International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 07 July 2025, pp: 87-96 www.ijaem.net ISSN: 2395-5252

A Case Study of Penetration Testing Implementation in a Financial Institution: Lessons Learned and Best Practices

[1]Areeza Shahirah Mohamad Safari, [2]Mullaishselvi A/P Krishnasamy, [3]Nakibuuka Jamirah, [4]Tan Xiao Qin, [5]Mohamad Fadli Zolkipli

School of Computing, UniversitiUtara Malaysia (UUM), 06010 Sintok, Kedah, MALAYSIA

Date of Submission: 01-07-2025 Date of Acceptance: 10-07-2025

ABSTRACT: Penetration testing has become a crucial component of financial institutions' cybersecurity frameworks due to the rise in cyber threats and increasingly complex regulatory requirements. This case study explores the implementation of penetration testing in a financial institution, highlighting both operational challenges and strategic approaches. The paper outlines the scope, testing methodology, tools, regulatory alignment and stakeholder involvement in the penetration testing process. It highlights several key challenges including complex regulatory requirements, outdated infrastructure, limited internal expertise, and organizational resistance. The study also presents recommended best practices, such as securing executive support, adopting threat-led penetration testing, incorporating manual testing techniques and ensuring well-defined testing scope.

KEYWORDS: Penetration testing, financial institution, cyberattacks, regulation compliance, risk assessment.

I. INTRODUCTION

In the rapidly evolving landscape of financial services, the imperative to safeguard sensitive data and maintain robust cybersecurity measures has never been more critical. Financial institutions are prime targets for cybercriminals due to the vast amounts of sensitive information they handle, making the implementation of comprehensive security strategies essential. Among these strategies, penetration testing has emerged as a pivotal component in identifying and mitigating vulnerabilities within organizational systems.

Penetration testing, often referred to as ethical hacking, involves simulating real-world cyberattacks to uncover and address potential weaknesses in an organization's IT infrastructure. This proactive approach enables financial institutions to assess their security posture, ensuring that defenses are robust enough to thwart actual cyber threats. According to a study published [1], 76% of financial institutions conduct penetration tests at least annually, with regular testing reducing the risk of successful cyberattacks by up to 60%.

The financial sector faces an ever-changing threat landscape, with cybercriminals employing increasingly sophisticated methods. The integration of advanced technologies, such as artificial intelligence (AI) and machine learning (ML), has further complicated the cybersecurity environment. While these technologies offer enhanced security capabilities, they also present new vulnerabilities that adversaries can exploit. A 2025 article in FinTech Futures highlights that AI-driven cyberattacks have become a significant challenge for financial services, necessitating equally advanced defensive measures.

In response to these evolving threats, regulatory bodies have intensified their focus on cybersecurity compliance. For instance, the Bank of Japan's On-Site Examination Policy emphasizes the importance of penetration testing in evaluating the effectiveness of cybersecurity frameworks within financial institutions. Compliance with such regulations not only ensures legal adherence but also fortifies the institution's resilience against cyber threats.

Traditional penetration testing methods have relied heavily on manual processes, which,

International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 07 July 2025, pp: 87-96 www.ijaem.net ISSN: 2395-5252

while thorough, are time-consuming and resource intensive. Recent advancements have seen the integration of AI and automation into penetration testing, enhancing efficiency and scalability. The development of systems like PenTest++, which combines automation with generative AI, exemplifies this trend. [2]Such systems streamline critical testing tasks, allowing for more comprehensive and rapid assessments of security postures.

Furthermore, the adoption of frameworks such as the Open Web Application Security Project (OWASP) and the Penetration Testing Execution Standard (PTES) have standardized testing processes, ensuring consistency and thoroughness in identifying vulnerabilities.

Despite the benefits, implementing penetration testing in financial institutions is not without challenges. The complexity of modern IT environments, coupled with resource constraints and the rapid evolution of cyber threats, can hinder effective testing. Additionally, ensuring minimal disruption to 24/7 operations during testing phases is a critical concern.

However, these challenges present opportunities for growth and improvement. Investing in employee training and fostering a culture of cybersecurity awareness can significantly enhance the effectiveness of penetration testing initiatives. [3]A study focusing on Malaysian banking employees underscores the importance of continuous education in mitigating cybersecurity risks.

Penetration testing stands as a cornerstone in the cybersecurity strategies of financial institutions. By proactively identifying and addressing vulnerabilities, these institutions can bolster their defenses against an increasingly sophisticated array of cyber threats. Embracing advancements in testing methodologies, adhering to regulatory standards, and fostering a culture of continuous improvement are essential steps in safeguarding the integrity and trust that underpin the financial sector.

II. BACKGROUND

Overview of Cybersecurity in Financial Institutions:

In the financial industry, cybersecurity plays an important role in protecting sensitive data, ensuring safe transactions, and maintaining customer trust. [4]That information is highly valuable and since financial institutions are mainly involved in monetary transactions, they become the prime target for cyberattacks. A successful attack can damage a company's reputation, cause customers to leave, and result in heavy fines from regulators. As online banking services expand, the risk of cyberattacks continues to rise. To effectively strengthen their security posture, it is crucial to understand the most common threats they face. Below are the most common cybersecurity threats encountered by financial institutions today.

Phishing

[5]Phishing is one of the most common and dangerous cyber threats in digital banking. It uses deceptive methods such as fake emails or websites to trick users into providing sensitive information like login credentials, password, or bank details. Phishing is particularly dangerous because it focuses on human behavior rather than technology vulnerabilities.

Malware

Malware includes harmful software like viruses, Trojans and spyware that can enter a user's device through phishing emails, suspicious downloads or unsafe websites. Once successful, malware cansteal login credentials, monitor bank transactions, or secretly control mobile banking applications.

Ransomware

Ransomware is a type of malicious software that locks or encrypts important files.In the context of digital banking, it can stop users from accessing their accounts or disrupt the bank's online operations. While ransomware is often linked to large-scale attacks, digital banking platforms can also be targets, especially if they lack strong backup and recovery systems. These attacks cause not only financial losses but also make customers lose confidence in using digital services.

DDoS Attacks

DDoS (Distributed Denial of Service) attack work by sending a large amount of fake traffic to make a website or server slow or unavailable to users. [6]In banking, this can prevent customers from accessing their accounts or completing transactions, leading to financial losses, customer frustration, and reputational damage. In banking systems that use Internet of Things (IoT) devices, like smart ATMs or connected services, DDoS attacks can be even more harmful.

Insider Threats

[7]Insider threats occur within individual and organization, such as employees or business partners either intentionally or accidentally cause harm to the system. Insiders have authorized access

International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 07 July 2025, pp: 87-96 www.ijaem.net ISSN: 2395-5252

to important system and sensitive data. This makes their actions much harder to detect compared to external hackers.

Strong cybersecurity helps prevent these threats by securing systems, detecting suspicious activity, and quickly responding to incidents. It also ensures that banking services remain available and reliable for customers. In short, cybersecurity is vital for protecting both the financial system and the people who depend on it.

Introduction to Penetration Testing:

Penetration testing, or pen testing, is a method of evaluating the security of a computer system, network, or web application by simulating a real cyberattack. The purpose is to identify vulnerabilities that could be exploited by malicious hackers. This helps organizations understand their security weaknesses and take action to fix them before an actual attack occurs.[8] By finding and addressing these vulnerabilities early, organizations can reduce the risk of cyberattacks and better protect sensitive data. Penetration testing can be conducted using two primary approaches: manual and automated. Manual penetration testing involves skilled cybersecurity professionals who simulate real-world attacks using their expertise, creativity, and in-depth analysis to uncover complex vulnerabilities that automated tools might miss. On the other hand, automated penetration testing uses specialized software tools to scan systems, networks, or applications for known vulnerabilities. It is faster, more consistent, and ideal for routine assessments, but may not detect more sophisticated threats. Combining automated scanning with manual testing provides better results. [9]Manual testing is more accurate because it depends on the tester's skills and experience. Testers who understand both manual techniques and automation tools can perform more effective attacks. In addition to these approaches, penetration tests are also classified based on the level of information available to the tester, typically Black Box, White Box, and Gray Box testing.

Black Box Testing

[9]Black box testing is a security method where the tester acts like an outsider with no inside knowledge of the system. The tester doesn't have access to the website's code or internal setup. Instead, they use tools and techniques to gather information from the outside—like scanning ports or mapping networks—to find possible weaknesses. The goal is to mimic real-world attacks and see what a hacker might discover. While this gives a realistic view of external threats, it can be slow and resource-heavy because the tester starts with nothing.

White Box Testing

[9]White box testing is the opposite of black box. Here, the tester is given complete access to the website's inner workings—source code, architecture, and internal documentation. This helps identify security flaws during the early stages of development. Because the tester knows everything about the system, they can check it in more depth. However, it might not show how vulnerable the site is to real attackers, since those attackers wouldn't have such full access. Also, it requires more time and expertise.

Grey Box Testing

[9]Grey box testing is a combination of the two of the above. The tester has limited inside information—such as user accounts, basic network info, or system layout—but not full access. This makes the test more realistic than the white box, while being more informed than the black box. It helps find flaws that someone with some access, like a low-level employee or a partner, might exploit. Still, it has limitations because the tester doesn't have full or zero access, and it often needs cooperation with the system owners.

III. METHOFOLOGIES

This case study uses a comprehensive and practical penetration testing method to assess the security measures of a financial organization. The engagement comprised an assessment of both internal and external attack surfaces, which were then checked against compliance frameworks. This was done in partnership with several stakeholders to ensure that both technical rigor and organizational coherence were maintained.

Scope of the Penetration Testing:

The following institutions were included in the penetration testing engagement's scope:

- Internal Infrastructure: This includes endpoints, internal databases, Windows domain controllers, and user access controls within the corporate LAN.
- Web Applications: [10]We looked for security holes, misconfigurations, and bad coding standards in public-facing apps such online banking portals, customer support platforms, and authentication systems.
- Third-Party Services:[11]APIs and cloud-hosted solutions that are part of the financial ecosystem were examined to see how well

International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 07 July 2025, pp: 87-96 www.ijaem.net ISSN: 2395-5252

they can handle threats from suppliers and inadequate service-level interfaces.
- The goal of this three-part test was to provide realistic attack surfaces that attackers may use and make sure that the test mimicked the actions of both internal and external threat actors.

Testing Approach and Duration

Both black-box and grey-box testing methods were used over the course of four weeks:

- Black-box testing acted like outside threat actors who did not have access to the inside. This phase was mostly about scouting, analyzing the perimeter, and taking advantage of weak services.
- Grey-box testing gave testers restricted credentials and access, [10]which was like having an insider threat or a hacked account to see how lateral movement and privilege escalation work.

The conversation was set up to happen once a week like this:

Table 1: Four-Week Penetration Testing Plan – Activities, Objectives, and Tools

Week	Activities	Objectives	Tools and Techniques
Week 1	Reconnaissance, scoping, andinfrastructure enumeration	Identify and map assets, determine test scope, and gather initial intelligence	Nmap, Whois, Shodan, asset inventory tools
Week 2	Vulnerability discovery and confirmation using static and dynamic scanning	Detect and verify known and unknown vulnerabilities through various scans	Nessus, OpenVAS, Nikto, custom scripts
Week 3	Controlled exploitation and impact analysis	Test exploitability of vulnerabilities and assess real-world implications	Metasploit, Burp Suite Pro, custom payloads
Week 4	Reporting, remediation suggestions, and validation	Document findings, provide fixes, and confirm resolution of issues	Reporting frameworks, retesting scripts, validation checklists

Tools and Techniques Utilized:

The testing team used both automatic tools and human procedures to make sure that the vulnerability assessment was thorough and accurate.

- Nmap: Used to find hosts, count ports, and fingerprint services.
- Nessus: [11]Turned on full vulnerability scanning and CVE enumeration based on the most recent threat intelligence feeds.
- Burp Suite: Used to do a full security check on web apps, looking for things like injection flaws, session management problems, and cross-site scripting.
- Metasploit Framework: Used for controlled exploitation, figuring out what it means in the real world, and safely showing how exploitable something is in limited testing scenarios.
- Manual methods including discovering logic defects, hijacking sessions, and chaining misconfigurations to back up our results and cut down on false positives.

Compliance and Regulatory Alignment:

The testing process followed the regulatory and standards set by the financial sector and the government.

- Requirement 11.3 of PCI DSS v4.0 says that systems that store and handle cardholder data must have been thoroughly tested for security holes. All tests were set up to meet the requirements for annual and post-significant-change testing.
- ISO/IEC 27001:2022 Controls: [11]Linked results and controls to the rules in Annex A for managing vulnerabilities (A.12.6), testing security (A.14.2), and working with suppliers.

The dual compliance alignment makes sure that the weaknesses found make it easier to be ready for an audit and keep your certification.

Stakeholder Involvement and Knowledge Transfer:

Different sets of stakeholders were involved in the process at all times.

- Internal Security Team: Helped find important assets, deal with real-time assessments, and make sure that corrective actions were taken.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 07 July 2025, pp: 87-96 www.ijaem.net ISSN: 2395-5252

- Compliance Officers: Made sure that the testing methods satisfied business policy and risk acceptability guidelines.
- [10]External auditors kept an eye on the examination of third-party assurance and regulatory openness.

Pre-assessment and post-assessment workshops were done to align the scope, results/findings, and set priorities for remediation based on operational risk levels.

IV. FINDING / SECURITY IMPROVEMENTS

Penetration testing uncovered business logic flaws and configuration weaknesses in customer-facing apps and third-party integrations, such as SQL injections and broken authentication mechanisms. The institution strengthened secure coding practices and infrastructure settings, including comprehensive patching of unpatched systems and adjustment of firewall rules to minimize misconfigurations.

Although informal cybersecurity practices existed, there was no formal documentation of policies and incident response processes. Development and inculcation of formal, written policies including incident response workflowsfacilitated better alignment with SOC audit requirements and regulatory readiness.

Testing revealed vulnerabilities stemming from human factor-poor password practices and susceptibility to social engineering. A structured cybersecurity training program was introduced, covering phishing, credential hygiene, and social engineering resilience, which increased awareness of threat scenarios and controls.

The post-test environment showed reinforced network defenses, including improved segmentation, secure access control, and refined perimeter security that limited lateral movement. Hardening measures across servers and endpoints resulted in a noticeably hardened network posture, enhancing overall resilience against intrusions.

[12]Regular testing uncovered more low- to medium-level vulnerabilities, reinforcing the benefits of continuous detection. Adoption of annual penetration tests, combined with progressive adoption of diverse testing methodologies (e.g., external/internal, red/grey team), evidenced by regulatory guidance.

[13]Penetration testers evaluated the effectiveness of incident response protocols in real-time attacks, discovering control gaps. The institution introduced regular tabletop and live response drills to improve response coordination and incident lifecycle management.

Penetration tests served dual roles: vulnerability assessment and regulatory compliance (e.g., PCI-DSS, GLBA). Formalized pentests enabled the organization to demonstrate due diligence to auditors, Bridge regulatory expectations, and avoid fines and reputational damage.

The outcome is a significantly stronger security posture—validated through regular testing, embedded awareness programs, and measurable improvements across technology, processes, and people.

Table 2: Summary of findings and security improvements

Area	Improvement Actions	Benefit
App & Infra Hardening	Secure coding, patching, config fixes	Fewer exploitable flaws
Policy & Documentation	Written cyber policies and incident plans	Audit readiness, consistency
User Awareness	Phishing/soc-eng training	Reduced human risk
Network Defense	Segmentation & endpoint hardening	Slowed lateral movement
Testing Cadence	Annual + varied pentests	Sustained security posture
Response Readiness	Tabletop & incident drills	Faster breach containment
Regulatory Compliance	Demonstrable testing and remediation	Lower risk of fines, trust building

International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 07 July 2025, pp: 87-96 www.ijaem.net ISSN: 2395-5252

V. CHALLENGES & LIMITATIONS

[14]The intricate web of regulatory frameworks encompassing the digital operational resilience Act ISO/IEC 27001 and the General Data Protection Regulation states that financial institutions adhere to rigorous standards regarding penetration testing. The confluence of these regulations, while intended to bolster cybersecurity, often results in operational complexities and strategies particularly within multinational financial institutions struggling with cross-border compliance mandates. Threat-led penetration testing as a component of DORA compliance necessitates alignment with regulatory expectations, introducing delays and uncertainties in execution. Compliance-driven penetration testing frequently transforms into a superficial exercise primarily aimed at satisfying auditors rather than identifying and remediating underlying vulnerabilities, an approach that can lead to false sense of security as institutions may prioritize meeting regulatory requirements over conducting thorough and comprehensive testing that uncovers deep-seated flaws in their system and infrastructure.

[15]Financial institutions, which are attractive targets for cyberattacks, face a continuous barrage of threats that necessitate robust and adaptive security measures, making penetration testing an essential component of their cybersecurity strategy. [16]The increasing interconnectedness of systems, the adoption of cloud computing, and the proliferation of mobile and IoT devices have further complicated the task of securing financial networks, requiring continuous improvement of security measures to safeguard against increasingly complex cyber threats. [17][18]Penetration testing, designed to proactively identify and mitigate vulnerabilities, simulates real-world attacks to evaluate the effectiveness of existing security controls and incident response capabilities. [19]However, the unique characteristics of the financial sector, including stringent regulatory oversight, legacy infrastructure, and the critical nature of financial services, introduce substantial hurdles to the seamless implementation of penetration testing programs. The financial sector's unique operational and regulatory landscape introduces additional layers of complexity that must be carefully managed to ensure the effectiveness and safety of penetration testing activities.

[20]The financial sector, a perennial target for cyberattacks, faces an escalating challenge in maintaining robust cybersecurity defences due to pronounced shortage of skilled professionals, especially those in penetration testing. [19]This deficiency compels many banking institutions to outsource critical security functions to third-party vendors, creating potential vulnerabilities and dependencies that guarantee careful considerations.[21]The increasing sophistication and frequency of cyber threats targeting financial systems require specialized expertise that is often lacking in internal IT departments. [11]The gap in cybersecurity expertise within banks forces them to strongly rely on external penetration testing services which can present challenges related to cost, coordination, and potential conflicts of interest. [22]A comprehensive understanding of emerging cybersecurity threats in financial technologies underscores the necessity for constant training awareness programs to empower professionals. The lack of in-house expertise in advanced penetration testing techniques such as exploit development and evasion methods leaves institutions vulnerable to sophisticated attacks that may bypass standard security measures and yet still the reliance on external testers can limit the depth and scope of assessments as these testers may not possess the same level of familiarity with the bank's internal systems and processes as dedicated in-house teams who can continuously monitor incident responses and proactive threat hunting tasks that are difficult to fully outsource.

[14]The organizational resistance and risk aversion is a big hindrance that frequently affect the comprehensive adoption of penetration testing methodologies resulting in a fragmented security landscape. [23]These barriers manifest as internal teams' reluctance to subject critical systems to comprehensive testing, stemming from apprehensions about potential disruptions or the revelation of latent vulnerabilities.[24]In highly regulated industries or sectors where reputational damage can have significant financial repercussions, this resistance is often amplified, leading to a cautious approach to security assessments. [14]Some organizations prioritize the avoidance of negative publicity over proactive risk mitigation which leads to the implementation of overly restrictive testing parameters such as confining assessments to non-production environments.

[25]Penetration testing within financial institutions encounters substantial obstacles due to the prevalent use of outdated infrastructure which often lacks contemporary security mechanisms including network segmentation, secure application programming interfaces and thorough logging capabilities. [26]These legacy systems characterized by their intricate architecture and reliance on older technologies frequently exhibit

vulnerabilities that cannot be readily addressed through modern penetration testing methodologies as they are often designed to withstand intrusive testing without risking system instability or failure. The integration of such legacy systems with modern security tools and practices poses a significant challenge that requires careful consideration of compatibility issues and potential disruptions to critical financial operations. Furthermore, [27]the complexity inherent in these systems often necessitates specialized expertise and customized testing approaches adding the cost and time required for comprehensive security assessments. The financial sector's increasing reliance on third-party vendors for specialized services such as cloud computing, data analytics and payment processing introduces additional layers of complexity to the penetration testing process.

[28]Financial institutions, particularly small medium-sized enterprises, encounter significant limitations in executing thorough penetration testing and ethical hacking exercises due to constrained financial resources and limited staffing. This is further aggravated by increasing sophistication and frequency of cyberattacks targeting financial systems. [14]Then also the frequency of penetration testing is often compromised due to the extensive time required for comprehensive assessments, especially in complex banking systems. Here the smaller institutions may opt for less frequent or less comprehensive tests to minimize disruptions and costs. Furthermore, comprehensive penetration testing encompasses red teaming, threat emulation and internal threat simulations that demand significant time investments which can restrain the already limited resources of smaller banks.

[28]While penetration testing is a valuable security assessment technique, it often suffers from limitations in scope that can significantly lead organizations to decline narrow testing parameters focusing primarily on easily quantifiable vulnerabilities such as those found in external network infrastructure or common web application flaws. Compliance mandates designed to provide a baseline level of security can paradoxically resist testing efforts by focusing solely on external facing systems or adhering to standardized vulnerability checklists thus neglecting internal threats or customized application vulnerabilities. These constraints can lead to false sense of security as organizations may believe they have adequately assessed their risk posture while in reality significant vulnerabilities remain unaddressed. The ever-changing landscape of cyber threats poses a challenge to all industries highlighting the importance of regularly scheduled information security audits which include penetration testing, vulnerability scans and network assessments produce reports that allow the organization to understand their security stance and what vulnerabilities may be present.

VI. BEST PRACTICES

The financial sector necessitates adaptive cybersecurity strategies that transcend vulnerability assessments. A fundamental approach like threat-led penetration testing methodologies encompassing multi-phase testing models is very important for enhancing the resilience of financial institutions. Due to the increasing complexity and severity of modern cyber threats, financial institutions must evolve beyond conventional surface-level vulnerability assessments and adopt a more comprehensive multi-layered testing methodology. [21]With the continuous rise of destructive cyberattacks, financial organizations face mounting pressure to enhance their cybersecurity measures necessitating the development and evolution of more viable protection mechanisms. Threat-led penetration represents a significant departure from traditional security evaluations, shifting the focus towards simulations that closely mimic real-world attack scenarios which is particularly crucial for financial institutions due to their frequent targeting by sophisticated and persistent cyberattacks.

[16]Penetration testing requires the active engagement and support of executive leadership which is essential for securing the necessary resources promoting collaboration across various departments and establishing a clear directive for addressing the vulnerabilities identified during testing. [22]Executive buy-in is critical because it ensures that security initiates are aligned with the overarching business objectives and risk management strategies of the institution. By embedding security assessments within the development and deployment pipelines, organizations can proactively identify and address vulnerabilities before they can be exploited by reducing the attack surface and minimizing the potential for disruptive and costly security incidents. A robust security culture is characterized by a shared understanding of security and a commitment to implement and adhere to security best practices at all levels of the organization.

[14]Automated tools offer efficiency in pinpointing common vulnerabilities like cross-site scripting and SQL injection but have limitations when it comes to complexities of financial systems.

[28]A critical aspect of effective penetration testing within financial institutions is the prioritization of manual techniques which are indispensable for uncovering vulnerabilities related to intricate business logic, privilege escalation mechanisms and session management protocols that often elude automated detection. [22]Manual penetration testing enables security professionals to simulate real-world attack scenarios meticulously exploring the application's functionality to identify potential weaknesses in its design and implementation. This approach is basically for financial platforms where complex transaction workflows and data handling processes demand a deep understanding of the system's inner workings to uncover vulnerabilities that could be exploited by malicious actors. [16]The increasing interconnectedness of systems, their adoption to cloud computing and rapid increase of mobile and IoT devices have further complicated the task of securing financial networks necessitating advanced security measures beyond traditional perimeter-based defenses.

A well-defined scope is fundamental to a successful penetration test, especially within the highly regulated and sensitive environment of financial institutions requiring a meticulous approach that balances comprehensiveness with practically encompassing all relevant systems, networks, applications and data repositories. [14]Penetration testing primarily identifies vulnerabilities that could be exploited by malicious actors necessitating a clear articulation of testing objectives that aligns with the institution's risk management strategy and regulatory compliance requirements.[22] Specific objectives might include evaluating the effectiveness of existing security controls, identifying potential attack vectors or assessing the resilience of critical systems against specific types of cyber threats. [29]A comprehensive set of engagements is crucial for ensuring that penetration testing activities are conducted in a safe, ethical, legal and compliant manner outlining the permissible testing techniques, communication protocols and escalation procedures to minimize the risk of disruption to critical business disruptions, unauthorized access to confidential information or violation of legal and regulatory mandates.

VII. CONCLUSION

Penetration testing implemented in financial institutions is not just a technical exercise but also a necessary practice for protecting important assets, guaranteeing regulatory compliance, and preserving public confidence. This case study shows that penetration testing is an essential component of a safe cybersecurity framework despite operational difficulties and restrictions like regulatory complexity, outdated infrastructure, lack of talents, and resource constraints.

Implementation of structured testing methodologies like black-box and grey-box techniques, financial institutions can simulate actual attack scenarios and find vulnerabilities that may go unnoticed. By means of the integration of manual and automated approaches, the comprehensiveness and accuracy of these evaluations are much enhanced, therefore enabling institutions to prioritise important risks and carry out quick corrective action.

Formulating testing strategies and ensuring conformity with industry best practices depend on regulatory frameworks such as PCI DSS and ISO/IEC 27001:2022. True cybersecurity readiness goes beyond simple compliance, and it requires proactive thinking, executive commitment, and culture of improvements. This includes regular knowledge exchange, involving stakeholders, and security assessments into more encompassing digital transformation initiatives.

Financial institutions have to embrace threat-led penetration testing techniques and risk-based strategies since cyber threats pattern change depending on evolving technology, enlarged attack surfaces, and sophisticated adversaries. By doing this, organizations improve their security protocols, ensure operational continuity, consumer confidence, and long-term resilience in a dynamic digital terrain.

This case study shows that penetration testing is an ongoing process that needs to adapt with varying threat environments and technological advancement rather than a one-time occurrence. It gives financial institutions actionable intelligence to fight both known and unknown risks when executed correctly, hence strengthen their position as guardians of the world financial system.

ACKNOWLEDGEMENT

The authors would like to thank all members of the School of Computing who are involved in this study. This study was carried out as part of Hacking and Penetration Testing Project. This work was supported by Universiti Utara Malaysia.

REFERENCES

[1]. Poli Reddy Reddem, "Cybersecurity in Banking and Finance : Navigating the Digital Threat Landscape," International Journal of Scientific Research in Computer

Science, Engineering and Information Technology, vol. 10, no. 5, pp. 852–861, Nov. 2024, doi: 10.32628/CSEIT241051073.

[2]. S. Onimisi Dawodu, A. Omotosho, O. Josephine Akindote, A. Oluwatoyin Adegbite, S. KuzankahEwuga, and C. Author, "CYBERSECURITY RISK ASSESSMENT IN BANKING: METHODOLOGIES AND BEST PRACTICES," Computer Science & IT Research Journal, vol. 4, no. 3, pp. 220–243, 2023, doi: 10.51594/csitrj.v659.

[3]. S. G. Krishnan, A. Al-Nahari, N. A. Ismail, and D. N. L. Yao, "Enhancing Cybersecurity Awareness among Banking Employees in Malaysia: Strategies, Implications, and Research Insights," International Journal of Academic Research in Business and Social Sciences, vol. 13, no. 8, Aug. 2023, doi: 10.6007/ijarbss/v13-i8/17413.

[4]. Anuj Thapliyal, "Importance of Cybersecurity in Financial Services Industry: An Analytical Perspective of Various Security Models," International Journal of Early Childhood Special Education, Jun. 2023, doi: 10.48047/intjecse/v14i2.1074.

[5]. Md. Waliullah, M. Z. H. George, M. T. Hasan, M. K. Alam, M. S. K. Munira, and N. A. Siddiqui, "ASSESSING THE INFLUENCE OF CYBERSECURITY THREATS AND RISKS ON THE ADOPTION AND GROWTH OF DIGITAL BANKING: A SYSTEMATIC LITERATURE REVIEW," American Journal of Advanced Technology and Engineering Solutions, vol. 1, no. 01, pp. 226–257, Feb. 2025, doi: 10.63125/fh49gz18.

[6]. U. Islam et al., "Detection of Distributed Denial of Service (DDoS) Attacks in IOT Based Monitoring System of Banking Sector Using Machine Learning Models," Sustainability (Switzerland), vol. 14, no. 14, Jul. 2022, doi: 10.3390/su14148374.

[7]. D. Javaheri, M. Fahmideh, H. Chizari, P. Lalbakhsh, and J. Hur, "Cybersecurity threats in FinTech: A systematic review," May 01, 2024, Elsevier Ltd. doi: 10.1016/j.eswa.2023.122697.

[8]. A. Kadir Bin Mahamood, M. Fadli, and B. Zolkipli, "Cybersecurity Strengthening through Penetration Testing: Emerging Trends and Challenges," 2023. [Online]. Available: www.majmuah.com

[9]. N. Rane and A. Qureshi, "Comparative Analysis of Automated Scanning and Manual Penetration Testing for Enhanced Cybersecurity," in 12th International Symposium on Digital Forensics and Security, ISDFS 2024, Institute of Electrical and Electronics Engineers Inc., 2024. doi: 10.1109/ISDFS60797.2024.10527240.

[10]. L. Harjunen, "Optimizing Web Application Security Testing Process in the Financial Sector," 2023.

[11]. T. N. Tran, "Systematic Review of Cybersecurity in Banking: Evolution from Pre-Industry 4.0 to Post-Industry 4.0 in Artificial Intelligence, Blockchain, Policies and Practice," 2025, doi: https://doi.org/10.48550/arXiv.2503.00070.

[12]. K. Chauhan, "Insider Threats Mitigation: Role of Penetration Testing," Jul. 2024, [Online]. Available: http://arxiv.org/abs/2407.17346

[13]. G. Egbedion and G. Efahn, "Impact Of Vulnerability Management And Penetration Testing On Security-Informed It Project Planning And Implementation," vol. 11, 2024, [Online]. Available: www.jmest.org

[14]. T. Adeniran et al., "Vulnerability Assessment Studies of Existing Knowledge-Based Authentication Systems: A Systematic Review," Sule Lamido University Journal of Science & Technology, vol. 8, no. 1, pp. 34–61, 2024, doi: 10.56471/slujst.v7i.485.

[15]. K. Priyadarshani and Dr. A. Rengarajan, "Cybersecurity in the Financial Sector," International Journal of Research Publication and Reviews, vol. 5, no. 3, pp. 751–756, Mar. 2024, doi: 10.55248/gengpi.5.0324.0709.

[16]. C. Daah, A. Qureshi, I. Awan, and S. Konur, "Enhancing Zero Trust Models in the Financial Industry through Blockchain Integration: A Proposed Framework," Electronics (Switzerland), vol. 13, no. 5, Mar. 2024, doi: 10.3390/electronics13050865.

[17]. R. Barik and A. K. Pradhan, "DOES FINANCIAL INCLUSION AFFECT FINANCIAL STABILITY: EVIDENCE FROM BRICS NATIONS?," 2021.

[18]. P. Chowdhary, M. Pandey, P. Singh, P. K. Sharma, and A. Shukla, "Factors Affecting Impact Investment among Generation Z: The Moderating Role of Behavioral Biases," International Review of Management and

Marketing , vol. 15, no. 3, pp. 438–449, Apr. 2025, doi: 10.32479/irmm.17547.

[19]. Williams Haruna, Toyin Ajiboro Aremu, and Ajao Yetunde Modupe, "DEFENDING AGAINST CYBERSECURITY THREATS TO THE PAYMENTS AND BANKING SYSTEM," 2022. doi: https://doi.org/10.48550/arXiv.2212.12307.

[20]. A. Chakraborty and S. Tiwari, "An analytical study on challenges and gaps in India's cyber security framework," International Journal of Criminal, Common and Statutory Law, vol. 5, no. 1, pp. 04–07, Jan. 2025, doi: 10.22271/27899497.2025.v5.i1a.110.

[21]. S. AlBenJasim, T. Dargahi, H. Takruri, and R. Al-Zaidi, "FinTech Cybersecurity Challenges and Regulations: Bahrain Case Study," 2023, Taylor and Francis Ltd.doi: 10.1080/08874417.2023.2251455.

[22]. Uchenna Joseph Umoga, Enoch Oluwademilade Sodiya, Olukunle Oladipupo Amoo, and AkohAtadoga, "A critical review of emerging cybersecurity threats in financial technologies," International Journal of Science and Research Archive, vol. 11, no. 1, pp. 1810–1817, Feb. 2024, doi: 10.30574/ijsra.2024.11.1.0284.

[23]. T. Hasani, N. O'Reilly, A. Dehghantanha, D. Rezania, and N. Levallet, "Evaluating the adoption of cybersecurity and its influence on organizational performance," SN Business & Economics, vol. 3, no. 5, Apr. 2023, doi: 10.1007/s43546-023-00477-6.

[24]. M. El Khatib, H. Al Shehhi, and M. Al Nuaimi, "How Big Data and Big Data Analytics Mediate Organizational Risk Management," Journal of Financial Risk Management, vol. 12, no. 01, pp. 1–14, 2023, doi: 10.4236/jfrm.2023.121001.

[25]. Rafiul Azim Jowarder, "Navigating digital transformation in financial services: Strategic management: concepts and cases for sustainable growth and innovation," World Journal of Advanced Engineering Technology and Sciences, vol. 13, no. 1, pp. 319–329, Sep. 2024, doi: 10.30574/wjaets.2024.13.1.0420.

[26]. Olorunyomi Stephen Joel, Adedoyin Tolulope Oyewole, Olusegun Gbenga Odunaiya, and Oluwatobi Timothy Soyombo, "The impact of digital transformation on business development strategies: Trends, challenges, and opportunities analyzed," World Journal of Advanced Research and Reviews, vol. 21, no. 3, pp. 617–624, Mar. 2024, doi: 10.30574/wjarr.2024.21.3.0706.

[27]. P. Kumar Joshi, "Azure Functions in Payment Gateways: A Serverless Approach to Financial Systems," Journal of Artificial Intelligence & Cloud Computing, vol. 2, no. 1, pp. 1–9, Mar. 2023, doi: 10.47363/JAICC/2023(2)390.

[28]. M. Alhamed and M. M. H. Rahman, "A Systematic Literature Review on Penetration Testing in Networks: Future Research Directions," Jun. 01, 2023, MDPI. doi: 10.3390/app13126986.

[29]. A. C. Moreno et al., "Analysis of Autonomous Penetration Testing Through Reinforcement Learning and Recommender Systems," Sensors, vol. 25, no. 1, Jan. 2025, doi: 10.3390/s25010211.