International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 5, Issue 4, July - August 2023 |

DOI:10.15662/IJEETR.2023.0504008

Enterprise Application Security Governance through Continuous Compliance Monitoring and Risk Assessment

Sreenivasa Rao Basavala

Independent Researcher, Brambleton, Virginia, USA

Email: basavala@gmail.com

ABSTRACT: Enterprise applications operate on distributed infrastructure, cloud environments, interconnected services, and dynamically changing business environments, leading to a complicated security and compliance problem. The conventional government practices that are based on periodic audits and manual checks do not permit much observance on the constant emergence of hazards, configuration blunders, breaching of policies, and other vulnerabilities. The paper proposes a more sophisticated security governance framework for enterprise applications which is based on the ongoing compliance checks and risk management process in real-time. The framework continually collects security, configuration, access-control, vulnerability, and audit related telemetry in both application and infrastructure environments and compares business security policies, regulatory requirements and pre-defined control goals. An evaluation layer of compliance identifies when the compliance is violated and classifies the deviations based on their potential security/operating impact. At the same time, an assessment of risks activity assists in relating the recognized vulnerabilities with the significance of the assets, exposure of threat, control efficiency, as well as the significance of compliance, to create the required contextual risk prioritization. The framework enables organizations to replace occasional compliance checking with dynamic and evidence-based governance. Continually, the compliance coverage, responsiveness in detection, risk prioritization, policy coverage, and governance transparency and indicates that continual reporting is in a better position to govern the security of enterprise applications and enhance regulatory responsibility and well-informed management of risks.

KEYWORDS: Enterprise Application Security, Security Governance, Continuous Compliance Monitoring, Risk Assessment, Regulatory Compliance, Security Policy Enforcement

I. INTRODUCTION

Enterprise applications have been core to organizational operations, facilitating financial transactions, customer services, supply-chain operations, human-resource management, analytics, communication, and more complicated digital workflows. Widening the enterprise security environment has also been contributed by the rising dependency on integrated applications, cloud applications, APIs, databases, identity platforms and distributed applications. Single security testing or periodic audits may therefore not be trusted as the only means of governing security anymore. Organizations need systems that will constantly monitor the state of application security, detect changes to the approved controls, understand their possible impacts, and present the changes to make governance decisions in a timely manner.

Traditionally, security assurance has been related to ensuring that the information systems are addressing the security requirements that have been set and that they are securing it to an acceptable level. The concept is expanded by operational security assurance, which looks at security states once systems are implemented and giving assurance information to interested stakeholders [1]. This operational view is especially important to enterprise applications since their operational security posture is dynamic. It might change the application configuration as a result of software upgrade, infrastructure migration, user provisioning, linking new services or alteration in business models. As a result, the compliance evidence obtained in the course of one assessment cannot be justifiably reflective of the current state of application in terms of security.

This is also compounded by the increasing use of hybrid infrastructures and multi-environment infrastructures, which are complicated to control the security of the enterprise. Applications may be executed at the same time in one or multiple private data centers, in the public and container platforms and most importantly in the third-party offerings and

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 5, Issue 4, July - August 2023 |

DOI:10.15662/IJEETR.2023.0504008

among integrated enterprise networks. Such heterogeneous environments need systematic assessment mechanisms that have the capability to take into account various components of infrastructure and security controls [2]. The conventional manifestations of governance that consider environments of individual constituents distinctly may create lapses of visibilities when the dependencies of applications transverse over the borders of the infrastructure. It therefore requires the standardized governance model to guarantee standard security and compliance management across the whole application ecosystem.

Another serious problem is the fact that security assessments need to be timely, the long inspection in the modern cloud environment might be ineffective in detecting the emerging security conditions as configuration and workload may change frequently. The concept of real-time security assessment methodology suggests the helpfulness of evaluating the security status of cloud on a regular, or rapid, basis, compared to analyzing this status periodically [3]. In the case of enterprise applications, an evaluation conducted on an ongoing basis may give a quicker insight into security flaws, compromised settings, unauthorized modifications, and control divergences. Still, the critical-reviews and checks-and-balances cannot be those elements that are inarguably conclusive as whether the perceived security status meets the organizational specifications, leadership responsibilities, or general out-of-command parameters.

Another basic aspect of enterprise application governance is compliance as shown in figure 1. The organizations will be expected to demonstrate compliance with the internal security policies and that of the external standards and regulatory requirements. Transparency of cloud security and auditing systems has brought to the fore the significance of retaining an exit of security controls and providing evidence that is likely to support audit and assurance practices [4]. Nevertheless, the compliance governance is challenging, when the evidence is disseminated across applications, infrastructure, identity, logs, vulnerability scanners, configuration repository and security monitoring systems. This is some of the evidence that can be lagged when the records are manually grouped and can be a challenge in detecting the change in formal times of the audit.

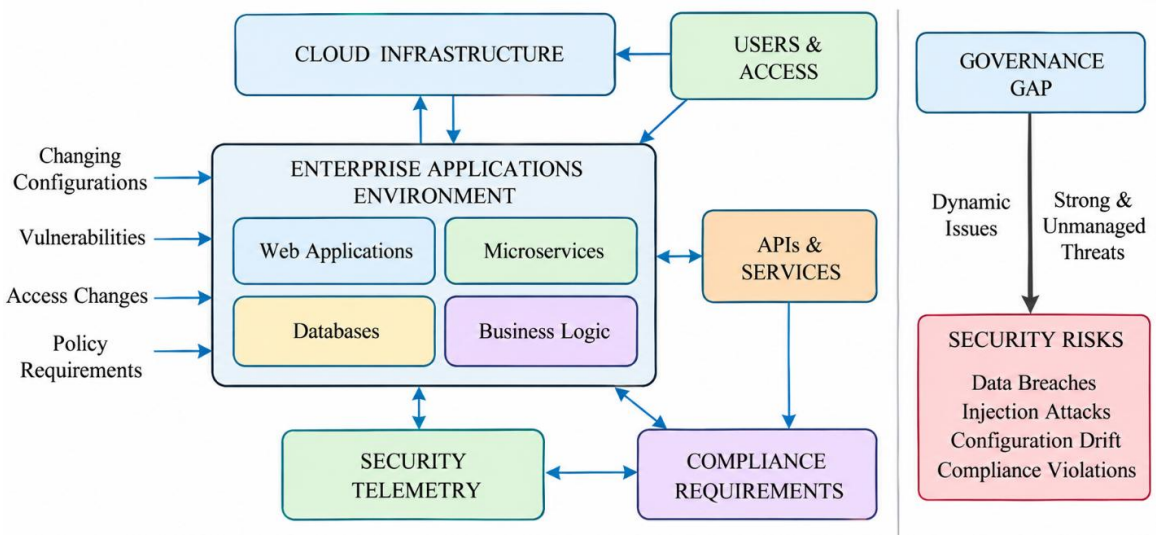


Figure.1. Enterprise Security Governance Challenge

Security risk assessment also offers a complementary viewpoint based not on whether a control is met or not but the possible impact of security vulnerability. Enterprise applications vary significantly when it comes to business acuity, data sensitivity, exposure, dependencies, and operational significance. This means that the business risk may not be the same as applications that are of the same level of compliance deviation. The importance of mixed-characteristics security evaluation methods shows that it is worth integrating various security properties to evaluate the security states of applications [5]. These practices provide the reasons why binary compliance judgment could be substituted by judgment and priority based on context.

Even with such developments, despite the present-day practices, security assurance, compliance monitoring and risk assessment are mostly isolated as individual processes. Compliance checks can be used to show control weaknesses that have not been adhered to during the development of their control form, and technical security checks can cause floods of alerts without the need to establish that they really matter in compliance. Similarly, when analyzing risks,

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 5, Issue 4, July - August 2023 |

DOI:10.15662/IJEETR.2023.0504008

processes may be based on the data collected manually, which becomes obsolete with the instabilities in the application environments. These constraints that create a need to possess a central governance mechanism that is used to consolidate security evidence on a periodical basis, compare it with suitable controls, identify a deviation in compliance and transform the deviation into contextual risk information.

The following research will meet this need by suggesting an enterprise application security governance model founded on ongoing compliance checks and risk evaluation. The framework integrates telemetry of applications and infrastructure, security controls, policy requirements, compliance assessment, risk analysis, prioritization, and governance reporting. The framework can identify the shift of security and compliance status as a result of constant monitoring, but the contextual risk assessment considers the asset, vulnerability, effectiveness and significance of control and compliance. The resultant data on governance can empower security personnel, and business decisionmakers to focus on remediation and keep on seeing into enterprise application security.

The suggested approach thus transforms the enterprise security governance to no longer be a more periodic and audit-driven model but rather a continuous, evidence-based and risk-conscious model of governance. This study creates a linkage of compliance observation to contextual risk assessment through inquiry of how to improve visibility of compliance, sensitivity to risk discovery, prioritization of risks and effectiveness in managing compliance in a dynamically evolving enterprise applications environment.

II. RELATED WORK

Enterprise application security has lost focus on individual security controls and has also taken up systematic assurance, governance, compliance assessment and continuous risk management. The current literature has tackled these dimensions in terms of security assurances models, operational assessment models, cloud security auditing, application-level security evaluation and security metrics. The literature mostly, however, has been on individual assurance or assessment activity but not interaction between continuous compliance monitoring and dynamic enterprise risk assessment.

The area of interest of Ouedraogo et al. is the level of security assurance during the operational systems level of appraisal and reporting [1]. In their work, they put emphasis on the importance of testing security assurance after the implementation of the system and delivering valuable information that can give confidence to the stakeholders [1]. The mapping of application to enterprise application governance in this bi-facet outlook is security posture can change in the post deployment condition depending on configuration changes, vulnerabilities generated, changes in access-control, and operational state change.

Hudic et al. have provided a security assurance evaluator technique of hybrid-cloud. Their contribution recognizes the heterogeneity of infrastructure and distributed security measures and makes their work more complex [2]. Hybrid-cloud setups compel their organizations to consider not only security properties but also across a variety of platforms and ensuring uniform assurance. The publication offers a significant basis of enterprise governance as contemporary workloads are often a mix of both private infrastructure and cloud services. Nevertheless, its main focus is on the security assurance testing to the ongoing association of compliance violations to the business-related risks priorities.

Modic et al. explored the real time assessment and came up with viable approaches to security assessment in clouds [3]. Timely security assessment is critical as it is demonstrated in their work in environments the state of infrastructure and applications is extremely volatile. As close to real time or real-time assessment as possible is capable of reducing the time gap between the occurrence and event of a security condition. Constant governance is immediately approved of such an idea because constant compliance monitoring too requires constant or constant monitoring. However, the existence or lack of conformance of application configurations to the organization control requirements or policies is not always established by security assessment.

Ismail and Islam analyzed the cloud security transparency, and audit using an integrated framework. Their research focuses on how submitting the value of auditability and visibility in establishing trust towards cloud environments [4]. The required evidence about the operation activities and security control provided to the organization by the audit mechanisms allows achieving compliance with regulatory requirements. The research thus adds value to governance aspect of enterprise security. However, traditional auditing may stick to being evidence-based, but continuous compliance governance must have automated deviation identification and its process blended with the continuous risk assessment.

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 5, Issue 4, July - August 2023 |

DOI:10.15662/IJEETR.2023.0504008

Knowledge-based approach to web application security testing methodology, created by Kumar et al. embraces hesitant fuzzy sets, AHP and TOPSIS. Their work illustrates that various security attributes could be combined to aid application-security testing [5]. Enterprise environments MCA applies well to enterprise environments as the risk of applications can hardly be identified within a single security feature. It is based on the approach on contextual security prioritization; however, its focus is on security-durability assessment instead of on long-term compliance assessment and governance.

Sakthivel et al. studied the problem of cybersecurity assurance by using adaptive machine learning-based solution based on clouds in a production context [6]. Their discussion shows that the adaptive use of analytical techniques can be seen to enhance security trust in interdependent enterprise settings. The implementation of machine learning is useful to identify the changing security state and increase responsiveness of assurance mechanisms. Nevertheless, the study is geared towards cybersecurity assurance within an industrial setting, but it fails to fully bring regulatory compliance, application policies, control deviations, and enterprise risk governance into the study.

Agrawal et al. suggested a multi-level fuzzy system of usable-security assessment [7]. The research indicates how the fuzzy logic can be implemented in the security evaluation in which there are numerous variables and potential uncertainty variables used to dictate the next state of security [7]. The strategies apply to enterprise risk assessment because there are unfinished or heterogeneous pieces of evidence to security decisions. Nonetheless, usability-informed security testing is not directly related to the ongoing compliance validation, or governance-level remediation.

Naeem et al. came up with a guideline of how to determine the authenticity of an application. Their effort is directed towards developing trust in applications and their related security attributes. Enterprise application security also requires application authenticity as we have the likelihood of unauthorized or untrusted software, which can pose a great risk to the organization. The concept of authenticity is, however, only one side of the coin of enterprise governance and does not provide a comprehensive examination of the compliance controls, vulnerabilities, and access controls and risks conditions [8].

Gutierréz-Martínez et al. examined security of a large-scale PACS environment by considering the compliance with ISO/IEC 27002. Their study indicates that settled information-security requirements in an enterprise-based environment can be harmonized with their security requirements [9]. This standards perspective is particularly relevant to compliance governance whereby the security controls within organizations are usually needed to demonstrate correspondence with the preexisting structures. Nevertheless, the strategy is mostly compliance based and fails to put in place a dynamic process of measuring the risk where compliance deficiencies are realized.

Deveci and Caglayan proposed a platform of software design and verification that is model based. Their studies include the systematic inclusion of security factors in the software development and verification procedures [10]. Security requirements and controls can be enhanced in consistency and traceability through the use of model-driven techniques. However, the verification at the development stage is not an all-inclusive coverage of the operating governance requirements of the business applications that must be run continuously.

Ouchani and Debbabi questioned the specification and verification, and quantification of security of model-based systems [11]. Their undertakings contribute towards formalizing security properties and quantifying security conditions. Such quantification is useful in quantifying the qualitative security requirements into quantifiable assessment criteria. Nonetheless, this study is more about model-based security analysis than ongoing compliance in a running environment of enterprise applications [11].

Guo has conducted a review of the security-related behavior as to utilization of information systems in the workplace [12]. The paper emphasizes the importance of human behavior in the information security of organizations. This is significant since compliance failures could be properly born out of not just technical frailties but also improper user conduct and policy breaches. Still, behavioral security research lacks enough to provide automated technical procedures needed to carry out continuous compliance audit of application applications.

Mellado et al. develop a Common Criteria (CC) based security requirements engineering process to produce safe information systems [13]. Their task offers a set of interrelationships between security requirements and the assurance process in a systematic manner and assists in traceability during system development. This gives a valuable conceptual basis of governance since enterprise security controls need to be trackable as far as unmistakable needs. However, the approach is more focused on security requirements engineering, more than continuous operational compliance [13].

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 5, Issue 4, July - August 2023 |

DOI:10.15662/IJEETR.2023.0504008

Pavlich-Mariscal et al. proposed a plan of a security assurance of an access-control implementing code [14]. Their research indicates how far access-control tools should be scrutinized in making sure that the protection policies that such controls should facilitate are appropriately enforced [14]. Enterprise application access is one of the main elements in access governance, especially where the information is sensitive and the information processed by the applications is relevant to the organization. However, the area of access-control assurance is only one of the domains of control and does not imply overall compliance monitoring, the vulnerability environment, configuration variations, and risk prioritization on an enterprise-level.

Finally, the measures of quality taxonomy as theorized by Ouedraogo et al. were developed with the idea of testing the security correctness [15]. In their work they observe that quantifiable metrics are fundamental in the quantification of the assurance of a security [15]. Security metrics play an important role in the governance process as it aids organizations in transforming heterogeneous security evidence into meaningful form in order to make decisions. The taxonomy does not provide a unified operational structure that continuously gathers compliance evidence, determines policy variations, computes context risk, and facilitates governance decision-making.

Overall, the literature has a good foundation in security assurance, application security verification, cloud auditing, security metrics, access-control verification and standards-based compliance. Nevertheless, these functions are typically dealt with individually. The gap that has been identified is the lack of integrated enterprise application governance approach that has been continuously testing compliance controls, deviation aligning with application and businesses risk that dynamically prioritizes risk and peaks to governance visibility. The proposed study will help fill this gap by integrating continuous compliance monitoring and contextual risk analysis into a single enterprise application security governance platform.

III. CONTINUOUS COMPLIANCE–RISK INTELLIGENCE GOVERNANCE FRAMEWORK

The proposed framework will provide a cohesive background to manage application security in the enterprise by conducting continuous compliance checks and risk assessments which depend on the circumstances. This framework is presented in figure 2. The framework considers compliance as a continually observable security property as opposed to other conventional governance models that only measure compliance periodically. It incorporates application telemetry, infrastructural settings, identity and access data, vulnerability data, security policies, regulatory provisions and operational events to create a dynamic image of operational security stance. The structure is designed to organize the interrelated layers to decrease heterogeneous security evidence into compliance, context risk priorities, and insights of governance level.

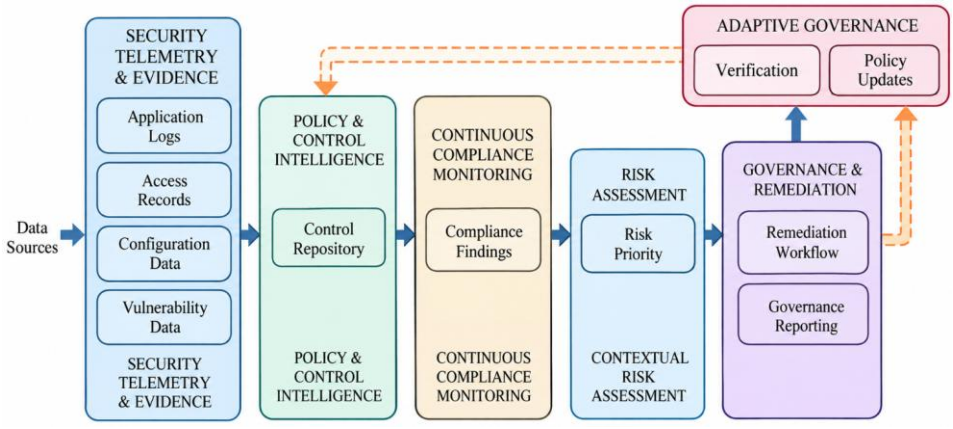


Figure.2. Continuous Compliance–Risk Intelligence Governance Framework

3.1 Enterprise Security Telemetry and Evidence Layer

Some of the data sources include application logs, API activity, authentication events, access-control log, configuration repositories, vulnerability scanners, cloud security services, endpoint controls, databases, network monitoring systems and security information and event management platforms. The aim is to have sustained visibility of the technical and operational situation that affects the security of applications.

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 5, Issue 4, July - August 2023 |

DOI:10.15662/IJEETR.2023.0504008

Evidence processing architecture is shown in figure 3. The evidence is normalized in a standardized form to allow dissimilarities in formats, timestamps, identifiers and data structures. Applications mapping and asset identification correspondents have correlated occurrences with applications, services, infrastructure, users and business processes. This connection is a necessity since isolated security events lack the value of governance until the connection with the assets of the enterprise that they protect can be defined.

The layer of evidence also traces out historical evidence with the view of marking a change of the security pose in applications to trace it out over a period. This assists in configuration drifting and reoccurring violations, recurrent access anomalies and continuing compliance gaps.

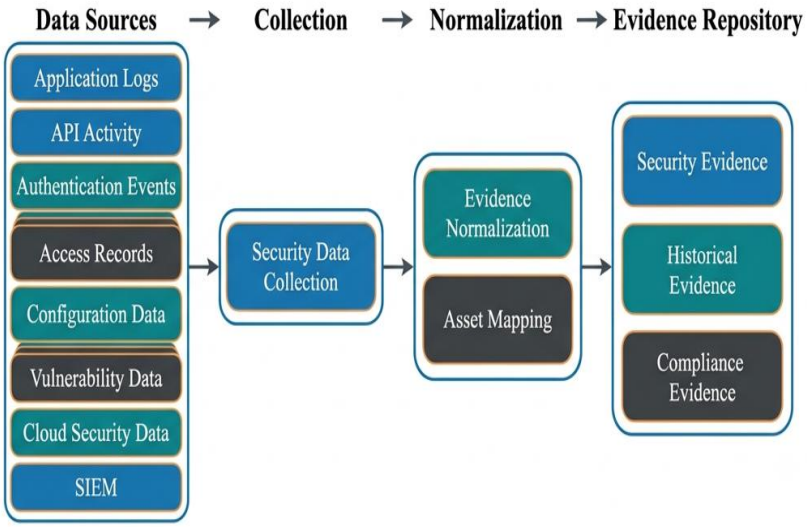


Figure.3. Security Telemetry and Evidence Processing Architecture

3.2 Policy and Control Intelligence Layer

The second level translates the organizational security needs into governance controls that are machine readable. Such controls can either be guided by enterprise security policies, regulatory requirements, contract required and industry security requirements and on application specific security requirements. Every requirement is relaxed to one or a number of observable control conditions.

Privileged-account configuration, authentication systems, an inactive-account state and authorization history could possibly be related to a single access-management requirement in the example. In the same manner, encryption configuration, data-storage locations, backup controls and transmission-security can be related to a data-protection requirement.

The control repository has control identifiers, conditions of applicability, evidence requirement, the frequency of assessment, severity classification, and remediation expectation. It provides governance requirements and technical evidence at high levels that are traceable. It also allows different applications to be juxtaposed to different sets of controls on their business or purpose, sensitivity of the data, regulatory exposures, and deployment infrastructure.

3.3 Continuous Compliance Monitoring Layer

The third layer does an ongoing comparison of security evidence obtained and governance controls that exist. Working of this layer is depicted in figure 4. Rather than revisiting the audits periodically, the monitoring framework updates the relevant evidence whenever there have been significant cases of configuration, development of vulnerability or operation.

The outcome of compliance testing is either compliant but non-compliant or partially compliant results or no evidence. All findings have a linkage with the impacted application, control, source of evidence and its time and status. This assists organizations to know not only whether a control was met or not but also when a deviation has taken place, and whether the deviation is yet to be addressed. It is also accompanied by continuous monitoring which aids compliance

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 5, Issue 4, July - August 2023 |

DOI:10.15662/IJEETR.2023.0504008

drift detection. A system that passes a control on an initial test may fail to do so because of software updates, change in policy, and changes by the administrators, new vulnerabilities or migration of its infrastructure. Identification of such changes offers a more realistic measure of operational compliance as compared to periodic assessment.

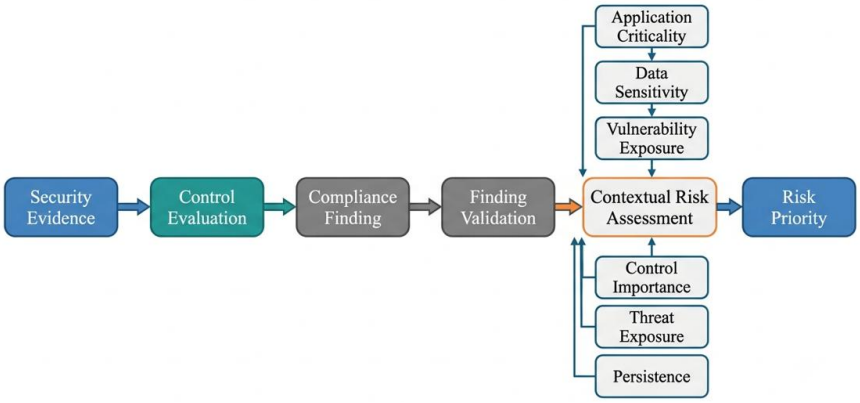


Figure.4. Continuous Compliance Monitoring and Risk Prioritization Workflow

The framework also makes a distinction between actual violations and soft or low confidence observations. Evidence correlation and validation mechanisms are capable of diminishing duplicate results and enhancing trustworthiness of compliance facts prior to entering the risk-assessment phase.

3.4 Contextual Risk Assessment and Prioritization Layer

Findings on compliance are not sufficient to reflect organization risk. The fourth layer thus interprets validated compliance changes into contextual risks. The application criticality, data sensitivity, vulnerability severity levels, exposure to the threats, the significance of the affected controls, exploitability, business dependency and the duration required to perform non-compliance, are all considered during the assessment.

The contextualization of such kind does not enable organizations to address all violations of compliance on the same level. One deviation that impacts one of the low-criticality internal functions might need a different remediation priority than a similar deviation that impacts a customer-facing application that operates on sensitive data. Relations among findings are also considered by risk assessment. The multiplication of multiple low-severity deviations might be considered an indication of the existence of more significant security vulnerability, and a single critical weakness in control can immediately require a governance response. Long-standing conclusions and common failures can be traced in the past as well to allow the governance teams to categorize either an isolated incidence, or a large-scale security issue.

The likelihood of the priorities of the risks obtained can be categorized as per the organization thresholds and remediation objectives. This will enable security teams to direct resources towards enterprise security and compliance objectives on the most potentially influential conditions.

3.5 Governance Decision and Remediation Layer

The fifth layer translates compliance and risk into pragmatic action of governance. Security dashboards offer the view of the compliance state, pending findings, risk allocation, affected applications, performance of the controls, remediation, and trends.

The model enables role-specific reporting and expert's technical determinations may be required by the security administrators, control-level evidence by the compliance officers, application proprietors may require remediation tasks and senior management may need risk and compliance aggregate indicators. This kind of differentiated reporting eliminates the need of governance information to get unduly complicated among decisionmakers.

Enterprise ticketing or workflow systems can be linked with remediation workflows. The outcomes are assigned to the respective agents, checked in particular processes of remedial efforts, and assessed after remedial efforts. The closure is achieved on re-evidence, as opposed to pointing out a finding as being resolved. This puts the governance process in a circle loop where monitoring, assessment process remediation and verification run in a circle.

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 5, Issue 4, July - August 2023 |

DOI:10.15662/IJEETR.2023.0504008

3.6 Feedback and Adaptive Governance Layer

The last layer injects continual feedback into the governance process. Threats, business priorities and organizational policies, application environments undergo change with time. In this way, the framework periodically alters applicability of controls, risk threshold, monitoring regulations and evidence.

Past compliance together with risk data might be considered to identify any instances of violations occurring repeatedly, controls that are often used, applications that get exposed to risks stealthily often, or places where existing controls are not sufficient to counter threats. Such observations have the potential to enhance the security policy and monitoring strategy.

The governance teams can also use the dynamically configurable layer to represent the vulnerabilities found, modified regulatory specifications, changing application criticalities, and changes in security state. Consequently, the framework is not associated with a fixed validation of compliance but aligns with the enterprise environment.

IV. GOVERNANCE EFFICACY AND CONTINUOUS COMPLIANCE VALIDATION

The suggested framework is used to test how it might be used to identify any compliance breach on the fly, building contextualization of any security breach, prioritize remediation and improving visibility of governance on enterprise application settings. Metrics are operationally relevant measures other than just focusing on the number of security incidents detected. Of particular interest are compliance coverage, responsiveness of committed detection, risk prioritization, remediation support and governance visibility.

4.1 Compliance Coverage Assessment

Relevant security controls in enterprise applications are continuously evaluated by the capability of the framework to test the compliance coverage. Relevant and traceable evidence of controls at a given percentage is put into consideration during the evaluation. Increased coverage implies that the governance mechanism is able to keep wider visibility on application security requirements.

Evidence-to-control mapping featured in the framework enables delocalization of application specific needs to configuration, identity, vulnerability, logging and access-control evidence. This reduces dependency on audit information collected manually such that the compliance status can be updated when the underlying application conditions change. The test thus looks at the ability of the framework to have uniform control footage in an environment which is heterogeneous in the application.

4.2 Continuous Deviation Detection

The second area of assessment examines the competence of the framework to detect disabilities as an adaptation to change occurs. These test scenarios might include rogue configuration settings, lapsed credentials, superfluous privileges, disabled security measures, compromised elements, missing security preferences and broken business policies.

The responsiveness to detection is determined by looking at the time interval that follows the incidence of a propensity security or compliance violations and how soon it is detected in the monitoring mechanism. Continuous observation is likely to reduce the delay, which periodical compliance assessment entails. It is also decided whether correlated evidence can help to reduce the incidence of no repeating results and distinguish between long-term violation and situation.

4.3 Contextual Risk Prioritization

Risk prioritization determines whether compliance findings can be converted to meaningful organizational risk profile information. The criticalities of the application, sensitivity of data, vulnerabilities exposure, importance control, threat condition, and continuation of the found deviation have been considered in the framework.

This evaluation is a comparison between plain compliance prioritization and based prioritization. On a simple note, all violations can be treated equally, depending on pre-defined severity. Contextual assessment on the other hand, views business and technical features of the impacted application. This will allow high-impact control failure to be given more attention, in situations when it is related to critical applications or sensitive information. Testing is also concerned with consistency when it comes to risk classification and ability to identify areas of individual consistent or recurring

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 5, Issue 4, July - August 2023 |

DOI:10.15662/IJEETR.2023.0504008

weaknesses. This will demonstrate the competence of the framework to enable risk-based remediation which is more than issuing huge volumes of compliance notifications.

4.4 Remediation and Verification Effectiveness

The fourth dimension assesses support by the framework of the remediation work, as soon as the issue with compliance or security has been identified. All the findings are associated with a detected affected asset, corrective control, evidence, priority of risk, responsible party and remediation status.

The assessment is concentrated on the monitoring of remediation, checking of closure and identification of reoccurrence. A remediation action that is operationally significant is such a remediation action that will be succeeded by evidence that the underlying deviation has been rectified. The framework mechanism is that of a closed loop mechanism in which there is a re-evaluation of the control at fault after the remediation as opposed to manual confirmation.

This method also allows detecting recurring issues. In case a non-compliant control is identified once again, the governance or compliance personnel might want to consider the fact that the problem is related to ineffective policy developments, unsound technical control, configuration procedures, or unsound operational controls.

4.5 Governance Visibility and Decision Support

Governance visibility measures the output in terms of the efficiency with which the technical security information is transformed into information usable by the different stakeholders of the organization. The assessment considers the compliance status in application layer, deficiencies in the control level, risk dispersion, remediation progress and historical trends.

The technical remediation can be performed by security teams using detailed findings, the evidence related to the regulatory controls can be reviewed by compliance teams, and the unresolved responsibilities can be tracked by application owners. Aggregate data on the level of compliance in the posture and high-risk areas can be displayed in dashboards at the management level. Tracing back to original source of evidence is also taken into account as the assessment carries out compliance, risk prioritization, remediation and verification. A good traceability increases audit preparedness, and it provides a better assurance that governance decisions are based on current evidence.

4.6 Overall Framework Validation

General validation regards the framework as a whole governance system instead of independent monitoring elements. The testing takes into consideration continuous evidence collection coherence, compliance testing, evaluation of risk of context production, administration of remedies and governance reporting.

This evaluation therefore targets five outcomes: expanded compliance coverage, faster deviation detection, more context risk prioritization, increased remediation checks and enhanced governance transparency. Combined, these aspects provide a methodological basis on which the sustainability or lack thereof of the suggested model, in dynamically changing operative environments, lead to sustained government in enterprise application security is ascertained.

V. DISCUSSION

The developed enterprise application security governance model is evidence of the significance of the balancing of continuous compliance monitoring and contextual risk assessment as opposed to considering these two activities as disaggregated security functions. The traditional modes of governance have been habitually based on annual auditing, which might provide a feasible picture of any security stance; however, this may overlook the transformations that might occur between audit durations. The suggested rule-of-thumb continuous monitoring solution can eliminate this drawback by having the consistent view of application settings, authorization, vulnerability, security breach, and compliance with the policy.

One of the strengths of the framework is that it allows relating technical security evidence to governance requirements. Deviations in compliance can be more effectively tracked by graphically mapping evidence retrieved in relation to associated controls. This facilitates the shift in using manual intensive completed forms of touch compliance verification to evidence-based governance. The approach also accompanies the prior research on security assurance that

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 5, Issue 4, July - August 2023 |

DOI:10.15662/IJEETR.2023.0504008

has emphasized on the assessment of operations, the evaluation of security in clouds, the auditing, and the quantifiable security assurance.

The other important governance ability is the incorporation of contextual risk assessment. Compliance violations may not necessarily equal degrees of organizational risk. The security teams can ensure that the remediation is mitigated based on the criticality to application, and the sensitivity of data, vulnerability, the importance of control, and that of persistence rather than the number of violations that occur and are detected. This will help in reducing alert overloading and channeling the little security resources towards more productive states.

The model also establishes closed-loop relationship between detection and remediation and verification. The framework does not contemplate remediation as the end of the compliance assessment but reassesses the control that has been affected after the correction action. This improves traceability and enables the recurrence of the inadequacies to be monitored. But, in practice implementation can be challenged due to non-homogeneous sources of telemetry, inconsistent quality of evidence, complexity of integration, regulatory requirements, and true or false or duplicate results. The implementation must therefore be successful with trusted data normalization, appropriate control mapping and governance policies which are controlled periodically.

The discussion in general suggests that the application of constant compliance and risk intelligence may offer a more dynamic basis on enterprise application security governance. The overwhelming provision of the framework is one that ensures that ever-changing technical landscapes are reconnected with compliance requirements and risk-based governance choices.

VI. CONCLUSION

The environment of application is decentralized over cloud platforms, interactive services, divergent infrastructure and operational circumstances and requires that the traditional periodic security and compliance testing are less effective in maintaining omnipresent administration control. This paper suggested a Continuous Compliance Risk Intelligence Governance Framework to integrate continuous security evidence collection, policy and control intelligence, compliance monitoring, context assessing risks, remediation management, governance feedback, and integrate it into a lifecycle.

The framework offers grounded in evidence on which application and infrastructure telemetry continues to be gathered, data standardized, measured in relation to the corresponding security controls, and by means of a set of predetermined compliance requirements. The identified deviations are then evaluated according to the risk factors of the context like the criticality of the application or sensitivity of the data, exposure to vulnerabilities, the degree of control, and consistency of the vulnerabilities. Integration would serve the purpose of assisting the organizations to distinguish between more basic compliance violations and any circumstance which might require more prior governance attention.
The framework evaluation also illustrates the importance of evaluating compliance coverage, deviation detection capabilities, risk prioritization capabilities, remediation verification capabilities and governance visibility capabilities as being interrelated capabilities as opposed to individual security functionalities. This cyclic system of governance aids with the continuous identification, prioritization, remediation, and checking of security and compliance environments. It further provides a wider traceability between technical evidence, technical control requirements, risk identified and governance choices.

The suggested solution will supplement the study of security assurance, the assessment of cloud security, transparency, audits, and the analysis of application security, making them focus on the continual governance of the enterprise application environment that varies. Regarding adoption, in the real world, it may involve addressing the issues surrounding the non-uniform nature of data sources, quality of evidence, control mapping, integration complexity, and regulations and scalability of operations.

Overall, the framework provides a logical foundation in transforming enterprise application security governance to shift periodic compliance checks and tests to a continuous, sensitive to risk and based on evidence management. The initial framework has the capacity to be expanded in the future with advanced analytics, automated control mapping, risk adaptive model and broader validation in diverse enterprise applications and regulatory settings.

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 5, Issue 4, July - August 2023 |

DOI:10.15662/IJEETR.2023.0504008

REFERENCES

[1] Ouedraogo, M., Mouratidis, H., Khadraoui, D., & Dubois, E. (2012). Appraisal and reporting of security assurance at operational systems level. *Journal of Systems and Software, 85*(1), 193–208. https://doi.org/10.1016/j.jss.2011.08.005

[2] Hudic, A., Smith, P., & Weippl, E. R. (2017). Security assurance assessment methodology for hybrid clouds. *Computers & Security, 70*, 723–743. https://doi.org/10.1016/j.cose.2017.06.007

[3] Modic, J., Trapero, R., Taha, A., Luna, J., Stopar, M., & Suri, N. (2016). Novel efficient techniques for real-time cloud security assessment. *Computers & Security, 62*, 1–18. https://doi.org/10.1016/j.cose.2016.07.005

[4] Ismail, U. M., & Islam, S. (2020). A unified framework for cloud security transparency and audit. *Journal of Information Security and Applications, 54*, 102594. https://doi.org/10.1016/j.jisa.2020.102594

[5] Kumar, R., Khan, A. I., Abushark, Y. B., Alam, M. M., Agrawal, A., & Khan, R. A. (2020). A knowledge-based integrated system of hesitant fuzzy set, AHP and TOPSIS for evaluating security-durability of web applications. *IEEE Access, 8*, 48870–48885. https://doi.org/10.1109/ACCESS.2020.2979215

[6] Sakthivel, R. K., Nagasubramanian, G., Al-Turjman, F., & Sankayya, M. (2020). Core-level cybersecurity assurance using cloud-based adaptive machine learning techniques for manufacturing industry. *Transactions on Emerging Telecommunications Technologies*, e3947. https://doi.org/10.1002/ett.3947

[7] Agrawal, A., Alenezi, M., Khan, S. A., Kumar, R., & Khan, R. A. (2019). Multi-level fuzzy system for usable-security assessment. *Journal of King Saud University–Computer and Information Sciences*.

[8] Naeem, R. Z., Abbas, H., Shafqat, N., Saleem, K., & Iqbal, W. (2019). A framework to determine applications' authenticity. *Procedia Computer Science, 155*, 268–275. https://doi.org/10.1016/j.procs.2019.08.038

[9] Gutiérrez-Martínez, J., Núñez-Gaona, M. A., & Aguirre-Meneses, H. (2015). Business model for the security of a large-scale PACS, compliance with ISO/27002:2013 standard. *Journal of Digital Imaging, 28*(4), 481–491. https://doi.org/10.1007/s10278-015-9784-2

[10] Deveci, E., & Caglayan, M. U. (2015). Model driven security framework for software design and verification. *Security and Communication Networks, 8*(16), 2768–2792. https://doi.org/10.1002/sec.1317

[11] Ouchani, S., & Debbabi, M. (2015). Specification, verification, and quantification of security in model-based systems. *Computing, 97*(7), 691–711. https://doi.org/10.1007/s00607-014-0432-8

[12] Guo, K. H. (2013). Security-related behavior in using information systems in the workplace: A review and synthesis. *Computers & Security, 32*, 242–251. https://doi.org/10.1016/j.cose.2012.08.002

[13] Mellado, D., Fernández-Medina, E., & Piattini, M. (2007). A Common Criteria based security requirements engineering process for the development of secure information systems. *Computer Standards & Interfaces, 29*(2), 244–253. https://doi.org/10.1016/j.csi.2006.03.001

[14] Pavlich-Mariscal, J. A., Demurjian, S. A., & Michel, L. D. (2010). A framework for security assurance of access control enforcement code. *Computers & Security, 29*(7), 770–784. https://doi.org/10.1016/j.cose.2010.06.004

[15] Ouedraogo, M., Savola, R. M., Mouratidis, H., Preston, D., Khadraoui, D., & Dubois, E. (2013). Taxonomy of quality metrics for assessing assurance of security correctness. *Software Quality Journal, 21*(1), 67–97. https://doi.org/10.1007/s11219-012-9181-3