AMPCUS CYBER
Zero Trust Compliance Service Provider

CASE STUDY

SECURING SUCCESS: A BANK'S PATH TO ISO 27001:2022 COMPLIANCE

ISO 27001 – IMPLEMENTATION & CERTIFICATION CASE STUDY

How a leading bank in the Middle East embarked on its journey to implement and certify ISO 27001:2022 as a steppingstone to achieve a robust Cybersecurity Maturity.

Summary

Customer: Leading Bank in Middle East

Industry: Banking Sector

Challenges

1. Scope identification and finalization due to multiple standards part of the scope.
2. Stakeholder's changes and availability post-merger.

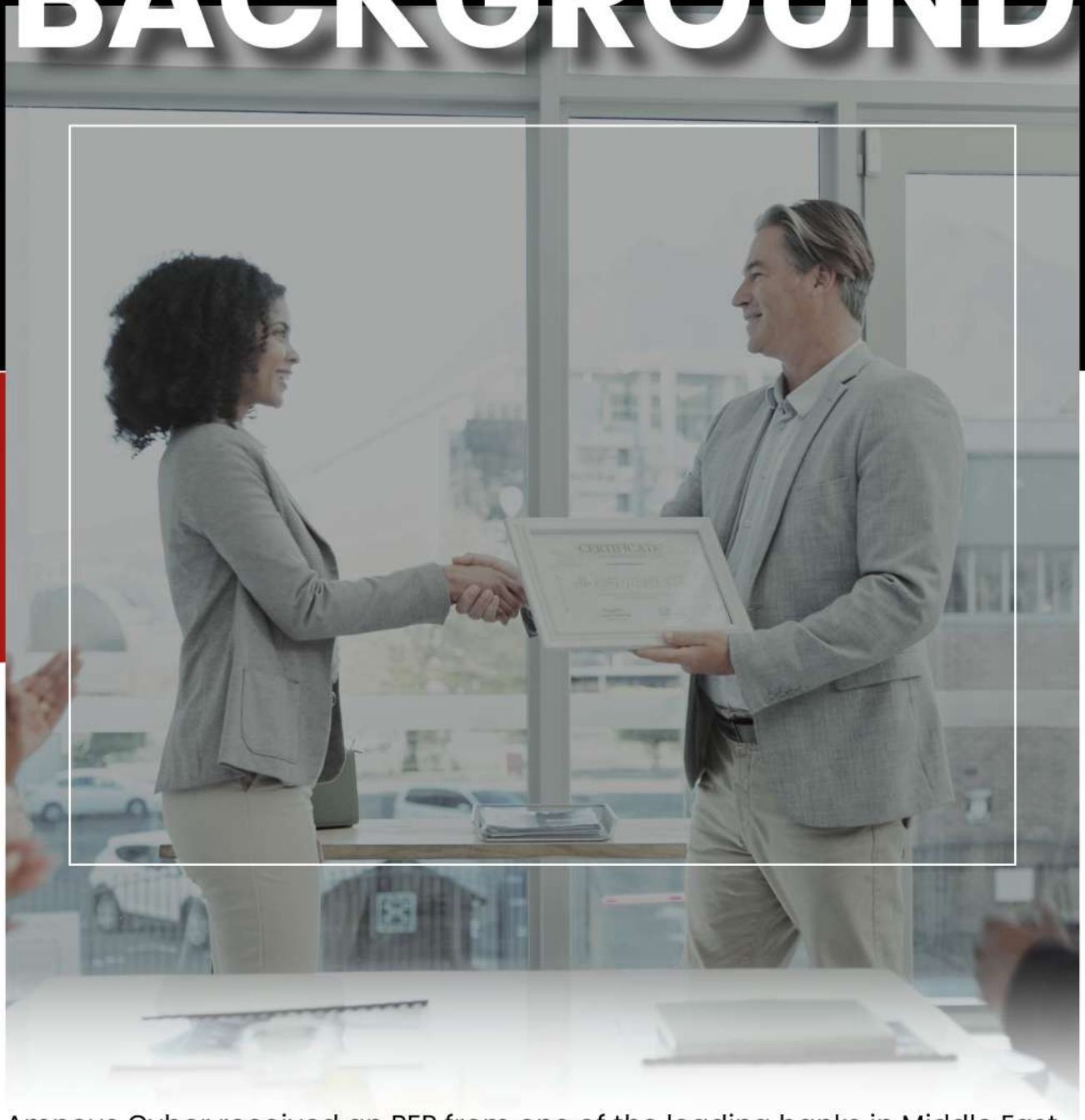
Results

The bank achieved certification in ISO 27001: 2022 which paved way to achieving other compliances as well, resulting in a strong cybersecurity maturity posture.

INTRODUCTION

In this case study, we delve into the implementation and certification of ISO 27001:2022 standard achieved by Ampcus Cyber for a leading bank in Middle East. We hope to take you through the entire journey highlighting on challenges and our unique solutions for them!

BACKGROUND



Ampcus Cyber received an RFP from one of the leading banks in Middle East, and the requirement was quite complex as they required assessment and current state understanding based on multiple standards, major among them being – ISO 27001:2022, PCI DSS v4.0, SWIFT CSP 2023. Although the initial requirement was only for a current state assessment, soon the requirement developed into providing support to implement and certify for ISO 27001:2022 entirely. The client is a multinational bank, providing a wide range of financial services including retail banking, corporate banking, and investment banking. With a customer-centric approach, the bank emphasizes the importance of safeguarding customer data and ensuring the confidentiality, integrity, and availability of its systems.

Challenges:

Prior to implementing ISO 27001, the bank faced several challenges:

Post-Merger Integration Challenge: The bank had recently undergone a huge merger which brought together diverse talent. However, aligning these diverse workstyles and streamlining internal processes to function as a cohesive unit remains a challenge.

Data Security Concerns: With the increasing frequency of cyber-attacks targeting financial institutions, the bank needed a robust framework to mitigate risks and protect sensitive customer information.

Regulatory Compliance: The banking sector is highly regulated, with stringent requirements for data protection. The bank needed to ensure compliance with various regulatory bodies such as the Central Bank of the country and the Payment Card Industry Data Security Standard (PCI DSS).

Risk Management: Identifying, assessing, and managing information security risks across diverse business units and geographies was a complex task for the bank especially after the merger.

ISO 27001 Implementation Journey

Along with the ISO 27001:2022 certification requirement, the bank was very keen on their current state evaluations against multiple standards, major among them being – ISO 27001:2022, PCI DSS v4.0, SWIFT CSP 2023. Ampcus Cyber decided to conduct a Unified Compliance Assessment to achieve this requirement.

Unified Compliance Assessment:

The key benefits from this approach were:

1. Streamlined Approach – Reduces redundancies and simplifies compliance efforts by applying common control identification across multiple standards and frameworks.
2. Cost Optimization – Minimizes resource allocation.
3. Elimination Duplication – Reduces redundancies in all aspects of the project.
4. Harmonized & Centralized Approach – Ability to practice/manage compliance centrally by aligning to requirements from multiple standards.

Process:

- The first step in achieving a unified compliance was to identify the common controls across the different standards in scope and analyzing the areas of gaps/vulnerabilities.
- Next, we targeted the unique requirements from each standard and analyzed the bank's current state against them.
- Now we documented a detailed report which provided a clear insight on the bank's current state and recommendations to arrive at the desired state.

ISO 27001:2022 Implementation

Initiation and Leadership: Ampcus Cyber initiated the ISO 27001 implementation project with the full support from the bank's senior management. A dedicated Information Security Steering Committee was formed to oversee the implementation process and ensure alignment with business objectives. The committee was made aware of all the gaps/ vulnerabilities identified during the unified assessment stage and the effort required to mitigate them.

Risk Assessment and Management: The corner stone of implementing ISO 27001 is to build a robust risk management methodology and practice. This methodology was used to conduct a comprehensive risk assessment and potential threats and vulnerabilities across all areas of operation, including IT infrastructure, applications, and personnel were identified. Risks were evaluated based on their likelihood and potential impact on the organization's objectives. Appropriate Risk Treatment plans were devised for the risks that were above the bank's tolerance levels.

Controls Implementation / Remediation: Based on the results of the risk assessment and unified gap assessment, Ampcus Cyber assisted the bank to implement multiple security controls to address identified risks and gaps. These controls encompassed technical measures such as encryption, access controls, and intrusion detection systems, as well as organizational measures including employee training and awareness programs. Ampcus Cyber also assisted the bank in developing a strong control measurement method and initiated the program for continuous monitoring of ISMS.

Information Security Policy & Other Supporting Documentation: Ampcus Cyber developed a strong Information Security Policy outlining the bank's commitment to information security, along with specific guidelines and procedures for safeguarding data assets. The policy was communicated to all employees and stakeholders, emphasizing their roles and responsibilities in maintaining security. Several other supporting policies, procedures and work instructions required for a robust ISMS was also developed.

Security Awareness Training: Curated training sessions were conducted to familiarize employees with the new security measures and ensure compliance with established protocols. This training also concentrated on specific standard and regulatory requirements, that all employees must be aware of.

Internal Audits and Reviews: Ampcus Cyber conducted an internal audit (by an independent consultant, who did not participate in the implementation) to assess the effectiveness of the implemented controls and identify areas for improvement. Findings from audits were reviewed by the Information Security Steering Committee, and corrective actions were taken as necessary to address any deficiencies.

ISO 27001 Certification Journey

Once the requirements from ISO 27001:2022 were successfully implemented and the bank's management and steering committee signed off on the internal audit results, it was time to initiate the certification body.

ISO 27001 Certification Journey

Ampcus Cyber has partnered with a leading certification body who made the whole process smooth and accommodating to the bank. The certification audit was conducted onsite for 3 days which included the following:

- Stage 1 Audit: The certification body conducts a preliminary audit to verify the bank's readiness for a full audit.
- Stage 2 Audit: The certification body performs a comprehensive audit to assess the ISMS's effectiveness and compliance with ISO 27001:2022 requirements.

Upon successful completion of the audit, the certification body issued an ISO 27001 certificate.

Conclusion

The bank was awarded the ISO 27001:2022 certificate by the certification body after the successful audit. This was a true testament to the banks and our effort throughout the project engagement!

The successful implementation of ISO 27001:2022 standard has positioned the bank as a leader in information security within the banking industry. By adopting a proactive approach to risk management and compliance, the bank has not only safeguarded its own interests but also reinforced its commitment to protecting the interests of its customers.

This project paved way for the bank to initiate projects to achieve other compliances as well, resulting in a strong cybersecurity maturity posture!

What did the bank Achieve by Implementing ISO 27001:2022?

Enhanced Security Posture: By aligning with ISO 27001 standards, the bank significantly strengthened its information security posture, reducing the risk of data breaches and cyber-attacks.

Regulatory Compliance: The implementation of ISO 27001 helped the bank demonstrate compliance with regulatory requirements, thereby avoiding potential fines and penalties.

Customer Trust and Confidence: The commitment to information security outlined in the ISO 27001 certification reinforced customer trust and confidence in the bank's ability to protect their sensitive financial information.

USA
Ampcus Cyber Inc., 14900 Conference Centre, Drive Suite #500, Chantilly, VA 20151.

India
Unit No. 601-608, 6th floor Beta Block, Sigma Tech Park, Varthur, Bengaluru - 560 066. Ph No. - (703) 621 - 1318

Philippines
Tower 3, Unit 1914, Grace Residences, Levi Mariano Avenue, Ususan Taguig City, Metro Manila 1632, Philippines

Dubai
Dubai Silicon Oasis, DDP, Building A1, Dubai, United Arab Emirates