BeyondTrust

Mapping BeyondTrust Capabilities to the Financial Regulatory Authority (FRA) Framework

This document is informational and is intended to provide guidance on how organizations may use BeyondTrust products to meet their own obligations under the Egyptian Financial Regulatory Authority (FRA) cyber security framework. BeyondTrust is not representing that we are subject to or compliant with Egyptian FRA.

BeyondTrust

TABLE OF CONTENTS

Overview

The Financial Regulatory Authority (FRA) governs non-banking financial services in Egypt, ensuring market stability, protecting consumers, and driving digital transformation.

In July 2023, Egypt's Financial Regulatory Authority (FRA) issued a comprehensive framework for technology governance and risk management across the non-banking financial sector.

This whitepaper explains the FRA compliance requirements in detail, identifies the key challenges, and demonstrates how using BeyondTrust solutions can enable customers to achieve compliance efficiently while strengthening overall security posture.

What is the Policy Objective?

This regulation, which applies to insurance, leasing, factoring, consumer finance, and fintech companies in Egypt, sets stringent requirements for cybersecurity, data protection, governance, and IT infrastructure.

The FRA framework introduces data sovereignty, stricter cybersecurity controls, and continuous oversight. Non-compliance may result in penalties, loss of license, and reputational risk.

There are three frameworks within the main policy:

- **IT Governance (ITG-F)**: Ensures board-level oversight, IT service management, data classification, and structured governance processes. Note: BeyondTrust solutions do not apply to this framework.
- **Technology Risk Management (TRM-F)**: Defines risk prevention, cybersecurity, resilience, incident handling, and business continuity, based on global standards such as NIST and ISO.
- **Cybersecurity Management Framework (CSM-F)**: Consists of strategic processes at the strategic level, planning processes at the executive level, and implementation procedures at the operational level.

What are FRA Compliance Requirements?

The FRA framework is extensive and covers multiple layers of organizational readiness. Key requirements include:

1. Infrastructure

- Licensed, up-to-date operating systems and servers
- Local data centers located within Egypt
- Redundancy and disaster recovery sites to ensure high availability
- Virtualization technologies must be hardened and monitored
- Segmentation of production, testing, and development environments

2. Cybersecurity Controls

- Next-Generation Firewalls (NGFW) and Web Application Firewalls (WAF)
- Encryption of data at rest and in transit using industry standards
- Antivirus and Endpoint Detection & Response (EDR) solutions deployed organization-wide
- Annual penetration testing and vulnerability assessments

- Incident response plans, tested regularly, and reporting of incidents to the FRA within 24 hours
- Secure coding standards for applications
- Multi-factor authentication for system access

3. Data Protection

- Customer data must remain within Egypt's geographical boundaries
- Logging and monitoring of all activities, retained for at least 5 years
- Centralized log management with real-time monitoring
- Data classification policies to ensure sensitive data is handled appropriately
- Secure backup systems with encryption and off-site storage

4. Governance

- IT and Risk Committees established at board level
- Clear segregation of duties for IT, risk, and audit functions
- Service Level Agreements (SLAs) with customers to guarantee performance and availability
- 24/7 customer support centers with documented escalation procedures
- Independent internal and external audits performed periodically

5. Outsourcing & Vendors

- Outsourced services and third-party vendors must comply with FRA requirements
- Service providers must undergo due diligence and risk assessments
- Vendor contracts require FRA approval and monitoring
- Outsourced cloud services must host data in Egypt and meet all FRA security standards

Mapping FRA Requirements to BeyondTrust Solutions

The table below maps how using BeyondTrust solutions can help FRA-dependent organizations comply with the different requirements and frameworks.

Requirements		BeyondTrust Products	Main Capabilities
TRM-F: Technology Risk Management Framework (Pg. 27)			
Strategic Operations: 1. Framing Risk 2. Assessing Risk 3. Responding to Risk 4. Monitoring of Risk		Identity Security Insights	Cross domain visibility, True Privilege graphical intelligence, AI/ML-powered security recommendations, identity security risks visibility, insights driven actions
CSM-F : Cybersecurity Management Framework (Pg. 40)			
إدارة الهوية والمصادقة والتحكم فـ ى الوصـول (Access & Authentication Control :) ويقصد به الوصول إلى الأصول المادية والمنطقيـة والم لحقـا ت المرتبطة بها على المستخدمين المعتمدين والعمليات والأجهزة ، ويتم إدارتهـا بما يتفق مع المخاطر المقدرة للوصول غيـر المـصرح بـه إلـى الأنـشطة والمعاملات المصرح بها .	Identity, Authentication & Access Control Management (controlling access to physical and logical assets for authorized users, processes, and devices in line with assessed risk).	Password Safe Privileged Remote Access Entitle	JIT access, session management, access control, least privilege access, role-based access
2. Protect (Pg. 41)			
التكنولوجيا الوقائية (Technology Protective :) ويقصد به أن تـدار الحلـول الأمنية التكنولوجية لضمان أمن ومرونة الأنظمة والأصول ، بما يتوافـق مـع السياسات والإجراءات والاتفاقيات ذات الصلة	Protective Technology (managing security technology solutions to ensure the security and resilience of systems and assets in line with relevant policies, procedures, and agreements).	Identity Security Insights Password Safe Privileged Remote Access Endpoint Privilege Management Entitle	Least Privilege enforcement, just-in-time access, role based access, identity threat detection, identity risk assessment
3. Detect (Pg. 41)			
الأحداث غير المألوفة والنمطية (Events & Anomalies :) ويقصد به الكـشف عن الأنشطة غير المألوفة وفهم التأثير المحتمل للأحداث .	Anomalies & Events (detecting unusual activities and understanding the potential impact of events).	Identity Security Insights	Cross domain visibility, True Privilege graphical intelligence, AI/ML-powered security recommendations, identity security risks visibility, insights driven actions, paths to privilege detection
تحسين عمليـ ة الرصـد (Improvement Process Detection :) ويقـصد بـه تحديث عملي ة الرصد وإجراءاتها واختبارها بما يتناسب مع مـا يطـرأ مـن أحداث غير متوقعة .	Detection Process Improvements (updating and testing monitoring processes and procedures in response to emerging and unexpected events).	Identity Security Insights	Cross domain visibility, True Privilege graphical intelligence, AI/ML-powered security recommendations, identity security risks visibility, insights driven actions, paths to privilege detection

Authentication and Access Control (Pg. 45)			
إصدار الهويات وبيانات الاعتماد وإدارتها والتحقق منها وإبطالها وتدقيقها للأجهزة والمستخدمين والعمليات المصرح لهم .	Identity and Credential Lifecycle Management (issue, manage, verify, revoke, and audit identities and credentials for authorized devices, users, and processes).	Password Safe Privileged Remote Access Entitle	Authentication (Local, LDAP, SSO, MFA), role-based access, ccess control, session management , JIT access
إدارة وحماية الوصول المادى إلى الأصول .	Manage and protect physical access to assets.	Password Safe Privileged Remote Access	Privileged access management, remote access management, session management
إدارة الوصول عن بعد .	Manage remote access.	Password Safe Privileged Remote Access	Privileged access management, remote access management, session management
· إدارة أذونات وتصاريح الوصول ، بما ف ى ذلك مبادئ الحد الأدنى من الامتياز والفصل بين الواجبات .	Manage access permissions and authorizations, including least privilege and segregation of duties.	Password Safe Privileged Remote Access Endpoint Privilege Management Entitle	Role-based access, JIT access, least privilege enforcement, access and session management
سلامة الشبكة محمية (على سبيل المثال ، الفصل بين الشبكات وتجزئة الشبكة) .	Protect network integrity (e.g., network separation and segmentation).	Password Safe Privileged Remote Access Remote Support	Segregated access, privileged sessions gateway, secure remote access
· إثبات الهوي ة الرقمية وربطها بعوامل ا لتعريف والتأكيد عليها فـ ى كل المعاملات طبقًا لضوابط الهيئة الصادرة فى هذا الشأن .	Verify digital identity and bind it to authentication/assurance factors for all transactions, in accordance with the authority's controls.	Password Safe Privileged Remote Access Remote Support Entitle	Authentication (Local, LDAP, SSO, MFA), role-based access, access control, session management , JIT access
Maintenance (Pg. 47)			
· تنفيذ عمليات الصيانة والإصلاح للأصول التنظيمية وتسجيلها باستخدام الأدوات المعتمدة والتى تم معايرتها .	Perform and record maintenance and repair activities for organizational assets using approved and calibrated tools.	Privileged Remote Access Remote Support	Remote access, remote support, session management, privileged access control and monitoring
Protective Technology (Pg. 47)			
استخدام مبدأ "الوظيفة الأقل لزوما " فى إعدادات التهيئة لعناصر مكونات الأنظمة لتوفير القدرات الأساسية فقط .	Apply the principle of Least Privilege in system component configurations, enabling only essential capabilities.	Endpoint Privilege Management	Least privilege enforcement, granular elevation of privileges, application control
Detect Anomalies & Events (Pg. 48)			
تحديد السلوك النمط ى لتشغيل الشبك ات و التدفقات المتوقعة للبيانات المتداولة بين المستخدمين والأنظمة .	Define baseline behavior for network operations and expected data flows between users and systems.	Identity Security Insights	Cross domain visibility, True Privilege graphical intelligence, AI/ML-powered security recommendations, identity security risks visibility, insights driven actions
تحليل الأحداث المكتشفة غير المألوفة بغرض فهم أهداف وأساليب الهجوم .	Analyze detected anomalous events to understand attack objectives and methods.	Identity Security Insights	Cross domain visibility, True Privilege graphical intelligence, AI/ML-powered security recommendations, identity security risks visibility, insights driven actions

جمع بيانات الأحداث وربطها من مصادر وأجهزة استشعار متعددة .	Collect and correlate event data from multiple sources and sensors.	Identity Security Insights	Cross domain visibility, True Privilege graphical intelligence, AI/ ML-powered security recommendations, identity security risks visibility, insights driven actions
إدارة وحماية الوصول المادى إلى الأصول .	Manage and protect physical access to assets.	Password Safe Privileged Remote Access	Privileged access management, remote access management, session management
إدارة الوصول عن بعد .	Manage remote access.	Password Safe Privileged Remote Access	Privileged access management, remote access management, session management
· إدارة أذونات وتصاريح الوصول ، بما ف ى ذلك مبادئ الحد الأدنى من الامتياز والفصل بين الواجبات .	Manage access permissions and authorizations, including least privilege and segregation of duties.	Password Safe Privileged Remote Access Endpoint Privilege Management Entitle	Role-based access, JIT access, least privilege enforcement, access and session management
سلامة الـشبكة محميـة (علـى سـبيل المثـال ، الفـصل بـين الـشبكات وتجزئة الشبكة) .	Protect network integrity (e.g., network separation and segmentation).	Password Safe Privileged Remote Access Remote Support	Segregated access, privileged sessions gateway, secure remote access
· إثبات الهوي ة الرقمية وربطها بعوامل ا لتعريـف والتأكيـد عليهـا فـ ى كـل المعاملات طبقًا لضوابط الهيئة الصادرة فى هذا الشأن .	Verify digital identity and bind it to authentication/assurance factors for all transactions, in accordance with the authority's controls.	Password Safe Privileged Remote Access Remote Support Entitle	Authentication (Local, LDAP, SSO, MFA), role-based access, access control, session management , JIT access
Maintenance (Pg. 47)			
· تنفيذ عمليات الصيانة والإصلاح للأصـول التنظيميـة وتـسجيلها باسـتخدام الأدوات المعتمدة والتى تم معايرتها .	Perform and record maintenance and repair activities for organizational assets using approved and calibrated tools.	Privileged Remote Access Remote Support	Remote access, remote support, session management, privileged access control and monitoring
Protective Technology (Pg. 47)			
استخدام مبدأ "الوظيفة الأقل لزوما " فى إعدادات التهيئـة لعناصـر مكونـات الأنظمة لتوفير القدرات الأساسية فقط .	Apply the principle of Least Privilege in system component configurations, enabling only essential capabilities.	Endpoint Privilege Management	Least privilege enforcement, granular elevation of privileges, application control
Detect Anomalies & Events (Pg. 48)			
تحديد السلوك النمط ى لتشغيل الشبك ات و التدفقات المتوقعة للبيانـات المتداولـة بين المستخدمين والأنظمة .	Define baseline behavior for network operations and expected data flows between users and systems.	Identity Security Insights	Cross domain visibility, True Privilege graphical intelligence, AI/ ML-powered security recommendations, identity security risks visibility, insights driven actions
تحليل الأحداث المكتشفة غير المألوفة بغرض فهم أهداف وأساليب الهجوم .	Analyze detected anomalous events to understand attack objectives and methods.	Identity Security Insights	Cross domain visibility, True Privilege graphical intelligence, AI/ ML-powered security recommendations, identity security risks visibility, insights driven actions

جمع بيانات الأحداث وربطها من مصادر وأجهزة استشعار متعددة .	Collect and correlate event data from multiple sources and sensors.	Identity Security Insights	Cross domain visibility, True Privilege graphical intelligence, AI/ ML-powered security recommendations, identity security risks visibility, insights driven actions
تحديد تأثير الأحداث .	Determine the impact of events.	Identity Security Insights	Cross domain visibility, True Privilege graphical intelligence, AI/ ML-powered security recommendations, identity security risks visibility, insights driven actions
وضع إعدادات ودراجات للتنبيه بالحوادث .	Configure incident alert settings and escalation levels.	Identity Security Insights	Cross domain visibility, True Privilege graphical intelligence, AI/ ML-powered security recommendations, identity security risks visibility, insights driven actions
Continuous Monitoring (Pg. 48)			
رصد نشاط الأفراد لاكتشاف أحداث الأمن السيبرانى المحتملة	Monitor user activity to detect potential cybersecurity events.	Identity Security Insights Password Safe Remote Support	Session monitoring, session recording, Identity threat detection and response
الأمن السيبرانى المحتملة .	Monitor third-party service provider activity to detect potential cybersecurity events.	Identity Insights Password Safe Privileged Remote Access Remote Support	Session monitoring, session recording, Identity threat detection and response

Practical Guide to Achieving FRA Compliance

The FRA framework sets a new standard for cybersecurity and governance in Egypt's non-banking financial sector.

Using BeyondTrust solutions, organizations can execute the following steps to streamline and accelerate their alignment to compliance.

Step 1: Assess Current State

Conduct a free, Identity Security Risk Assessment, using our award-winning tool, to gain cross-domain visibility into identities, accounts, privileges, and access paths. Identify excessive permissions, orphaned accounts, and hidden attack paths that may violate FRA requirements. This risk assessment yields immediate, actionable intelligence and establishes a clear, data-driven baseline to prioritize remediation efforts.

Step 2: Identify Key Controls

Focus on high-impact control areas such as privileged access, session monitoring, and endpoint privilege enforcement. The goal should be to quickly reduce standing privileges by enforcing least privilege and just-in-time access, while strengthening authentication and access governance, without slowing down day-to-day productivity. Once you identify these control areas post-assessment, you can leverage cybersecurity solutions to achieve better security posture, shrink the attack surface, and better align with FRA's core security expectations.

Step 3: Implement BeyondTrust Solutions

Deploy cloud infrastructure entitlement management (CIEM), privileged account and session management (PASM), and secure remote access capabilities that secure identities, endpoints, and remote access pathways through centralized policy enforcement. Enable just-in-time access, credential vaulting, and secure remote sessions to eliminate persistent privileges and limit attack surfaces. Integrating these controls ensures consistent enforcement across cloud, on-prem, and hybrid environments.

Step 4: Monitor and Audit Continuously

Establish continuous monitoring of user activity, privileged sessions, and access events across the environment. Capture detailed logs and session recordings to support real-time detection, forensic investigations, and audit requirements. Centralized visibility ensures organizations can quickly respond to incidents and demonstrate ongoing compliance.

Step 5: Report and Improve

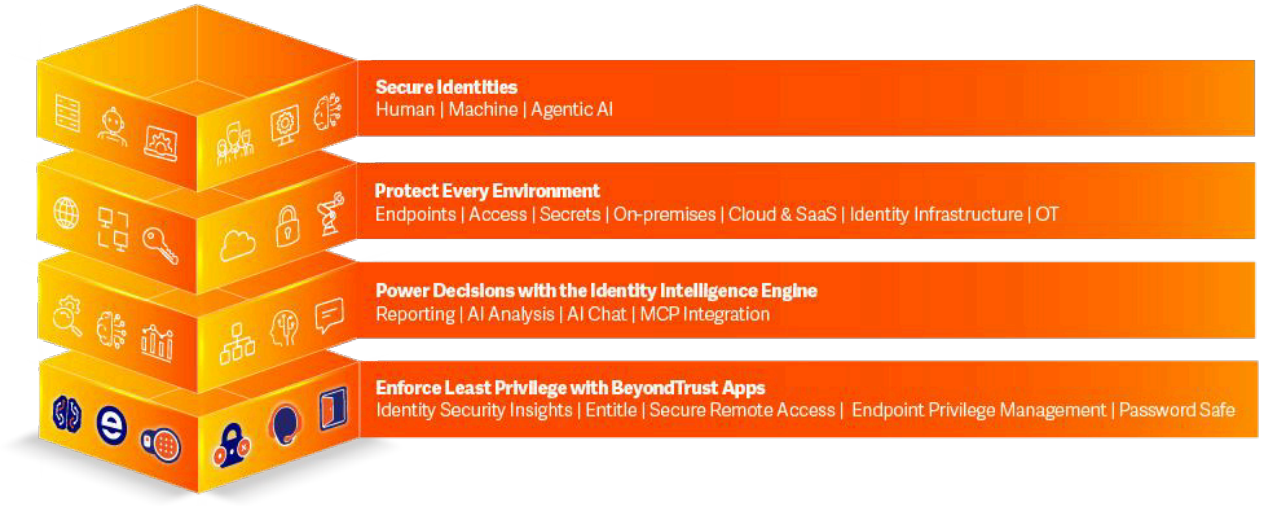
Deliver clear, audit-ready reports that map security controls and activities directly to FRA requirements. Provide stakeholders and regulators with evidence of enforcement, risk reduction, and policy adherence. Continuously refine access policies and controls based on insights to strengthen security posture over time.

The BeyondTrust Pathfinder Platform

The BeyondTrust Pathfinder Platform unifies identity visibility, intelligence, and control in a single, AI-driven control plane. It maps and manages privilege relationships across human, machine, AI agent, and workload identities—revealing hidden Paths to Privilege™ and enabling proactive risk reduction across the entire identity attack surface.

BeyondTrust delivers what industry experts consider to be the complete spectrum of privileged access management solutions. BeyondTrust was named a Leader in the The Forrester Wave™: Privileged Identity Management Solutions, Q3 2025 report, the Gartner® Magic Quadrant™ for Privileged Access Management, and the 2026 GigaOm Radar for Cloud Infrastructure Entitlement Management (CIEM). We believe these accolades reflect strong execution and a comprehensive vision for identity security.

As a centrally managed, extensible platform, Pathfinder allows organizations to deploy a full set of PAM and identity security capabilities at once—or adopt them incrementally over time—while maintaining unified visibility, consistent policy enforcement, and operational efficiency from a single, unified console.



Identity Security Insights® – Gives organizations unified visibility into identity risk by continuously analyzing human and non-human identities, privileges, and access paths, revealing hidden escalation risks and enabling proactive threat detection.

Entitle - Cuts off privilege attack paths by eliminating always-on access, replacing it with just-in-time (JIT) automation that reduces risk without slowing down organizations.

Password Safe® - Enables automated discovery, onboarding, management, and auditing of all privileged accounts, privileged credentials (passwords, secrets, keys, etc.).

Privileged Remote Access - Delivers secure, just-in-time remote access to cloud, on-premises, and OT environments—using identity-based controls, credential injection, and session auditing —without relying on traditional VPNs.

Endpoint Privilege Management - Enforces least privilege and application control across Windows, macOS, Unix, and Linux systems by removing standing administrative rights and granting elevated access only to approved applications and tasks.

Remote Support – Enables service desk technicians to support any user or device, anywhere, all while ensuring enhanced security. Applies least privilege and robust audit controls to all remote access required by employees, vendors, and service desks.

Active Directory Bridge - Extends Microsoft Active Directory authentication, single sign-on (SSO), and policy controls to Unix and Linux systems, enabling centralized identity governance, consistent access enforcement, detailed auditing, and compliance across mixed operating system environments

Conclusion

While compliance may appear complex, BeyondTrust solutions can help make it achievable. By aligning FRA requirements with BeyondTrust's privilege-centric identity security platform, organizations can:

- Ensure regulatory compliance
- Strengthen cybersecurity defenses
- Protect sensitive customer data
- Build trust with regulators, customers, and partners

Contact BeyondTrust today to schedule your FRA Compliance Readiness Assessment and learn how our solutions can help your organization improve alignment to compliance objectives.

About BeyondTrust

BeyondTrust is the global identity security leader protecting Paths to Privilege™. Our identity-centric approach goes beyond securing privileges and access, empowering organizations with the most effective solution to manage the entire identity attack surface and neutralize threats, whether from external attacks or insiders.

BeyondTrust is leading the charge in transforming identity security to prevent breaches and limit the blast radius of attacks, while creating a superior customer experience and operational efficiencies. We are trusted by 20,000 customers, including 75 of the Fortune 100, and our global ecosystem of partners.

Learn more at **www.beyondtrust.com.**