| e-ISSN: 2948-460X | https://ibaf.usim.edu.my

AUDITING INCIDENT RESPONSE AND DISASTER RECOVERY PLANS IN THE EVENT OF A MASS DATA BREACH OF EPF-I IDENTIFICATION DATA

Aufa Nabila Binti Muhamad Sukri[1,a*], Nuratul Anis Binti Ahmad Shapiki[2,b], Mohamad Khairol Aqil Bin Ahmad[3,c] and Zurina Binti Shafii[4,d]

[1]*Faculty Economics and Muamalat, Universiti Sains Islam Malaysia, Nilai, Negeri Sembilan, Malaysia*
[2] *Faculty Economics and Muamalat, Universiti Sains Islam Malaysia, Nilai, Negeri Sembilan, Malaysia*
[3] *Faculty Economics and Muamalat, Universiti Sains Islam Malaysia, Nilai, Negeri Sembilan, Malaysia*
[a]*3251861@raudah.usim.edu.my*
[b]*3251927@ raudah.usim.edu.my*
[c]*3252036@ raudah.usim.edu.my*
[d]*zurina.shafii@usim.edu.my*

*Corresponding Author: *3251927@ raudah.usim.edu.my*

Abstract**:** *Over the last 15 years, Islamic financial institutions in Malaysia have changed a lot due to new technology and digitalization. While this brings many benefits to EPF-i members, it also creates new risks. One of the biggest problems today is cybersecurity, specifically large-scale data breaches and identity theft caused by phishing links. This study evaluates the operational effectiveness of EPF-i's Incident Response Plan (IRP) and Disaster Recovery Plan (DRP) from an Information Systems Audit perspective. The research uses a conceptual design, mapping institutional resilience against the ISO 22301:2019 standard, COBIT 2019, and COSO 2017 ERM frameworks, while integrating the Islamic principle of Hifz al-Mal (preservation of wealth). Critical audit evaluations reveal that EPF-i's current plans are partially effective due to significant weaknesses in the system and only respond to threats after they happen, instead of catching or preventing them. The main findings highlight a lack of real time automated fraud controls and practicing for the wrong emergency scenario, where recovery protocols prioritize physical infrastructure over protecting critical identity registries. This creates a paper compliance risk where untested plans may accidentally restore polluted data during an identity crisis. To build better resilience, the study recommends three main actions, the adoption of specialized mass-credential playbooks, automated transaction holds, and mandatory identity revalidation procedures. Finally, sustained board oversight and executive commitment are essential to maintain public trust and protecting the retirement savings of millions.*

Keywords: Employees Provident Fund (EPF); Data Breach; Information Systems Audit; Incident Response; Disaster Recovery.

1. Introduction

Digitalisation of financial services has transformed the way institutions handle and secure client information. In Malaysia, the Employees Provident Fund (EPF) or KWSP has digital portals such as i-Akaun to provide members with faster access to information about their

accounts, donations, withdrawals and personal profiles. These services may increase efficiency and accessibility but may also increase cybersecurity threats such as phishing scams, identity theft, unauthorised access and data breaches.

While digital services improve operational efficiency and accessibility, they also increase the susceptibility of institutions and users to cyber security risks such as phishing, identity theft, fraudulent websites and unauthorised access. Official warning against messages, social-media interactions and websites impersonating the EPF to obtain members' personal and financial information (Employees Provident Fund [EPF], 2024a). This risk is also present in the Malaysian cybersecurity landscape. CyberSecurity Malaysia (2025) recorded 810 phishing cases out of a total of 1,108 fraud cases in the fourth quarter of 2024.

EPF-i members are very critical of the protection of personal and financial information, as the data comprises sensitive identification information such as name, identification number, contact information, account details, employment records and withdrawal information. "But if the information is leaked or misused, it will cause members to suffer financial loss, identity theft, unauthorised access to their account and loss of confidence towards KWSP as a retirement savings institution.

This is a crucial issue from the standpoint of an audit information system, as auditors are required to assess whether the company has appropriate controls in place to prevent, detect, respond and recover from cyber incidents. In case of a mass data breach of the EPF-i identity data, the incident response strategy and the disaster recovery plan should be assessed for effectiveness. A good incident response strategy means the organisation can respond swiftly to the scam, and a disaster recovery plan means vital systems, data and digital services can be restored if they are affected.

The motivation for this study is the growing scale of phishing and data security incidents in Malaysia and the significance of EPF as the custodian of members' retirement funds. A security breach at iPay88, a Malaysian payment-gateway provider, demonstrated the impact that financial data compromises can have on many organisations and customers. Following the incident, Bank Negara Malaysia directed the company to strengthen its security protocols (Bank Negara Malaysia, 2022). Official scam alerts on phishing messages, websites and impersonation activities in EPF context show members are still exposed to credential-theft, but do not confirm that EPF's internal systems have been infiltrated (EPF, 2024a).

Existing discussions of disaster recovery frequently emphasise infrastructure failure, system downtime and data restoration. However, a phishing-driven incident may occur while the EPF's core systems remain operational, even though the reliability of member credentials, profile information and withdrawal instructions has been compromised. Therefore, there is a need to examine whether incident response and disaster recovery arrangements can address an identity-integrity crisis rather than only a conventional system-availability disruption.

This study is significant because it extends the evaluation of business continuity beyond the restoration of information systems to include the restoration of trusted member identities and financial records. From an information systems audit perspective, the study identifies the evidence required to assess whether incident response and disaster recovery controls operate effectively during a mass credential-compromise event. Practically, the findings provide recommendations for strengthening EPF-i's detection, containment, identity revalidation and recovery processes. The study also contributes a Shariah perspective by explaining how effective cybersecurity controls support hifz al-mal, or the preservation of wealth, and maintain public trust in the management of Shariah-compliant retirement savings.

2. Scenario: Scam Alert EPF

Stage	Scam activity	Control weakness being examined	Potential impact
Reconnaissance	Scammer collects member information	Excessive public exposure or previous leaked data	More convincing targeted messages
Delivery	Fake SMS, WhatsApp message, email or social-media advertisement	Weak domain monitoring and delayed warnings	Members directed to fake websites
Credential harvesting	Fake portal collects username, password and TAC	Low member awareness and convincing interface imitation	Account takeover
Account access	Attecker logs in using stolen credentials	Insufficient risk-based authentication	Unauthorised access
Profile manipulation	Contact or bank details are changed	Inadequate cooling-off or confirmation controls	Fraudulent profile becomes accepted record
Transaction attempt	Withdrawal request is submitted	Absence or failure of transaction-risk controls	Financial loss
Recovery	Accounts or database is restored	Failure to verify restored identity fields	Corrupted information becomes the recovery baseline

Figure 1. Expand and critically analyse the scam scenario

The following scenario is hypothetical and was developed based on documented EPF scam warnings and phishing trends reported in Malaysia. It is not presented as evidence that EPF's internal information systems or databases have experienced a mass data breach. EPF has warned its members that fraudulent messages sent through social media, SMS or WhatsApp may impersonate the institution and direct members to websites designed to obtain personal or account information (EPF, 2024a).

This hypothetical scenario involves a coordinated phishing campaign targeting EPF members, particularly members who access their accounts through the i-Akaun platform. The scam begins when fraudsters send fake messages via SMS, WhatsApp, email, Telegram or social media. "The mail could be from EPF and may request members to verify their account, update their personal details, apply for withdrawal or avoid account suspension. "The message contains a link that appears to be the official EPF website but is a fake website operated by scammers.

The scam's success may be facilitated by a variety of factors. Initially, the fraudulent website may closely mimic the colours, logos, and layout of the official EPF website, thereby complicating the identification of the deception for members. Second, fraudsters may incite urgency by asserting that the member's account will be suspended or that immediate verification is necessary. Third, the message may be personalised and appear to be legitimate

by utilising personal information that has been previously disclosed. The probability of account compromise may be further heightened by the disclosure of transaction authentication codes, weak password practices, and limited awareness.

The attack may progress from credential harvesting to account takeover. After obtaining a username and password, the attacker may attempt to access the member's account, change registered contact or bank information and submit an unauthorised transaction. Therefore, the incident is not limited to the disclosure of personal data; it may also compromise the integrity of member profiles and transaction instructions.

Upon clicking the link, members will be routed to a bogus website that mimics an official EPF page. The website may request sensitive information such as complete name, MyKad number, phone number, email address, EPF member number, i-Akaun username and password, bank account number and one-time password. Some members believe the website is real and enters their personal data.

The scam gets serious when a lot of EPF-i members give their details on the phoney website. The data could be exploited for identity theft, unauthorised log-in attempts, false withdrawal applications, impersonation or other scam activities. Even though the incident does not involve hacking of the EPF's internal system directly, it has nevertheless created a major data breach risk as the members' identification data has been exposed to unauthorised people.

From an auditing point of view, various hazards are created in this situation. First, it is a confidentiality issue, because the scammers now have personal data. Second, there is an integrity risk if attackers try to update member details or withdrawal information. Third, there is availability risk if EPF must temporarily restrict online services or enhance human verification to protect affected members. The incident might also damage EPF's reputation, as members anticipate the institution safeguarding their retirement assets and personal data.

The magnitude of the incident would depend on the number of affected members, the sensitivity of the information disclosed, the duration of the phishing campaign and the value of attempted or completed unauthorised transactions. Other indicators include the number of compromised accounts, fraudulent profile amendments, identity-revalidation cases, member complaints and the period required to contain the incident. A large-scale campaign could also increase investigation and remediation costs, disrupt online services and reduce public confidence in EPF.

The impact may extend beyond immediate financial loss. Compromised identification information can be reused to impersonate members in other transactions, while fraudulent changes to contact or banking information may remain undetected after the initial incident. Consequently, recovery must address the accuracy of member identities and account records rather than merely restoring system availability.

EPF should promptly notify members via official channels, report or block fraudulent links, request the removal of fake websites, monitor suspicious account activities, and provide support to affected members in securing their accounts. In addition, EPF needs to find out if the event is purely external phishing or if some internal system, third-party service or database has been compromised. If there is a system interruption or data integrity problem, the disaster recovery plan will be invoked to secure member data and resume service.

This example illustrates the importance of having a catastrophic recovery strategy and a good incident response plan. It should not rely entirely on its members to uncover fraud. In addition, strong monitoring, reporting, communication, recovery, and post-incident assessment protocols are crucial. From the audit information system perspective, the key issue is whether EPF-i has sufficient controls to limit the impact of the breach, to handle the fraud occurrence and to maintain the confidence of its members.

3. Methodology

This study adopted a qualitative document analysis and scenario-based control-gap assessment. Publicly available documents concerning EPF's risk management, cybersecurity, business continuity and scam-prevention measures were examined. The documents included the EPF Integrated Annual Report, official EPF scam alerts, CyberSecurity Malaysia incident statistics, relevant Malaysian regulatory publications, ISO 22301:2019, COBIT 2019, COSO ERM and selected academic studies on incident response, disaster recovery and Maqasid al-Shariah.

Documents were selected based on four criteria: relevance to incident response or disaster recovery, applicability to financial or pension institutions, publication by an authoritative organisation or peer-reviewed source, and availability within the study period. The documents were coded according to five incident-management stages: preparation, detection, containment, recovery, and post-incident improvement.

The disclosed EPF controls were then compared with selected COBIT governance objectives, COSO ERM components, and ISO 22301 continuity principles. Each control was classified as publicly evidenced, partially evidenced or not demonstrable from public information. A hypothetical mass phishing and credential-compromise scenario was used to assess potential control gaps relating to identity integrity, transaction containment, communication, and recovery.

The study did not involve access to confidential EPF policies, system logs, personnel interviews, or live control testing. Therefore, the findings evaluate the sufficiency of publicly available evidence and should not be interpreted as a definitive assurance opinion on EPF's internal control effectiveness.

4. Auditing Perspective

This section evaluates the effectiveness of the Incident Response Plan (IRP) and Disaster Recovery Plan (DRP) implemented by EPF-i. The evaluation is based on the Risk Management Statement disclosed in the EPF-i Annual Report. To strengthen organisational resilience against disruptions such as data breaches, cyberattacks, and other operational incidents, EPF-i has established a Business Continuity Management (BCM) Framework. The framework is developed based on the adoption of the ISO 22301:2019 standard. Within this BCM Framework, both the Incident Management Plan (IMP or IRP), and the IT Disaster Recovery Plan or DRP are key components that support business continuity and recovery. **Figure 2** illustrates the Business Continuity Management (BCM) Framework adopted by EPF-i.

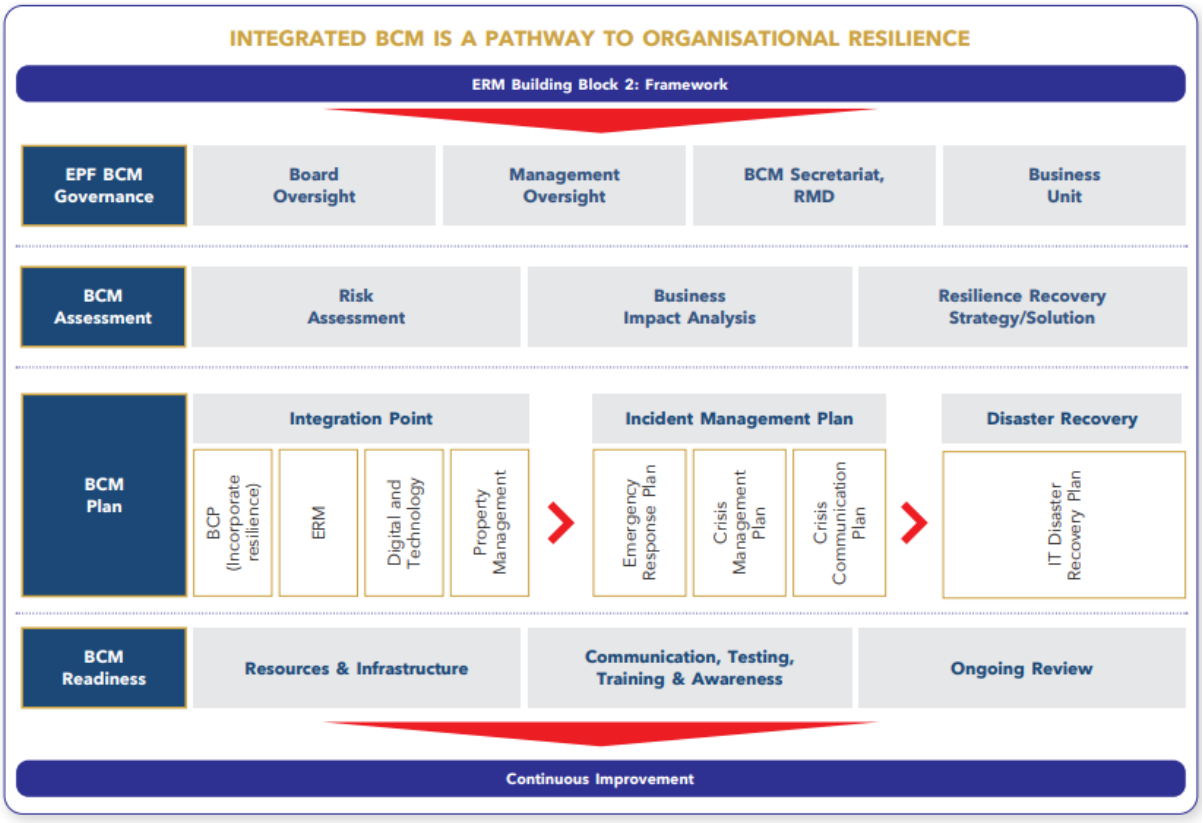


Figure 2

Entrusted with the financial security of 16.22 million members, the Employees Provident Fund (EPF), locally known as Kumpulan Wang Simpanan Pekerja (KWSP) acts as a systemic custodian of massive volumes of citizen wealth and sensitive personally identifiable information (PII) (Employees Provident Fund, 2024). Given its status as a critical national infrastructure entity, the risk management frameworks and strong EPF's governance are central to maintaining public confidence and national economic stability.

As detailed in the Integrated Annual Report 2024, the EPF's strategic outlook is guided by the "ACE-YT" focus areas, there are Adequacy, Coverage, Experience, Yield, and Trust. The "Trust" pillar is especially important and requires the fund to act of integrity and transparency to deliver on its fiduciary mandates. To deal with growing cyber threats, the organization has refreshed its "Digitise EPF 2025" roadmap (Employees Provident Fund, 2024), a robust strategic designed to make the operations more efficient while simultaneously strengthening cybersecurity defences. The Fund's public promises regarding risk governance are operationalized through its ongoing five-year Digital Security Programme (2022–2026) (Employees Provident Fund, 2024). And through the program, it adopts a Zero Trust framework to safeguard digital assets and ensure continuous operational continuity. Lastly, this posture is further supported by a Three Lines Model of Governance. Which under this model, where everyday business units, risk management functions, and internal audits provide multi layered protection against operational and technology risks.

A fundamental principle of the Employees Provident Fund's (EPF) resilience strategy is its alignment with International Organization for Standardization (ISO) 22301, the globally recognized benchmark for Business Continuity Management Systems (BCMS) (Employees Provident Fund, 2024). According to SIRIM QAS International (n.d.), International Organization for Standardization (ISO) 22301 compliance is a vital indicator of an

organization's institutional preparedness, providing a structured framework to protect, prepare, respond, and recover operations when unexpected disruptions or disasters occur. And in the Malaysian corporate landscape, this certification or standard shows that an institution has clearly defined roles and responsibilities based on international best practices, allowing for the institutions or entities to quickly restore important business operations (SIRIM QAS International, n.d.). So, by compliance these rules, the Employees Provident Fund (EPF) proves its commitment to building a "culture of preparedness". Which ensuring that its recovery strategies are meet with global benchmarks and that the institution proved has the proven strength for structured recovery and long-term organizational resilience.

According to Greenwood et al. (2025), Business Continuity Management (BCM) is not simply an emergency-only checklist, rather, it is a strategic system designed to ensure that mission-critical operations continue "no matter what" in an increasingly volatile and interconnected risk landscape. For the Employees Provident Fund (EPF), this resilience must be operationalized through a "Continuity Governance" (CG) model. As proposed by Loyarte et al. (2024), CG introduces a new stage in the BCM system where considerations of resilience are deeply embedded into the organization's daily, routine operational decisions and management practices. This shift ensures that Business Continuity Management (BCM) and International Organization for Standardization (ISO) 22301 compliance are not just left to the IT department. So, instead of just updating a recovery manual once a year, then left it on a shelf, the managers will use safety data every day to make better business decisions and spot risks early.

Furthermore, these operational and resilience standards can be viewed through the lens of Islamic jurisprudence, specifically the Maqasid al-Sharia (the ultimate goals of Islamic Law). Protecting the EPF's massive asset, particularly the RM167.41 billion allocated to its Simpanan Shariah portfolio, it serves as a modern way of *Hifz al-Mal* (the preservation and protection of wealth) (Al Hadana et al., 2025). With the growth of digital era or technology, this means the fund's duty is not just to grow these investments, but also to actively protect them from cybercriminals. Failing to secure these digital assets is a direct threat to the financial well-being and future security of millions of Muslim savers. In this framework, Al Hadana et al. (2025) argue that cybersecurity and resilience are instruments to protect fundamental interests such as life, intellect, property, and social order. Because of this, a failure to protect customer identification data and digital wealth is often understood or seen as a failure of the state's duty to protect the collective wealth of its citizens, damaging the trust that is essential for a stable digital economy.

4.1 Incident Response Plan

When evaluating the operational resilience of a systemic financial entity like the Employees Provident Fund (EPF), the internal auditor will act as the third line of defense. They must move beyond high-level governance reviews to granular, evidence-based validations of technical controls (Ferreira et al., 2025). According to Ferreira et al. (2025), for an IRP to be judged effectively in a modern financial environment, the auditor must verify two distinct perspectives: how well the strategy is organized, and how well the system performs in real life. A very important standard for the EPF-i (Simpanan Shariah) plan is the use of a Zero Trust Security Model (Employees Provident Fund, 2024). Which requires the auditor to test the efficacy of continuous real-time monitoring tools such as User and Entity Behavior Analytics (UEBA) and Security Information and Event Management (SIEM) systems (Ferreira et al., 2025), to ensure they can detect the threats as early as impossible. Effectiveness is further

demonstrated and proven through the auditor's evaluation of Red Team practices and automated penetration testing (PenTesting) (Ferreira et al., 2025), which challenges the IRP by practice responding to a major data theft incident to identify undetected security weaknesses before actual hackers can exploit them.

Furthermore, an effective audit of the Incident Response Plan (IRP) relies on the quantification of recovery performance through strict technical metrics. Relying on the information assurance frameworks established by Osman and Rahman (2024), auditors must measure the Mean Time to Detect (MTTD) to evaluate the sensory capabilities of the organizational infrastructure. In the specific event of a mass Personally Identifiable Information (PII) or personal data breach, the auditor must look closely at the Mean Time to Containment (MTTC) and Mean Time to Response to judge the efficiency of automated or manual team actions (Osman & Rahman, 2024). This comparison reveals whether manual teams are slowing down the response, or if automated systems are successfully stopping the breach before human intervention is even needed. In fact, Mathematical modelling of the spread of cybersecurity incidents suggests that organizations utilizing structured frameworks with automated recovery mechanisms can achieve a 67% faster mean time to recovery compared to those relying on traditional manual methods (Osman & Rahman, 2024). In real situations, cutting recovery time by more than half means a major attack that would normally stop the fund's operations for days can now be quickly brought under control and fixed in just a few hours. Therefore, an effective response plan must include smart resource models that automatically adjust response strategies based on how serious the data theft was and how it spread through the organization's systems.

4.2 Disaster Recovery Plan (DRP)

Within the implementation of ISO 22301:2019, a widespread vulnerability exists where organizations fall victim to the trap of paper compliance. And which means Disaster Recovery (DR) plans that are well designed but operationally not tested (Greenwood et al., 2025). This creates a false sense of security. The executives will assume the organization is secure just because they have checked all the audit boxes, even though the teams have never actually practiced how to handle the real incident or crisis. Historically, DR testing has focused only on predictable incident or disruptions (Greenwood et al., 2025). Such as localized hardware failures or power outages, which fail to capture the complexity of modern systemic risks that can affect multiple interconnected systems at the same time. According to Covarrubias (2025), in the context of a critical national pension fund, a truly effective Disaster Recovery (DR) plan must move beyond these simplified assumptions to be proven against highly realistic, malicious cyberattack incident scenarios, including stolen login credentials, massive identity theft, and the active theft of sensitive member data. Usually, static testing protocols ignore the "ripple effects" and failure in one system can quickly spread to others that occur when a cyber incident damages not only data, but the integrity of the recovery process itself (Greenwood et al., 2025). Hackers rarely stop at the main database. They usually actively search for and lock up the backup files first. So, when IT team goes to restore the systems, they find their safety nets have already been destroyed.

Next, the most dangerous moment in disaster recovery is the switch itself (SIRIM QAS International, n.d.). Which during this transition phase, firewalls, identity access controls, and active monitoring tools are often briefly running in a reduced performance or limited functionality and making it much easier for the hackers to exploit and gain deeper access. According to Greenwood et al. (2025), in the urgent effort to meet Recovery Time Objectives

(RTO) and minimize downtime, organizations frequently encounter "failover friction," leading to the intentional relaxation or bypassing of access controls to expedite data restoration. Which means the organization skips or ignores security controls just to make the restoration faster. By turning off strict authentication or skipping security checks just to bring systems back online faster, the organization accidentally leaves the digital front door wide open for the same attackers to return and cause even further damage. Fitriani et al. (2023) also mentioned that this chaotic transition creates significant secondary security vulnerabilities, as the removal of restrictive layers often viewed as operational bottlenecks, which provides an unintended window for lateral movement by threat actors. Therefore, strict identity verification and access control measures must be actively maintained during the recovery state to prevent "breach contamination" (Employees Provident Fund, 2025). This prevents hackers from hijacking the newly restored backup environment and ensures that compromised login credentials or malicious administrative accounts used during the initial attack cannot be used again to launch a second attack.

5. Auditing Evaluation (COSO / COBIT)

This section evaluates the true operational limits of the Employees Provident Fund's (EPF-i) resilience plans. Standard compliance checks often report flawless results if internal networks are not directly hacked. However, this analysis challenges that passive assumption by focusing on the real culprit: decentralized phishing networks that harvest user credentials completely outside the fund's firewall. By executing an effectiveness-based audit model through a dual lens of COBIT 2019 and the COSO 2017 ERM Framework, this section exposes critical structural gaps in EPF-i's Incident Response Plan (IRP) and Disaster Recovery Plan (DRP) when the human layer is weaponized. The COSO ERM Framework critiques how upper management governs systemic information flow and its ultimate failure or success in preserving Shariah fiduciary duties during an identity crisis. Concurrently, the COBIT 2019 Framework evaluates the technical maturity of operational IT handoffs, revealing why compliance metrics do not automatically guarantee threat containment.

The audit evaluation of EPF's immediate response should be based on evidence demonstrating how the incident was detected, classified, escalated and contained. For detection, the auditor should examine security alerts, member complaints, threat intelligence notifications, and the time taken to identify the fraudulent infrastructure. The auditor should then determine whether the incident was assigned to an appropriate severity level and escalated to the responsible operational, risk, legal, and communication functions.

For containment, the auditor should inspect evidence of fraudulent domain blocking, affected account restrictions, transaction hold, credential resets, and enhanced authentication. Communication records should also be examined to determine whether affected members and relevant authorities were informed accurately and within an appropriate period. Where third-party service providers were involved, the auditor should review the coordination, reporting and accountability arrangements between EPF and those providers.

The recovery evaluation should include identity revalidation records, transaction reconciliation, restored data integrity tests, and approval for account reactivation. Relevant audit measures may include Mean Time to Detect (MTTD), Mean Time to Contain (MTTC), the percentage of affected accounts quarantined, the percentage of suspicious transactions prevented, and the percentage of affected identities successfully revalidated. These procedures would allow the auditor to determine whether the plans operated effectively rather than merely confirming that the plans existed.

5.1 Incident Response Plan (IRP)

An effective Incident Response Plan (IRP) within a sovereign digital financial portal must possess high-capacity capabilities to detect, contain, and communicate external security incidents before they cascade into widespread identity theft and unauthorized withdrawals.

5.2 Framework Mapping and Structural Control Gaps (IRP)

The structural evaluation of the fund's operational resilience begins with the synchronization of specialized governance parameters under the COBIT 2019 and COSO 2017 Enterprise Risk Management (ERM) frameworks. Within the technical operations domain, the mapping of COBIT 2019 Core Domains, specifically DSS02 (Manage Service Requests and Incidents) and DSS03 (Manage Problems) establishes the analytical baseline required to evaluate the performance of the Computer Security Incident Response Team (CSIRT) and the Digital Risk Working Committee (DRWC). This structural mapping dictates that an effective incident response ecosystem must proactively ingest external threat intelligence to intercept systemic perimeter liabilities and minimize the institutional risk posture before external threats materialize. Concurrently, this operational framework intersects with the COSO ERM component of Information, Communication, and Reporting, which measures the design structure and transfer velocity of threat data distribution channels during volatile risk windows. This integrated evaluation model serves to critique the fund's systemic capacity to issue high-visibility, adaptive controls capable of neutralizing downstream fraud vectors before they impact the end-user registry.

Through this framework alignment, a clear control gap emerges regarding proactive detection architectures under COBIT DSS02, characterized by a persistent reliance on a reactive, user-reported threat detection loop. While optimal financial infrastructures require automated telemetry networks to optimize the Mean Time to Detect (MTTD), the practical execution of the response plan fails to deploy continuous, external threat-hunting mechanisms capable of actively identifying and taking down duplicate *i-Akaun* phishing infrastructures. This control latency creates a critical visibility window that allows decentralized threat networks to collect member credentials without immediate detection, directly challenging the fund's strategic KPI of sustaining an 83%+ Stakeholder Trust Score under the established ACE-YT roadmap.

Furthermore, evaluating these operational barriers through the COSO Information and Communication baseline highlights severe communication latencies and transactional containment gaps across the digital ecosystem. Contemporary research consistently identifies the decentralized human layer as the primary exploit vector in modern financial technology networks (Zainal & Sulaiman, 2025). While corporate metrics highlight periodic broad warning distributions by the Integrity & Governance Department, the manual dissemination model for these alerts lacks the speed necessary to match the rapid launch velocity of modern phishing links.

This risk grew significantly after May 2024 Account Restructuring. The launch of *Akaun Fleksibel* caused an unprecedented 874% spike in digital withdrawals, with 89% of these requests processed through the *i-Akaun* portal. This massive surge in online traffic created a perfect opportunity for hackers to launch phishing attacks.

However, the fund's active IRP is only Partially Effective because its technical workflows lack automatic safety controls. The system cannot automatically freeze a transaction in real

time even when it detects major red flags like failed e-KYC facial recognition or multiple logins from different locations at the same time. Without these automated ‘brakes’, scammers can easily steal members' money before human security teams can react.

5.3 Disaster Recovery Plan (DRP)

While a traditional compliance audit evaluates a DRP based on infrastructural availability during physical failures, an effectiveness-based information system audit prioritizes the DRP's capacity. Main reason is to maintain data integrity, systemic availability, and rigid access controls during a mass identity compromise.

5.4 Framework Mapping and Structural Control Gaps

The configuration of organizational recovery capabilities is systematically analysed by cross-mapping technical operation controls under the COBIT 2019 framework against the administrative control metrics of the COSO 2017 Enterprise Risk Management (ERM) architecture. Within this structural evaluation, COBIT 2019 Core Domain DSS04 (Manage Continuity) functions as the definitive technical baseline. It is to evaluate whether the institution's Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) remain resilient during a total compromise of user authentication mechanisms, moving beyond simple infrastructure or hardware availability metrics. This technical layer operates in tandem with the COSO ERM components of Control Activities and Monitoring Activities, which serve to audit the enforcement of internal identity policies, the preservation of administrative control boundaries, and the structural verification of the backup architecture during critical failover events. By deploying this integrated framework lens, the audit shifts away from basic availability checklists. It is to critique the fund's systemic capacity to safeguard both long-term financial data integrity and its overarching Shariah governance mandates during severe identity compromise.

A rigorous critique of this operational framework reveals a critical scenario-drill mismatch within the validation protocols under COSO Monitoring Activities. Historically, the disaster recovery simulations supervised by the Board Risk Management and Sustainability Committee (BRMSC) under EPF are heavily optimized to withstand localized physical disruptions, such as hardware center downtime, power grid drops, and database storage corruption. The recovery architecture conceptually lacks comprehensive playbooks designed for a cyber-crisis where the physical infrastructure remains fully available, yet the validity of the member identity registry has collapsed. When decentralized threat networks execute mass credential exploitation, the recovery workforce is left without automated, pre-tested operational scripts to systematically manage large-scale identity validation and account restoration.

This lack of specialized scenario playbooks introduces severe down-line risks regarding financed data pollution under COBIT DSS04. Even though EPF has high-security backups that are safe from hackers, their Disaster Recovery Plan (DRP) has one major flaw; there is no automatic system to verify data accuracy. If a scammer changes a member's profile information (like their bank account number) just before the account gets blocked, the recovery system might copy that fake info as the 'correct' update. As a result, the system ends up restoring polluted data without anyone realizing it. If an unauthorized actor changes a member's banking details or contact information right before defensive isolation is triggered, standard data restoration risks locking in the fraudulent state as the valid baseline. Furthermore, a severe control vulnerability is identified under COSO Control Activities regarding emergency

privileged access governance. To achieve low RTO metrics during high-pressure system recoveries, active emergency playbooks allow technical response teams to temporarily bypass multi-factor authentication (MFA) or assume broad administrative rights. This operational compromise introduces dangerous insider threat exposure during the institution's most vulnerable recovery window, directly challenging the strict mandates established under the Risk Management in Technology (RMiT) framework.

The severe risk of maintaining loose incident frameworks or compromising access controls under pressure is validated by Bank Negara Malaysia's (BNM) regulatory actions. In early 2026, BNM levied a historic RM1,000,000 administrative monetary penalty against Bank Kerjasama Rakyat Malaysia Berhad (BKRM) specifically due to systemic deficiencies in customer information protection and incident response capabilities following a major siber exploit. This precedent underscores that Malaysian regulators strictly penalize structural failures under RMiT mandates. For EPF-i, this conceptual failure directly compromises the Shariah Governance Framework (SGF), as a failure to systematically protect retirement assets from illicit extraction represents a direct breach of the fiduciary duty to safeguard wealth (*Hifz al-Mal*) under *Maqasid al-Shariah*.

5.5 Maqasid al-Shariah Evaluation

The effectiveness of EPF-i's incident response and disaster recovery arrangements should also be evaluated through the objectives of Maqasid al-Shariah. The most directly relevant objective is hifz al-mal, or the preservation of wealth. In the context of EPF-i, this objective requires more than the long-term investment and growth of members' retirement savings. It also requires preventive, detective and corrective controls that protect those savings from unauthorised access, fraudulent withdrawals and inaccurate account information.

The principle of amanah, or trusteeship, is also relevant because EPF is entrusted with members' financial assets and sensitive identification information. Effective governance, timely communication, transparent remediation and accountable decision-making demonstrate the fulfilment of this responsibility. Conversely, failure to prepare for a foreseeable cyber incident may weaken the institutional trust placed in EPF-i.

Protection of personal and identification information also supports the preservation of dignity and privacy. Identity theft may expose affected members to financial and non-financial harm beyond the immediate EPF account. Therefore, incident response should contain both the immediate threat and the possibility that compromised information will be reused for further fraudulent activities.

The principle of preventing harm requires EPF-i to respond before compromised credentials result in irreversible loss. Controls such as risk-based transaction holds, step-up authentication and account quarantine are therefore consistent with Maqasid al-Shariah because they prioritise the prevention of financial harm. Similarly, identity revalidation and record reconciliation promote justice by ensuring that affected members' information and financial rights are restored accurately.

From the perspective of maslahah, or public interest, effective incident response also preserves confidence in Malaysia's retirement and Islamic financial systems. A recovery process cannot be regarded as successful merely because the digital platform becomes operational again. Recovery is consistent with Maqasid al-Shariah only when member identities, access rights, financial records and retirement savings have been restored accurately, securely and fairly.

5.6 Audit Findings

The framework analysis indicates that EPF's publicly disclosed governance, digital security and business continuity arrangements provide an important foundation for institutional resilience. Nevertheless, the existence of a framework does not automatically demonstrate that its controls operate effectively during a mass credential-compromise event. Operating effectiveness must be supported by system-generated evidence, incident records, simulation results, and independently reviewed performance measures.

The first finding concerns the readiness of the IRP for mass credential compromise. Although EPF provides scam warnings and reports on cybersecurity initiatives, publicly available information does not demonstrate whether a specialised response playbook has been tested for the simultaneous compromise of many member credentials. Without a scenario-specific playbook, responsibilities for account quarantine, credential reset, transaction suspension and member revalidation may not be performed consistently during a major incident.

The second finding concerns rapid containment. Public information does not provide sufficient evidence regarding the use and operating results of automated controls that respond to combinations of high-risk events, such as access from a new device, changes to banking information and a withdrawal request immediately following a credential reset. A delay in containment could allow compromised credentials to be converted into unauthorised profile changes or financial transactions before manual intervention occurs.

The third finding concerns the integrity of recovered information. A conventional DRP may successfully restore servers and databases but still restore unauthorised changes made before the incident was detected. If compromised contact or bank details are treated as valid recovery data, system availability may be restored without restoring the reliability of member information. Therefore, the DRP should include procedures for account quarantine, record reconciliation and independent identity revalidation.

These findings indicate that the main issue is not necessarily the absence of EPF controls. Rather, there is insufficient public evidence to determine whether the controls have been designed and tested for a mass identity-compromise scenario. The proposed framework addresses this issue by connecting COBIT incident and continuity objectives with COSO governance and monitoring requirements, thereby ensuring that detection, containment and recovery are evaluated as one continuous process.

6. Conclusion

Based on the audit evaluation, the Employees Provident Fund (EPF) has established a credible governance and resilience foundation for protecting its digital services and members' information. The EPF Integrated Annual Report 2024 discloses the use of a Zero Trust framework, a five-year Digital Security Programme, global threat-intelligence services, simulated social-engineering exercises, an ISO 22301:2019-aligned Business Continuity Management framework, an Incident Management Plan, and an IT Disaster Recovery Plan (Employees Provident Fund [EPF], 2025). These measures indicate that the design of the organisation's cybersecurity, incident-management, and continuity controls is broadly consistent with the governance expectations reflected in COSO and the service, incident, problem, and continuity objectives of COBIT 2019.

Nevertheless, the existence of policies, frameworks, and reported initiatives does not by itself establish operating effectiveness. From an information systems audit perspective,

effectiveness must be supported by evidence that controls function as intended during a realistic and high-pressure event. This is especially important in the scenario examined in this report because a mass phishing campaign may occur outside the EPF's internal network. The i-Akaun platform and core infrastructure could remain available while the confidentiality of member credentials and the integrity of member profiles, contact details, bank information, or withdrawal instructions are already compromised. Therefore, an availability-focused recovery test would not be sufficient to demonstrate that the organisation can safely restore trust in the affected identities and transactions.

The threat is not speculative; it's foreseeable. CyberSecurity Malaysia received 1,108 reports of fraud in the fourth quarter of 2024, of which 810 were phishing related. The research also mentioned personally identifiable information and account passwords as some of the categories of data implicated in reported breaches (CyberSecurity Malaysia, 2025). In these cases, the audit must determine not only the ability to restore systems, but also to detect fraudulent changes, isolate affected accounts, revalidate member identities, and reverse inaccurate transactions or profile changes without contaminating the recovered environment.
As such, this research indicates that the EPF Incident Response Plan and Disaster Recovery Plan are partially effective for the particular scenario of a mass phishing-driven breach of EPF-i identifying data. Plans seem reasonably mature in governance and control-design terms. However, public information does not provide sufficient audit evidence to validate that plans are fully effective in the areas of large-scale credential theft, rapid transaction containment, mass identity revalidation, recovery-data integrity, and coordinated member remediation. This assessment does not determine that the EPF has no cybersecurity controls. Rather, it reflects the audit premise that a control cannot be deemed totally effective until its operating performance has been demonstrated by tested documents, measurable results and independently examined evidence.

For EPF-i, this conclusion also has a Shariah governance dimension. The protection of members' retirement savings, identity information, and access rights forms part of the institution's fiduciary responsibility and supports the objective of safeguarding wealth, or hifz al-mal. A technically available platform cannot be considered successfully recovered if members' identities remain unreliable or their savings are exposed to unauthorised transactions. Consequently, the final measure of resilience should be the safe restoration of confidentiality, integrity, availability, accountability, and public trust.

While the study indicates that EPF's governance and continuity arrangements provide a credible foundation for cyber resilience, the principal limitation of relying on public disclosures is that they do not demonstrate the operating effectiveness of controls for mass credential-compromise events. In particular, the analysis of current resilience was problematic regarding external phishing detection, rapid transaction containment, and the integrity of restored member information. In order to address these evidence gaps, a credential-compromise playbook and automated risk-based holds were proposed to connect incident detection with containment and safe recovery. The benefit of this approach is that it provides a practical means of ensuring resilience through trusted-data reconciliation and scenario-specific exercises

7. Recommendations

First, in response to the first finding concerning the absence of publicly demonstrable scenario-specific procedures, EPF should develop a dedicated response playbook for a large-scale compromise of member credentials and identification data. The playbook should also include

criteria for incident severity and escalation thresholds, as well as decision authority and the roles of the Computer Security Incident Response Team, business units, legal and communications functions, third-party service providers, and senior management. Steps to preserve evidence, identify affected members, suspend high-risk activity, reset credentials, re-enroll authentication factors and validate the safety of accounts before restoring normal access should be included. This approach takes advantage of the recommendations found in NIST SP 800-61 Revision 3, which advocates for the integration of incident response activities into cybersecurity risk-management activities to improve preparation, detection, response, and recovery (Nelson et al., 2025).

In response to the second finding concerning rapid transaction containment, EPF should implement or strengthen risk-based controls for high-risk account events. The EPF should apply step-up verification, temporary transaction holds, and enhanced review when there is a combination of unusual indicators, such as a new device, abnormal location, rapid changes to contact or bank details, failed identity verification, repeated login attempts, or a withdrawal request immediately following a credential reset. Changes to key profile attributes should be subject to a cooling-off period and out-of-band confirmation through a previously verified channel. These controls should be carefully calibrated and monitored to prevent excessive false positives or unfair disruption to legitimate members, but the risk of limited inconvenience is preferable to an irreversible unauthorised withdrawal.

In response to the third finding concerning the integrity of recovered information, the DRP should incorporate procedures for restoring confidence in member identity data rather than merely restoring servers and applications. Affected accounts should be quarantined and classified according to the type of information exposed. The recovery team should compare critical profile fields and transactions against trusted historical checkpoints, immutable logs, and independently verified member information. Where a discrepancy is detected, the member's identity should be revalidated before account access or withdrawals are reactivated. The procedure should also include transaction reconciliation, reversal approval, member confirmation, and a documented chain of custody for all corrected records. Recovery should be declared complete only after the accuracy and legitimacy of restored data have been tested. Finally, in terms of implementation, to provide continuing evidence of operating effectiveness, EPF should conduct periodic mass credential-compromise exercises supported by measurable audit indicators and board-level monitoring. Short- to medium-term improvements include external phishing monitoring, identity-integrity recovery, privileged access control, and improved backup validation. Scenario exercises, audit metrics and Board oversight need to be ongoing. These recommendations would, together boost confidence that EPF-i can protect members' identification data and retirement savings, while maintaining operational resilience and institutional trust in the event of a major cyber incident.

References

Al Hadana, M. F., Haron, M. S., & Latif, F. A. (2025). Cyber-security through the lens of Maqasid al-Shariah: Protecting wealth and public trust in the digital economy. Journal of Islamic Financial Governance, 11(1), 45–62.

Athena, M. (2024, August 9). Don't be a victim of online theft. Employees Provident Fund. https://www.kwsp.gov.my/en/w/article/how-to-avoid-online-scam

Bank Negara Malaysia. (2026). Imposition of administrative monetary penalty on Bank Kerjasama Rakyat Malaysia Berhad for cybersecurity and customer information protection breaches.

Committee of Sponsoring Organizations of the Treadway Commission. (2013). Internal control—Integrated framework.

Committee of Sponsoring Organizations of the Treadway Commission. (2017). Enterprise risk management—Integrating with strategy and performance.

Covarrubias, G. E. (2025). Threat modeling for sovereign wealth and pension funds: Decentralized attacks on centralized registries. Cyber Resilience Review, 19(3), 204–219.

CyberSecurity Malaysia. (2024). Reported incidents based on general incident classification statistics 2024.

CyberSecurity Malaysia. (2026). Reported incidents based on general incident classification statistics 2024. https://www.cybersecurity.my/portal-main/statistics-details?id=21

Employees Provident Fund. (n.d.-a). KWSP i-Akaun app: Features and benefits.

Employees Provident Fund. (n.d.-b). Scams and alerts.

Employees Provident Fund. (2024a). 3 popular online scams to avoid in Malaysia.

Employees Provident Fund. (2024b). Strategy and business outlook 2024.

Employees Provident Fund. (2025a). i-Akaun Secure.

Employees Provident Fund. (2025b). Integrated annual report 2024.

Employees Provident Fund. (2026). Protecting our trust: Integrated annual report 2024.

Ferreira, L., Santos, M., & Silva, T. (2025). Internal audit function as the third line of defense: Moving from checklist compliance to effectiveness testing. International Journal of Accounting Information Systems, 48, 100–117.

Fitriani, R., Subagiyo, R., & Asiyah, B. N. (2023). Mitigating IT risk of Bank Syariah Indonesia: A study of cyber attack on May 8, 2023. Al-Amwal: Jurnal Ekonomi dan Perbankan Syariah, 15(1), 86–100.

Greenwood, R., Miles, J., & Thorne, P. (2025). Beyond paper compliance: Pressure testing ISO 22301 frameworks against modern cyber crises. Journal of Business Continuity & Emergency Planning, 18(4), 312–329.

ISACA. (2019). COBIT 2019 framework: Governance and management objectives.

Loyarte, E., Urizar, E., & Garay, J. (2024). Continuity governance: Integrating business impact analysis into daily strategic management. European Management Journal, 42(2), 277–291.

Osman, N., & Rahman, A. (2024). Mathematical modeling of cybersecurity sensory efficacy and mean time to containment (MTTC) in financial nodes. Malaysian Journal of Computer Science, 37(2), 89–106.

SIRIM QAS International. (n.d.). Business continuity management system: Protect your business during disruptions and build a culture of preparedness (ISO 22301).

Zainal, A., & Sulaiman, R. (2025). Between law and technology: A qualitative study of online scam challenges and legal responses in Malaysia. International Journal of Research and Innovation in Social Science, 9(9), 4013–4022.