FORTRA

DATASHEET (TRIPWIRE)

The Egypt Financial Cybersecurity Framework

Achieving Compliance Using Tripwire Solutions

Central Bank of Egypt (CBE) identified key areas of focus to tailor a cybersecurity framework to the unique requirements of the Egyptian financial sector. This framework will serve as the foundational guidance for cybersecurity capability development within this critical sector. This is the kick-off of a larger-scale effort by the CBE to build a robust and sustainable cybersecurity ecosystem within the financial sector.

The CBE has established this framework as a starting point to bolster the cybersecurity posture and cybersecurity resilience for the financial sector of Egypt. This framework incorporates a number of cybersecurity best practices and controls to be incorporated into financial sector's cybersecurity programs.

Security controls are specified throughout the framework and serve as the primary measure of compliance. Baselining and hardening involve completing prudent and specific tasks to reduce attack surface which is mentioned in the framework.

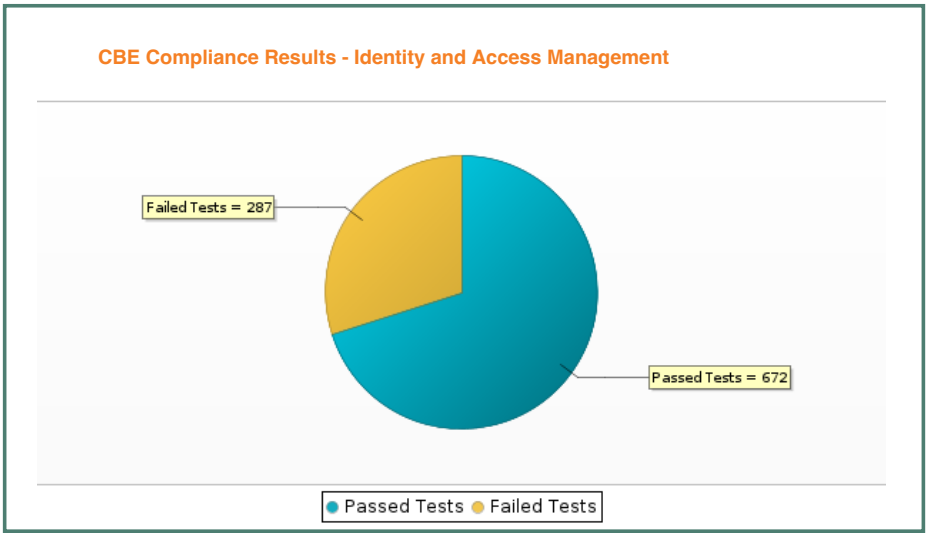
Fortra's Tripwire® Enterprise proactively hardens systems by assessing configurations against internal and external security standards, benchmarks, and industry regulations, then continuously assesses changes against security, policy and compliance requirements for "good" vs. "bad" change and "policy drift".

Tripwire Enterprise provides the broadest range of policies and platforms in the industry, including PCI, CIS, Egypt Financial Cybersecurity Framework (CBE), UAE NESA, Qatar NIA, Saudi ECC, HIPAA, NERC CIP, SOX, COBIT, DISA STIGs and many others.

The following explanations show how Tripwire Enterprise is mapped to Egypt Financial Cybersecurity Framework (CBE) requirements and controls.

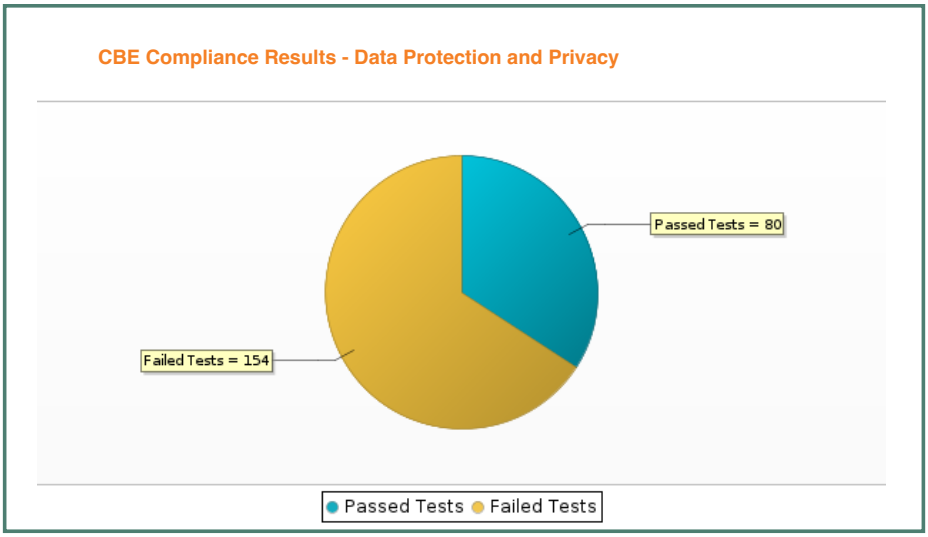
Identity and Access Management

Identity and Access Management 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 that users are only granted the minimal level of access needed to perform core job functions. The report displayed shows high level compliance with Identity and Access Management requirements.



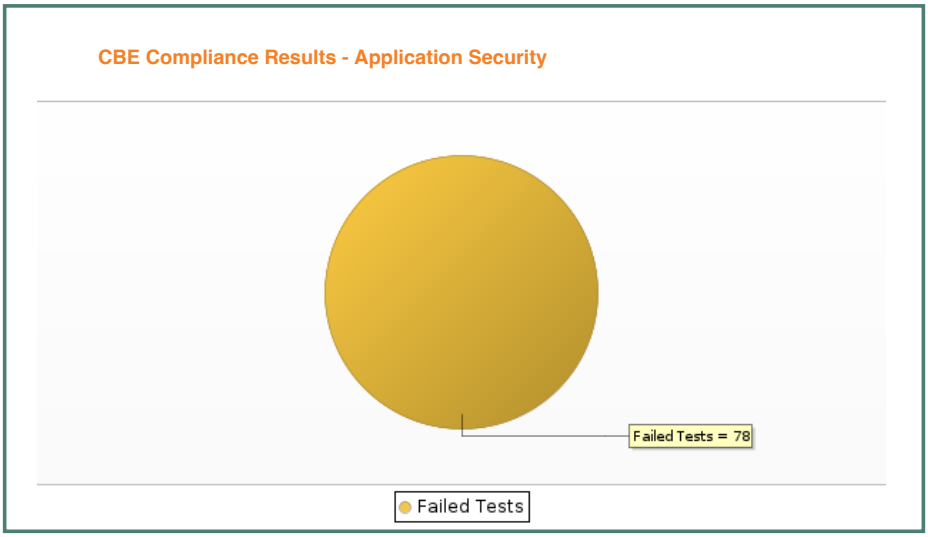
Data Protection and Privacy

Data Protection and Privacy aims to protect the availability, integrity, and privacy of data. Data protection measures focus on safeguarding client and business data, intellectual property, and personally identifiable information belonging to employees and clients. High level compliance with Data Protection and Privacy is displayed in the sample report.



Application Security

Application Security aims to reduce systemic risk exposure inherited from the use of software applications required to support business operations. Application Security focuses on safeguarding applications from exploitation by adversaries throughout an application's life. The report displayed shows high level compliance with Application Security requirements.

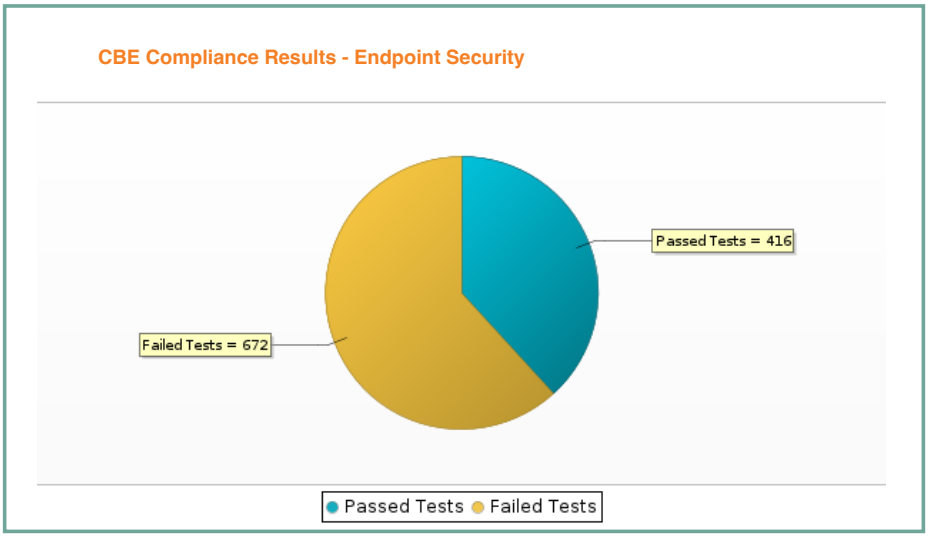


Endpoint Security

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

The report displayed shows high level compliance with Endpoint Security requirements.

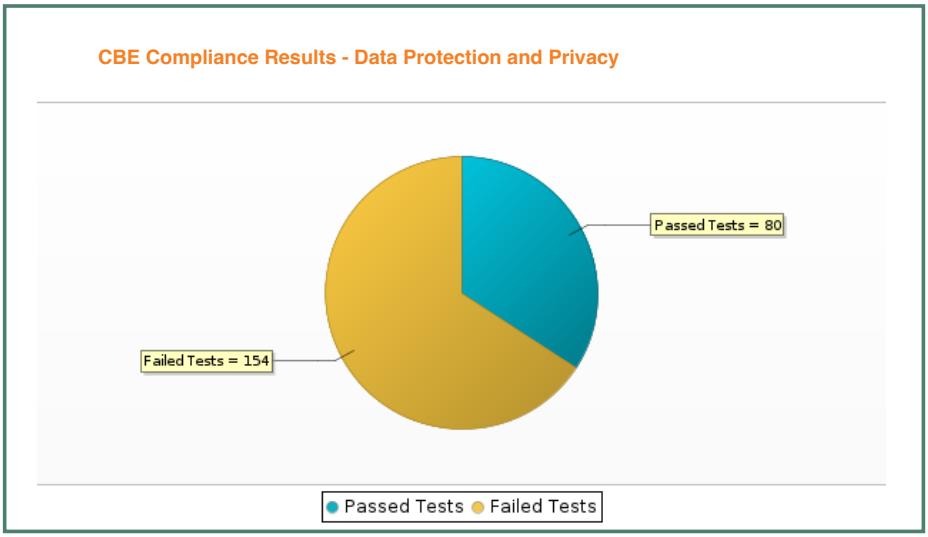


Network Security

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
- Command and Control activity
- Data exfiltration
- Ransomware/Data destruction

High level compliance with Network Security requirements is displayed in the sample report.

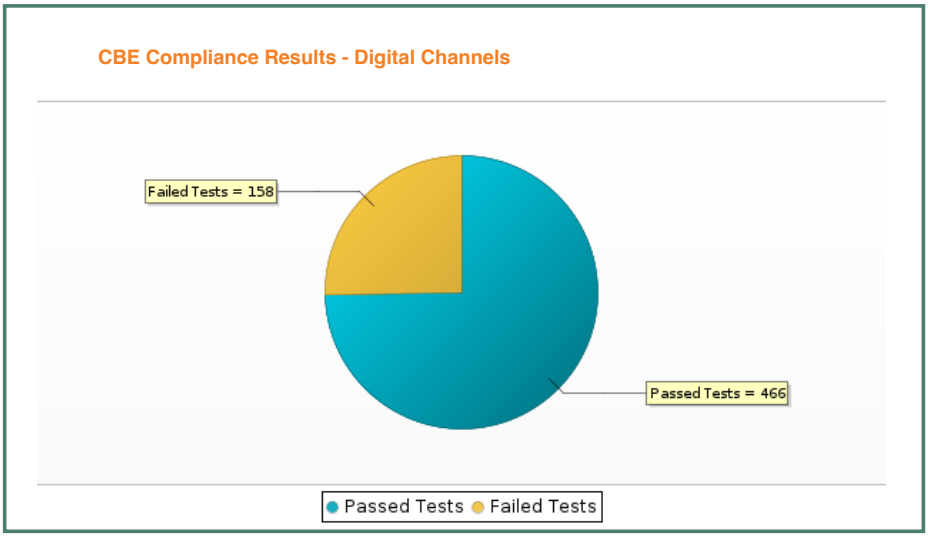


Digital Channels

Digital Channels supports security controls needed to protect against threats, including those listed below, to today's technology and those on the horizon as society shifts towards a digital and largely cashless economy.

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

The report displayed shows high level compliance with Digital Channels requirements.

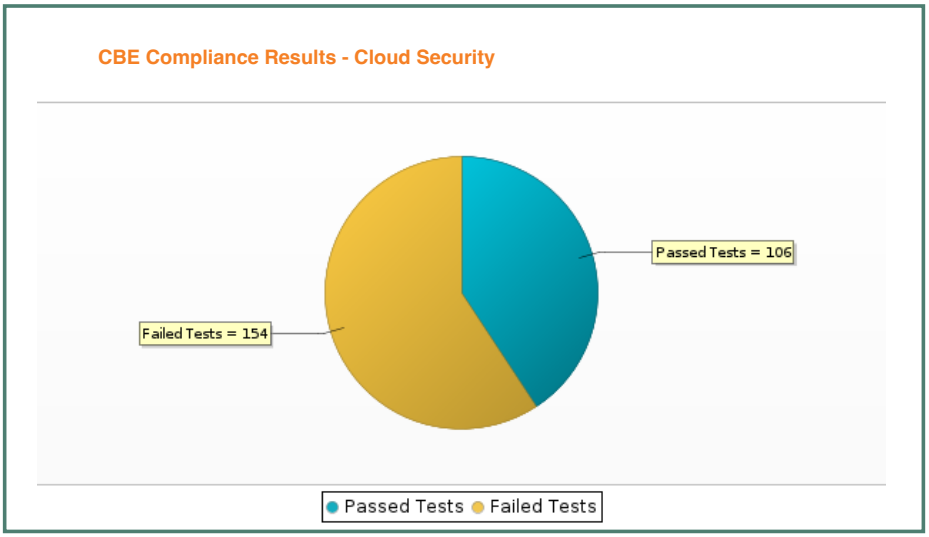


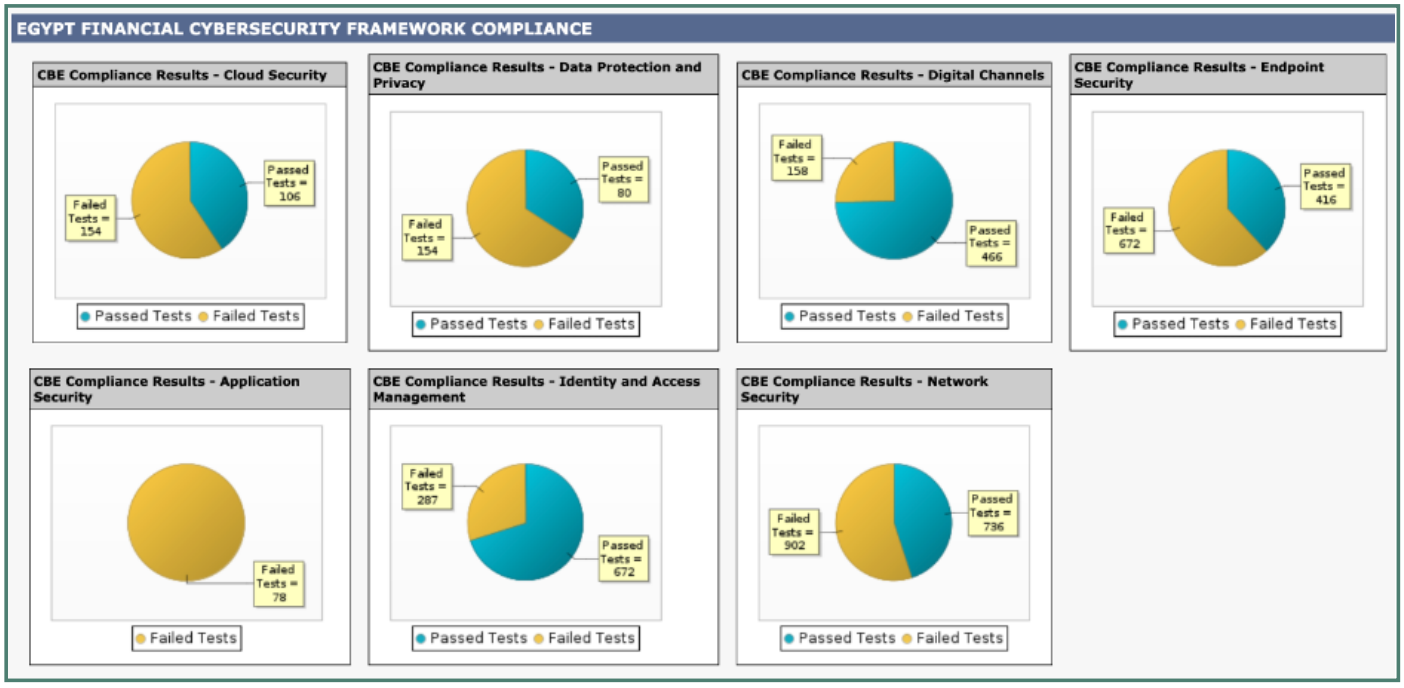
Cloud Security

Cloud Security aims to address unique risks posed by using Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), or Software-as-a-Service (SaaS) cloud computing offerings. Cloud Security addresses the following threats:

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

High level compliance with Cloud Security requirements is displayed in the sample report.





Tripwire Enterprise Executive dashboard showing compliance overview with the Egypt Financial Cybersecurity Framework.

Data Integrity Monitoring

In addition, Egypt Financial Cybersecurity Framework requires integrity monitoring to be deployed to detect changes across the assets to regularly review the changes and alert and report to the security operations for unauthorized changes.

Tripwire is the inventor of file integrity monitoring that has the unique, built-in capability to reduce noise by providing multiple ways of determining low-risk change from high-risk change as part of assessing, prioritizing and reconciling detected change. Auto-promoting countless business-as-usual changes reduces noise so IT has more time to investigate changes that may truly impact security and introduce risk.

Tripwire has taken its original host-based intrusion detection tool to detect changes to files and folders, and expanded it into a robust file integrity monitoring (FIM) solution, able to monitor detailed system integrity: files, directories, registries, configuration parameters, DLLs, ports, services, protocols, etc. Additional enterprise integrations including SIEM provide granular endpoint intelligence that supports threat detection, generate rich event data with business context to determine what requires immediate investigation, enable better correlations and alerting workflows, etc.

Tripwire Enterprise Executive Integrity Monitoring dashboard.

Ready To Dig Deeper?

To learn more about Tripwire Enterprise capabilities, reports, available policies, and platform support, visit tripwire.com.

FORTRA

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.