Computer Science & Information Technology Department

College of Engineering

CSE-210 SPRING 2024-25

Cybersecurity Risk & Resilience Audit for First Abu Dhabi Bank (FAB): A Strategic Consultancy Report

STUDENT NAME:	STUDENT ID:
MEZRAIT MENBER	1093911
JOSHUA THOMAS	1097125

INSTRUCTOR NAME: DR. SHEHZAD ASHRAF

SUBMISSION DEADLINE: 30TH MAY

جامعة أبوظبي
Abu Dhabi University

Table of Contents

جامعة أبوظبي
Abu Dhabi University

Abstract

First Abu Dhabi Bank (FAB), a major participant in the Middle East's financial industry and one of the top banks in the United Arab Emirates, is the subject of this report's thorough IT security analysis. Due to its size and the delicate nature of the financial services it provides, FAB is finding it increasingly difficult to defend its digital assets against changing cyber threats. Profiling FAB's organizational security landscape, with a focus on its digital services, critical infrastructure, and security objectives, is the first stage of the research process. An information classification approach is then used to classify important data assets that are accessible to the general public, such as customer records, internal systems, and applications. Following a comprehensive risk assessment that identifies potential threats, vulnerabilities, and their associated effects, a prioritized risk registry is established. Based on a cost-benefit analysis, the paper recommends a set of technical and organizational controls to ensure efficient resource allocation. Focused awareness and training measures are put into place to reduce human risks after a methodical IT security plan has been developed to strengthen FAB's security posture. Configuration management, maintenance, and change control are covered in the report's conclusion to ensure long-term security and compliance. The present security environment of FAB is highlighted in this research, along with strategic recommendations to enhance resilience against cybersecurity threats.

1. Organizational Security Profile

1.1 Overview of the Enterprise

First Abu Dhabi Bank (FAB) was formed in 2017 through the merger of the late First Gulf Bank and National Bank of Abu Dhabi which were the largest financial institution in the UAE. FAB now operates in over 20 countries. It offers many financial services for example retail banking, corporate banking, investment banking, and Islamic banking. FAB's growth strategy and focus on digital banking highlight the critical need for robust cybersecurity to protect its extensive operations and customer data. As a leader in the regional banking sector, FAB's reliance on technology and secure digital channels is paramount for maintaining operational integrity and customer trust **(Infosys, 2024)**.

1.2 Security Goals and Policies

FAB has put in place a strong framework for addressing regional and global cyber threats. The security policies of the bank meet global standards, and it has an extensive Financial Crime Compliance Program. The program covers Anti-Money Laundering (AML), Counter-Terrorist Financing (CTF), sanctions, and anti-bribery controls. The program is also externally audited periodically to ascertain whether the bank's activities comply with local laws and global expectations. FAB has attained key certifications such as the Payment Card Industry Data Security Standard (PCI DSS), which guarantees the safe handling of payment card data, and SOC 2 certification which is an assertion of the effectiveness of its controls related to security, availability, processing integrity, confidentiality, and privacy (First Abu Dhabi Bank, n.d.-a; First Abu Dhabi Bank, n.d.-b).

Moreover, FAB is highly dedicated to proactive threat detection and risk management. The bank employs both technical and organizational controls to protect key customer information and mitigate monetary risks. These cover the use of encryption technology, multi-factor authentication, and constant monitoring to detect and nullify cyber threats in real time (Cyntexa, 2024).

1.3 Digital Services and Channels

FAB has significantly enriched its digital banking services, which provide customers with access to online services ranging from fund transfer to bill payment and account management. Its online and mobile channels are protected by rigorous security features such as multi-factor authentication and biometric authentication to ensure an assured customer experience. FAB has also launched “Payit," the government-approved digital wallet enabling safe peer-to-peer payment, merchant transactions, and transfer using QR code. Payit has attracted praise for enabling digital cashless transactions within the UAE, bringing the country on track with its digitalization and financial inclusiveness drive **(Gulf News, 2020).**

In FAB, Customers now have access to a wide range of online services, such as fund transfers, bill payments, and account management, thanks to its's significantly improved digital banking offerings. Strict security measures, such as biometric and multi-factor authentication, protect the bank's mobile and online platforms to guarantee a positive client experience. Additionally, FAB unveiled "Payit," a digital wallet approved by the UAE government that facilitates secure peer-topeer exchanges, merchant payments, and QR-based transfers. The Payit system has received praise for handling digital cashless transactions in the United Arab Emirates, which is in line with the country's ambitions for financial inclusivity and digital advancement **(Gulf News, 2020)**

FAB further launched the FAB eSign platform, which allows customers to digitally sign documents securely.

The platform is built on public key infrastructure (PKI), which ensures the integrity and authenticity of the signed documents, which are in line with the UAE's digital signature law framework. The innovation is one of the many endeavors of FAB to offer end-to-end digital banking solutions with maximum customer convenience and safe and legally binding transactions **(First Abu Dhabi Bank, n.d.-c)**.

1.4 Systems and Infrastructure Analysis

To fulfill the increasing needs of its clients, FAB has made considerable efforts to transform its IT infrastructure. In 2024, the bank collaborated with Infosys to enhance its IT capabilities and

incorporate AI-based automation, cloud technologies, and advanced security systems. As part of the agreement, Infosys Cobalt which is a platform using AI, will be leveraged by the bootcamp for service management, proactive monitoring, and resource optimization **(Infosys, 2024)**.

Full-Stack Observability apps such as AppDynamics and ThousandEyes are among the Cisco solutions that FAB also relies on to monitor and manage the performance of its core banking app. This has resulted in FAB achieving 99.92% system availability of its mission-critical business solutions and fast response time to incidents that affect services, thus improving the overall service availability and customer satisfaction **(Cisco, n.d.)**.

On top of that, FAB is adopting a cloud-first strategy, while leveraging Core42 as a sovereign cloud partner, to help it move data center and workloads to Microsoft Azure. The shift not only allows the bank to operate more efficiently, it also helped it become compliant with data localization laws in the UAE, which stipulate that certain data of a sensitive nature need to be stored in the country. This strategic pivot allows FAB to more flexibly respond to the changing requirements of its digital-first customers, growing their operations in a safer and more agnostic way **(Microsoft, 2024)**.

2. Information Classification Strategy

An information classification strategy is a critical component of protecting an enterprise's data according to its value, sensitivity and legal requirements. Especially for an organization such as First Abu Dhabi Bank (FAB), which is a multijurisdictional entity with massive amount of financial, personal, and operational data, the classification serves as a bedrock for access control, risk remediation, and compliance.

The FAB's categorization model aligns with ISO/IEC 27001 best practice that requires identification of information assets and the application of protection and safeguarding appropriate to their criticality and exposure level **(ISO, 2022)**. This approach also helps inform FAB's wider cyber security aims by establishing control requirements and simplifying the processes for reacting to incidents.

2.1 Classification Model Overview

FAB uses an industry standard framework and regulatory guidance to categorize fraudulent activity into four levels:

Public – Distribution authorized to public release; distribution is unlimited.
Internal – Additional operational data for use within FAB; unauthorized exposure causes only limited damage.

Confidential – Proprietary information intended to be protected for business and legal reasons.

Limited – Sensitive or controlled information; unauthorized disclosure may result in conscious damage.

This model of classification allows resources to be concentrated on locking down those most sensitive and high-impact assets without rendering them completely inaccessible or unusable to authorized users.

2.2 Public Information

Public information in FAB includes externally released publications such as press releases, investor presentations, job announcements, marketing, and the company's website. These files are prepared for public access and are used for branding, transparency, and corporate governance purposes. These items are not classified and are controlled using standard publishing management and web protection mechanisms **(First Abu Dhabi Bank, n.d.)**.

But even public information needs to be monitored. FAB keeps versions and digital watermarks for control and verification of the integrity of public content.

2.3 Internal Information

Internal content is intended for internal operations only and can consist of departmental policies, intranet postings, staff schedules, and employee correspondence. Not on the public by regulations standards, but it could leak what the organization is set up like at a high level. For example, release dates for an internal IT deployment or a non-classified memo could still be useful for social engineering or phishing.

Access is via FAB's digital workspace, and viewing rights are role-based. Although internal data may not be required to be encrypted, access logging and endpoint monitoring is **(Cisco, n.d.)**.

2.4 Confidential Information

Sensitive data in FAB may consist of, but not limited to, customer transaction records, loan documents, non-disclosure agreements, internal audit reports, and strategic roadmaps. This data, if breached, can result in significant financial, legal, and/or reputation damage. Customer and employee data are also subjected to strict data handling by the UAE's Data Protection Law **(Gulf News, 2021)**.

Encryption (data-at-rest and data-in-transit) is deployed to protect the data from leaks, while secure digital signatures for electronic signatures (FAB eSign) are used. Monitoring tools built into the Core42 environment are also in place to detect anomalies and to ensure compliance **(First Abu Dhabi Bank, n.d.-a; Microsoft, 2024)**.

2.5 Restricted Information

"Restricted" data includes admin login information, biometric data, the root server's setup, private crypto keys, and sensitive personal data like scans of Emirates IDs and passports. Unauthorized exposure of such information can pose an existential threat to the bank, ranging from compliance and financial impact to undermining the entire system.

FAB secures this information with MFA, HSM, DLP solutions, and segregated networks using a least-privilege access model **(Cisco, n.d.; ISO, 2022)**. The Restricted environment is closely watched and can take real-time threat detection measures to guard against lateral movement and privilege escalation.

Table 1:Summary Table of classification of information

Information Asset	**Classification**	**Justification**
Marketing brochures and website	Public	Designed for public distribution; no impact if disclosed
Employee training guides	Internal	Used internally; moderate operational risk if shared
Loan applications and agreements	Confidential	Includes customer financial data; legally protected
Internal audit reports	Confidential	Operational insights; leakage could cause reputational harm
Emirates ID / Passport documents	Restricted	Critical personal identifiers; governed by data protection laws
Database admin credentials	Restricted	Access to systems; compromise could lead to data breaches
Internal IT project plans	Internal	Contains non-sensitive but strategic content; requires internal restriction
Payment transaction logs	Confidential	Subject to compliance with anti-fraud and KYC laws

2.6 Strategic Importance of Classification

FAB's data classification approach allows the bank to rank cybersecurity controls according to the risk level of each asset. It makes operations more resilient, helps manage resources for data protection efficiently and legally and allows to comply with the law in multiple jurisdictions. Classification also aids the speed and effectiveness with which FAB are able to react to incidents, since response procedures are different for each type of data.

Additionally, for mutlicloud environments facilitated through services such as Microsoft Azure Core42, classification allows for fine-grained access to cloud-native encryption, backup, and identity governance tools **(Microsoft, 2024)**. It also demonstrates FAB's strategic position to deliver safe customer centric banking on a digital first economy.

3. Risk Assessment

Risk management is an integral part of FAB's cybersecurity program. With the bank both upscaling its digital activity, while processing enormous amounts of sensitive data, it is more exposed than ever to cyber threats, system malfunctions and human mistakes. Proactively, systematically assessing the risk enables FAB to allocate limited resources efficiently, fortify its defense in depth strategy, and ensure adherence to the regulatory requirements such as the UAE Data Protection Law and internationally recognized standards such as ISO/IEC 27005:2018 **(ISO, 2018)**.

3.1 Methodology and Framework

FAB uses risk management approach approach that is based on the ISO/IEC 27005 -= standard. It does that by identifying important information assets and classifying them based on sensitivity. It then studies threats to the system — hacking, internal misuse, and operational failures, among others — and then pinpoints vulnerabilities, such as feeble access controls, outdated software, or

employee carelessness. On the basis of potential impact and probability each risk is then assessed - and thus classifiable into high, medium or low priority.

3.2 High-Value Assets and associated Threats

The customer's financial information, authentication credentials and transaction logs are the most sensitive risk category. These are classified as “Confidential” or “Restricted” under FAB’s classification scheme because of their commercial sensitivity and potential regulatory content. A key vulnerability is the high risk of phishing and social engineering for customer accounts, resulting in theft of identity and illicit transactions. These attacks continue to increase both in numbers and in their level of complexity across the financial services industry, despite investment in employee training, and secure email gateways **(ENISA, 2023)**. Phishing is able to cause devastating financial and regulatory outcomes. Another vulnerability is credential theft, especially of system administrators handling FAB’s core banking systems. In the event of a compromise of these credentials (for example by key logging, brute force entry, or insider abuse) an unauthorized party would be able to have full access to a database resulting in a service outage or dataloss. The result would, of course, be calamitous, you are much less likely to have this occur due to layered controls, such as MFA but it still deserves some attention **(ISO, 2022)**.

Another valuable possession is FAB's records for payment transactions. These logs are responsible for the health of the day to day logistics of banking. And if ransomware were to attack them, it could freeze operations, prevent customers from accessing their accounts and lead to permanent data loss. Microsoft (2024) suggests that many financial institutions in the UAE are moving to hybrid clouds environment, which –despite providing a high degree of flexibility– can increase the attack surface, if the security is not properly managed.

3.3 Insider Threats and Leakage of Confidential Information

Content such as Emirates ID or passport scans, gathered in the course of customer onboarding is very sensitive. If you have poorly defined access controls or limited audit trails this could be accessed by unauthorised persons, notably from within. Given the regulatory system in UAE, defaults of this nature could lead to severe sanctions and harm FAB’s reputation **(Gulf News, 2021)**.

Similarly, internal audit reports and the strategic deployment plans, even if labeled “Confidential” or “Internal,” may open up weaknesses if leaked. Those papers often have confidential discoveries about the flaws in systems, gaps in compliance and in project timelines. Unauthorized release of information–whether the result of human error or from an applied malicious insider– could furnish competitors or adversaries with useful information on FAB’s inner workings **(Cisco, n.d.)**.

3.4 Digital environment and integrity risks

FAB’s use of digital channels (e.g., FAB eSign) expose it to the risk of session hijacking, token theft and man-in-the middle attacks. If insecure session management and lack in a timeout policy exists, an attacker could hijack the guest history session to be authenticated as the user and sign contracts or documents, fraudulently. This can be particularly risky within high-value corporate banking transactions when digital signing replaces the traditional face-to-face verification processes **(First Abu Dhabi Bank, n.d.-a)**. Even those low-risk systems, such as FAB’s publicfacing website, can present reputational risks. Consider, for instance, website defacement – which is frequently perpetrated using CMS vulnerabilities – it doesn’t necessarily disrupt internal activity, but can damage the FAB reputation and client confidence. Those risks are often lesser in significance, but should still not be disregarded.

4. Control Recommendations & Considerations of Cost and Benefit

Based on the risk frame proposed in the previous section, to overcome cybersecurity threats, FAB is required to implement a combination of technical and organizational measures. Those mitigations work against traditional high risk items: phishing, credential theft, insider threats, system integrity failures. We have evaluated these controls based on their cost of implementation, security effect while also taking organisational impact into account. These controls are described below and were accompanied by an approximate cost benefit analysis to inform decisions.

4.1 Controls Against Credential Theft and Unauthorized Access

One of the highest risks for FAB involves unauthorized access through stolen or weak credentials. The following controls address these vulnerabilities:

Control	Type	Cost	Benefit	Justification
Multi-Factor Authentication (MFA) for all employees and privileged access	Technical	Low	Very High	MFA significantly reduces the effectiveness of password theft. According to Microsoft (2024), MFA can block 99.9% of account compromise attacks.
Role-Based Access Control (RBAC) with regular access reviews	Technical / Organizational	Moderate	High	RBAC ensures that employees only access information necessary for their roles, reducing risk of privilege misuse **(ISO, 2022)**.

4.2 Controls Against Phishing and Social Engineering

Given the global increase in phishing attacks targeting financial institutions, FAB must address social engineering threats effectively.

Control	Type	Cost	Benefit	Justification
Advanced Email Filtering and AntiPhishing Tools (e.g., Microsoft Defender, Proofpoint)	Technical	Moderate	High	These tools detect and quarantine suspicious emails before users interact with them. ENISA (2023) reports a significant drop in phishing incidents in banks using advanced filters.

Simulated Phishing Campaigns and Training	Organizational	Low	Medium	Educates employees on real phishing scenarios, improving recognition and response **(Gulf News, 2021)**.

4.3 Controls to Safeguard Data Integrity and Availability

FAB's core systems depend on the uninterrupted availability and integrity of transaction and authentication data. These controls reduce the risk of ransomware and system outages.

Control	Type	Cost	Benefit	Justification
Endpoint Detection and Response (EDR) with real-time threat analytics	Technical	High	Very High	EDR tools offer deep visibility into endpoints and can isolate compromised systems. Cisco (n.d.) recommends this for financial institutions with large digital footprints.
Data Backup and Offline Replication	Technical	Moderate	High	Regular offline backups protect against ransomware and accidental data loss. ISO/IEC 27001 (2022) stresses the importance of resilient data recovery mechanisms.

4.4 Controls for Insider Threat and Confidential Data Leakage

Insider misuse or accidental leaks are common risks in any large enterprise, especially when handling restricted personal and financial data.

Control	Type	Cost	Benefit	Justification
Audit Logging and User Behavior Analytics (UBA)	Technical	Moderate	High	Tracks anomalous behavior from authorized users and triggers alerts. Helps detect insider threats early (ISO, 2018).
Data Loss Prevention (DLP) Tools on email and endpoint devices	Technical	High	High	Prevents intentional or unintentional transmission of sensitive data. DLP is particularly critical under the UAE Data Protection Law (Gulf News, 2021).

4.5 Controls for System Configuration and Change Management

Poorly managed system changes can introduce vulnerabilities, leading to compliance violations or operational failures.

Control	Type	Cost	Benefit	Justification
Formal Change Management Workflow with approvals and rollback plans	Organizational	Low	Medium	Ensures consistency and traceability in IT system modifications. This reduces misconfiguration risks (ISO, 2018).
Automated Patch Management and Configuration Monitoring Tools	Technical	Moderate	High	Keeps systems up-to-date and flags insecure configurations. Microsoft (2024) highlights automation as key in securing hybrid cloud setups.

4.6 Controls for Digital Platforms and Document Integrity

As FAB continues its push into digital services like FAB eSign, maintaining the integrity of digital transactions becomes essential.

Control	Type	Cost	Benefit	Justification
Token-based Secure Digital Signing and Session Timeout	Technical	Low	High	Prevents unauthorized session hijacking and digital fraud. Essential for systems like FAB eSign (First Abu Dhabi Bank, n.d.-a).
Web Application Firewall (WAF) for public-facing services	Technical	High	High	Protects customer-facing portals from OWASP Top 10 threats and data exfiltration (ENISA, 2023).

4.7 Strategic Summary

Implementing these layered controls allows FAB to align its security investments with its risk exposure. Cost-effective measures like MFA and awareness campaigns offer substantial protection, while more advanced systems like EDR and DLP support long-term resilience and compliance. These recommendations strike a practical balance between operational efficiency and regulatory obligation.

5. IT Security Plan

5.1 Introduction and Strategic Objectives

With its substantial digital expansion and innovation appetite, First Abu Dhabi Bank (FAB) having a robust IT Security Plan to address the advanced threats to the company will be essential to ensuring continued business operations. The move aligns with global cyber-security regulation—ISO/IEC 27001:2022 and UAE Federal Decree-Law No. 45 of 2021 Concerning the Protection of Personal Data. The main strategic goals are to support continuous banking, to protect customer and business confidential data, to comply with regulatory requirements, and to promote a culture of security in the organization. In alignment with FAB's heavy investment in digital technologies like cloud-enabled AI solutions with Microsoft **(Microsoft News Center, 2024)**, the proposition is apt and indispensable.

5.2 Defense in Depth Design

In order to securely cover its systems, FAB uses a multi-layered security system that spans the entire infrastructure. On the perimeter, NGFWs and Web Application Firewalls (WAFs) filter traffic and shield against attacks at the layer-7 level. These are complemented by Distributed Denial of Service (DDoS) defenses, which ensure service provisioning even during an attack. Within the internal network, network segmentation reduces the extent of the proliferation of incidents when a breach takes place and Endpoint Detection and Response (EDR) solutions monitor and respond to malicious activity on endpoints in real-time.

Yet another area of the security plan is the Identity and Access Management (IAM). FAB entails the utilization of MFA on privileged accounts and sensitive systems, reducing the likelihood of compromise. A Role-Based Access Control (RBAC) policy controls access based on the role to be assumed and is aligned with the least privilege principle.

5.3 Protection and Compliance of Data

FAB has implemented stringent data protection processes to protect confidentiality, integrity, and availability of data. Protection of data-at-rest is through the Advanced Encryption Standard (AES-256), and protection of data-in-transit is through TLS 1.3. Data Loss Prevention (DLP) solutions monitor and block unapproved data transfer activities to protect sensitive information like personal (PII) and financial data. These undertakings support compliance with the UAE Personal Data Protection Law, which prescribes explicit roles for data controllers and processors (DLA Piper, 2024). FAB also supports the UAE Central Bank's requirements on cybersecurity for banks, which are centered on having a risk-based structure and continuous reviews **(Central Bank of the UAE, 2023)**.

5.4 Organizational Security Policies and Procedures

These activities are a complement to the UAE Personal Data Protection Law, which mandates specific functions for data controllers and processors **(DLA Piper, 2024)**. FAB also complements the UAE Central Bank's cybersecurity policies for banks, which are focused on risk-based design and on-going review **(Central Bank of the UAE, 2023)**.

5.4 Organizational Security Policies and Procedures

Supplemented by explicit organizational policies, the technical controls are even more robust. FAB embraces ISO/IEC 27001:2022 as its Information Security Management System (ISMS), which regulates all security arrangements. A change management process means all IT changes are riskassessed before they are implemented to best protect against threats to security. A documented Cybersecurity Incident Response Plan (CIRP) also has a formal process to discover and respond to breaches and to remediate. Incident response drills and business continuation training are regularly undertaken to practice and enhance readiness.

5.5 Integration of Human Factors and Security

Realizing that technology by itself cannot be adequate to fight against breaches, FAB puts a cybersecurity mindset at the center of its security policy. The staff is constantly provided

cybersecurity awareness training in the form of simulated attacks and internal educational sessions. Specialized training modules are created and delivered to high-risk functions such as IT operations, finance, or customer service. These also minimize social engineering and insider attacks—recurring threats to the financial sector **(ENISA, 2023)**.

5.6 Monitoring and Continuous Improvement

Continuous monitoring is essential to identify vulnerabilities and respond to threats in real time. FAB employs Security Information and Event Management (SIEM) solutions to aggregate and analyze security logs throughout its infrastructure. SIEM is augmented by threat intelligence feeds to facilitate advanced threat detection. Internal and external audits are regularly conducted to monitor effectiveness of controls and policy compliance. Feedback from such monitoring is used to refine risk assessment and policy to reinforce a culture of ongoing improvement. Key performance indicators such as response time to incidents, policy compliance, and awareness among employees are regularly monitored to monitor the effectiveness of the IT Security Plan and influence subsequent investments in security.

6. Security Awareness & Training

6.1 Strategic Importance of Security Awareness

Given First Abu Dhabi Bank's (FAB) ecosystem is increasingly digital we can't do security and not address the human. Despite FAB's considerable investment in strong technical controls—firewalls, encryption, access controls—these can be circumvented through human error. In fact, ENISA (2023) lists phishing and social engineering as the top causations of data breaches, especially within the financial industry. So it is your staff that are the first line of defense and that common level of failure.

FAB's approach to cyber security awareness training seeks to equip its workforce with the knowledge, attitude and behavioral skills required to identify and respond to cyber threats. The program is based on international best practices as indicated in the NIST SP 800-50 framework which highlights task-specific training, drill and practice, and evidence based obtainable standards

(NIST, 2003). This process helps prevent awareness from being approached as a box-ticking exercise and to treat it as an ongoing cultural shift across the business.

6.2 Multi-Tiered Training Program

The awareness initiative is designed to accommodate the wide range of roles and responsibilities of FAB employees. Various organizational functions will face different types of risk such as a finance and HR dealing with PII sensitive data that could be exposed to phishing attempts while IT may face insider threats or misconfigurations of systems. Thus a common training program would not be appropriate.

The narrative uses a combination of classroom plus e-learning modules, mock phishing campaigns, workshops, and posters / internal bulletins and other media. And every training exercise, is specifically created to instruct and, more importantly, to affect long term behavior. Furthermore, all blocks of the system are compatible with the obligatory regulations of the UAE's Personal Data Protection Act and the Central Bank cybersecurity regulations **(DLA Piper, 2024; Central Bank of the UAE, 2023)**.

Training Module	Audience	Delivery Format	Content Focus	Frequency
Phishing & Email Security	All Employees	Simulations, Email Campaigns	Spotting phishing attempts, reporting suspicious mails	Quarterly
Password & MFA Practices	All Employees	Interactive eLearning	Secure password habits, use of MFA	Biannually

Data Classification & Handling	HR, Finance, IT	Workshop + Policy Handbook	Managing sensitive, restricted data securely	Annually
Remote Work Security	Hybrid/Remote Workers	Video Tutorials, Intranet Guides	Safe Wi-Fi, VPN usage, endpoint security	Quarterly
Incident Response Protocol	All Staff	Posters, Quickreference Leaflets	Reporting steps during security incidents	Ongoing
Compliance & Legal Obligations	Legal, Compliance Teams	LMS Course + Assessment	Understanding PDP Law, GDPR, CBUAE policies	Biannually

6.3 Measurement and Continuous Improvement

In that way, FAB incorporates strong evaluative procedures as components of its training programs. These can be through post-training quizzes, simulated attack statistics and KPIs (Key Performance Indicators) such as phishing click rates, incident reporting volumes and attendance figures. Departments that demonstrate patterns of risk may be offered targeted re-training or individual advisory support.

Consistent with ISO/IEC 27001:2022, Section 9 (Performance Evaluation), data is used to adjust the sensitivity of training modules, reduce content ambiguity, and fine-tune the frequency of delivery. By formalizing a feedback loop and iteration cycle, FAB not only keeps pace with emerging threats but advances our human firewall—so that we recognize, report and manage security risks in real time.

7. Maintenance & Configuration Management

The proper maintenance, configuration, and management of your systems are important elements of a robust cybersecurity infrastructure. For a business entity, such as First Abu Dhabi Bank (FAB) having a huge digital ecosystem and handling consumption of large number of transactions with the flow of sensitive data are highly sensitive and the system integrity and dependability are crucial. In this way, improperly maintained configurations or postponed patching can result in serious vulnerabilities up to and including zero-day and system outages and non-compliance. Therefore, FAB needs to maintain and configure its IT structures according to standardized global standards such as the ISO/IEC 27001:2022, and NIST (2020) guidelines. The trick is to do more than just detect threats in real-time, but also keep an eye on overall system health, performance metrics, and user behavioral patterns. Regular scanning and system checking is required weekly or monthly depending on the importance of asset.

A more precise attribution of provides particular form for this is that in the UAE s National Cybersecurity Strategy, FAB will integrate isinto automated warning and support based on AI may shorten the response time to events and improve operational resilience **(UAE Cybersecurity Council, 2023)**. The datasets, server, antivirus and health inspection should also be part of the maintenance that to reduce the outages and recovery.

7.1 Ongoing Monitoring and Maintenance

It is important to maintain order and keep the system in proper working condition, especially during updates and new deployments. FAB should implement an ITIL-based formal procedures process for change management. This includes well-documented changes, test cases, approval processes and contingencies for any system modification.

Changes need to be classified as to their effect and urgency - from immediate patches to planned software upgrades. Risk assess and CAB review every change request, with members of security, IT and compliance. Fixed Change Control Change control minimizes configuration drift and provides traceability/archive as well as preparation for audit **(NIST, 2011)**.

There should also be post-implementation evaluations to determine the extent of the change and any unintended consequences. Automation tools such as Ansible or Puppet can also improve the consistency and security of configuration deployments between cloud and on-premises environments.

7.2 Change Control Procedures

Control of Change Change control is essential to prevent accidental change and to protect the integrity of systems when they are modified or as new systems are added. FAB should have a process for normalizing changes according to the standard ITIL (Information Technology Infrastructure Library) guidelines. This means to document, test and approve the changes and plan for when the change makes us roll the change back.

All changes must be given a business impact and an urgency -- or an emergency fix, even down to a quarterly software update. Any change request of them must be evaluated by a risk and be reviewed by a Change Advisory Board (CAB) whose members are sec, IT, and compliance. 'Managed change control' to i) combat configuration drift; ii) offer traceability, iii) be in a state of readiness for audit **(NIST, 2011)**.

Such a process will need to include post-hoc reviews to check whether the change being made and any unexpected open issues can be evaluated. Automation possibilities with e.g. Ansible or Puppet may as well enhance similarity and security of configuration distribution in cloud as well on-premise.

7.3 Configuration and Patch Management

According to NIST in SP800-128, defines it as the “collection of activities focused on establishing and maintaining the integrity of products and systems, through control of the processes for initializing, changing and monitoring the configurations of those products and systems.” **(Internal Revenue Service [IRS], 2025)**

Configuration Management ensures that employees and all that are working under an organization uses settings and system configurations approved by the senior management to offer the optimal

and basic cybersecurity for all organizations. If it were to be misconfigured, systems are more liable to become hacked through untended vulnerabilities which are a result of these misconfigurations.

Patch Management is another crucial aspect to security maintenance. It is often we have security flaws and crevices that were not addressed during its conception, development and deployment and consequentially exploited by threat actors. To circumvent these issues, the organization or vendor releases software ‘patch’ updates to rectify these flaws and/or add extra features for better security. Without such patch updates, Threat actors can easily compromise an organization’s assets as price of their incompetence and lack of awareness.

جامعة أبوظبي
Abu Dhabi University

INDIVIDUAL CONTRIBUTIONS (Joshua Thomas-1097125)

Key Responsibilities: (IT Security Plan, Security Awareness & Training and Maintenance & Configuration Management)

- Project Documentation
- Final formatting and modifications for the project
- Consistent communication & coordination for the completion of the project
- Citing any missing citations

What was learned:

- The importance of compliance of security policies for organizations to maintain confidentiality, integrity and availability of data and avoid brand damages and fines.
- Emphasis on training programs for employees given that humans are the biggest liability in Cybersecurity for damage to occur in the digital landscape.
- Significance of security configurations and software updates to enhance digital security of an organization.

Reflections:

- Cybersecurity is more than simply individual work, but rather it is collaborative effort of many people; much like this project. Cybersecurity is a paradigm of diverse sub-fields where technology security interlaps with business goals.

جامعة أبوظبي
Abu Dhabi University

INDIVIDUAL CONTRIBUTIONS (Mezrait Menber-1093911)

Key Responsibilities: (Organizational Security Profile, Information Classification Strategy, Risk Assessment and Control Recommendations & Cost-Benefit Analysis)

- Discretion of choice of topic
- Project Documentation
- Final additions and modification for the project
- Significant contribution to the project
- Consistent communication and coordination for the completion of the project

What was learned:

- Cruciality of information classification to discern the value of each information asset and thereby implement necessary levels of security to secure it.
- The importance of Risk Assessment in organizations induces employees to identify assets and threats, anticipate on what bad event can occur and its ramifications and assess its possibility of occurring. All in which requires organizations to make astute analysism observations and decision-making.
- Key essence of Cybersecurity is implementing security controls which not only circumvents digital attacks but also hinders real-life intrusions as well.

Reflections:

- Cybersecurity is not just a technical world of digital security but also a field where established policies must be adhered to, risks must be assessed and estimated, and careful decisions are to be made regarding implementation of security controls.

Conclusion

In conclusion, every organization has established policies and guidelines that ensure business operations sail smoothly and prevent deterrents. These policies must be well-defined and structured and not ambiguous and above all else must be effective. These organizations also must take the initiative to assess all assets for possible risks of being compromised. In order to do so, organizations must make a classification of these assets in terms of value for its beneficial contributions, ramifications if compromised, and implement sufficient levels of security controls for each asset depending on its value. While implementing these security controls, the cost of implementation must be considered whether if it is sufficient for the threat to be circumvented and worth the cost. Besides implementing security controls, properly configuring the installed controls is just as important if not more. If systems and devices belonging to an organization do not have the required system configurations, threat actors can easily exploit those devices. That is why policy compliance is another integral aspect in Cybersecurity. Aside from outsider digital attacks facilitated by threat actors, insider employees are also capable of both intentional and unintentional damages. For the unintentional, it is a fact that humans are the largest source of error from such digital attacks. Therefore, it is crucial for organizations to have training programs and security awareness to educate employees on best practices and measures to be adopted for optimal security, performance and business operations. For employees to even correctly configure systems, install controls and make evaluations; they must be given the required training.

جامعة أبوظبي
Abu Dhabi University

References

[1]. Cisco. (n.d.). *First Abu Dhabi Bank chooses Cisco FSO*. Cisco. https://www.cisco.com/c/en/us/about/case-studies-customer-successstories/first-abu-dhabi-bank.html

[2]. Cyntexa. (2024, June 12). *FAB's digital transformation with ServiceNow hits the right notes*. https://cyntexa.com/blog/first-abu-dhabi-bank-digitaltransformation-with-servicenow/

[3]. ENISA. (2023). *Threat landscape 2023*. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/topics/threat-risk-management [4]. First Abu Dhabi Bank. (n.d.-a). *Financial crime compliance program*. https://www.bankfab.com/en-ae/about-fab/corporate-governance/fab-financialcrime-compliance-program

[5]. First Abu Dhabi Bank. (n.d.-b). *Security and certifications*. https://www.bankfab.com/en-ae/about-fab/security-and-certifications [6]. First Abu Dhabi Bank. (n.d.-c). *FAB eSign – Sign documents digitally*. https://www.bankfab.com/en-ae/personal/help-and-support/digitalbanking/fab-esign

[7]. First Abu Dhabi Bank. (n.d.-d). *Corporate governance and transparency*. https://www.bankfab.com/en-ae/about-fab

[8]. GAO. (2018). *Data protection: Actions taken by Equifax and federal agencies in response to the 2017 breach* (GAO-18-559). United States Government Accountability Office. https://www.gao.gov/products/gao-18-559

[9]. Gulf News. (2020, November 18). *First Abu Dhabi Bank launches digital marketplace through Payit*. https://gulfnews.com/business/banking/first-abudhabi-bank-launches-digital-marketplace-through-payit-1.74560461

[10]. Gulf News. (2021, October 21). *UAE enacts data protection law as part of new legal reforms*. https://gulfnews.com/business/uae-enacts-data-protectionlaw-as-part-of-new-legal-reforms-1.83272440

[11]. Infosys. (2024, May 14). *Infosys collaborates with First Abu Dhabi Bank to optimize and modernize its IT infrastructure services*. https://www.infosys.com/newsroom/press-releases/2024/optimize-modernizefab-it-infrastructure-services.html

[12]. Internal Revenue Service. (2025). *Configuration and patch management planning*. https://www.irs.gov/privacy-disclosure/configuration-and-patchmanagement-planning

[13]. ISO. (2018). *ISO/IEC 27005:2018 – Information security risk management*. International Organization for Standardization.

[14]. ISO. (2022). *ISO/IEC 27001:2022 – Information security management systems requirements*. International Organization for Standardization.

[15]. ISO/IEC. (2022). *ISO/IEC 27001:2022 – Information security management systems*. International Organization for Standardization.

[16]. Microsoft News Center. (2024, March 7). *First Abu Dhabi Bank unlocks new business excellence opportunities with Core42, supported by Microsoft*. https://news.microsoft.com/en-xm/2024/03/07/first-abu-dhabi-bank-unlocksnew-business-excellence-opportunities-with-core42-supported-by-microsoft/

[17]. NIST. (2011). *SP 800-128: Guide for security-focused configuration management of information systems*. National Institute of Standards and Technology.

[18]. NIST. (2020). *Framework for improving critical infrastructure cybersecurity* (Version 1.1). National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[19]. UAE Cybersecurity Council. (2023). *UAE National Cybersecurity Strategy*. https://www.csc.gov.ae

[20]. Center for Internet Security. (2022). *CIS Controls v8*. https://www.cisecurity.org/controls/

[21]. NIST. (2003). *Special Publication 800-50: Building an Information Technology Security Awareness and Training Program*. National Institute of Standards and Technology.

[22]. DLA Piper. (2024). *Data Protection Laws of the World: UAE Overview*. https://www.dlapiperdataprotection.com

[23]. Central Bank of the UAE. (2023). *Cybersecurity Standards for Financial Institutions*. Retrieved from https://www.centralbank.ae

[24]. ISO/IEC. (2022). *ISO/IEC 27001:2022 – Information Security Management Systems*.