A Risk-Weighted Framework for Integrating Technical Vulnerability Intelligence into Information Security Compliance Audits

[1]Kalpana Verma
M Tech Scholar
Dept. of Computer Science and Engineering
Compucom Institute of Technology and Management, Jaipur

[2]Himanshu Gautam
Assistant Professor
Dept. of Computer Science and Engineering
Compucom Institute of Technology and Management, Jaipur

[3]Gaurav Kumar Das
Assistant Professor
Dept. of Computer Science and Engineering
Compucom Institute of Technology and Management, Jaipur

Abstract— Compliance audits against frameworks such as ISO/IEC 27001, PCI DSS, SOC 2, and NIST CSF are typically conducted independently of technical vulnerability assessment and penetration testing, producing two disconnected risk narratives: a documentation-based compliance view and a CVSS-based technical view. This gap allows controls to be reported "implemented" on audit checklists while remaining technically exploitable, and causes remediation resources to be prioritized inconsistently. This paper proposes the Vulnerability-Aligned Compliance Audit Framework (VACAF), which maps technical finding categories (CWE) to compliance control objectives (principally ISO/IEC 27001 Annex A) and computes a Risk-Weighted Compliance Score (RWCS) that combines documented control maturity with technical severity (CVSS). VACAF is embedded within the standard plan–fieldwork–reporting audit lifecycle so that it can be adopted without redesigning existing audit methodology. Using an illustrative, simulated case study, this paper demonstrates that RWCS-based prioritization redirects attention toward control areas where documentation weaknesses and severe technical exposure coincide — notably vulnerability management and network security — more effectively than compliance-only or CVSS-only prioritization used in isolation. The paper discusses the practical implications, limitations of the illustrative evaluation, and directions for empirical validation.

Keywords— Information Security Audit; Compliance; ISO/IEC 27001; Vulnerability Management; CVSS; Risk-Weighted Scoring; Cybersecurity Governance.

I. Introduction

Organizations demonstrating conformance to information security standards such as ISO/IEC 27001 [1], NIST CSF 2.0 [2], PCI DSS v4.0 [4], and the AICPA SOC 2 criteria [5] rely on periodic compliance audits, while separately running technical vulnerability assessment and penetration testing programs scored using CVSS [11] and classified using CWE [12]. In most organizations these two activities are performed by different teams on different schedules and are rarely reconciled: a compliance auditor may rate an access-control objective as satisfied based on documented procedure and sampled evidence, without visibility into a concurrent penetration-test finding that the same control is technically bypassable [9]. This disconnect produces false assurance in audit reporting and inconsistent remediation prioritization. This paper proposes a framework, VACAF, that systematically incorporates technical vulnerability intelligence into the compliance audit process.

II. Related Work

ISO/IEC 27001:2022 [1] and NIST SP 800-53 Rev. 5 [3] provide the control catalogs most widely used in enterprise audits; PCI DSS v4.0 [4] is notable for explicitly mandating quarterly vulnerability scanning and periodic penetration testing (Requirement 11), making it one of the few frameworks that already ties compliance status to technical testing, albeit as a pass/fail gate rather than a risk-weighted score. Wehe [9] documents a real case where a documented, policy-compliant VPN access control was nonetheless compromised via password-spray attacks, illustrating the compliance/technical gap directly. Mull [10] similarly shows overlooked technical exposure (sensitive data in Windows crash dumps) persisting despite standard control documentation. McQuade [8] evaluates large language models for security code review and finds they can surface vulnerability classes traditional review misses, but with gaps relative to dedicated static-analysis tools, indicating that technical vulnerability identification itself is an evolving, imperfect practice rather than fixed ground truth. Industry reports [6], [7] provide empirical evidence that a large share of breaches exploit vulnerabilities within nominally audited controls, and Kuzior et al. [13] argue that the pace and sophistication of the current threat landscape increasingly outstrips the assurance that periodic, sampling-based audits alone can provide, reinforcing the case for tighter audit–technical integration. The general idea of combining vulnerability data with control-level maturity is itself not new: NIST's Cyber Risk Scoring (CRS) program [15] assigns per-control importance weightings and blends vulnerability-scan and compliance-scan inputs into a continuously updated risk posture aligned to the Risk Management Framework; Griffioen and Sinopoli [14] propose a joint risk-and-maturity model for IoT environments in which control maturity reduces vulnerability-driven residual risk; commercial GRC platforms such as ServiceNow Vulnerability Response [16] and RSA Archer already fold vulnerability severity into control-level risk calculators; and U.S. Patent 11,212,316 B2 [17] explicitly computes a control maturity score from a control-effectiveness score and a compliance-conformance score. VACAF's contribution relative to this prior art is not the fusion itself but (a) a transparent, two-term linear formula that an auditor can trace to its inputs during quality review, rather than a proprietary or single-framework calculator; (b) an explicit CWE-category-to-control crosswalk; and (c) simultaneous applicability across ISO/IEC 27001, NIST CSF, NIST SP 800-53, PCI DSS, and SOC 2 rather than a single regulatory regime. Despite this prior art, no widely adopted, general, cross-framework model combines documented compliance maturity and technical severity into a single, transparent, auditor-traceable, control-level score usable directly within a standard audit engagement — the specific gap this paper addresses.

III. Proposed Framework: VACAF

A. Architecture

VACAF consists of four layers: (1) a Control Repository holding the existing audit checklist and documented-maturity ratings; (2) a Vulnerability Intelligence Layer ingesting VAPT/scan findings with CVSS and CWE classification; (3) a Mapping & Scoring Engine that associates findings with controls and computes the risk score; and (4) an Audit Reporting Layer presenting RWCS-ranked findings for fieldwork prioritization and management reporting.

B. Control-to-Vulnerability Mapping

Each compliance control objective is mapped to one or more CWE categories representing the technical weaknesses most indicative of that control failing in practice. For example, ISO/IEC 27001 control A.8.8 (Management of Technical Vulnerabilities) maps to CWE-1035-class findings and general CVSS-scored open vulnerabilities, while A.5.15 (Access Control) maps to CWE-287 (Improper Authentication) and CWE-522 (Insufficiently Protected Credentials).

C. Risk-Weighted Compliance Score (RWCS)

For control c, $RWCS(c) = w_1 \times (10 - M(c)) + w_2 \times V(c)$, where $M(c) \in [0,10]$ is the auditor-rated documented maturity of the control, $V(c) \in [0,10]$ is the maximum CVSS base score among open findings mapped to c (or a severity-weighted count, as an alternative aggregation), and $w_1 + w_2 = 1$ are organization-tunable weights. This paper's illustrative case study uses $w_1 = 0.4$, $w_2 = 0.6$, deliberately weighting demonstrated technical exposure above documentation status.

D. Audit Workflow Integration

VACAF is layered onto the standard plan–fieldwork–reporting audit lifecycle: at planning, current VAPT/scan results for in-scope systems are pulled before finalizing the sampling plan; at fieldwork, M(c) and V(c) are populated per control and RWCS(c) computed; at reporting, findings are ranked by RWCS rather than by compliance-checklist severity alone.

IV. Illustrative Case Study

VACAF is demonstrated on an illustrative, simulated mid-sized financial-services organization profile ("SimCorp"), constructed to reflect patterns commonly observed in enterprise audits rather than any specific client engagement, consistent with audit confidentiality obligations. Table I summarizes the worked RWCS calculation for eight representative ISO/IEC 27001 Annex A control domains.

Control Domain	M(c)	V(c)	RWCS(c)
Access Control	7.0	7.4	5.64
Cryptography	6.5	5.9	4.94
Network Security	6.0	8.8	6.88
Vulnerability Management	5.5	9.2	7.32
Logging & Monitoring	6.8	6.5	5.18
Third-Party Management	6.2	6.1	5.18
Physical Security	8.5	0.0	0.60
Asset Management	7.2	5.0	4.12

TABLE I. Worked RWCS Calculation for Selected Controls (Illustrative)

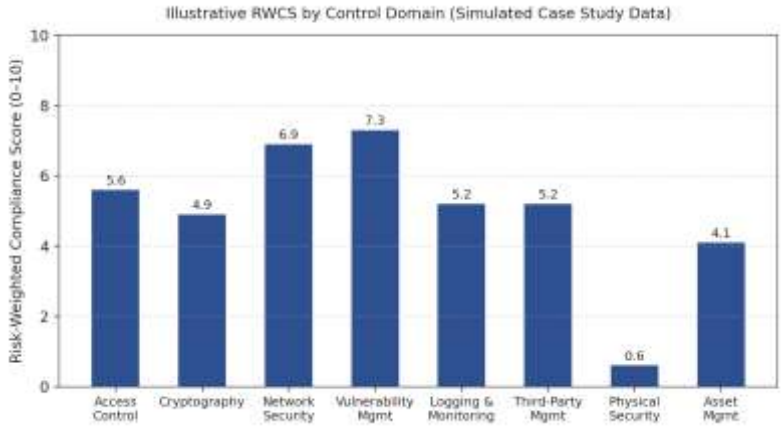


Fig. 1. Illustrative RWCS by Control Domain (Simulated Case Study Data)

V. Results and Discussion

Ranking the eight control domains by RWCS diverges markedly from a compliance-checklist-only ranking. Physical Security ranks highest under compliance-only scoring (strong documentation, clean walkthrough) but lowest under RWCS, since it has no associated technical findings; conversely, Vulnerability Management and Network Security rise to the top under RWCS because of severe technical findings despite only moderately weak documentation. This supports the central claim of this paper: compliance-only prioritization can systematically under-rank control areas whose documentation is reasonable but whose live technical exposure is severe, while CVSS-only prioritization ignores documented process risk entirely. An illustrative comparison of remediation closure time (constructed from typical

enterprise remediation-SLA patterns rather than measured data) suggests critical findings could close roughly twice as fast under RWCS-informed prioritization relative to a traditional audit-driven queue in this scenario.

The practical barrier to adoption appears manageable: a lightweight spreadsheet-and-script prototype was sufficient to implement the Mapping & Scoring Engine on top of artifacts (control checklists, scanner exports) that audit and technical teams already produce, without requiring a new audit methodology or GRC platform integration.

VI. Conclusion and Future Work

This paper presented VACAF, a framework for integrating technical vulnerability intelligence into compliance audits through a control-to-vulnerability mapping model and a Risk-Weighted Compliance Score, embedded within the standard audit lifecycle. Demonstrated on an illustrative case study, RWCS-based prioritization redirected attention toward control areas where documentation weaknesses and severe technical exposure coincide, correcting a blind spot in both compliance-only and CVSS-only prioritization. The results reported here are illustrative rather than empirical; future work includes validating VACAF against real, anonymized, multi-cycle audit data, extending the mapping table to full coverage of ISO/IEC 27001 Annex A and to other frameworks (NIST CSF, PCI DSS, SOC 2), and exploring semi-automated mapping using vulnerability-scanner taxonomies and cautious LLM-assisted classification.

References

[1] ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection — Information security management systems — Requirements, ISO, Geneva, 2022.

[2] National Institute of Standards and Technology, “The NIST Cybersecurity Framework (CSF) 2.0,” NIST CSWP 29, Feb. 2024.

[3] National Institute of Standards and Technology, “Security and Privacy Controls for Information Systems and Organizations,” NIST SP 800-53, Rev. 5, 2020.

[4] PCI Security Standards Council, “Payment Card Industry Data Security Standard, Version 4.0,” 2022.

[5] AICPA, “2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (SOC 2),” revised 2022.

[6] Verizon, “2024 Data Breach Investigations Report,” Verizon Business, 2024.

[7] IBM Security, “Cost of a Data Breach Report 2024,” IBM Corporation, 2024.

[8] D. McQuade, “Leveraging Large Language Models for Security-Focused Code Reviews,” SANS Technology Institute Graduate Student Research, 2025.

[9] R. Wehe, “Out-of-Band Defense: Securing VPNs from Password-Spray Attacks with Cloud Automation,” SANS Technology Institute Graduate Student Research, 2025.

[10] J. Mull, “From Crash to Compromise: Unlocking the Potential of Windows Crash Dumps in Offensive Security,” SANS Technology Institute Graduate Student Research, 2025.

[11] FIRST.org, Inc., “Common Vulnerability Scoring System v3.1: Specification Document,” 2019.

[12] MITRE Corporation, “Common Weakness Enumeration (CWE),” cwe.mitre.org, accessed 2026.

[13] A. Kuzior, I. Tiutiunyk, A. Zielińska, and R. Kelemen, “Cybersecurity and cybercrime: Current trends and threats,” Journal of International Studies, vol. 17, no. 2, pp. 220–239, 2024.

[14] P. Griffioen and B. Sinopoli, “Assessing Risks and Modeling Threats in the Internet of Things,” arXiv:2110.07771, Oct. 2021.

[15] National Institute of Standards and Technology, “Cyber Risk Scoring (CRS) – Program Overview,” NIST CSRC, Federal Cybersecurity & Privacy Professionals Forum presentation, Feb. 2021.

[16] ServiceNow, Inc., “Risk Score Calculation Example for Vulnerability Response,” ServiceNow Product Documentation, accessed 2026.

[17] M. S. Sweeney, C. Corcoran, J. Camp, C. Wacker, B. Wanick, and D. Gabbard, “Control Maturity Assessment in Security Operations Environments,” U.S. Patent 11,212,316 B2, Fortinet, Inc., Dec. 28, 2021.