

CASE STUDY

International Money Transfer Firm

Cybersecurity Audit ensures CBUAE compliance in IT Security and BCMS functions for a money exchange serving over half a million customers.

The International Money Transfer Firm has built its reputation over 3 decades as a trustworthy and reliable facilitator of international fund transfers. They rely on K7's Cybersecurity Audit to maintain this reputation by ensuring compliance with the standards set by the Central Bank of the UAE (CBUAE) for IT Security and Business Continuity Management Systems (BCMS).

Client Snapshot

- » 14 Branches
- » 500,000+ Customers
- » 100,000+ Agents
- » C-category License

The client offers money transfers at scale across multiple continents, making the firm a target of financially-motivated cyberattacks. K7's Cybersecurity Audit ensures the client meets the security standards set by the CBUAE for IT Security and BCMS, enabling guaranteed security and reliability in funds transfer.

Satisfying IT Security and BCMS Compliance Requirements of CBUAE

K7 Security approached the assignment by evaluating the client's nature of business and digital infrastructure within the context of CBUAE's stipulated standards for IT Security and Business Continuity Management Systems, and assessed the following controls based on Confidentiality, Integrity, Availability, Legality (CIAL) ratings:

1. Operations and Management
2. Information Security
3. Business Continuity Management
4. Risk Assessment
5. Documentation

Significant Findings

Some of the critical findings from K7's audit, that would impact the client's compliance with CBUAE standards if not addressed, are highlighted below.



Operations and Management

Findings	Recommendations
• HR policies lack information security related disciplinary actions • HR functions lack information security related protocols for employee exit, change of employee role, policy awareness programmes, and accountability • Network performance monitoring system or solutions have not been implemented • Role-based access to IT systems is not enabled • Information asset classification and disposal policies have not been created • Third party access to secure areas is not controlled	• Strengthen asset management – Track, dispose of data securely • Secure third-party access – Audit rights, enforce policies • Enhance HR – Disciplinary actions for security breaches, formal organisation- and role-exit processes • Monitor performance – Track service agreements, conduct training, form Information Security Governance Council

Information Security

Findings	Recommendations
• Lack of network segmentation allows threats to spread within the network • Firewall policies permit any-to-any traffic • Servers permit unlimited login attempts • DMZ is not configured for servers • Access permission for shared folders in servers is enabled for everyone • USB ports are enabled to permit backups • PAM/IAM systems are not implemented	• Protect critical servers – Segment network, configure DMZ, implement PAM • Harden defences – Strengthen firewalls, disable USB ports, enforce timeouts • Improve minimum security standards – Implement baseline policy, MDM solution

Business Continuity

Findings	Recommendations
• Redundant or highly-available switches were not deployed to avoid single point of failure • Stable failback connectivity link was not configured, impairing business continuity • Offsite data backup is not available • Network access credentials are available only with the IT department • Connectivity diagram with dependencies, naming conventions, and point-to-point data throughput is not available	• Prevent single points of failure – Improve network redundancy, implement disaster recovery and tertiary off-site backups • Improve connectivity reliability – Obtain secondary connectivity link and configure to failover from primary link • Conduct drills – Test business continuity plans, record impact • Secure access – Introduce encrypted password vault • Maintain documentation – Update IT infrastructure diagram

Risk Assessment

Findings	Recommendations
• Data exchange between applications using APIs is not encrypted • No centrally managed access control for applications and logs for audit trail • Surveillance logs are not checked for accessibility and integrity • No data integrity checks were performed by restoring long term archives	• Encrypt data – Implement encryption for internal and external data transfer • Centralise controls – Improve access control and log management • Ensure data availability – Verify data integrity • Continuously improve – Refine risk assessment and treatment processes

Documentation

Findings	Recommendations
Documentation is not available for • Risk assessment – risk management • Access control – secure areas and assets • Information security policy – internal organisation • Asset management – classification, disposal • Human resource security – prior to employment, termination • Information/data backup policy – off-site back up maintenance • Third party service delivery management • Log management and monitoring • User access management	Create policies for • Information Security • Human Resources Security • Information Asset Management • Physical and Environmental Security • Access Control Policy • Operations Security • Electronic Communications • Customer Information Security • Third Party Security • Information Systems Acquisition, Development, and Maintenance • Information Security Incident Management • Information Systems Continuity • Compliance Policy • Acceptable Usage • Antivirus • Clear Desk and Clear Screen • Information/Data Backup • Internet Usage • Password Security • Remote Access Security

K7's findings, and recommendations, helped the client ensure their compliance with CBUAE standards is maintained and their customers enjoyed secure money transfers.

K7's team help enterprises meet their compliance obligations and strengthen cybersecurity through comprehensive assessments backed by multi-jurisdictional regulatory exposure. **Contact Us** to learn more about our cybersecurity services and solutions and how we can help you improve your organisation's cybersecurity posture.



Copyright © 2025 K7 Enterprise Security Private Limited. All Rights Reserved.

This work may not be sold, transferred, adapted, abridged, copied, or reproduced in whole or in part in any manner or form or any media without the express prior written consent of authorised personnel of K7 Enterprise Security Private Limited. All product names and company names and logos mentioned herein are the trademarks or registered trademarks of their respective owners.

www.k7cybersecurity.com