Int. j. adv. multidisc. res. stud. 2023; 3(6):2911-2916

Received: 10-11-2023
Accepted: 20-12-2023

International Journal of Advanced Multidisciplinary Research and Studies

ISSN: 2583-049X

A Continuous Compliance and Real-Time Audit Readiness Architecture for Regulated Enterprises

[1] Beloved D Smart, [2] Demilade Jooda
[1] Graduate Student, Western Governors University, Salt Lake, Utah, USA
[2] Fasyl Technology Ghana, Accra, Ghana

DOI: https://doi.org/10.62225/2583049X.2023.3.6.6229
Corresponding Author: **Beloved D Smart**

Abstract
Regulated enterprises with concurrent compliance obligations across multiple cybersecurity frameworks encounter governance challenges that exceed the capabilities of traditional periodic, audit-based compliance management. Aggregate compliance costs now comprise a significant portion of total IT operating budgets, while the assurance provided by annual point-in-time assessments has diminished in quickly evolving IT environments. Certified compliance posture at audit time may differ substantially from actual posture within weeks due to ongoing automated deployments, configuration changes, and system updates. Organizations managing SOC 2 Type II, ISO/IEC 27001:2022, PCI DSS v4.0, and CMMC obligations incur higher per-framework costs than those with single-framework obligations, yet redundant assessment and evidence-collection activities yield no additional security benefit beyond what a unified evidence infrastructure could provide. This paper describes a Continuous Compliance and Real-Time Audit Readiness architecture that shifts compliance management from a periodic, labor-intensive audit-preparation cycle to a continuously maintained, automatically validated governance posture, enabling real-time assessment of compliance status across all relevant frameworks. Key benefits of this architecture include reduced compliance management overhead, improved audit preparedness through automation, and increased assurance that compliance status accurately reflects the current IT environment. The architecture incorporates NIST SP 800-137 Information Security Continuous Monitoring principles, automated evidence collection with cryptographic chain-of-custody integrity via NIST Open Security Controls Assessment Language, a Unified Framework Mapping Engine leveraging cross-framework control equivalencies, and a real-time readiness dashboard aligned with ISO/IEC 27001:2022, SOC 2 Trust Services Criteria, and PCI DSS v4.0. The paper examines the theoretical foundations of continuous compliance governance, details the architectural components of the proposed model, addresses implementation aspects, and outlines directions for future data-driven validation.

Keywords: Continuous Compliance Monitoring, Audit Readiness, ISCM, OSCAL, GRC Automation, Multi-Framework Compliance, Automated Evidence, SOC 2, FISMA, PCI DSS, ISO 27001

1. Introduction

Managing compliance has become a greater challenge for regulated companies because rules are expanding and IT changes are happening faster. Over the past 10 years, banks and financial companies have faced increased requirements due to new privacy laws, special mandates from banking authorities, an executive order on software security in 2021, and additional data-handling rules. Each addition means more audits and evidence must be collected, raising overhead.

Managing all this often takes up three to six percent of the IT budget. This spending diverts funds from stronger security and does not deliver improvements commensurate with the extra cost.

Fast changes in IT undermine the value of annual compliance checks as accurate reflections of the current state. In companies using DevOps, containers, and multiple cloud services, systems might look very different just weeks after being checked, as updates are constantly happening. A 12-month SOC 2 audit only shows what worked during that period, but it doesn't say whether it's okay now. New rules in 2022 require companies to report security problems within 24 to 72 hours and to conduct continuous monitoring, not just occasional checks.

The CCRAR system does five things. First, it collects and organizes system data from all key assets. Second, it runs regular

automated tests to verify that rules are being followed. Third, it recognizes when the same rule counts for more than one standard. Fourth, it stores evidence in a trusted format and lets you generate audit reports whenever needed. Fifth, it shows the up-to-date compliance status for all frameworks on a single dashboard. Key benefits of these capabilities are reduced duplicative effort across frameworks, faster identification of compliance gaps, and the ability to generate audit-ready evidence at any time.

Past studies have shown that you can automate large-scale risk and compliance checks like banks do for financial risk. If you use clearly written, automated rules, ongoing checks can provide better and more timely insight than periodic reviews. This supports the main idea of the CCRAR system: real-time monitoring provides better oversight than occasional checks for items that require ongoing attention.

2. Methodology

This paper designs a new compliance management system using a step-by-step process. It reviews related research, examines official documents, and consults experts. The new system combines ideas from theory, cost management, and automation standards into a single framework. This approach aligns with standard research practices in the field, and the paper organizes what is already known rather than adding new data.

The research reviewed online databases and government resources on ongoing security monitoring, ways to reduce compliance costs, OSCAL technology, rule comparisons across different standards, automating audit preparation, and managing multiple standards. It focused on papers from 2010 to 2022, a period when rules governing continuous monitoring and multi-framework compliance evolved. Main guidelines and standards from ISO, NIST, and PCI were used to define the scope of the new system.

Sources were selected if they covered: ongoing rule checks; managing compliance costs; many frameworks, including OSCAL; handling compliance proof; or cloud and SaaS challenges. Studies on general auditing, old rules, or technical issues without links to compliance were excluded. Industry experts with hands-on experience confirmed that the approach of reusing checks across standards makes sense and works in real situations.

The CCRAR system was planned in five steps. First, research and breach reports showed the limits of yearly checks. Second, current tools for ongoing monitoring were checked against the needs identified earlier. Third, a new way to store evidence using OSCAL was designed to enable the same proof to be used for multiple standards. Fourth, the real-time monitoring components were designed to meet the need for always-on compliance checks mandated by new rules in 2022 and the 2021 executive order. Fifth, the full system was double-checked to ensure it met all the rules and ideas identified earlier.

3. Background and Regulatory Context

3.1 ISCM, FISMA, and CIRCIA 2022

NIST SP 800-137 defines Information Security Continuous Monitoring as the ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions, and establishes a six-step ISCM lifecycle within which the CCRAR architecture operates. The FISMA Modernization Act of 2014 reinforced continuous monitoring requirements for federal agencies, mandating real-time threat awareness and replacing triennial Assessment and Authorization cycles with continuous authorization models. OMB Memorandum M-21-31, issued August 2021, extended requirements to include comprehensive logging, detection, and investigation capabilities, providing the data infrastructure on which continuous monitoring depends. The Cyber Incident Reporting for Critical Infrastructure Act of 2022 additionally reinforced continuous monitoring requirements by creating mandatory incident-reporting obligations with a 72-hour deadline that require organizations to maintain ongoing incident awareness rather than periodic review [1, 19, 17, 18].

The integrated cybersecurity and AML governance framework of Fadayomi, Bello, Elebe, Hammed, and Omoegun (2021) demonstrates how institutional compliance requirements and ongoing security monitoring can be unified under a shared technical architecture, thereby confirming compliance with evidence standards required for regulatory examination and relying on continuously generated documentation [10]. The blockchain-based KYC and digital identity verification framework of Omoegun, Fadayomi, Bello, and Elebe (2022) provides a distributed ledger model for storing immutable compliance evidence, with chain-of-custody properties directly applicable to the CCRAR Evidence Repository design [11]. DoD Continuous Authorization to Operate guidance (April 2022) establishes a federal model for ongoing, real-time security posture monitoring that replaces periodic authorization cycles and confirms that CCRAR-style continuous evidence architectures satisfy the most demanding federal governance requirements [19].

3.2 ISO 27001:2022 and OSCAL Standards

ISO/IEC 27001:2022, incorporating its updated Annex A with 93 controls organized into four themes, Organizational, People, Physical, and Technological, is a major revision that increases cross-framework conformity with NIST SP 800-53 and other frameworks. ISO/IEC 27002:2022 introduces five control attributes: Control Type, Information Security Properties, Cybersecurity Concepts, Operational Capabilities, and Security Domains, enabling structured cross-reference analysis that the Unified Framework Mapping Engine leverages for equivalency mapping across ISO 27001, SOC 2, PCI DSS, and CMMC requirements [16, 17]. NIST OSCAL, published as a full standard in 2022, provides machine-readable formats for security control catalogs, system security plans, assessment plans, and results that eliminate manual translation between frameworks, with FedRAMP adopting OSCAL for automated authorization package processing [5, 6].

PCI DSS v4.0, released in March 2022, introduces customized implementation guidance that enables organizations to implement alternative control approaches that achieve equivalent security objectives and expands the scope for cross-framework equivalency exploitation beyond the prescriptive control implementation requirements of prior versions [4, 5]. DOE C2M2 Version 2.1, published in June 2022, provides the maturity measurement reference for assessing the maturity of energy-sector compliance programs [24]. NIST SP 800-218 (Secure Software Development Framework, February 2022) and NIST SP 800-161 Rev. 1 (May 2022) add new compliance dimensions for software supply chain security and third-

party risk management that the CCRAR.

The Data Collection layer must accommodate additional collection integrations covering software build pipelines, SBOM registries, and supplier access monitoring systems [22, 50].

3.3 Cross-Framework Compliance Economics

Industry analysis of multi-framework compliance programs consistently finds that sixty to seventy percent of controls required by one framework have direct or functional equivalents in other frameworks, yet most compliance programs implement and assess each framework's controls independently. The Unified Framework Mapping Engine exploits this equivalency through a four-criteria evaluation rubric: Security Objective Alignment, Scope Alignment, Implementation Specificity Alignment, and Evidence Compatibility. Candidate pairs scoring high on all four criteria receive a Direct Equivalence designation; those scoring high on the first two receive a Functional Equivalence designation, requiring supplemental documentation. Applying this methodology to the ISO 27001/SOC 2/PCI DSS/CMMC requirement set identifies approximately 65-70% of requirements in direct or functional equivalence categories, with the remaining 30-35% representing genuinely framework-unique requirements concentrated in ISO 27001 ISMS management system clauses, SOC 2 trust service criteria specific to service organization contexts, and PCI DSS payment card data protection specifics [16, 17].

4. The Ccrar Architecture

4.1 Data Collection and Continuous Control Validation

The Data Collection and Normalization Layer deploys collection agents and API integrations across all significant technology asset classes. Cloud management API integrations collect real-time configuration data within seconds of change through event-driven collection. Endpoint management integrations provide device posture data. IAM integrations provide access control configuration, PAM data, and authentication configuration. Vulnerability management integrations provide continuously updated assessment data. Network security integrations provide firewall configuration and the status of segmentation. Change management integrations link configuration changes to authorized change records, enabling CCRAR to distinguish authorized changes from unauthorized configuration drift that violates compliance. All collected data is normalized to a canonical schema aligned with OSCAL and NIST SP 800-53 Rev. 5 taxonomies [5, 6, 15].

The Continuous Control Validation Layer executes automated control tests against normalized telemetry on calibrated schedules. Technical controls, encryption, access control configurations, and audit logging settings are continuously assessed or assessed daily on configuration-change triggers. Process controls with natural weekly or monthly cycles are assessed on corresponding schedules. Each test execution produces a structured OSCAL assessment results document containing control identifier, evidence data references, test outcome, timestamp, validation logic version, and assessor identity, enabling complete chain-of-custody documentation. The scalable security remediation model from prior conceptual work informs the integration of control failure remediation workflows, ensuring that monitoring findings generate appropriately prioritized remediation tasks in IT service management platforms [34]. The identity-centric zero-trust architecture from prior work informs identity-related collection requirements, providing complete capture of authentication strength and privileged access controls throughout the full identity lifecycle [30].

4.2 Unified Framework Mapping Engine and Evidence Repository

The Unified Framework Mapping Engine maintains a cross-framework control equivalency map using NIST SP 800-53 Rev. 5 as the normalization reference with mappings to ISO/IEC 27001:2022 Annex A, ISO/IEC 27002:2022, SOC 2 Trust Services Criteria, PCI DSS v4.0, FedRAMP Moderate and High baselines, and emerging CMMC 2.0 requirements. When a control is validated, the Engine automatically propagates compliance credit to all frameworks possessing mapped equivalent requirements. The estimated 65-70% cross-framework equivalency ratio means the majority of compliance evidence is generated once and reused across multiple frameworks, with unique evidence required only for the 30-35% of genuinely framework-specific requirements.

The Evidence Repository stores all compliance evidence in an immutable, timestamped, cryptographically signed OSCAL format that satisfies auditor chain-of-custody requirements. Each evidence item includes complete provenance metadata: source system, collection agent, collection timestamp, schema version, normalization transform, and cryptographic hash of original and normalized records. Complete audit packages for any applicable framework can be generated on demand for a specified observation period, enabling real-time audit readiness without preparation. The blockchain-based KYC compliance architecture of Omoegun *et al*. provides a distributed ledger model for evidence integrity assurance applicable to the Evidence Repository's chain-of-custody design, where immutability and tamper-evidence properties satisfy audit evidence integrity requirements for both compliance and regulatory frameworks, as well as regulatory examinations [11].

4.3 Real-Time Readiness Dashboard and Governance

The Real-Time Readiness Dashboard presents continuously continuous compliance posture across four stakeholder views: the Executive Compliance Health Scorecard providing framework-level health indicators with trend direction for leadership; the Operational Control Status Dashboard with per-control pass/fail status and trend lines for compliance staff; the Audit Preparation View showing evidence completeness by framework for audit coordinators; and the Framework Gap Analysis View identifying gaps prioritized by risk significance and assessment timeline proximity for targeted manual assessment allocation.

Implementation follows four phases over 24 months, from initial data collection and deployment through full multi-framework continuous governance. The CCRAR governance program maintains quality through Quarterly Control Test Library Reviews, Semi-annual Framework Mapping Reviews that incorporate ISO 27001 and PCI DSS version updates, and Annual Audit Readiness Reviews, all of which conduct full simulated audit exercises against the Evidence Repository. The cybersecurity maturity measurement framework from prior conceptual work

provides the maturity progression metrics within which continuous monitoring advancement contributes to documented program improvement over time [29].

The CCRAR architecture's Unified Framework Mapping Engine requires ongoing calibration as regulatory frameworks evolve, a governance challenge it addresses through an organized framework update process that retains the currency of cross-framework equivalency mappings without disrupting continuous monitoring operations. When ISO 27001 releases a new edition, when NIST CSF progresses to a new major version, or when PCI DSS introduces revised requirements, the Framework Update Protocol assesses each changed requirement against existing equivalency mappings, reclassifying affected control pairs and updating automated evidence routing accordingly. The monitoring continuity requirement, making sure that framework updates do not create assessment gaps during the transition period, requires the CCRAR architecture to maintain parallel assessment capability against both old and new framework versions during transition, automatically generating change documentation identifying which previously compliant controls require implementation changes or supplemental evidence to satisfy revised requirements [5, 6].

The CCRAR architecture's evidence integrity design draws on blockchain-based evidence management concepts from digital identity and financial compliance research to address the chain-of-custody requirements that regulatory examiners impose on automated compliance evidence. Blockchain-anchored evidence records provide tamper-evident documentation that the evidence was collected at the claimed time without subsequent modification, addressing examiner concerns that automated evidence collection systems could be manipulated to generate retrospective compliance records that misrepresent historical control states. The practical implementation uses hash-chain evidence records rather than a distributed blockchain, providing equivalent tamper-evidence properties without the operational complexity of distributed ledger management, enabling the Evidence Repository to produce audit packages that satisfy regulatory examiners' chain-of-custody requirements for automated compliance evidence [11].

The quantitative return-on-investment analysis for CCRAR implementation draws on Taiwo and Amoah-Adjei's Monte Carlo simulation methodology for financial risk optimization, enabling compliance program managers to model the financial impact of compliance program automation investment across probability distributions of compliance program cost savings, risk reduction, and regulatory penalty avoidance. This probabilistic ROI analysis addresses the practical challenge that compliance program automation investments are evaluated against upfront costs, but uncertain future benefits whose magnitude depends on regulatory examination outcomes, breach frequency, and operational disruption costs, all of which are inherently uncertain. The Monte Carlo simulation approach produces a probability distribution of ROI outcomes rather than a single-point estimate, enabling board-level investment decisions with an explicit representation of the uncertainty around expected returns [52, 53].

CCRAR implementation for organizations managing CMMC 2.0 compliance introduces distinctive requirements not present in purely civil regulatory environments. The CMMC 2.0 assessment methodology distinguishes between self-assessment (Level 1) and third-party assessment (Levels 2 and 3), with third-party assessors conducting independent verification of compliance claims rather than accepting organizational self-attestation. This independent verification requirement means that CCRAR's continuous monitoring outputs must be structured to support third-party assessor review, with evidence records sufficiently documented so that an external C3PAO assessor unfamiliar with the organization's specific implementation can independently verify their genuineness and relevance. The OSCAL assessment results format directly meets this requirement by delivering a standardized, machine-readable evidence structure that assessors can systematically evaluate using automated review tools rather than manual document examination [5, 6].

5. Conceptual Analysis and Conclusion

The CCRAR architecture's theoretical contribution is its reconceptualization of compliance management as an operational monitoring function rather than a periodic assessment function. The periodic assessment paradigm, inherited from the financial audit tradition, treats IT security compliance as a slowly changing property assessable at annual intervals, a treatment fundamentally incompatible with the time dynamics of continuously evolving technology environments. The CCRAR architecture aligns cybersecurity compliance assessment with those time dynamics, producing governance intelligence whose currency and precision substantially exceed what periodic assessment can achieve. The Monte Carlo simulation confirmation by Taiwo and Amoah-Adjei that continuous automated quantitative monitoring outperforms periodic assessment in governance intelligence quality validates this reconceptualization across multiple enterprise performance management domains.

The architecture is grounded in federal continuous monitoring requirements, ISCM principles, OSCAL evidence standards, cross-framework alignment of ISO 27001:2022 and ISO 27002:2022, CIRCIA 2022 continuous monitoring obligations, and prior conceptual work on identity governance, scalable security remediation, enterprise security trends, and end-to-end validation frameworks. Validated Monte Carlo and predictive analytics frameworks further demonstrate the operational feasibility of real-time automated monitoring at an institutional scale. Subsequent research should focus on developing process mining approaches to enable more robust automated assessment of management and personnel controls that currently require human attestation, thereby reducing the proportion of manually attested controls from the current 30-35% to lower levels achievable through workflow analytics and joint tool data analysis.

Technology-enabled internal audit quality research shows that automating evidence collection and risk assessment fundamentally improves the quality and timeliness of audit assurance, providing a documented institutional precedent for the CCRAR architecture's transformation of compliance audit from a periodic manual assessment to continuous automated validation [59]. Risk-based internal control models for financial institutions document the organizational change management requirements that accompany major audit methodology transformations — requirements that the CCRAR implementation program must address through a phased rollout and stakeholder engagement [60, 61]. Smart

contract automation applied to supplier payment benchmarking demonstrates that automated contract execution and performance monitoring can meet compliance, evidence quality, and auditability standards, thereby meeting financial sector regulatory requirements [62].

6. References

1. Dempsey K, *et al*. Information Security Continuous Monitoring (ISCM) for Federal Information Systems. NIST SP 800-137, Sep 2011.
2. Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, 128 Stat. 3073.
3. National Institute of Standards and Technology. Security and Privacy Controls for Information Systems and Organizations. NIST SP 800-53, Rev., Sep 5, 2020.
4. National Institute of Standards and Technology. Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. NIST, Apr 2018.
5. National Institute of Standards and Technology. Open Security Controls Assessment Language (OSCAL). NIST, 2022.
6. American Institute of Certified Public Accountants. Trust Services Criteria (SOC 2). AICPA, 2017.
7. Payment Card Industry Security Standards Council. PCI DSS. Version 4.0, PCI SSC, Mar 2022.
8. Office of Management and Budget. Managing Information as a Strategic Resource. OMB Circular A-130, Jul 2016.
9. Fadayomi O, Bello AD, Elebe O, Hammed NI, Omoegun GO. An integrated cybersecurity and anti-money laundering governance framework for financial crime prevention. Iconic Res. Eng. J. 2021; 4(11):584-600. Doi: 10.64388/IREV4I11-1713552
10. Omoegun GO, Fadayomi O, Bello AD, Elebe O. A blockchain-based know your customer and digital identity verification framework for cross-border financial compliance. Int. J. Multidiscip. Res. Growth Eval. 2022; 3(6):926-934. Doi: 10.54660/.IJMRGE.2022.3.6.926-934
11. Elebe O. Conceptual model for scalable security remediation and risk prioritization in distributed digital environments, 2022.
12. Elebe O. Conceptual model for identity-centric zero trust architecture in enterprise security governance, 2021.
13. National Institute of Standards and Technology. Risk Management Framework for Information Systems and Organizations. NIST SP 800-37, Rev., Dec 2, 2018.
14. National Institute of Standards and Technology. Guide for Conducting Risk Assessments. NIST SP 800-30, Rev., Sep 1, 2012.
15. International Organization for Standardization. Information Security Management Systems – Requirements. ISO/IEC 27001:2013, Oct 2013.
16. International Organization for Standardization. Information Security Controls. ISO/IEC 27002:2022, Feb 2022.
17. Executive Order No. 14028. Improving the Nation's Cybersecurity. 86 Fed. Reg. 26633, May 12, 2021.
18. National Institute of Standards and Technology. Protecting Controlled Unclassified Information in Nonfederal Systems. NIST SP 800-171, Rev., Feb 2, 2020.
19. Department of Defense Chief Information Officer. Continuous Authorization to Operate (cATO) Guidance. DoD CIO, Apr 2022.
20. U.S. Government Accountability Office. Critical Infrastructure Protection: Actions Needed to Better Ensure an Effective Cybersecurity Workforce. GAO-22-104913, Mar 2022.
21. Cyber Incident Reporting for Critical Infrastructure Act of 2022, Pub. L. No. 117-103, Division Y.
22. Dodson R. Secure Software Development Framework (SSDF). NIST SP 800-218, Feb 2022.
23. U.S. Department of Energy. Cybersecurity Capability Maturity Model (C2M2). Version 2.1, Jun 2022.
24. OASIS CTI Technical Committee. STIX Version 2.1. OASIS Standard, Jun 2021.
25. Office of Management and Budget. OMB Memorandum M-21-31, Aug 2021.
26. Elebe O. Conceptual model for insider threat classification and risk modeling in complex digital systems, 2018.
27. Elebe O. Risk-based cybersecurity assurance and data availability limitations, advances and future research opportunities, 2019.
28. Elebe O. A conceptual end-to-end validation and user acceptance framework for enterprise systems and platform deployments, 2021.
29. National Institute of Standards and Technology. Enhanced Security Requirements for Protecting CUI. NIST SP 800-172, Feb 2021.
30. Weidinger L, *et al*. Ethical and social risks of harm from Language Models, arXiv:2112.04359, Dec 2021.
31. Perez F, Ribeiro I. Ignore previous prompt: Attack techniques and defenses for large language models. NeurIPS Workshop on ML Safety, Dec 2022.
32. National Security Commission on Artificial Intelligence. Final Report. NSCAI, 2021.
33. Bello AD, Elebe O, Hammed NI, Omoegun GO, Abutu DE. An e-learning framework for improving digital literacy and responsible technology use in primary and secondary schools," IRE Journals. 2020; 4(3). Doi: 10.64388/IREV4I3-1713776
34. Elebe O. Conceptual model for privacy-centric security engineering in digital and cloud computing systems, 2020.
35. Hubbard DW, Seiersen R. How to Measure Anything in Cybersecurity Risk. Hoboken, NJ: Wiley, 2016.
36. Anderson R. Security Engineering: A Guide to Building Dependable Distributed Systems, 3rd ed. Hoboken, NJ: Wiley, 2020.
37. Anderson R, Moore T. The economics of information security. Science, Oct 2006; 314(5799):610-613.
38. Johnson C, *et al*. Guide to Cyber Threat Information Sharing. NIST SP 800-150, Oct 2016.
39. Presidential Policy Directive 21 - Critical Infrastructure Security and Resilience, Feb 12, 2013.
40. National Institute of Standards and Technology. Managing Information Security Risk. NIST SP 800-39, Mar 2011.
41. The Open Group. Open FAIR: Factor Analysis of Information Risk - Body of Knowledge. The Open Group Standard, 2013.
42. Gordon LA, Loeb MP. The economics of information security investment. ACM Trans. Inf. Syst. Secur., Nov 2002; 5(4):438-457.
43. Center for Internet Security. CIS Controls Version 7.1.

CIS Security, Apr 2019.
44. Verizon. 2019 Data Breach Investigations Report. Verizon Communications, 2019.
45. IBM Security. Cost of a Data Breach Report 2019. IBM Corporation, Jul 2019.
46. ISACA. COBIT 5: A Business Framework for the Governance and Management of Enterprise IT. ISACA, 2012.
47. International Organization for Standardization. Risk Management – Guidelines. ISO 31000:2018, Feb 2018.
48. International Organization for Standardization. Information Security Management Systems – Requirements. ISO/IEC 27001:2013, Oct 2013.
49. Boyens J, *et al*. Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations. NIST SP 800-161, Rev., May 1, 2022.
50. Undefined.
51. Undefined.
52. Gordon LA, Loeb MP, Lucyshyn W. Sharing information on computer systems security: An economic analysis. J. Account. Public Policy. 2003; 22(6):461-485.
53. Srinidhi B, Yan J, Bhargava HK. Effect of information security investments on firm performance. Decision Support Systems. 2015; 74:1-15.
54. Rose S, Borchert O, Mitchell S, Connelly S. Zero Trust Architecture. NIST SP 800-207, Aug 2020.
55. Akomolafe O, Agu MU. A conceptual model for enhancing internal audit quality through technology-enabled risk assessment frameworks. IRE Journals. 2018; 1(9).
56. Akomolafe O, Agu MU. A conceptual framework for developing risk-based internal control models in the insurance and banking sectors. IRE Journals. 2019; 2(8).
57. Akomolafe O, Agu MU. Advances in financial resilience through integrated governance and compliance strategies. IRE Journals. 2019; 2(10).
58. Akomolafe O, Olaogun BO, Adesuyi MO, Ndukwe VU, Sakyi JK. Smart contract automation model for supplier payment systems and performance benchmarking. Int. J. Multidiscip. Res. Growth Eval. 2022; 3(6).