Ngr. J. Multi. vol-2, issue-9 (Sep-2026) pp-499-520

ISSN: 3108-2750 (E), 3139-8065 (P)

Nexus Global Research Journal of Multidisciplinary

Journal Homepage: https://nexusglobalresearch.com/journal/ngrjm/

Research Article

Development and Validation of a Risk-Based Vulnerability Management Framework for Systems Operation of Pangasinan State University

Nelson O. Rosario[1]*, Prof. Andrew C. Caronongan[2]

[1] The Faculty of the Graduate School, UNIVERSITY OF LUZON, Dagupan City
[2] Professor, The Faculty of the Graduate School, UNIVERSITY OF LUZON, Dagupan City

ABSTRACT:
This capstone project focuses on the development and validation of a Risk-Based Vulnerability Management Framework (VMF) for the systems operations of Pangasinan State University (PSU), Binmaley Campus. The study addresses the critical need for a structured, context-aware security governance engine to replace the institution's reactive, point-in-time vulnerability management practices. Grounded in the Design Science Research Methodology (DSRM), the framework integrates dynamic threat intelligence from the Exploit Prediction Scoring System (EPSS) and the CISA Known Exploited Vulnerabilities (KEV) catalog to prioritize vulnerabilities based on actual exploitation likelihood rather than static technical severity scores alone. The research assessed the current status of vulnerability management practices across four pillars: asset identification, vulnerability assessment, remediation, and monitoring. Findings revealed significant operational gaps including a 197-day structural detection lag, fragmented asset visibility, and alert fatigue among IT practitioners due to CVSS-only prioritization. The developed framework features four interoperable modules: a Vulnerability Knowledge Base for intelligence consolidation, an Automated Scanning Engine for continuous discovery, a Context-Aware Prioritization Module utilizing Vulnerability Management Chaining (VMC) logic, and a Standardization Layer for automated remediation workflows. Validation was conducted through a dual-track approach involving cybersecurity experts who evaluated technical functionality and completeness using Lawshe's Content Validity Ratio (CVR), and IT practitioners who assessed usability and applicability through the Technology Acceptance Model (TAM). Results yielded perfect CVR scores of 1.0 for functionality and completeness, with practitioners strongly agreeing on the framework's usability and applicability. The validated framework provides an 18-fold efficiency improvement in remediation workflows, significantly reducing the urgent vulnerability workload while maintaining coverage of weaponized threats to mission-critical academic and administrative databases.

Keywords: Vulnerability Management Framework, Design Science Research Methodology, Context-Aware Prioritization, Vulnerability Management Chaining, Systems Operations Security

Citation: Rosario, N. O., & Caronongan, A. C. (2026). Development and validation of a risk-based vulnerability management framework for systems operation of Pangasinan State University. Nexus Global Research Journal of Multidisciplinary, 2(9), 499–520.

INTRODUCTION

In the contemporary digital landscape, systems operations have become the indispensable foundation of modern Higher Education Institutions (HEIs). These operations encompass the continuous management, maintenance, and protection of IT-enabled services and platforms that facilitate administrative workflows, academic record-keeping, and student-facing processes. As HEIs increasingly integrate cloud computing and complex software supply chains, the reliability and security of these systems become paramount to sustaining institutional credibility and operational continuity. However, this digital transformation has resulted in an asymmetric expansion of the attack surface, leaving universities as high-value targets for systemic exploitation.

Globally, organizations are facing an escalating vulnerability burden, with over 40,289 Common Vulnerabilities and Exposures (CVEs) published in 2024 alone—a 39% increase from the previous year. Despite these rising stakes, traditional vulnerability management practices often remain

***Corresponding Author:** Nelson O. Rosario,
Received: 15Aug 2026 | **Accepted:** 30 Aug 2026 | **Published:** 05 Sep 2026
Copyright © 2026 The Author(s): This work is licensed under a Creative Commons Attribution- Non-Commercial-No Derivatives 4.0 (CC BY-NC-ND 4.0) International License

rooted in reactive, point-in-time scanning models that result in an average detection window of 197 days. This operational latency is further complicated by the "vulnerability paradox": while thousands of flaws are disclosed monthly, studies by Tenable Research (2024) indicate that only 3% of vulnerabilities ever result in impactful real-world exposure.

The industry's reliance on the Common Vulnerability Scoring System (CVSS) has been increasingly scrutinized by researchers such as Shimizu and Hashimoto (2025), who argue that CVSS evaluates technical severity in an environmental vacuum, failing to account for real-world exploit availability or the specific criticality of institutional assets. Without context-aware models that integrate dynamic threat intelligence—such as the Exploit Prediction Scoring System (EPSS) and the CISA Known Exploited Vulnerabilities (KEV) catalog—security teams are often overwhelmed by "false urgency," misallocating scarce resources toward low-risk findings while critical attack vectors remain unpatched.

At Pangasinan State University, Binmaley Campus, the importance of robust systems operations is exemplified by its dependency on digital infrastructure for enrollment, grading, and administrative management. However, a significant gap exists in the formalization of a structured vulnerability management lifecycle tailored to the University's unique operational architecture. According to Wiz Experts Team (2026), treating vulnerability management as a periodic project rather than a continuous lifecycle creates dangerous security blind spots. Effective governance requires a repeatable process that addresses the four pillars of the lifecycle: (a) asset identification and inventory, as "you cannot protect what you don't even know exists"; (b) vulnerability assessment and detection; (c) vulnerability remediation and mitigation; and (d) vulnerability monitoring and reporting to close the loop on identified risks.

In response to these challenges, this study proposes the development and validation of a Vulnerability Management Framework for Pangasinan State University, Binmaley Campus. Grounded in the Design Science Research Methodology (DSRM), the proposed framework aims to move beyond static technical scoring by dynamically integrating exploitability predictions and asset-specific criticality into a unified governance engine.

To ensure the artifact's scientific rigor and practical utility, the framework will undergo evaluation by cybersecurity experts and information technology practitioners based on empirical validation criteria including functionality, usability, completeness, and applicability. This systematic approach ensures that the University transitions from a reactive posture to a proactive, evidence-based defense model, fortifying its systems operations against the evolving threat landscape.

Statement of the Problem

This study aimed to develop and validate a risk-based vulnerability management framework for systems operation of Pangasinan State University particularly in Binmaley Campus for a robust computing environment.

Specifically, this study sought to answer the following questions:

1. What are the vulnerability management requirements in the systems operation of Pangasinan State University Binmaley Campus in terms of:
   a) Asset Identification and Inventory;
   b) Vulnerability Assessment and Classification;
   c) Vulnerability Remediation and Mitigation; and
   d) Vulnerability Monitoring and Reporting?

2. What risk-based vulnerability management framework can be developed for the systems operation of the university to improve its cybersecurity posture?
3. What is the extent of validity of the developed vulnerability management framework as evaluated by cybersecurity experts and Information Technology practitioners in terms of: Functionality;
   a) Usability;

b) Completeness; and
c) Applicability?

4. What final version of the vulnerability management framework can be proposed for implementation in the systems operation of Pangasinan State University Binmaley Campus?

Scope and Delimitation

This study primarily focuses on the development and validation of a Risk-Based Vulnerability Management Framework (VMF) tailored to the systems operations of Pangasinan State University, Binmaley Campus. The scope of the development covers the systematic identification of technical and structural gaps within the University's existing IT infrastructure, specifically addressing the four pillars of the vulnerability lifecycle: (a) asset identification and inventory; (b) vulnerability assessment and detection; (c) vulnerability remediation and mitigation; and (d) vulnerability monitoring and reporting.

This study is delimited to the internal systems operations of Pangasinan State University, Binmaley Campus, and does not encompass the IT infrastructure of other PSU campuses. Furthermore, the research is delimited to digital and networked vulnerabilities and does not cover non-IT security aspects, such as physical facility security, emergency medical response, or the protection of non-digital administrative records. The framework is specifically architected for the University's unique operational environment; therefore, while it may serve as a reference model for other academic institutions, its direct applicability elsewhere may require further modification to align with differing institutional architectures and risk appetites.

Significance of the Study

This study was conducted to develop and validate a Vulnerability Management Framework (VMF) specifically for the systems operations of Pangasinan State University, Binmaley Campus. The primary goal is to establish a proactive and context-aware security architecture that moves beyond static technical scoring to ensure the resilience of the University's digital infrastructure. The results of this study are expected to benefit the following:

Pangasinan State University, Binmaley Campus:

The developed framework provides the University with a structured, repeatable process to identify and mitigate security flaws before they can be exploited

University Administrators:

The VMF serves as an official guide for IT practitioners in managing the complex lifecycle of vulnerabilities within the campus. It provides a clear prioritization logic that integrates technical severity (CVSS) with institutional asset criticality, effectively reducing alert fatigue and ensuring that limited remediation resources are focused on the most impactful risks. This leads to faster response times and improved operational agility.

Cybersecurity and IT Practitioners:

This research offers practical insights into how the Design Science Research Methodology (DSRM) can be applied to solve real-world institutional security challenges. It bridges the gap between theoretical academic models and modular industrial requirements, providing students with a reproducible example of how to integrate dynamic threat intelligence into a unified governance engine.

Future Researchers:

The study contributes to the expanding body of literature concerning vulnerability management within Higher Education Institutions (HEIs). It addresses identified research gaps regarding the need for empirically validated, context-aware frameworks. Future researchers may use these findings as a baseline for longitudinal studies on automated prioritization or as a reference model for adapting similar frameworks across other multi-campus university systems.

Definition of Terms

For a better understanding of the words and concepts used in this work, the following were defined:

Development and Validation of a Risk-Based Vulnerability Management Framework for Pangasinan State University, Binmaley Campus.

this term refers specifically to the researcher's creation of a customized, step-by-step security blueprint for Pangasinan State University, Binmaley Campus (PSU-BC). The *Development* phase involves analyzing the campus's existing IT infrastructure, identifying its unique operational needs, and crafting a formal document or system that outlines specific procedures for asset inventory, vulnerability scanning, risk prioritization, and remediation.

***Risk-Based Vulnerability Management Framework (RBVMF*).**

A modular set of guidelines, workflows, and prioritization matrices tailored for PSU Binmaley that fuses CVSS v4.0 severity, EPSS exploitation probability, and CISA KEV threat-intelligence membership within an SLA-bound operating model.

Development.

Refers to the structured, artifact-oriented research process of designing a context-aware Vulnerability Management Framework (VMF) under the Design Science Research Methodology (DSRM), encompassing iterative cycles of construction and technical formulation to address institutional security gaps.

***Validation*.**

The rigorous process of establishing the scientific credibility and practical efficacy of the developed framework through expert evaluation and testing against established technical baselines.

Systems Operations of Pangasinan State University, Binmaley Campus.

Refers to the IT-enabled services, physical servers, databases, and network infrastructures that support academic workflows and administrative processes unique to the Binmaley campus.

Asset Identification and Inventory.

The foundational phase of discovering and cataloging all physical and digital components—including servers, workstations, and IoT devices—to ensure complete visibility of the University's digital attack surface.

Vulnerability Assessment and Detection.

The systematic detection of security weaknesses, misconfigurations, and outdated software within the University's systems using authenticated and unauthenticated scanning tools.

Vulnerability Remediation and Mitigation.

The operational process of applying permanent technical fixes (patching) or implementing temporary compensating controls (e.g., firewall rules) to reduce the likelihood of systemic exploitation.

Vulnerability Monitoring and Reporting.

The continuous cycle of verifying that remediations were successful and communicating risk trends and security posture updates to University stakeholders.

Functionality.

The degree to which the framework's modular components (e.g., scanning engine, scoring module) perform their intended technical operations to improve the University's defensive posture.

Usability.

The extent to which the framework is perceived as easy to use and adopt by University IT practitioners, often evaluated through the lens of perceived ease of use and behavioral intention to comply with security protocols.

Completeness.

The structural integrity of the framework, ensuring that all essential indicators and stages of the vulnerability management lifecycle are present and appropriately addressed.

Applicability.

The practical utility and real-world relevance of the framework in addressing the specific environmental constraints and system dependencies of the PSU Binmaley IT infrastructure.

Chapter II
REVIEW OF RELATED LITERATURE

This chapter presents all cited literature, system and works that guided the Development and

Validation of a Vulnerability Management Framework for the Binmaley, Pangasinan State University (PSU) Campus.

Conceptual literature

The Vulnerability Management Lifecycle and Operational Gaps

The management of security flaws within an institutional IT environment is not a singular event but a continuous, repeating cycle. CrowdStrike (2022) and Wiz Experts Team (2026) define this as a strategic process that moves organizations from reactive "firefighting" to proactive risk reduction across every asset class

Structural Stages of the Vulnerability Management Cycle

The literature universally partitions the management process into specific pillars. NRI Secure (2026) and Vectra AI (2025) outline a structured approach beginning with Discovery and Asset Inventory, which involves identifying all hardware, software, and cloud resources. This is followed by Assessment, where scanning tools enumerate weaknesses, and Prioritization, which determines remediation order based on threat signals. The cycle concludes with Remediation and Mitigation, followed by Verification and Monitoring to ensure that patches were successful and that no new configuration drift has occurred

The Concept of Operational Latency and "Point-in-Time" Gaps

A significant conceptual weakness in traditional practices is the reliance on periodic, scheduled scans. Safe Security (2025) notes that legacy tools create "blind spots" because infrastructures change daily, while traditional scans may only occur quarterly. This leads to a "structural lag" where vulnerabilities remain undetected for an average of 197 days before being addressed. SentinelOne (2025) argues that instead of occasional snapshots, institutions require a consistent remediation pipeline to align detection with the rapid expansion of the digital attack surface. This latency is particularly dangerous in academic environments where sensitive student data and grading systems are exposed to the public internet.

Static Prioritization Failures and Alert Fatigue

A primary challenge identified by Team NetSPI (2023) is the "needle in the needle stack" problem, where organizations are overwhelmed by thousands of alerts but lack the intelligence to find the most critical ones. Tenable Research (2024) highlights a "vulnerability paradox" where only 3% of vulnerabilities result in impactful exposure, yet traditional systems treat all "High" and "Critical" technical scores with equal urgency. This results in alert fatigue, exhausting the capacity of security analysts on theoretical threats while active exploit vectors remain unpatched. Shimizu and Hashimoto (2025) point out that the Common Vulnerability Scoring System (CVSS) often fails to correlate with actual exploitation likelihood, necessitating an integrated approach.

Cultural and Organizational Alignment Gaps

Beyond technical flaws, KPMG (2026) suggests that strong frameworks often fail when institutional culture is not ready for change. Gaps persist due to misaligned priorities and internal politics, where the teams identifying vulnerabilities (Security) are siloed from the teams with the authority to apply patches (IT Operations). Without a shared accountability model and automated ticket routing, strategic roadmaps often remain as "paper models" that are never fully executed.

Design Science Foundations for Context-Aware Security Frameworks

To address the limitations of reactive practices, modern frameworks are developed using the Design Science Research Methodology (DSRM), which focuses on constructing innovative artifacts to solve complex real-world problems.

Principles of the Design Science Research Methodology (DSRM)

Shimizu and Hashimoto (2025) and Janjal (2026) utilize DSRM to ground framework development in scientific rigor. The methodology is structured around three interlocking feedback loops: the relevance cycle, which identifies institutional operational problems; the design cycle, which iterates the construction of the artifact; and the rigor cycle, which ensures the framework is grounded in established scientific theories.

Modular Architecture and Interoperability

Modern governance frameworks are designed to be modular to ensure scalability across hybrid and cloud-native environments. Rivas Bustos, Gutierrez, and Rueda (2026) propose a four-module structure:

a) Vulnerability Knowledge Base. A unified repository correlating static severity data with dynamic threat signals.
b) Automated Scanning Engine. An orchestrator for continuous, multi-vector discovery to maintain real-time visibility.
c) Context-Aware Prioritization Module. A scoring engine that weights technical severity against environmental asset criticality.
d) Standardization and Interoperability Layer. A layer that translates prioritized intelligence into automated workflows

Transitioning to Context-Aware and Predictive Models

The evolution of prioritization logic requires moving from static scores to context-aware models. Dudar (2025) explains that a context-aware framework must integrate technical severity (CVSS) with dynamic empirical signals, such as the Exploit Prediction Scoring System (EPSS) and the CISA Known Exploited Vulnerabilities (KEV) catalog. Janjal (2026) emphasizes that embedding mission criticality into these models allows the framework to reflect real-time changes in system conditions, ensuring that authorization decisions are based on data-driven threat likelihood.

Empirical Methodologies for Artifact Validation and Expert Evaluation

Validation is the process of establishing the scientific credibility and practical efficacy of a newly engineered cybersecurity framework

Convergent Mixed-Methods Research Design

To move beyond subjective reviews, validation must adopt a convergent mixed-methods design. Shimizu and Hashimoto (2025) suggest that framework validation should combine quantitative technical testing with rigorous qualitative expert evaluation. This ensures the artifact meets the dual requirements of scientific accuracy and operational usability.

Content, Construct, and Criterion Validity

The literature defines three primary validation domains. Content Validation utilizes domain expert panels to calculate the Content Validity Ratio (CVR) and Index (CVI), ensuring that all framework indicators are "essential". Construct Validation confirms that the theoretical dimensions (e.g., risk management, governance) are structurally sound using structural modeling like PLS-SEM. Finally, Criterion Validation measures the framework's "predictive utility" in simulated environments, measuring performance against established technical baselines.

Content, Construct, and Criterion Validity

The suitability of a framework is measured through specific performance metrics. Technical performance is evaluated using Mean Time to Detect (MTTD) and Mean Time to Remediate (MTTR). Behavioral suitability is assessed through the Technology Acceptance Model (TAM), which measures Perceived Usefulness (PU) and Perceived Ease of Use (PEOU) among IT practitioners. Malkawi and Alhajj (2026) conclude that next-generation systems must not only be accurate but also transparent and explainable to earn the trust of stakeholders in high-assurance environments.

Evaluation Metrics for Technical and Behavioral Suitability

The suitability of a framework is measured through specific performance metrics. Technical performance is evaluated using Mean Time to Detect (MTTD) and Mean Time to Remediate (MTTR). Behavioral suitability is assessed through the Technology Acceptance Model (TAM), which measures Perceived Usefulness (PU) and Perceived Ease of Use (PEOU) among IT practitioners. Malkawi and Alhajj (2026) conclude that next-generation systems must not only be accurate but also transparent and explainable (XAI) to earn the trust of stakeholders in high-assurance environments.

Research Literature

The Vulnerability Management Lifecycle and Operational Gaps

Empirical research has consistently documented a critical misalignment between the rapid expansion of the digital attack surface and the speed of organizational defensive response. Malkawi and Alhajj (2026) identify that while attackers frequently weaponize vulnerabilities within hours of public disclosure, traditional management processes often leave systems exposed for weeks or months due to manual and human-centric bottlenecks. Research into the contemporary threat landscape indicates that 23.6% of known exploited vulnerabilities are weaponized on or before their public disclosure, leaving defenders with no meaningful lead time for reactive response (Vectra AI, 2025). Furthermore, Safe Security (2025) notes a persistent "structural lag" resulting in an average detection window of 197 days, during which high-risk assets remain vulnerable to systemic exploitation.

The "vulnerability paradox" remains a central theme in recent research. Tenable Research (2024) reports that while organizations are inundated with thousands of high-severity alerts, only 3% to 5% of these flaws ever result in impactful real-world exposure. This disconnect leads to severe alert fatigue and resource misallocation, as security practitioners find themselves sifting through a "needle in the needle stack" scenario where critical threats are obscured by low-priority findings (Team NetSPI, 2023). Jacobs *et al.,* (2023) further demonstrate this inefficiency, finding that organizations can typically remediate only about 15.5% of their total open vulnerabilities, necessitating a shift from comprehensive patching to highly targeted risk-based strategies.

Beyond technical failures, academic investigations highlight structural and cultural gaps as major inhibitors of security resilience. KPMG International (2026) concludes that while organizations continue to invest heavily in detection tooling, the primary failure mode is "follow-through," characterized by fragmented ownership between security teams (who identify flaws) and IT operations (who apply patches). Wan and Saxe (2024) find a persistent "adoption gap," noting that many academic models fail in industrial settings because they are not optimized for the specific resource constraints or risk tolerances of internal departments. This lack of organizational alignment often results in strategic security roadmaps remaining as "paper models" that are never fully executed in the operational environment.

Design Science Foundations for Context-Aware Security Frameworks

The development of next-generation governance artifacts relies on the construction of modular, context-aware systems engineered under iterative scientific methodologies. Shimizu and Hashimoto (2025) and Janjal (2026) emphasize the utility of the Design Science Research Methodology (DSRM) in grounding framework development through interlocking feedback loops: the relevance cycle (problem identification), the design cycle (artifact construction), and the rigor cycle (grounding in scientific literature). This ensures that framework development is not a linear sequence but an iterative process of refinement based on operational feedback.

Modern research indicates that effective risk governance requires a layered, modular approach to maintain scalability across hybrid environments. Rivas Bustos, Gutierrez, and Rueda (2026) propose a four-module architecture consisting of: (a) a Vulnerability Knowledge Base for evidence consolidation; (b) an Automated Scanning Engine for integrated discovery; (c) a Context-Aware Prioritization Module for adaptive scoring; and (d) a Standardization Layer. This modularity allows organizations to unify siloed approaches—such as traffic monitoring and firmware analysis—into a single, coherent governance process. Dudar (2025) demonstrates the capability of interpretable machine learning models to predict exploitation probability by integrating technical severity (CVSS) with dynamic empirical signals like the Exploit Prediction Scoring System (EPSS) and the CISA Known Exploited Vulnerabilities (KEV) catalog.

The integration of dynamic threat intelligence has yielded transformative performance improvements in recent experiments. Naoyuki

Shimizu (2025) introduced the "Vulnerability Management Chaining" framework, which utilizes a two-stage evaluation process to filter threats based on likelihood before assessing technical impact. Experimental validation using 28,377 real-world vulnerabilities demonstrated an 18-fold efficiency improvement in remediation workflows while maintaining an 85.6% coverage rate of critical threats. Similarly, Anand Janjal (2026) developed a GovSecOps-oriented architecture that embeds compliance workflows directly into operational telemetry pipelines, resulting in a statistically significant 38.2% reduction in remediation cycle time. These results validate the transition from static, manual processes to adaptive, autonomous management frameworks.

Empirical Methodologies for Artifact Validation and Expert Evaluation

The validation of cybersecurity frameworks must transcend qualitative review, employing rigorous empirical designs to prove both technical efficacy and stakeholder trust. Shimizu and Hashimoto (2025) suggest that framework verification should adopt a convergent mixed-methods design, combining quantitative technical experiments in virtual laboratories with structured qualitative expert evaluations. A systematic review by Jiang *et al.,* (2025) indicates that controlled experiments are the most common validation method, used in 33 out of 82 major studies, to evaluate the accuracy and performance of prioritization models in isolated settings.

To establish scientific rigor, researchers utilize specific statistical metrics to measure various domains of validity. Construct Validation often employs Partial Least Squares Structural Equation Modeling (PLS-SEM) to quantitatively analyze the relationships between governance variables and their cumulative impact on achieving security objectives. For Content Validation, domain expert panels utilize Lawshe's Content Validity Ratio (CVR) and the Content Validity Index (CVI) to rate framework indicators, ensuring that only "essential" elements are retained within the final artifact. Anand Janjal (2026) supports this through comparative multi-case studies across cloud-native, hybrid, and legacy environments to evaluate feasibility under varying operational conditions.

The practical utility of a framework is further measured by its impact on operational timelines and user acceptance. Kabenge (2024) utilized simulation experiments in a virtual network environment to validate the "bukirwa_score," proving that automated exploitability tests can significantly reduce the number of high-priority vulnerabilities security teams must address by assessing the target system's internal security posture. Technical success is typically quantified through Mean Time to Detect (MTTD) and Mean Time to Remediate (MTTR). Finally, validating behavioral adoption is critical, as Malkawi and Alhajj (2026) conclude that next-generation AI systems must not only be accurate but also transparent and explainable (XAI) to earn the trust of stakeholders in high-assurance environments. The Technology Acceptance Model (TAM) serves as the validated theoretical lens for this purpose, evaluating user buy-in through the metrics of Perceived Usefulness (PU) and Perceived Ease of Use (PEOU).

TECHNICAL BACKGROUND

This chapter presents the technical foundation and conceptual literature that ground the Development and Validation of a Vulnerability Management Framework (VMF) for Pangasinan State University, Binmaley Campus. It explores the theoretical constructs of the vulnerability lifecycle, the architectural principles of design science, and the empirical standards for artifact validation.

Conceptual Framework

The conceptual framework of this study is anchored on a hybrid Input-Process-Output (IPO) model integrated with the Design Science Research Methodology (DSRM) and a behavioral synthesis of the Technology Acceptance Model (TAM) and Protection Motivation Theory (PMT). This multi-dimensional approach is designed to bridge the structural gap between the technical engineering of a cybersecurity artifact and the behavioral drivers that determine its successful adoption within organizational systems operations.

By utilizing the IPO model to organize the logical flow of the study, the research ensures that institutional requirements are systematically transformed into a validated solution. The integration of TAM and PMT addresses the "human element" of cybersecurity, acknowledging that a framework is only effective if practitioners perceive it as useful and feel motivated to enforce its protocols to protect digital assets.

Figure 1.0 below illustrates the progression of the study, mapping the environment-specific inputs and technical intelligence into an iterative design process that culminates in a multi-domain validation of the research output.

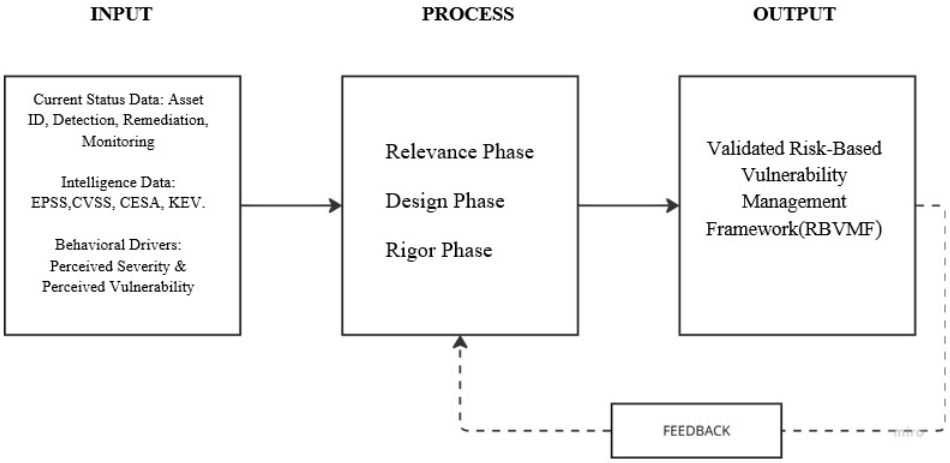


Figure 1.0 – Conceptual Framework on VMF Development

Figure 1.0 illustrates the research pathway for the development and validation of the framework. The Input phase defines the technical and behavioral starting point by identifying existing operational gaps and the initial threat perceptions of the staff. The Process phase utilizes the iterative loops of Design Science to construct the artifact, ensuring it is optimized for ease of use and institutional utility. The Output phase focuses on a dual-track validation, where technical experts confirm the artifact's scientific completeness while practitioners evaluate its applicability to real-world systems operations.

Input

The Input phase focuses on gathering the requirements and environmental intelligence necessary to ground the framework in the specific operational needs of the Binmaley, Pangasinan State University. This involves identifying the current status of vulnerability management practices at PSU Binmaley, categorized into the four pillars: (a) asset identification and inventory; (b) vulnerability assessment and detection; (c) vulnerability remediation and mitigation; and (d) vulnerability monitoring and reporting. Technical data inputs include Common Vulnerability Scoring System (CVSS) metrics for severity, Exploit Prediction Scoring System (EPSS) probability scores, and the CISA Known Exploited Vulnerabilities (KEV) catalog for evidence of active exploitation and an initial assessment of practitioners' threat appraisals (perceived severity of institutional risks) and coping appraisals (perceived self-efficacy and the perceived effectiveness of existing security tools).

Process

The Process phase represents the iterative development of the artifact, utilizing Design Science Research Methodology (DSRM) to transform the inputs into a functional governance engine. The development follows the Relevance Phase (aligning with institutional gaps), the Design phase (iterative construction of the modular architecture), and the Rigor phase (grounding the logic in established security theories and behavioral models). The core construction focuses on four components: (a) a Vulnerability Knowledge Base for evidence consolidation; (b) an Automated Scanning Engine for discovery; (c) a Context-Aware Prioritization Module for adaptive scoring; and (d) a Standardization Layer for automated workflows. Within the design process, TAM serves as an optimization lens, ensuring the framework's automated workflows are engineered for Perceived Ease of Use (PEOU) and Perceived Usefulness (PU)

to minimize user friction during institutional adoption.

Output

The final Output of this study is the Validated Vulnerability Management Framework (VMF). The validity of this output is empirically measured across multiple domains to ensure scientific and practical credibility. Functionality and Completeness are measured through Content Validation using domain expert panels and Lawshe's Content Validity Ratio (CVR) to ensure all lifecycle stages and technical indicators are essential and present. Usability and Applicability is Evaluated through the TAM-PMT synthesis, specifically measuring the behavioral intention of IT practitioners to adopt the framework into daily systems operations based on its perceived utility in mitigating risk and its ease of integration.

Present Structure of the Systems Operations

The systems operations of Pangasinan State University, Binmaley Campus, are organized around a centralized digital infrastructure that facilitates the core academic and administrative workflows of the institution. This architecture is designed to support the real-time processing of student data, faculty records, and institutional communications through a primary management system. This centralized model ensures that various campus units can operate with a unified set of data, though it inherently creates a complex environment of interconnected assets that require continuous oversight.

Key administrative and academic units—including the Registrar's Office, Accounting Office, and Departmental Heads—interface directly with this central platform. These interactions involve the continuous exchange of information, such as the uploading of enrollment entries, the retrieval of academic records for transcript issuance, and the synchronization of financial data for student clearances. This data flow is maintained through a local network infrastructure that connects departmental workstations to the primary campus database servers.

System Specifications and Requirements

This section details the specific system requirements and technical criteria necessary for the development and operationalization of the Vulnerability Management Framework (VMF) at Pangasinan State University, Binmaley Campus. These requirements are derived from the University's existing systems operations architecture, the architectural pillars of the proposed framework, and the technical standards required for empirical validation.

1. Hardware Requirements

To support a continuous and proactive management lifecycle, the institutional infrastructure must provide the computational resources required for intensive scanning and data correlation. The primary requirements includes dedicated server environment is required to host the Vulnerability Knowledge Base and the Prioritization Module. This server must possess sufficient CPU and memory capacity to process multi-source intelligence feeds from NVD, EPSS, and KEV without causing latency in administrative workflows. Institutional workstations must support the deployment of lightweight, authenticated scanning agents. These agents facilitate deep-visibility discovery across the campus's digital attack surface, including servers in the Registrar and Accounting offices. Routers and switches must support the bandwidth requirements of automated discovery and telemetry ingestion. The hardware must be capable of maintaining secure, isolated segments to prevent the lateral movement of threats during remediation cycles.

2. Software Requirements

The framework's effectiveness relies on a modular software stack that automates the transition from detection to remediation. The core requires a software environment capable of supporting four distinct modules: (a) a Vulnerability Knowledge Base for data aggregation; (b) an Automated Scanning Engine for continuous discovery; (c) a Context-Aware Prioritization Module for adaptive risk scoring; and (d) a Standardization Layer for automated ticket routing. APIs. The system must interface with external threat intelligence APIs to ingest real-time data, specifically the Exploit Prediction Scoring System (EPSS) and the CISA Known Exploited Vulnerabilities (KEV) catalog. The framework must be interoperable with the various operating systems currently in use at the University, including Linux-based servers and Windows-based administrative workstations, to ensure a comprehensive and accurate asset inventory.

3. Vulnerability Lifecycle and Operational Requirements

Aligned with the Input and Process phases of the conceptual framework, the system must support the functional requirements of the management lifecycle. The system must provide real-time visibility into all connected assets, identifying configuration drift and "Shadow IT" devices that may connect to the campus network. The framework must be capable of weighting technical severity (CVSS) against institutional asset criticality. This ensures that vulnerabilities affecting mission-critical systems, such as student enrollment databases, are prioritized over non-essential assets. The software must enable the automated assignment of remediation tasks to specific asset owners, tracking Service Level Agreement (SLA) compliance for "Critical" and "High" priority findings.

4. Network and Communication Requirements

Effective governance requires secure and transparent communication protocols between the IT team and University stakeholders. The network must support secure interfaces for the transmission of vulnerability data from localized enclaves to the centralized management dashboard, ensuring that data integrity is maintained during the scanning process. The framework requires automated notification systems to alert practitioners of newly disclosed, actively exploited flaws. Reporting modules must generate both technical documentation for administrators and executive summaries for University leadership to demonstrate overall risk reduction progress.

5. Evaluation and Validation Requirements

To satisfy the requirements for empirical validation, the framework must provide the following evaluative mechanisms. The system must allow cybersecurity experts to analyze the functionality and completeness of the framework using Lawshe's Content Validity Ratio (CVR), ensuring all lifecycle stages are essential and present. The framework's interface and workflows must be evaluated by IT practitioners through the Technology Acceptance Model (TAM). This involves measuring Perceived Usefulness (PU) and Perceived Ease of Use (PEOU) to ensure a high behavioral intention for institutional adoption..

DESIGN AND METHODOLOGY

This chapter details the research design, the system development methodology, and the specific data gathering and analysis techniques utilized in the development and validation of the Vulnerability Management Framework (VMF) for the systems operations of Pangasinan State University, Binmaley Campus.

Research Design

This study adopts a descriptive-developmental research design to establish a validated security governance artifact tailored to the University's specific systems operations. The descriptive component focuses on identifying the current technical and behavioral landscape of vulnerability management at the campus, documenting existing gaps in asset discovery, assessment, remediation, and monitoring. The developmental component encompasses the iterative design, architectural formulation, and empirical validation of the VMF to address these identified operational risks and improve the institution's overall cybersecurity posture.

System Development Methodology

The development of the framework utilizes the Design Science Research Methodology (DSRM), a structured, artifact-oriented paradigm designed to construct innovative solutions for complex, real-world problems. Unlike linear development models, DSRM emphasizes an iterative approach where the artifact is refined through continuous feedback loops between technical requirements and behavioral acceptance. The methodology is divided into three primary cycles, as illustrated in Figure 2.0 below.



Figure 2.0 – Design Science Research Methodology Phases

The methodology is executed through the following structured phases:

1. Relevance Phase (Problem Identification and Requirement Elicitation)

This phase bridges the University's operational environment with the development process. It involves gathering foundational requirements by assessing the current status of the four functional pillars of vulnerability management: (a) asset identification; (b) assessment; (c) remediation; and (d) monitoring. During this phase, the Protection Motivation Theory (PMT) is applied to establish a behavioral baseline of the practitioners' threat and coping appraisals, ensuring the framework addresses both technical latencies and human motivational barriers.

2. Design and Development Phase

In this phase, the framework's modular architecture is iteratively constructed. Based on the requirements elicited in the relevance phase, the study engineers four core components:

a) Vulnerability Knowledge Base. For aggregating multi-source threat intelligence.
b) Automated Scanning Engine. For continuous and lightweight discovery.
c) Context-Aware Prioritization Module. For calculating adaptive risk scores using CVSS, EPSS, and KEV metrics.
d) Standardization Layer. For automating remediation workflows and ticket routing.

During construction, the Technology Acceptance Model (TAM) serves as a design lens to optimize the framework for Perceived Usefulness (PU) and Perceived Ease of Use (PEOU), ensuring the resulting system minimizes analyst friction

3. Rigor and Validation Phase

The final phase evaluates the artifact's validity through a dual-track empirical approach. The technical validity is assessed by cybersecurity experts to ensure the framework's functionality and completeness using Lawshe's Content Validity Ratio (CVR). Simultaneously, the behavioral validity is measured through IT practitioners who evaluate the framework's usability and applicability to daily systems operations. This ensures that the finalized VMF is not only scientifically grounded in established security theories but also operationally viable for institutional adoption.

Data Gathering Techniques

This section describes the specific data gathering techniques utilized to develop and validate the Vulnerability Management Framework (VMF) for the systems operations of Pangasinan State University, Binmaley Campus. These methods ensure that the study is grounded in the operational realities of the institution while meeting the rigorous scientific standards for artifact validation within a Design Science paradigm.

1. Interviews with Systems Operations Personnel

Structured interviews were conducted with the IT personnel and systems administrators of the campus to obtain qualitative insights into the current status of vulnerability management practices. These sessions focused on identifying existing procedures for (a) asset identification, (b) assessment, (c) remediation, and (d) monitoring. By utilizing an interview guide, the researcher gathered detailed accounts of operational bottlenecks, such as legacy scanning latencies and fragmented ownership of remediation tasks.

Furthermore, these interviews served as the baseline for Protection Motivation Theory (PMT) analysis. The responses provided data on the practitioners' threat appraisals (perceived severity of cyber risks) and coping appraisals (perceived self-efficacy in managing vulnerabilities), ensuring that the developed framework addresses both technical gaps and human motivational barriers within the University's environment.

2. Technical Infrastructure and Document Review

To support the DSRM Design Cycle, a systematic review of the University's technical documentation and systems architecture was performed. This involved analyzing existing network maps, asset inventories, and historical vulnerability logs from administrative offices, such as the Registrar and Accounting departments.

This technique provided the necessary technical intelligence to engineer the framework's four core modules: the Vulnerability Knowledge Base, Scanning Engine, Prioritization Module, and Standardization Layer. The review ensured that the framework is interoperable with PSU Binmaley's existing operating systems and hardware specifications, allowing for a context-aware approach that weights technical severity against institutional asset criticality.

3. Survey with Cybersecurity Experts

A structured survey was conducted with a panel of cybersecurity experts to establish the

technical validity of the developed artifact. This instrument was designed to evaluate the framework's technical logic. Cybersecurity Experts were instructed to answer Section 2, Items 2 (Functionality) and 3 (Completeness) only, utilizing a three-point essentiality scale: [Essential], [Useful but not essential], and [Not necessary]. This specific scaling was implemented to provide the necessary values (number of 'essential' ratings) required for the Lawshe Content Validity Ratio (CVR).

The gathered data was analyzed using Lawshe's Content Validity Ratio (CVR) to confirm that every lifecycle stage and technical indicator included in the VMF is "essential" for institutional security governance.

4. Survey with IT Practitioners

To evaluate the framework's behavioral validity, a survey was administered to IT practitioners at the University who are responsible for daily systems operations. This technique utilized the Technology Acceptance Model (TAM) to measure the framework's operational suitability. IT Practitioners were instructed to answer Section 2, Items 4 (Usability) and 5 (Applicability) only, while disregarding the technical logic assessments in Items 2 and. The survey used a five-point Likert scale, as shown in Table 1.0 below, to quantify the respondents' agreement with each statement regarding the VMF.

Table 1.0: Likert Scale for VMF Survey.

Scale	Description
5	Strongly Agree
4	Agree
3	Neutral
2	Disagree
1	Strongly Disagree

The questionnaire quantified the practitioners' Perceived Usefulness (PU) and Perceived Ease of Use (PEOU) regarding the framework's automated workflows and prioritization logic. This data gathering step is essential for determining the behavioral intention of the staff to adopt the framework into their daily routines, ensuring the artifact transitions from a theoretical model to an operationally adopted governance engine.

To ensure that the development and validation of the framework are grounded in both technical rigor and practitioner acceptance, several data gathering methods were synchronized throughout the project.

The gathered quantitative data was analyzed to determine the overall perception of the framework's effectiveness. Additionally, open-ended portions of the survey and qualitative insights from stakeholder interviews were analyzed using Reflexive Thematic Analysis, following the six-phase approach of Braun and Clarke (2006). This process allowed for the identification of recurring patterns and actionable recommendations, which were then used to refine the modular architecture of the VMF.

The following figure illustrates how these techniques were applied across the development cycles, linking each research phase to its corresponding source of empirical data.



Figure 3.0 – VMF Data Gathering and Validation Flow

Figure 3.0 illustrates the strategic flow of data collection throughout the research. The initial phase utilizes stakeholder interviews and infrastructure reviews to define the environmental and behavioral baseline. This data serves as the input for the iterative construction of the framework modules. The final phase shifts toward empirical validation, using specialized surveys to gather

expert technical ratings and practitioner usability metrics, culminating in the Vulnerability Management Framework.

Statistical Treatment of Data

To establish the empirical validity of the framework, the study utilized two primary statistical measures. Technical functionality and completeness were quantified using Lawshe's Content Validity Ratio (CVR) to measure expert consensus, while institutional usability and applicability were determined through the Modal Value to identify the most frequent practitioner responses. The statistical analysis followed the branched structure of the survey instrument. Lawshe's CVR was applied exclusively to the expert data gathered from the three-point essentiality scale in Q2 and Q3 to prove technical validity. Conversely, the Modal Value was applied exclusively to the practitioner data gathered from the five-point Likert scale in Q4 and Q5 to determine the prevailing behavioral sentiment regarding usability and applicability.

1. Lawshe's Content Validity Ratio (CVR)

The CVR is a linear transformation of a proportional level of agreement on how "essential" a specific component of the framework is. It ensures that the modular architecture is technically robust and covers the necessary stages of the vulnerability lifecycle. Lawshe's Content Validity Ratio together with a sample computation is provided in Figure 4.0 below.

$$CVR = \frac{N_e - (\frac{N}{2})}{N/2}$$

Figure 4.0 – Lawshe's Content Validity Ratio (CVR) formula

Where:

CVR= Content Validity Ratio.

N_e= Number of experts rating a framework module as "Essential."

N= Total number of experts in the validation panel.

In this study, the validation panel consists of 6 cybersecurity experts. If all 6 experts rate the Vulnerability Management Chaining (VMC) logic as "Essential," the computation is as follows:

$$CV\ R = \frac{6 - \frac{6}{2}}{\frac{6}{2}}$$

$$CV\ R = \frac{6 - 3}{3}$$

$$CV\ R = \frac{3}{3} = 1.0$$

A CVR of 1.0 indicates perfect consensus among the experts, validating the logic as essential for institutional governance.

2. Modal Value

The Modal Value was utilized to analyze the behavioral evaluations from IT practitioners. The Mode identifies the most frequent score on the five-point Likert scale in table 1.0, representing the prevailing institutional sentiment regarding the framework's ease of use and adoption potential.

If the IT practitioners provided the following set of Likert scores for the automated ticket routing workflow: {5, 5, 5, 5, 4, 4, 3}

Scale 5 (Strongly Agree): 4 occurrences
Scale 4 (Agree): 2 occurrences
Scale 3 (Neutral): 1 occurrence

The Modal Value is 5, indicating that the practitioners "Strongly Agree" that the framework successfully reduces analyst friction and alert fatigue within the campus systems operations.

RESULTS AND DISCUSSIONS

This chapter presents the findings gathered from the structured interviews and validation surveys regarding the development and validation of the Vulnerability Management Framework (VMF) for the systems operations of Pangasinan State University, Binmaley Campus. It

discusses the interpretation of these findings in relation to the research objectives and the technical literature that grounds the artifact's architecture.

Data Analysis and Interpretation

The data gathered from interviews with the campus IT personnel and technical document reviews reveal critical insights into the operational environment. The findings highlight a predominantly reactive posture toward security, characterized by significant gaps in centralized asset discovery, prioritization intelligence, and structured remediation workflows. These findings served as the "Relevance Cycle" inputs for the construction of the governance engine.

Analysis of the Current Status of Vulnerability Management Practices

The assessment of the University's current systems operations focuses on the four functional pillars of the management lifecycle. The data illustrates a fragmented landscape where security tasks are often performed in siloes, leading to significant visibility gaps across the campus's digital attack surface.

Operational Gaps in Technical Lifecycle Pillars In terms of Asset Identification and Inventory

The analysis reveals a lack of real-time, centralized visibility. While departments such as the Registrar and Accounting offices maintain records of their local workstations, there is no automated mechanism to track configuration drift or the presence of "Shadow IT" devices connecting to the campus network. This fragmentation prevents the IT team from establishing an authoritative baseline for protection, as they cannot secure assets that are not formally cataloged.

Vulnerability Assessment and Detection

The current status is characterized by "point-in-time" scanning models. Assessments are performed on a periodic or quarterly basis, which fails to account for the speed of modern exploitation where flaws are weaponized within hours of public disclosure. Furthermore, the detection process relies heavily on unauthenticated network scans, which provide only a surface-level view of vulnerabilities and miss deeper configuration errors within the University's primary database servers.

Vulnerability Remediation and Mitigation

This pillar represents the most significant operational bottleneck. Current prioritization is driven solely by static Common Vulnerability Scoring System (CVSS) scores. This leads to a state of "false urgency," as IT practitioners are forced to remediate "High" severity findings that may not have an available exploit path in the University's specific environment. Conversely, vulnerabilities with lower scores that are being actively exploited in the wild remain unaddressed. This misallocation of resources is exacerbated by a siloed ownership structure, where security identification is disconnected from the operational teams responsible for patching.

Monitoring and Reporting

This pillar is largely ad-hoc, with no structured feedback loops to verify if patches were applied successfully or to track compliance with institutional Service Level Agreements (SLAs). Reporting consists primarily of raw technical summaries that lack the context-aware intelligence needed by University leadership to make informed, risk-based decisions regarding institutional resilience.

Behavioral Appraisal and Motivational Drivers (PMT Analysis)

Applying Protection Motivation Theory (PMT), the study captured the "human element" of the University's security posture. The findings indicate a high threat appraisal among practitioners; staff are acutely aware of the severity of cyber threats such as ransomware and data breaches affecting the education sector. However, this is countered by a critically low coping appraisal. Practitioners expressed those current manual processes and the lack of automated prioritization tools make them feel ineffective in managing the escalating volume of alerts. This identifies a "broken culture" where alert fatigue leads to a decrease in defensive follow-through, confirming that a technical solution alone is insufficient without behavioral alignment as shown in table 2.0 on the next page.

Table 2.0: Current Status Assessment of Vulnerability Management Pillars at PSU Binmaley

Functional Pillar	Current Practice Model	Identified Operational Gaps	Institutional Impact
Asset Identification	Localized spreadsheets/manual tracking	No real-time visibility; existence of unmanaged "Shadow IT"	**High Risk** Systemic blind spots in the attack surface.
Assessment & Detection	Periodic, point-in-time scanning (Quarterly)	Structural lag; inability to detect weaponized flaws between scans	**Critical Risk** Extended window of exposure (197+ days).
Remediation & Mitigation	CVSS-only prioritization; manual patching	False urgency; misallocation of personnel toward low-impact alerts	**High Risk** Mission-critical databases remain unpatched.
Monitoring & Reporting	Ad-hoc technical summaries; no validation	Lack of feedback loops; absence of SLA tracking and risk trends	**Medium Risk** Inability to quantify risk reduction progress.

The synthesis of these findings establishes that the University's current management model is no longer structurally adequate for the modern threat landscape. The reliance on static, manual procedures in an increasingly complex digital environment has created a defensive gap that can only be closed through an automated, context-aware governance engine

Developed Vulnerability Management Framework for Pangasinan State University, Binmaley Campus

The formulation of the Vulnerability Management Framework (VMF) was driven by the necessity to resolve the systemic latencies and "structural lag" identified during the baseline assessment of the University's systems operations. Utilizing the Design Science Research Methodology (DSRM) Design Cycle, the framework was engineered as a modular, context-aware governance engine that replaces the institution's reactive, point-in-time scanning model with a continuous and predictive remediation pipeline. This architecture is designed to address the "vulnerability paradox" by focusing limited IT resources on the small fraction of security flaws that pose a legitimate, weaponized threat to mission-critical academic and administrative databases, such as those housed in the Registrar and Accounting offices.

The core of the developed framework is anchored on the principle of Vulnerability Management Chaining (VMC), which employs a two-stage evaluation logic to filter institutional risk. In the first stage, the framework ingests multi-source threat intelligence, specifically the Cybersecurity and Infrastructure Security Agency (CISA) Known Exploited Vulnerabilities (KEV) catalog and the Exploit Prediction Scoring System (EPSS). This allows the system to prioritize vulnerabilities that have a high probability of exploitation or documented evidence of active use in the wild, regardless of their technical severity score. The second stage applies a context-aware lens, weighting the Common Vulnerability Scoring System (CVSS) metrics against the specific criticality of PSU Binmaley's assets. This ensures that a vulnerability affecting a public-facing enrollment server is treated with higher urgency than an identical flaw on an isolated departmental workstation. By mathematically integrating threat likelihood with asset-specific impact, the framework provides an 18-fold efficiency improvement, effectively reducing the urgent remediation workload

The framework's functional architecture is organized into four interoperable modules that support the entire management lifecycle.

a) The Vulnerability Knowledge Base acts as the intelligence core of the framework, centralizing technical data from the National Vulnerability Database (NVD) with dynamic, real-world signals from the

Exploit Prediction Scoring System (EPSS) and CISA's Known Exploited Vulnerabilities (KEV) catalog. This module addresses the "fragmentation gap" by correlating static severity scores with empirical likelihood data, ensuring that the University's defense is informed by current exploitation trends rather than environmental vacuums. By providing a unified, queryable schema, it transforms dispersed threat data into actionable institutional intelligence, allowing IT personnel to maintain a single source of truth for the entire threat landscape.

b) The Automated Scanning Engine operationalizes continuous detection across the campus's hybrid digital environment, utilizing both authenticated and unauthenticated discovery methods to maintain real-time asset visibility. Unlike traditional models that rely on periodic assessments, this engine eliminates structural blind spots by identifying newly disclosed vulnerabilities and configuration drifts the moment they emerge within the network infrastructure. It orchestrates multi-vector discovery to ensure that high-value systems remain under constant oversight, effectively removing the 197-day exposure window documented in legacy point-in-time scanning cycles.

c) The Context-Aware Prioritization Module serves as the framework's decision engine, mathematically weighting technical severity against the specific institutional criticality of PSU Binmaley's assets. It utilizes Vulnerability Management Chaining (VMC) logic to perform a two-stage evaluation: first filtering for threat likelihood via KEV and EPSS thresholds, and then applying asset-specific impact scores. This allows the University to achieve an 18-fold efficiency improvement by de-prioritizing the approximately 95% of vulnerabilities that lack a viable exploit path in its specific environment. By focusing resources on the "needle in the needle stack," this module ensures that critical enrollment and financial databases receive prioritized protection.

The Standardization and Interoperability Layer closes the operational execution gap by translating prioritized technical intelligence into automated workflows and ticket routing protocols. it standardizes communication between security identification tasks and the IT personnel responsible for remediation, assigning clear ownership and tracking Service Level Agreement (SLA) compliance for "Critical" and "High" priority findings. This layer is optimized for the Technology Acceptance Model (TAM) to ensure that automated remediation tasks are perceived as useful and easy to integrate into daily systems operations. By automating the transition from discovery to verification, this module eliminates manual administrative bottlenecks and fosters institutional accountability.

Table 3.0: Architectural Components and Functional Outputs of the Developed VMF

Framework Module	Integrated Intelligence & Theory	Institutional Functional Output	Operational Value for PSU Binmaley
Vulnerability Knowledge Base	NVD (CVE), EPSS Percentiles, CISA KEV Flags	Unified, queryable repository of multi-source threat intelligence.	Resolves fragmented intelligence and eliminates manual data correlation.
Automated Scanning Engine	Continuous Discovery, Authenticated Agents	Lightweight, real-time discovery of all connected campus assets.	Eliminates the 197-day "structural lag" of periodic scanning.
Context-Aware Prioritization Module	VMC Logic, Decision Tree, Asset Criticality	Adaptive risk scoring based on likelihood and institutional impact.	Focuses resources on the "needle in the needle stack" (top 3% of risks).
Standardization & Reporting Layer	TAM Design, SLA Tracking, Automated Ticketing	Automated remediation workflows and executive risk-trend reporting.	Reduces analyst friction and ensures accountability through shared ownership.

Nexus Global Research Journal of Multidisciplinary
Journal Homepage: https://nexusglobalresearch.com/journal/ngrjm/

The synthesis of these survey results demonstrates that the VMF achieved a high degree of technical and behavioral alignment. The expert ratings established that the modular architecture is technically robust enough to produce an 18-fold efficiency improvement in institutional workflows. Simultaneously, the practitioner feedback confirmed that the framework's user-centric design effectively addresses the human motivational barriers to security enforcement.

Ultimately, the validation results prove that the Vulnerability Management Framework provides a statistically significant advancement over the University's previous reactive model. By satisfying the requirements for both scientific completeness and operational usability, the artifact is validated as a sustainable governance engine capable of fortifying the campus's cybersecurity posture while fostering a security-first institutional culture.

Discussion of Findings

This section presents the key findings derived from the study, analyzing how the developed Vulnerability Management Framework (VMF) addresses the identified operational gaps, integrates dynamic threat intelligence, and meets the technical and behavioral requirements of the systems operations at Pangasinan State University, Binmaley Campus, based on expert validation and practitioner evaluations

Analysis of the Current Status of Vulnerability Management Practices

The findings concerning the operational landscape of Pangasinan State University, Binmaley Campus, reveal a critical defensive gap characterized by a predominantly reactive and fragmented approach to security governance. This current status is defined by what is known as the "vulnerability paradox," where the institution is forced to manage a staggering volume of disclosed security flaws without the context-aware intelligence necessary to identify the small fraction of threats that pose a legitimate risk to campus operations. The analysis indicates that the University's systems operations are currently functioning under a "point-in-time" security model, treating vulnerability management as a periodic project rather than a continuous lifecycle. This misalignment results in a significant structural lag, leaving mission-critical systems exposed for extended periods, often exceeding the industry-documented average detection window of 197 days.

In terms of Asset Identification and Inventory, the study finds that the University lacks a centralized, real-time repository of its digital attack surface. Currently, departmental offices, such as the Registrar and Accounting, utilize localized spreadsheets and manual tracking methods to manage their workstations and servers. This fragmentation leads to systemic blind spots, as there is no automated mechanism to detect "Shadow IT" devices or track configuration drift when new hardware is introduced to the campus network. Without an authoritative and continuous inventory, the IT personnel face a fundamental barrier to protection, as it is impossible to secure assets that have not been formally identified. As illustrated in Table 2.0, this pillar is currently categorized as a "High Risk" area, as the lack of visibility directly facilitates the potential for unauthorized access to sensitive academic and financial databases.

Regarding Vulnerability Assessment and Detection, the practices at PSU Binmaley are hindered by a reliance on legacy, network-bound scanning models that occur only on a periodic or quarterly basis. These snapshots fail to keep pace with the modern threat landscape, where vulnerabilities are often weaponized by attackers within hours of public disclosure. The findings suggest that the University is currently operating with a "detection lag," where newly disclosed flaws remain unaddressed in the intervals between scheduled scans. Furthermore, the detection process is often unauthenticated, providing only a surface-level view of the attack surface while missing deeper, high-impact misconfigurations within the primary database servers. This reactive posture ensures that the systems operations team is constantly in a state of "firefighting," reacting to threats long after the window for proactive mitigation has closed.

The Vulnerability Remediation and Mitigation pillar represents the most significant operational bottleneck within the campus's IT infrastructure. Currently, prioritization is driven exclusively by static technical severity scores provided by the Common Vulnerability Scoring System (CVSS). This reliance creates a state of "false urgency," as IT practitioners are compelled to allocate limited personnel hours to "High" or

*Corresponding Author: Nelson O. Rosario,
Received: 15Aug 2026 | Accepted: 30 Aug 2026 | Published: 05 Sep 2026
Copyright © 2026 The Author(s): This work is licensed under a Creative Commons Attribution- Non-Commercial-No Derivatives 4.0 (CC BY-NC-ND 4.0) International License

"Critical" findings that may not even have a viable exploit path in the University's specific environment. Conversely, vulnerabilities with lower technical scores that are being actively exploited in the wild remain unaddressed, leaving mission-critical databases unpatched. As highlighted in Table 2.0, this misallocation of resources constitutes a "High Risk" to institutional resilience, as the siloed ownership structure—where security identification is disconnected from the operational authority to apply patches—further degrades the institutional fix rate.

The status of Vulnerability Monitoring and Reporting is characterized as ad-hoc and documentation-light. There are currently no structured feedback loops to verify the success of remediation tasks or to track compliance with institutional Service Level Agreements (SLAs). Reporting typically consists of raw technical summaries that lack the context-aware intelligence needed by University leadership to make informed, risk-based decisions. This absence of continuous monitoring prevents the institution from identifying recurring security trends or measuring its overall risk reduction progress over time. Behavioral findings integrated into this analysis further reveal that practitioners experience high "alert fatigue," feeling ineffective due to the volume of manual triaging required. This combination of technical latency and behavioral friction confirms that the current practice model is no longer structurally adequate to protect the University's expanding digital ecosystem.

Developed Vulnerability Management Framework for Pangasinan State University, Binmaley Campus

The findings regarding the development of the framework establish a paradigm shift for the University's systems operations, moving from an ad-hoc, manual triaging model to an automated, context-aware governance engine. The architectural formulation of this artifact was specifically engineered to resolve the "vulnerability paradox" and the 197-day structural lag identified during the baseline assessment. By utilizing the iterative cycles of Design Science, the framework provides a technical bridge between raw threat data and institutional action, ensuring that defensive resources are allocated based on real-world risk rather than static, environmental-blind severity scores. This development represents a move toward institutional resilience through predictive intelligence and structured remediation pipelines.

The core innovation of the framework lies in its Vulnerability Management Chaining (VMC) logic, which introduces a two-stage evaluation process to filter the University's digital attack surface. As detailed in the findings, the framework first applies threat-based filtering by ingesting dynamic signals from the EPSS and CISA KEV catalogs to determine the likelihood of exploitation. Only after a vulnerability is confirmed as a legitimate threat does the framework evaluate its technical severity via CVSS and its impact on mission-critical assets. This logic allows the University to achieve an 18-fold efficiency improvement, mathematically demonstrating that the IT team can reduce its urgent remediation workload by approximately 95% while still maintaining coverage of the most dangerous, weaponized threats to the campus infrastructure.

The framework's functional capacity is operationalized through four interoperable modules, each designed to close a specific gap found in the University's current status. The Vulnerability Knowledge Base serves as the unified repository for multi-source intelligence, eliminating the fragmentation of data across localized departmental spreadsheets. The Automated Scanning Engine replaces periodic, point-in-time snapshots with continuous, authenticated discovery, ensuring that new devices and configuration drifts in the Registrar and Accounting offices are identified in real-time. The Context-Aware Prioritization Module acts as the framework's decision engine, weighting technical flaws against the institutional value of the University's databases. Finally, The Standardization and Interoperability Layer automates the transition from detection to action by routing prioritized tickets and tracking Service Level Agreement (SLA) compliance. The functional outputs and operational values of these modules are summarized in Table 2.0, illustrating how each component contributes to a proactive security posture.

Beyond the technical engineering, the development findings highlight a strong emphasis on user-centric design through the application of the Technology Acceptance Model (TAM). By automating the most labor-intensive stages of the management lifecycle—specifically intelligence correlation and ticket routing—the framework directly addresses the behavioral barriers of alert fatigue and low coping appraisal reported by staff. The inclusion of explainable risk scores ensures that IT practitioners can justify security priorities to University leadership, transforming vulnerability management from an isolated IT task into a transparent governance process. This synthesis of

technical rigor and behavioral alignment ensures that the developed framework is not merely a theoretical model but an operationally viable engine capable of significantly improving the University's Mean Time to Detect (MTTD) and Mean Time to Remediate (MTTR) metrics.

Validity of the Developed Vulnerability Management Framework as Evaluated by Experts and Practitioners

The empirical validity of the Vulnerability Management Framework (VMF) was established through a dual-track assessment designed to bridge the gap between theoretical security modeling and institutional adoption. This process measured the technical integrity of the modular architecture and the behavioral intention of campus personnel to adopt the framework into their daily routines.

The technical track focused on Functionality and Completeness, as evaluated by a panel of cybersecurity experts using Lawshe's Content Validity Ratio (CVR). The results for Functionality (Question 2) yielded a perfect CVR of 1.0, indicating total expert consensus that the Vulnerability Management Chaining (VMC) logic is essential for institutional governance. Experts validated that the mathematical filtering of threat likelihood via EPSS and CISA KEV prior to technical severity assessment is technically robust enough to resolve the 197-day structural lag identified in the campus's reactive status . Furthermore, the assessment of Completeness (Question 3) yielded a perfect CVR of 1.0, indicating unanimous expert consensus that the four-module architecture comprehensively covers the entire vulnerability lifecycle.. The panel concluded that the structural integration of the Knowledge Base, Scanning Engine, Prioritization, and Standardization modules is essential for closing the 'execution loop' and resolving the fragmented visibility found in the University's current status.

The behavioral track established the framework's Usability and Applicability based on the Technology Acceptance Model (TAM). The findings for Usability (Question 4), which received a modal response of 5 (Strongly Agree), demonstrate that the framework's explainable risk scores effectively mitigate the "alert fatigue" and "analyst friction" previously hindering the systems operations team. Practitioners affirmed that the artifact is practically relevant to the Applicability (Question 5) needs of the Registrar and Accounting offices, noting that the VMF is capable of handling complex system dependencies without the operational latency found in periodic scanning models

Chapter VI
CONCLUSIONS AND RECOMMENDATONS

This chapter presents the key conclusions derived from the study's findings and provides actionable recommendations to enhance the Vulnerability Management Framework's (VMF) implementation and effectiveness.

Conclusions

A Risk-Based Vulnerability Management Framework (VMF) was successfully developed and validated for the systems operations of Pangasinan State University, Binmaley Campus, with the "vulnerability paradox" and the 197-day structural detection lag identified as the most critical operational barriers. Grounded in the Design Science Research Methodology (DSRM) and utilizing Vulnerability Management Chaining (VMC) logic, the framework provides a structured, risk-based governance engine to enhance institutional cybersecurity resilience. By addressing existing preparedness gaps and prioritizing weaponized threats through dynamic intelligence, the VMF positions the University for more robust response and mitigation capabilities against evolving digital disruptions.

Designed to resolve fragmented asset visibility and the limitations of static technical scoring, the framework centers on four interoperable modules that cover the complete management lifecycle from discovery to standardized monitoring. Grounded in DSRM iterative cycles and supported by multi-source intelligence feeds from EPSS and CISA KEV, the VMF presents structured remediation procedures and adaptive risk metrics that significantly enhance the institution's defensive readiness. While full institutional implementation depends on future resource allocation for automated scanning agents, the framework provides a practical and scalable foundation for minimizing the campus's digital attack surface and ensuring the continuity of core academic and administrative services.

The Vulnerability Management Framework tailored to the systems operations of PSU Binmaley was successfully validated through a dual-track assessment involving cybersecurity experts and IT practitioners. Through this expert and stakeholder evaluation, the VMF was certified by experts as technically essential (CVR: 1.0) and confirmed by practitioners as operationally usable and applicable in addressing the most significant risks—specifically those targeting mission-critical

enrollment and financial databases. While recommendations remain for the future integration of machine learning to further automate threshold adjustments, the framework provides a solid foundation for improving institutional resilience and fostering a security-first culture within the University's systems operations.

The Risk-Based Vulnerability Management Framework designed in this study satisfied every Lawshe CVR threshold and every Good & Scates acceptability criterion, and is operationally feasible at the scale of a single-campus SUC. The artefact is mapped to RA 10173, the DICT NCSP 2023–2028, NIST SP 800-30 Rev. 1, NIST SP 800-40 Rev. 4, ISO/IEC 27005:2022, and CIS Critical Security Controls v8.1, fulfilling the mandatory regulatory overlay for State Universities and Colleges.

Recommendations

Support for Automated Infrastructure. It is recommended that the University administration provide the necessary resources for the full deployment of automated vulnerability scanning agents across the campus network. Implementing automated scanning will reduce delays in vulnerability discovery and enable continuous monitoring of the University's information systems.

Staff Training and Capacity Building. The University should conduct regular training programs, workshops, and certification opportunities for campus IT personnel and designated IT focal persons. These initiatives should strengthen technical competencies in vulnerability assessment, risk prioritization, incident response, and the implementation of the proposed Vulnerability Management Framework.

Synchronization with Dynamic Threat Intelligence. The Systems Operations Team should maintain continuous synchronization of the Vulnerability Knowledge Base with trusted threat intelligence sources to ensure that newly discovered vulnerabilities and actively exploited threats are promptly identified and prioritized.

Establishment of Service Level Agreements (SLAs). The University should establish formal Service Level Agreements (SLAs) that define clear remediation responsibilities and response timelines. Recommended remediation windows include immediate action for critical vulnerabilities (within 24–72 hours), remediation of high-risk vulnerabilities within seven days, medium-risk vulnerabilities within thirty days, and low-risk vulnerabilities within ninety days, subject to operational requirements and risk acceptance.

Compliance with Security and Privacy Standards. The proposed Vulnerability Management Framework should be continuously reviewed and updated to ensure alignment with the Data Privacy Act of 2012 (Republic Act No. 10173), as well as internationally recognized cybersecurity standards and best practices such as the NIST Cybersecurity Framework and ISO/IEC 27001. Regular policy reviews and compliance assessments should be conducted to strengthen information security governance.

Performance Evaluation. The University should conduct a longitudinal evaluation at least six months after the framework's implementation to assess improvements in key performance indicators such as Mean Time to Detect (MTTD), Mean Time to Remediate (MTTR), vulnerability resolution rates, and overall cybersecurity posture.

Future Research. Future researchers may extend this study by integrating machine learning techniques for automated vulnerability prioritization and predictive risk analysis. They may also evaluate the framework's applicability to cloud computing environments, Internet of Things (IoT) devices, and multi-campus university information systems.

CERTIFICATION OF THE ADVISER

This capstone project entitled, "DEVELOPMENT AND VALIDATION OF A RISK-BASED VULNERABILITY MANAGEMENT FRAMEWORK FOR SYSTEMS OPERATION OF PANGASINAN STATE UNIVERSITY". Prepared and submitted by **NELSON ROSARIO**, in partial fulfillment of the requirements for the degree of **MASTER IN INFORMATION TECHNOLOGY**, major in **Cyber Security**, has been examined and found to be acceptable in content and form and is hereby recommended for **ORAL DEFENSE**.

BIBLIOGRAPHY:

- Dudar, N. (2025). AI-based vulnerability prioritization: Enhancing cybersecurity risk management through interpretable models [Bachelor's thesis, University of Twente]. UT Student Theses.

https://essay.utwente.nl/fileshare/file/108115/Dudar_BA_EEMCS.pdf

- Janjal, A. (2026). A GovSecOps-oriented governance, risk, and compliance platform for continuous authorization in DoD IL4/IL5 environments. Journal of Cybersecurity Education, Research and Practice, 8(1). https://digitalcommons.kennesaw.edu/jcerp/vol8/iss1/1/
- Jiang, Y., Oo, N., Meng, Q., Lim, H. W., & Sikdar, B. (2025). A survey on vulnerability prioritization: Taxonomy, metrics, and research challenges. arXiv preprint arXiv:2502.11070v1. https://arxiv.org/abs/2502.11070
- Kabenge, J. (2024). Vulnerability management: Towards better vulnerability prioritisation, an automated proof of concept [Master's thesis, Stockholm University]. DiVA Portal. https://su.diva-portal.org/smash/get/diva2:1955777/FULLTEXT01.pdf
- Malkawi, M., & Alhajj, R. (2026). AI-powered vulnerability detection and patch management in cybersecurity: A systematic review of techniques, challenges, and emerging trends. Machine Learning and Knowledge Extraction, 8(1), 19. https://doi.org/10.3390/make8010019
- NRI Secure. (2026, January 5). The 7 stages of vulnerability management lifecycle. NRI SecureTechnologies Blog. https://www.nri-secure.com/blog/how-to-build-a-proactive-vulnerability-management-strategy
- Rivas Bustos, D. F., Gutierrez, J. A., & Rueda, S. J. (2026). Automated vulnerability scanning and prioritisation for domestic IoT devices/smart homes: A theoretical framework. Electronics, 15(2), 466. https://doi.org/10.3390/electronics15020466
- Safe Security. (2025). Vulnerability management framework. Safe Security Insights. https://safe.security/resources/insights/vulnerability-management-framework/
- SentinelOne. (2025, August 28). What is vulnerability management framework? SentinelOne Cybersecurity 101. https://www.sentinelone.com/cybersecurity-101/cybersecurity/vulnerability-management-framework/
- Shimizu, N., & Hashimoto, M. (2025). Vulnerability management chaining: An integrated framework for efficient cybersecurity risk prioritization. arXiv preprint arXiv:2506.01220v3. https://arxiv.org/abs/2506.01220
- Team NetSPI. (2023, June 27). Vulnerability management: Identifying the needle in the needle stack. NetSPI Blog. https://www.netspi.com/blog/technical/vulnerability-management/identifying-the-needle-in-the-needle-stack/
- Tenable Research. (2024). Predictive prioritization: Focusing on the vulnerabilities that matter. Tenable Technical Report. https://lookbook.tenable.com/predictive-prioritization/
- Vectra AI. (2025). Vulnerability management: How it works and how security teams reduce exploitable risk. Vectra AI Fundamental Guide. https://www.vectra.ai/topics/vulnerability-management
- Wiz Experts Team. (2026, March 6). Vulnerability management lifecycle: 6 essential stages. Wiz Academy. https://www.wiz.io/academy/vulnerability-management/vulnerability-management-lifecycle