, and a global partner network. Learn more at beyondtrust.com