OPEN ACCESS

International
Journal
Of Modern Engineering Research (IJMER)

Proactive Defense: IT Problem Management's Strategic Role in Enhancing Data Security for Saudi Digital Projects

Ramy Abdelmonem Matrawy

Abstract
Background: *As Saudi Arabia accelerates its entire national transformation under Vision 2030, the proliferation of mega digital projects and smart city plans has exponentially increased the number and value of the nation's data assets. This online expansion also increases the attack surface of sophisticated cyber threats, and data security is elevated to a national security and economic stability top concern. The conventional IT Incident Management model, designed for rapid service restoration, is not proving sufficient to address the root causes of security vulnerabilities.*
Objective: *The research supposes that the strategic shift from reactive Incident Management to proactive IT Problem Management is a critical and inevitable evolution in the Kingdom's data security ecosystem. This paper suggests a customized framework, the "Proactive Problem Management Framework for Data Security (PPM-DS)," for detecting, analyzing, and eradicating permanently the root causes of security incidents, thus enhancing the system's resilience.*
Methodology: *The study adopts a qualitative constructive research method. The study begins with an extensive literature review of IT Service Management (ITSM), data security paradigms, and Saudi Arabia's regulatory landscape. It then builds the PPM-DS framework. The applicability of the framework is demonstrated by undertaking an in-depth analysis of three representative case studies, which are archetypal scenarios derived from real-life problems in Saudi Arabia's FinTech, giga-project, and government digital services domains.*
Results: *Comparison reveals that traditional incident-based responses have a tendency to leave systemic vulnerabilities uncorrected, and therefore, security incidents repeat and escalate. In contrast, the application of the PPM-DS framework in the case studies demonstrates an easy method to unearth latent software bugs, flawed architectural designs, and inadequate security measures that are the true root causes of incidents. The framework not only addresses immediate problems but also builds a strong knowledge base for avoiding future occurrences throughout the whole digital ecosystem. Conclusion: The establishment of a formal IT Problem Management discipline is not merely an operational improvement but a strategic imperative for the secure and successful realization of Vision 2030. It provides the way to create a strong, self-improving security posture, increasing confidence for citizens, investors, and international partners, and safeguarding the Kingdom's digital future.*
Keywords: *IT Problem Management, Data Security, Cybersecurity, Saudi Vision 2030, ITIL, National Cybersecurity Authority (NCA), Digital Transformation, Root Cause Analysis (RCA).*

Date of Submission: 15-09-2025 Date of acceptance: 30-09-2025

I. Introduction

1.1. The Digital Imperative of Vision 2030

Saudi Arabia's Vision 2030 is a driver for one of the world's most ambitious social and economic reforms. A key pillar of this vision is an extensive digital transformation, with a vision to create a leading digital economy, a smart government, and an innovative, technology-enabled society. This has opened the doors to a wave of massive digital projects, stretching from NEOM's cognitive city and KAFD's financial hub to the nationwide rollout of 5G, IoT infrastructure, and a multitude of e-government services via platforms like Absher and Najiz. This rapid digitization is generating an unprecedented volume of data—stretching from citizen information to vital infrastructure operations and sensitive business intelligence. This data is now among the Kingdom's most valuable strategic assets.

1.2. The Evolving Threat Landscape

With such tremendous opportunity also comes attendant risk. The Kingdom's growing digital prominence and geopolitical significance render it a tempting target for a wide range of threat actors, ranging from nation-state actors to cybercriminals to hacktivists. The regional threat landscape is characterized by sophisticated Advanced Persistent Threats (APTs), an increase in devastating ransomware attacks, and supply chain vulnerabilities. Saudi Arabia is among the most targeted nations in the Middle East by cyberattacks, based on industry reports. The hyper-connectivity of new projects has the consequence that a weakness in one system can cascade, affecting the entire national infrastructure, and as a result, data security is a matter of the utmost national importance.

1.3. The Problem: The Vicious Cycle of Reactive Incident Management

The default IT operations mode in the majority of organizations is Incident Management. Its primary objective is speed: to resume a failed or interrupted service as quickly as possible. When a data breach alarm is sounded, an incident response team works to isolate the affected systems, eject the intruder, and recover services. Important as it is, this approach is fundamentally reactive in nature. It cures the symptom (the security incident) but does not necessarily investigate and heal the disease (the root cause). This creates a dangerous and costly "vicious cycle":

1. A security incident occurs (e.g., a data leak).
2. The Incident Management team restores service (i.e., patches the immediate vulnerability, restores from backup).
3. The underlying root cause problem (i.e., an intrinsic weakness in the application's authentication logic) is not found or fixed due to time pressure.
4. Attackers exploit the same or a similar root cause vulnerability in a different part of the system and create another, possibly more harmful, incident.

This reactive loop consumes significant resources, erodes trust, and prevents the organization's security posture from maturing.

1.4. Research Objectives and Scope

This paper argues that breaking this cycle requires a disciplined, proactive approach rooted in IT Problem Management. The research objectives are:

1. To critically differentiate between IT Incident Management and Problem Management within the context of data security.
2. To review the contemporary literature on ITSM frameworks (like ITIL 4) and Saudi-specific cyber security regulations (from NCA and SAMA).
3. To propose a specialized framework, the "Proactive Problem Management Framework for Data Security (PPM-DS)," for the Saudi digital ecosystem.
4. To rigorously demonstrate the worth of the framework via extensive, realistic case studies.
5. To analyze the strategic fit of this framework with Vision 2030 objectives and discuss the challenges of implementation.

II. Literature Review

2.1. IT Service Management (ITSM) and the ITIL Framework

IT Service Management is a strategic approach to planning, delivering, managing, and constantly improving the use of information technology (IT) within an organization. The most common framework for ITSM is the IT Infrastructure Library (ITIL), now in its fourth iteration (ITIL 4). ITIL 4 describes a service value system with an emphasis on co-creating value with stakeholders. Within this system, it makes a clear distinction between key practices:

- **Incident Management:** Aims to minimize the negative impact of incidents by resuming normal service operation as quickly as possible. Its key measure is Mean Time to Resolution (MTTR).
- **Problem Management:** Aims to eliminate the likelihood and impact of incidents by identifying actual and potential incident root causes, and managing workarounds and known errors. It has two main aspects:
  - Reactive Problem Management: Triggered after an incident has happened, with the purpose of determining its root cause.
  - Proactive Problem Management: Tries to discover and fix problems and known errors before they result in incidents, typically by analyzing trends, logs, and other data.

The literature is unanimous: while Incident Management is a critical reactive function, a mature IT organization achieves stability and resilience through a strong Problem Management practice. However, the leveraging of Problem Management as a prime driver for data security, and not just service availability, is a topic that has had limited investigation.

2.2. The Current Data Security Environment

Current data protection has shifted from the perimeter defense of the past (firewalls, antivirus) to a more holistic, data-centered strategy known as "Cyber Resilience." It is founded on the belief that breaches are not a question of if, but when. The key tenets are:

• **Zero Trust Architecture (ZTA):** It operates on the "never trust, always verify" principle. It eliminates implicit trust and is constantly validating every stage of a digital interaction. A mature Problem Management function is required to find and remediate areas where implicit trust models still exist and are yielding vulnerabilities.

• **Defense in Depth:** The principle is to have multiple layers of security measures. If one layer is compromised, another exists to thwart the attack. Problem Management analyzes incidents to identify which layers failed and why, so that the entire defensive mechanism can be made stronger.

• **Threat Intelligence:** This involves gathering and analyzing information about current and potential future attackers and their methods. Proactive Problem Management is a big consumer of threat intelligence, where it is used to search for potential vulnerabilities in the organization's systems before they are exploited.

2.3. Cybersecurity Governance in Saudi Arabia

The Saudi government has come to appreciate the significance of cybersecurity and has established a sound governance structure:

• **The National Cybersecurity Authority (NCA):** NCA is the primary organization responsible for cybersecurity in the Kingdom. NCA introduced the Essential Cybersecurity Controls (ECC), a mandatory set of controls for all government and critical national infrastructure organizations. ECC includes domains for cybersecurity governance, management, and defense. Problem Management directly supports ECC compliance by the formal process of identifying and remediating control failures that result in incidents.

• **The Saudi Central Bank (SAMA):** SAMA has issued its own comprehensive Cybersecurity Framework that applies to all financial institutions in the Kingdom. It calls for strict controls on data protection, risk management, and incident response. A formal Problem Management function is highly essential for banks and FinTechs in order to be able to demonstrate to SAMA that they are not just responding to incidents but are doing something about preventing their recurrence.

Although these frameworks specify what needs to be done, they do not prescribe the actual operational practice of how to reach a state of continuous improvement. This research argues that IT Problem Management is the key operational discipline that operationalizes the NCA and SAMA frameworks' principles.

III. The Proactive Problem Management Framework for Data Security (PPM-DS)

To bridge the gap between reactive incident response and proactive security improvement, this paper presents the PPM-DS framework. It's a four-stage, cyclical model that's designed to be integrated into any digital project's security practice.

3.1. Phase 1: Proactive & Reactive Problem Identification

This is the entry point for all potential problems. It's all about gathering inputs from different sources.

- **Reactive Inputs:**

  - **Major Security Incidents:** Any severe breach or disruption automatically creates a problem ticket.
  - **Recurring Incidents:** The system recognizes several seemingly minor incidents with commonalities (e.g., same user account, same application module, same alert type).

- **Proactive Inputs:**

  - **Log and Trend Analysis:** An AI/ML-powered Security Information and Event Management (SIEM) system analyzes logs from all systems (networks, servers, applications) to identify anomalous trends or patterns that could indicate a latent vulnerability. For example, a slow but steady increase in authentication failures for a specific database could be a sign of a persistent brute-force attack or a software component failing.
  - **Threat Intelligence Feeds:** The system is nourished with data on new attack vectors or vulnerabilities discovered globally. Problem Management then proactively searches for such vulnerabilities in their landscape.
  - **Penetration Test & Audit Findings:** Negative findings from security audits or penetration tests are handled as issues that have been discovered and require root cause analysis, as opposed to a quick fix.

3.2. Stage 2: In-Depth Root Cause Analysis (RCA)

This is the analytical core of the model, where the team digs below the symptoms to find the root cause.

- **Techniques:** A variety of formal RCA techniques are blended:
  - **The "5 Whys":** Simple yet effective method for drilling through levels of causality. Example: The website was defaced. Why? A vulnerability was exploited by an attacker. Why? A critical patch wasn't applied.

Why? The automatic patching system failed. Why? A firewall rule modification blocked its access to the update server. Why? The modification was not communicated to the security team (Root Cause).

- **Fault Tree Analysis:** Top-down deductive analysis used to chart all the potential contributing factors that can lead to a specific security failure.
- **Chronical Analysis (Attack Timeline):** Reconstruction of the entire lifecycle of an attack, from the beginning reconnaissance to the last data exfiltration, in order to identify every individual control failure that allowed the attack to persist.

• **Objective:** The aim is to identify a root cause that is an architectural, policy, or process fault. A "root cause" is never "human error"; instead, it is the failure of the process or system that allowed the human error to occur.

3.3. Stage 3: Error Control, Resolution, and Workarounds

Now that the root cause has been identified, this stage deals with remediation.

- **Workaround:** If a long-term fix is complex and will take time, a workaround is implemented and recorded to cover the risk on a short-term basis. For example, temporarily blocking an IP range or disabling a vulnerable feature.
- **Known Error Record:** Both the problem and the workaround are documented in a Known Error Database (KEDB). It is a valuable knowledge management tool that allows the incident team to resolve future incidents far more speedily while a lasting solution is being developed.
- **Permanent Fix:** This is when an alteration is implemented that removes the mistake once and forever. This could be a software patch, a redesign of the network design, an update to security policy, or more staff training. This alteration will have to go through a formal Change Management process to ensure that it does not introduce new risks.

3.4. Stage 4: Knowledge Management and Systemic Prevention

This final stage ensures that the learning from a problem is transferred to the entire organization.

- **Post-Resolution Review:** The Problem Management team holds a review session in order to analyze how successful the resolution was and how effective was the RCA process itself.
- **Knowledge Sharing:** The findings, root causes, and fixes are documented and shared across all relevant teams. This may involve updating security best practices, creating new training material, or improving automated security testing within the software development lifecycle (DevSecOps).
- **Proactive Feedback Loop:** The findings are fed back to Phase 1. As an example, a specific type of coding vulnerability may be found and a new automated scanner then built to actively seek out the identical vulnerability in all other applications across the enterprise. This closes the loop and converts the reactive process to a continuous, proactive enhancement system.

IV. Illustrative Case Study Analysis

To demonstrate the framework's practical applicability, we consider three archetypal scenarios in the Saudi digital ecosystem, comparing a traditional Incident Management response with the outcome from applying the PPM-DS framework.

Case Study 1: Data Breach in a FinTech Payment Platform

- **Scenario:** A recently released, highly popular Saudi FinTech payment app experiences a data breach where the transaction history of 50,000 users is exfiltrated. The attack is only discovered when the data is listed for sale on a dark web forum.
- **Traditional Incident Management Response:**
  - **Action:** Incident response team is activated. They identify the victim server, locate and patch a SQL injection vulnerability in a publicly exposed API endpoint, and inform SAMA. They make a public announcement and offer credit monitoring to victims. The incident is "closed."
  - **Outcome:** Service is restored, and the immediate vulnerability is fixed. However, the dev team that constructed the flawed API is not re-trained. The identical logical vulnerability exists in three other, non-public APIs within the same application. Six months later, a second attacker discovers one of these internal APIs via a partner integration and exploits it, causing a much larger and more damaging breach.

•PPM-DS Framework Application:

- **Identification (Stage 1):** Problem record is automatically triggered by the critical incident.
- **RCA (Stage 2):** Detailed RCA is performed by the problem manager. The "5 Whys" technique reveals the root cause as not the specific SQL injection vulnerability, but a "lack of mandatory security training for new developers" and "lack of static code analysis tools integrated into the CI/CD pipeline."
- **Resolution (Phase 3):** The workaround is the temporary solution. A Known Error Record is created. The permanent solution involves acquiring and introducing a static analysis security testing (SAST) tool into the development pipeline and mandating security training for all developers.

- **Knowledge Management (Step 4):** The SAST tool is now used to scan all other applications in the company, exposing the three same vulnerabilities before they are exploited. The training program is executed, improving the security of all future code. The repetitive breach cycle is broken.

Case Study 2: Ransomware Attack on a Giga-Project's Supply Chain Partner

- **Scenario:** A giga-project's major logistics partner is hit by ransomware that encrypts their entire inventory and shipping data. It grindingly halts a very critical part of the project supply chain for 72 hours, resulting in massive financial losses and delays. The entry point was initially a phishing email to a worker at the logistics company.

- **Traditional Incident Management Response:**
  - **Action:** The giga-project IT team focuses on severing all network connections to the partner. The partner's team tries to restore their systems from backup, eventually paying ransom to receive the decryption key to speed up the process. The incident is viewed as a "third-party issue."
  - **Outcome:** The direct connection is restored within a few days. The giga-project leadership does not, however, receive any visibility into the security posture of the partner. The same vulnerability (insufficient employee phishing awareness) exists in hundreds of other small and medium-sized suppliers in the project's ecosystem. The project remains highly vulnerable to the same type of disruption.

- **PPM-DS Framework Application:**
  - **Identification (Phase 1):** The major disruption triggers a problem record, not just for the partner, but for the "Third-Party Risk Management" process of the giga-project.
  - **RCA (Phase 2):** The RCA reveals the proximal cause (phishing email) but digs deeper. The root cause is found to be "inadequate security requirements in the supplier onboarding process" and "a lack of a shared threat intelligence platform for the project ecosystem."
  - **Resolution (Stage 3):** Long-term resolution is a complete overhaul of the supplier security policy. There are new contract requirements established, mandating all major suppliers to comply with a minimum baseline of security controls (mapped to NCA ECC). There is a central, shared platform for reporting and analyzing phishing attempts for the entire giga-project ecosystem.
  - **Knowledge Management (Stage 4):** The structured information from the new platform is examined proactively. The Problem Management team identifies a coordinated phishing campaign against a number of suppliers and is able to warn them before they are breached, preventing future disruption and rendering the entire supply chain more resilient.

Case Study 3: Insider Threat Incident in a Government Digital Service

- **Scenario:** A low-level government agency worker who provides a vital digital service to citizens is found to be accessing and selling citizens' personal information. The activity is identified by a routine audit.
- **Traditional Incident Management Response:**
  - **Action:** The worker is caught, terminated, and legal action is initiated. Their user account is immediately disabled. The audit finding is closed.
  - **Outcome:** The immediate risk is avoided. However, the vulnerability of the system that allowed the employee to possess access far beyond job requirements remains. The principle of "least privilege" is not applied. The next disgruntled employee with the same job position can do exactly the same thing.

- **PPM-DS Framework Application:**
  - **Identification (Stage 1):** The audit finding triggers a problem record.
  - **RCA (Phase 2):** The RCA reveals that the root cause was not the rogue employee, but a "flawed access control architecture" and "a lack of regular access reviews." The system had been configured to grant broad default access, and there wasn't a mechanism to review and restrict user privileges over time.
  - **Resolution (Stage 3):** The ultimate resolution is a complete re-architecture of the platform's Identity and Access Management (IAM) system to deploy the principle of least privilege by default. A new quarterly access review process for all managers is implemented and automated.
  - **Knowledge Management (Stage 4):** The findings trigger a government-wide requirement to review IAM policies for all citizen-facing digital services. Lessons from this single issue are proactively applied to secure dozens of other services from identical insider threats across the government.

V. Discussion: Strategic Implications for Vision 2030

The institution of a mature Problem Management discipline for data security has profound strategic implications that directly impact the Vision 2030 goals.

5.1. Building a Thriving and Trusted Digital Economy

Vision 2030 aims to build a strong digital economy that embraces investment and innovation in FinTech, e-commerce, and AI. This cannot be achieved without a basis of trust. Foreign investors, technology partners like Google and Microsoft (which are building cloud regions in the Kingdom), and Saudi citizens themselves must be assured that their data is secure. Every successive security incident erodes this assurance. Proactive Problem Management demonstrates a commitment to security maturity and systematics, which makes the Saudi digital ecosystem a secure and thus more attractive space in which to invest and innovate.

5.2. Enhancing National Security and Resilience

As critical national infrastructure—energy, water, transportation, and finance—becomes increasingly digitized and interdependent, its security is indistinguishable from national security. The PPM-DS approach provides a systematic method of enhancing the resilience of that infrastructure. By excavating and eliminating root causes of vulnerabilities in a segment of the system and sharing those lessons, the approach essentially inoculates the entire national ecosystem from cascading failure and synchronized cyberattack. This is in accordance with the NCA's role in securing the Kingdom's cyberspace.

5.3. Challenges in Implementation

Despite its evident benefits, the transition from a reactive to proactive model has significant challenges:

- **Cultural Resistance:** The biggest challenge is typically cultural. Incident Management is adrenaline-fueled and delivers immediate, visible results ("the fire is out"). Problem Management is plodding, slow, and its successes are typically invisible ("the fire that never happened"). It takes firm leadership commitment and new performance metrics that reward problem prevention, not firefighting, to break the "tyranny of the urgent.".
- **Skills Gap:** Effective RCA requires a special set of skills that blends sound technical knowledge with analytical, questioning, and dogged investigational abilities. Developing and sustaining this talent within Saudi Arabia will require a concerted effort on the behalf of universities, training institutions, and organizations themselves.
- **Inter-Agency Coordination:** As the case studies demonstrate, many root causes are systemic and traverse organizational boundaries. Effective Problem Management requires a high degree of collaboration and information exchange between different government agencies, regulators, and private sector institutions. Creating the trust and technical infrastructure to support this is a significant but necessary undertaking.

VI. Conclusion

The digital revolution driving Saudi Vision 2030 presents both an unprecedented opportunity and a formidable security challenge. The scale and speed of this revolution demand a security paradigm at least as dynamic and sophisticated. The reactive, incident-driven stance is no longer viable; it is an unsustainable approach that guarantees recurring failures and escalating risk.

This research has argued that the formal application of IT Problem Management, specifically tailored to data security, provides the necessary strategic improvement. The Proactive Problem Management Framework for Data Security (PPM-DS) offers a compact, structured approach to looking beyond symptoms and systematically identifying and removing the underlying causes of security vulnerabilities. As the case studies demonstrate, not only are one-off incidents more effectively dealt with by this approach, but a robust, resilient, learning, and continuously improving security posture is set up across the digital landscape.

Lastly, a culture of forward-thinking problem-solving is at the heart of safeguarding the Kingdom's digital assets. It is the operational engine that will drive compliance with NCA and SAMA frameworks, build long-term trust with global partners and citizens, and ensure that the incredible digital future envisioned by Vision 2030 is built on a foundation of security and resilience.

References

[1]. AXELOS. (2019). ITIL Foundation: ITIL 4 Edition. TSO (The Stationery Office).
[2]. Information Technology Infrastructure Library (ITIL). Official website and publications. AXELOS.
[3]. International Organization for Standardization. (2018). ISO/IEC 27001: Information technology — Security techniques — Information security management systems — Requirements.
[4]. National Cybersecurity Authority (NCA), Kingdom of Saudi Arabia. (2022). Essential Cybersecurity Controls (ECC-1: 2022). Retrieved from nca.gov.sa.
[5]. Saudi Central Bank (SAMA). (2020). SAMA Cybersecurity Framework. Retrieved from sama.gov.sa.
[6]. Vision 2030, Kingdom of Saudi Arabia. Official Website and Documentation. Retrieved from vision2030.gov.sa.