A Proactive Cyber Asset Discovery Framework for Enhancing Vulnerability Management and Cyber Risk Governance

Syaiful Andy[1]

[1] Telkom Corporate University, Jakarta, Indonesia
syaifulandy@gmail.com

Abstract. The rapid expansion of digital transformation initiatives has increased organizational exposure to cybersecurity risks through unmanaged, undocumented, or insufficiently governed cyber assets. In this study, shadow IT is specifically scoped as technically discoverable cyber assets, such as IP-addressed systems, domains, subdomains, applications, and reachable services that are active but not properly registered within formal asset inventory or vulnerability assessment coverage. Traditional vulnerability assessment practices are often request-driven, relying on assets formally submitted by system owners, which may leave such assets outside regular security review. This study proposes a proactive cyber asset discovery framework designed to enhance enterprise asset visibility, vulnerability management, and cyber risk governance. The framework is developed by synthesizing established cybersecurity and governance references, including ISO/IEC 27001, NIST Cybersecurity Framework 2.0, CIS Critical Security Controls, and the OWASP Vulnerability Management Guide. The proposed framework consists of five stages: baseline asset identification, proactive asset discovery, asset gap analysis, vulnerability assessment, aggregation, and prioritization, and governance integration and lifecycle decision-making. By integrating proactive discovery, vulnerability aggregation, remediation consolidation, and asset lifecycle governance, the framework supports compliance readiness, audit evidence, cyber risk governance, and cyber resilience. This study contributes a practical and governance-oriented design framework for transitioning from request driven vulnerability assessment toward proactive and accountable cyber risk management.

Keywords: Cyber Asset Discovery; Vulnerability Management; Shadow IT; Cyber Risk Governance; Cyber Resilience

1 Introduction

Digital transformation has accelerated the deployment of digital services across modern organizations. Business units increasingly rely on web applications, internal dashboards, application programming interfaces, cloud-connected platforms, remote access services, and other network-reachable systems to support operational

A. Sobandi and E. Suryadi (eds.), *Proceedings of the International Conference on Digital Transformation in Business and Organisations (ICDTBO 2026)*, Advances in Economics, Business and Management Research 400,
https://doi.org/10.2991/978-94-6239-754-5_9

efficiency and service delivery. While these initiatives create business value, they also expand the organizational cyber asset landscape and increase the need for accurate asset visibility, vulnerability management, and governance accountability.

Recent industry evidence reinforces the urgency of improving cyber asset visibility and vulnerability management. Verizon's 2026 Data Breach Investigations Report highlights that 31% of breaches now start with software vulnerabilities, surpassing stolen credentials as the leading initial access path and indicating a shift toward exploiting vulnerable systems [1]. Similarly, Kaspersky's 2026 Global Report shows that exploits in public-facing applications represented the largest observed initial attack

vector in 2025, accounting for 43.7% of incidents [2]. These findings support the need for organizations to proactively identify exposed assets, assess reachable services, prioritize vulnerabilities, and strengthen risk-based remediation governance.

One challenge in this context is the existence of unmanaged or insufficiently governed cyber assets. Shadow IT has been described as unofficial IT systems, processes, or organizational units developed autonomously within business departments and generally not known, accepted, or supported by the official IT department [3]. From an IT management and governance perspective, prior research emphasizes the need to identify, assess, and control such unofficial IT [3]. However, this study intentionally narrows the scope of Shadow IT to technically discoverable cyber assets, particularly assets associated with IP addresses, domains, subdomains, applications, or reachable services that are active but absent from formal asset inventory, ownership records, or periodic vulnerability assessment coverage.

Traditional vulnerability assessment practices are often request-driven. In this model, cybersecurity teams assess assets that have been formally submitted by system owners or included in an approved assessment scope. Although this approach is useful for known and well-managed systems, it may fail to detect assets that are undocumented, newly deployed, migrated, forgotten, unmanaged, or no longer clearly owned. As a result, organizations may develop a false sense of vulnerability management coverage because assessments are performed only on assets that are already visible to governance processes. This creates an upstream visibility gap: assets that are not known, registered, or assigned to accountable owners may never enter the vulnerability management lifecycle.

Existing standards, guidance, and prior process studies provide important foundations for this problem. Nikumaa's vulnerability management process study reviews several standards, frameworks, guidelines, and process models relevant to vulnerability management, including ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005, Katakri 2020, NIST SP 800-53 Revision 5, CIS Critical Security Controls, OWASP Vulnerability Management Guide, CRR guidance, PwC's vulnerability management perspective, and several operational patching or vulnerability assessment workflows [4]. The key conclusion of the study is that there is no one-size-fits-all vulnerability management process; organizations need to extract best practices from available references and adapt them to their own organizational structure, existing processes, and operational needs [4]. The study also emphasizes that comprehensive asset managementis critical to vulnerability management effectiveness because

missing asset information may lead to incorrect severity classification or delayed mitigation [4].

Building on this foundation, this paper positions proactive cyber asset discovery as an upstream capability that strengthens vulnerability management coverage before vulnerability assessment begins. CIS Critical Security Controls provide relevant practices for inventory and control of enterprise assets and continuous vulnerability management [5]. The OWASP Vulnerability Management Guide supports the repeatable operational structure of vulnerability management through detection, reporting, and remediation cycles [6]. NIST SP 800-115 further supports the technical assessment aspect by providing guidance for conducting information security testing and assessment [7]. Together, these references support the design of a framework that connects asset visibility, vulnerability assessment, reporting, and governance action.

Proactive Cyber Asset Discovery Framework 3

However, in practice, organizations still need an integrated operational workflow that connects proactive identification of unmanaged IP and domain-based assets, comparison against baseline inventory, vulnerability management process, and asset lifecycle governance. This study addresses that integration need by combining complementary governance, control, and vulnerability management practices into a proactive cyber asset discovery framework. The framework further incorporates risk

based follow-up and remediation consolidation so that discovered assets and vulnerability findings can be translated into prioritized governance actions rather than remaining as raw technical findings.

This study proposes a Proactive Cyber Asset Discovery Framework for enhancing enterprise vulnerability management and cyber risk governance. The framework is designed as a practical and governance-oriented model synthesized from established cybersecurity references and prior vulnerability management process research, including ISO/IEC 27001 as discussed in prior vulnerability management literature, NIST Cybersecurity Framework 2.0, CIS Critical Security Controls, NIST technical security assessment guidance, and the OWASP Vulnerability Management Guide [4]–[7], [9]. The proposed framework consists of five stages: baseline asset identification, proactive asset discovery, asset gap analysis, vulnerability assessment, aggregation & prioritization, and governance integration and lifecycle decision.

The key novelty of the proposed framework lies in connecting upstream asset visibility with downstream governance action. The framework compares formally registered assets against proactively discovered assets to identify visibility gaps, maps reachable services, assesses and enriches vulnerability findings, aggregates related CVE-level findings into remediation-oriented work items, and routes the results into ownership validation, remediation tracking, exception handling, access restriction, or decommissioning decisions. This paper addresses the question of how organizations can design a proactive cyber asset discovery framework that improves vulnerability management coverage, reduces remediation noise, and strengthens cyber risk governance. The study contributes a five-stage framework that extends vulnerability management upstream through proactive discovery and asset gap analysis for IP- and domain-based cyber assets, introduces vulnerability aggregation and remediation consolidation to reduce raw CVE-level noise, and connects technical discovery

outcomes with governance mechanisms such as ownership assignment, inventory update, remediation tracking, and lifecycle decision-making. Through these contributions, the framework supports compliance readiness, audit evidence, and cyber resilience by helping organizations transition from request-driven vulnerability assessment toward proactive and accountable cyber risk management.

2 Design Foundations and Scope

2.1 Design Foundation

The proposed framework combines complementary practices from information security governance, cybersecurity risk management, prioritized control safeguards, and vulnerability management process guidance. ISO/IEC 27001 provides the ISMS governance perspective, including defined scope, asset inventory, ownership, and technical vulnerability management. Clause 4.3 emphasizes that an ISMS operates within a defined scope; therefore, ISO 27001 certification should not be interpreted as automatic coverage of all organizational cyber assets. Annex A 5.9 supports maintaining an inventory of information and associated assets with clear ownership, while Annex A 8.8 supports technical vulnerability management through asset inventory, vulnerability monitoring, risk assessment, patching, and accountability [10]. These ISO-related controls support the first stage of the proposed framework by requiring organizations to collect, maintain, and assign ownership over asset information. However, they also raise a practical governance question: whether the declared inventory actually reflects all active IP- and domain-based cyber assets. The proposed framework addresses this question by treating owner-declared asset information as a baseline that must be validated and extended through proactive discovery and asset gap analysis.

To address this visibility and governance gap, NIST CSF 2.0 is used as the cybersecurity risk governance reference. The framework is particularly aligned with the Govern, Identify, Detect, and Respond functions. Govern provides the structure for roles, oversight, policy, and risk-based direction; Identify supports asset and risk understanding; Detect supports the discovery of previously unknown or unmanaged exposure; and Respond supports follow-up actions for unauthorized, vulnerable, or unmanaged assets [11]. CIS Controls v8.1 complements this high-level structure by providing operational safeguards for enterprise asset inventory, active and passive discovery, unauthorized asset handling, vulnerability management, and remediation [5]. The official CIS mapping of CIS Controls v8.1 and CIS Safeguards to NIST CSF 2.0 further supports this alignment by connecting CIS safeguards to CSF functions and outcomes [12]. Finally, the OWASP Vulnerability Management Guide provides the process-level foundation for vulnerability management by structuring activities into repeatable detection, reporting, and remediation cycles, including scoping, asset grouping, prioritization, remediation, false-positive handling, and exception management [6].

Table 1. Design foundations for the proposed framework

Level	Reference	Relevant Concept	Role in the Proposed Farmework
Governance standard	ISO/IEC 27001	ISMS scope, asset inventory, ownership, technical vulnerability management	Supports baseline asset identification, ownership accountability, audit readiness, and vulnerability governance [10].
Cybersecurity framework	NIST CSF 2.0	Govern, Identify, Detect, Respond	Governance aspect for directing technical asset discovery, vulnerability assessment, and follow-up actions. [11]
Control framework	CIS Controls v8.1	Enterprise asset inventory, active/passive discovery, unauthorized asset handling, continuous vulnerability management	Operationalizes asset discovery, vulnerability scanning, remediation, and governance alignment [5].
Vulnerability management process	OWASP OVMG	Detection, reporting, remediation	Supports repeatable vulnerability management workflow [6].

2.2 Scope of Cyber Asset Discovery

This study focuses on technically discoverable cyber assets associated with IP addresses, domains, subdomains, applications, and reachable services. It does not attempt to cover every form of Shadow IT, such as unofficial spreadsheets, manual business processes, or unsanctioned SaaS usage without a discoverable technical footprint. Instead, the framework addresses the subset of Shadow IT that can become unmanaged cyber exposure: active systems, services, applications, or infrastructure that are reachable but absent from formal inventory, ownership records, or periodic vulnerability assessment coverage. These assets may be identified through baseline inventory review, DNS and domain enumeration, public or private IP discovery.

2.3 **Risk Based Follow-up and Remendation Consolidation**

Risk-based prioritization in this framework is used to determine which discovered assets and findings require follow-up first. Unlike conventional vulnerability management, where prioritization mainly determines which vulnerabilities should be patched earlier, prioritization in proactive cyber asset discovery has a broader governance function. It helps determine whether unmanaged or suspected Shadow IT assets should be validated for ownership, remediated, restricted, taken down, decommissioned, or formally included in the asset inventory and vulnerability management scope. This study adapts CISA's risk-based remediation principle into follow-up prioritization by considering asset exposure, known exploitation status, whether exploitation is automatable by adversaries, technical impact, and ownership clarity [8].

For CVE-based findings, known exploitation status, automatable exploitation, and technical impact may be enriched using CISA KEV, EPSS scores, or other credible vulnerability intelligence sources. Technical impact is treated as a categorical assessment of whether exploitation can cause partial or total control, data exposure, or service disruption. When CISA-style technical impact data is unavailable, CVSS impact information may be used as supporting evidence. For non-CVE findings, such as exposed administrative interfaces, risky open services, custom web application vulnerabilities, insecure configurations, or weak access controls, the same principle can be applied using exposure, automation potential, and estimated technical impact. For example, findings from dynamic application security testing, such as SQL injection, cross-site scripting, local file inclusion, remote file inclusion, insecure file upload, or authentication and authorization weaknesses, may not have CVE identifiers but can still be prioritized when they are reachable, exploitable, automatable, or capable of causing meaningful business or technical impact.

The framework also incorporates remediation consolidation to reduce noise. Rather than treating every CVE or technical finding as a separate work item, related finding saffecting the same component, software package, library, runtime version, service, or configuration area are grouped into remediation-oriented actions. This is aligned with OWASP OVMG's grouping and reporting principles [6]. For example, multiple CVEs affecting the same outdated web server version may be aggregated into one remediation recommendation, such as upgrading the affected component to a supported stable version. Similarly, multiple non-CVE findings on the same exposed service may be consolidated into one hardening or access restriction recommendation.

3 Proposed Framework

The proposed framework is designed to connect proactive cyber asset discovery with vulnerability management and cyber risk governance. The framework starts from an owner-declared or formally registered asset baseline, validates that baseline through proactive discovery, identifies visibility gaps, assesses reachable services, enriches and aggregates vulnerability findings, and finally routes the results into governance follow up. The objective is not only to discover unmanaged assets, but also to determine whether each discovered asset should be registered, assigned to an owner, assessed, remediated, restricted, taken down, decommissioned, or included in the organization's recurring vulnerability management scope

The framework consists of five stages: baseline asset identification, proactive asset discovery, asset gap analysis, vulnerability assessment, aggregation, and risk enrichment, and governance integration and lifecycle decision-making. These stages are summarized in Table 2.

Table 2. Proposed proactive cyber asset discovery framework

Stage	Main Input	Core Activities	Main Output
Stage 1: Baseline Asset Identification	Existing asset inventory, CMDB, owner-submitted asset list, domain list, IP ranges, application list	Collect owner-declared assets, identify asset owners, document known domains/IPs/applications, define discovery scope	Baseline asset register and authorized discovery scope
Stage 2: Proactive Asset Discovery	Baseline scope, domains, subdomains, public/private IP ranges, DNS data, network segments	Perform domain/subdomain discovery, IP discovery, active/passive discovery, service identification, and endpoint enumeration (Intranet/Internet)	Discovered asset list and observable service inventory
Stage 3: Asset Gap Analysis	Baseline asset register anddiscovered asset list	Compare declared vs discovered assets, identify unknown/unmanaged assets, classify exposure	Asset visibility gap list
Stage 4: Vulnerability Assessment, Aggregation & Prioritization	Reachable assets and services	Assess CVE and non-CVE findings, enrich with risk signals, group related findings, consolidate remediation recommendations	Risk-enriched and consolidated remediation/follow-up backlog
Stage 5: Governance Integration and Lifecycle Decision	Prioritized asset/finding backlog	Validate ownership, assign follow-up, track remediation, approve exceptions, update inventory, restrict/takedown/decommission assets	Governance actions, updated inventory, remediation evidence, lifecycle decisions

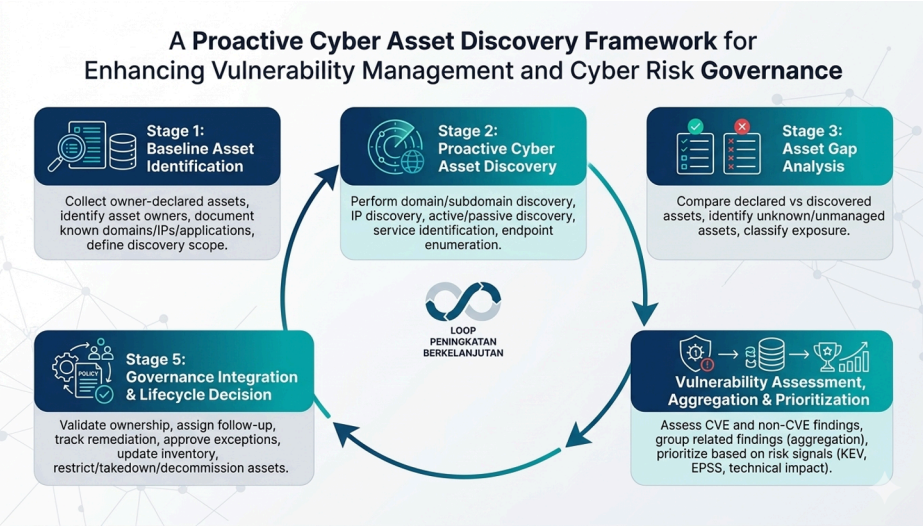

Fig. 1. Five-stage framework for proactive cyber asset discovery and governance integration

4 Implementation Considerations and Discussion

Implementation of the framework depends on the organization's environment, available data sources, authorization boundaries, and governance maturity. In Stage 1, the baseline asset register may be collected from CMDB records, asset inventories, DNS records, IP address management systems, application catalogs, vulnerability assessment scopes, and business unit declarations. This baseline should include at least asset name, owner, business unit, IP address or domain, service purpose, exposure, and environment type.

Stage 2 proactive asset discovery, should combine passive and active reconnaissance. Passive reconnaissance may include DNS review, subdomain enumeration, certificate transparency logs, search engine results, historical DNS, and external exposure intelligence. These results should be treated as candidate evidence because passive sources may contain stale, duplicated, or unreachable assets. Active reconnaissance is then used to validate the candidates through DNS resolution checks, port scanning, service enumeration, HTTP probing, virtual host discovery, and service fingerprinting within authorized scope. A key consideration is that discovery tools complement each other and should not be treated as complete sources of truth. For example, an IP-oriented exposure source may show that a public IP exposes TCP/443, but it may miss multiple web applications hosted behind the same IP through name based virtual hosting, where applications only respond correctly when the appropriate

Host header or TLS Server Name Indication is used. Therefore, IP-based discovery should be combined with DNS/subdomain discovery, certificate transparency analysis, and virtual host probing. The framework does not depend on a single vendor or toolchain; tool outputs are treated as discovery evidence that must be validated, correlated, and compared against the baseline inventory.

In Stage 3 asset gap analysis, discovered assets can be classified into practical categories: known and registered assets, known assets with incomplete metadata, unknown or unmanaged assets, potentially unauthorized assets, and retired or orphaned assets that remain reachable. Service reachability should also be classified, for example as internet-facing, internally reachable, restricted to specific segments, or unexpectedly exposed. This classification helps determine which assets require immediate governance follow-up.

In Stage 4, vulnerability assessment can combine conventional security testing tools with AI-assisted capabilities where appropriate. Vulnerability scanners, DAST tools, configuration assessment tools, and deterministic scripts remain essential for repeatable evidence collection and controlled technical validation. Recent systematic analyses of Agentic and Generative AI for autonomous VAPT observe that generative models can augment evidence reasoning, compliance documentation, and report synthesis, but strictly require deterministic grounding to remain reliable. Challenges also persist in hallucination control, prompt injection, explainability, safety-aware evaluation, benchmark standardization, and trustworthy human-in-the-loop governance [13]. Accordingly, this proposed framework treats scanner results, DAST findings, deterministic scripts, and AI-assisted outputs as raw evidence inputs that must be reviewed, validated, aggregated, and routed through governance workflows before any operational action is taken.

The next step involves vulnerability aggregation and risk enrichment for prioritization CVE-based findings are enriched using CVSS, Exploit Prediction Scoring System (EPSS) scores, and Known Exploited Vulnerability (KEV) intelligence. In this context, KEV intelligence refers to curated repositories identifying CVEs with active real-world exploitation such as the CISA KEV catalog (containing 1,619 CVEs as of June 13, 2026) and Vuln Check KEV (containing 4,957 CVEs). Conversely, non-CVE findings including exposed administrative interfaces, risky open services, insecure configurations, and custom web application vulnerabilities (e.g., SQL injection, XSS, LFI/RFI, and broken authentication) are prioritized based on reachability, automatability, and technical impact. Finally, related CVE and non-CVE findings are consolidated into remediation-oriented actions, such as upgrading an outdated component or hardening an exposed service, to minimize noise and streamline the remediation backlog.

In Stage 5, governance follow-up is driven by the prioritized and consolidated backlog produced in Stage 4. Each prioritized asset or finding is routed to the relevant stakeholder for ownership validation, remediation planning, exposure review, or lifecycle decision-making. A legitimate asset may be registered and included in the recurring vulnerability management scope. A vulnerable asset may require remediation, exposure restriction, or compensating controls. An asset without business justification, unclear ownership, or unacceptable exposure may be taken down, isolated, or decommissioned. When immediate remediation is not feasible, an exception may be approved with documented justification, owner approval, expiration date, and compensating controls. These decisions create audit evidence through updated inventory records, ownership assignments, remediation tickets, exception records, exposure restriction records, and decommissioning evidence.

The framework supports compliance readiness and cyber resilience, but it should not be interpreted as a guarantee of compliance with any specific standard. Its effectiveness depends on inventory quality, discovery coverage, tool accuracy, authorization scope, and organizational responsiveness. Future work should validate the framework through empirical implementation and develop maturity indicators such as asset ownership coverage, percentage of discovered assets added to inventory, vulnerability assessment coverage, mean time to ownership validation, remediation completion rate, exception rate, and decommissioning rate.

5 Conclusion

This paper proposed a proactive cyber asset discovery framework for enhancing vulnerability management and cyber risk governance. The framework addresses the upstream visibility gap that occurs when vulnerability assessment depends primarily on owner-declared or formally registered assets. Through five stages-baseline asset identification, proactive asset discovery, asset gap analysis, vulnerability assessment with aggregation and risk enrichment, and governance integration with lifecycle decision-making, the framework connects technical discovery with accountable follow up. Its main contribution is not a new scanning technique or vulnerability scoring algorithm, but an integrated workflow that helps organizations identify unmanaged IP

and domain-based cyber assets, reduce vulnerability assessment noise through remediation consolidation, and route discovered assets and findings into ownership validation, remediation, restriction, exception handling, inventory update, or decommissioning. By doing so, the framework supports a transition from request driven vulnerability assessment toward proactive, evidence-driven, and governance oriented cyber risk management.

References

1. Verizon Business: 2026 Data Breach Investigations Report. Verizon Business (2026), https://www.verizon.com/business/resources/reports/dbir/, last accessed 2026/06/13
2. Kaspersky Security Services: Anatomy of a Cyber World: Global Report by Kaspersky Security Services 2026. Kaspersky (2026), https://www.kaspersky.com/enterprise-security/resources/reports/mdr-ir-analyst-reports, last accessed 2026/06/13
3. Rentrop, C., Zimmermann, S.: Shadow IT: Management and control of unofficial IT. In: The Sixth International Conference on Digital Society (ICDS 2012), pp. 98–102 (2012)
4. Nikumaa, T.: Vulnerability management process. Master's thesis, JAMK University (2022)
5. Center for Internet Security: CIS Critical Security Controls v8.1. Center for Internet Security (2024)
6. OWASP Foundation: OWASP Vulnerability Management Guide. OWASP (2020), https://owasp.org/www-project-vulnerability-management-guide/OWASP-Vuln-MgmGuide-Jun05-2020.pdf, last accessed 2026/06/13
7. Scarfone, K., Souppaya, M., Cody, A., Orebaugh, A.: Technical guide to information security testing and assessment. NIST Special Publication 800-115, National Institute of Standards and Technology (2008)
8. Cybersecurity and Infrastructure Security Agency: Binding Operational Directive 26-04: Prioritizing security updates based on risk. CISA (2026), https://www.cisa.gov/news-events/directives/bod-26-04-prioritizing-security-updates-based-risk, last accessed 2026/06/13
9. Mell, P., Spring, J.: Likely exploited vulnerabilities: A proposed metric for vulnerability exploitation probability. NIST Cybersecurity White Paper NIST CSWP 41, National Institute of Standards and Technology (2025)
10. ISMS.online: What is ISO/IEC 27001, the information security standard. ISMS.online (2026), https://www.isms.online/iso-27001/, last accessed 2026/06/13
11. National Institute of Standards and Technology: The NIST Cybersecurity Framework (CSF) 2.0. NIST CSWP 29, National Institute of Standards and Technology (2024)
12. Center for Internet Security: CIS Controls v8.1 mapping to NIST Cybersecurity Framework (CSF) 2.0. Center for Internet Security (2024), https://www.cisecurity.org/insights/white-papers/cis-controls-v8-1-mapping-to-nist-csf-2-0, last accessed 2026/06/13
13. Truss, S.R.A., Ghanem, M.C., Lacerda, M.J., Kheddar, H., Alshawki, M., Kenaza, T., Kalganova, T.: Agentic and generative AI for intelligent autonomous vulnerability assessment and penetration testing: A systematic analysis. Preprint submitted to Elsevier (2026)