Multiverse Journal
E-ISSN: 3080-3942, P-ISSN: 3080-3934
Volume 3, Issue 1, June 2026 | PP. 171-186

Research Paper

Governance, Risk, and Compliance (GRC) Automation: From Periodic Audits to Continuous Assurance

Oyindamola Aboaba[1], Yewande Kolade[2]

[1]University of North Carolina, USA

[2]Amazon, Texas, USA

* aboabaoyin@gmail.com

Received: 21 January, 2026 **Accepted:** 19 March 2026 **Published:** 30 June, 2026

Abstract

The traditional approach to governance, risk, and compliance (GRC) management, characterized by periodic audits and fragmented control systems, has become increasingly inadequate in addressing the dynamic risk landscape of modern organizations. This paper examines the transformation from periodic audit-based compliance to continuous assurance models enabled by automation technologies. Drawing upon the conceptual framework of integrated governance proposed by Chinenye (2013), this research explores how automation technologies facilitate the unification of risk, security, and regulatory controls into cohesive systems. The analysis reveals that fragmented periodic audits create temporal gaps in assurance, expose organizations to undetected risks, and generate inefficiencies through duplicated efforts across compliance silos. In contrast, continuous monitoring systems leverage real-time data analytics, automated control testing, and integrated risk intelligence to provide ongoing assurance. This paper synthesizes theoretical frameworks and practical implementations to demonstrate how GRC automation transforms compliance from a reactive, point-in-time activity to a proactive, continuous process. The findings suggest that organizations adopting integrated GRC automation platforms achieve enhanced risk visibility, improved regulatory compliance, reduced audit costs, and more agile governance structures. Three comparative tables illustrate the distinctions between traditional and automated approaches, the evolution of GRC technologies, and the benefits realization framework for continuous assurance systems.

Keywords: Governance, Risk and Compliance, GRC Automation, Continuous Monitoring, Continuous Auditing, Integrated Governance, Compliance Management, Risk Management Automation

Introduction

The contemporary business environment presents organizations with an unprecedented array of regulatory requirements, operational risks, and governance challenges. Organizations must navigate complex frameworks including Sarbanes-Oxley Act (SOX), Basel III, International Financial Reporting Standards (IFRS), Health Insurance Portability and Accountability Act (HIPAA), and numerous industry-specific regulations (Governatori & Sadiq, 2009). Traditional compliance approaches, built upon periodic audits conducted quarterly or annually, struggle to maintain pace with the velocity of regulatory change and the sophistication of modern risk exposures (Chinenye, 2013). The fundamental limitation of periodic audit methodologies lies in their retrospective nature and temporal discontinuity. Audits provide snapshots of compliance at specific points in time, leaving substantial intervals during which control failures, regulatory breaches, or emerging risks may go undetected (Teeter & Brennan, 2008). Furthermore, traditional GRC frameworks often operate in organizational silos, with separate teams managing information security, operational risk, financial compliance, and regulatory affairs, each employing distinct methodologies, technologies, and reporting structures (Chinenye, 2013). This fragmentation creates redundancies, inconsistencies, and gaps in organizational risk intelligence. Chinenye (2013) articulated a compelling critique of fragmented compliance approaches, arguing that the separation of risk, security, and regulatory controls into disconnected domains fundamentally undermines organizational governance effectiveness. The author proposed an integrated governance framework that unifies these traditionally siloed functions into a cohesive system, enabling organizations to achieve comprehensive risk visibility and coordinated control responses. This conceptual foundation provides the theoretical basis for examining how automation technologies can operationalize integrated governance through continuous monitoring and assurance.

The emergence of GRC automation technologies represents a paradigm shift from periodic verification to continuous assurance. These systems leverage real-time data integration, automated control testing, continuous risk assessment, and intelligent analytics to provide ongoing visibility into organizational compliance status (Dempsey, Chawla, Johnson, et al., 2011). Rather than waiting for scheduled audit cycles, automated GRC platforms continuously evaluate control effectiveness, identify emerging risks, and alert stakeholders to potential compliance breaches as they occur. This paper examines the transformation from periodic audits to continuous assurance through the lens of GRC automation. The analysis addresses three fundamental questions: First, what are the inherent limitations of periodic audit-based compliance that necessitate continuous approaches? Second, how do automation technologies enable the integration of fragmented governance, risk, and compliance functions? Third, what organizational benefits and implementation challenges characterize the transition to continuous assurance models? By synthesizing

theoretical frameworks with technological capabilities, this research provides a comprehensive understanding of how GRC automation transforms organizational governance.

2. The Limitations of Periodic Audit-Based Compliance

2.1 Temporal Gaps and Delayed Detection

The periodic nature of traditional audits creates inherent temporal gaps between compliance assessments. Organizations conducting quarterly or annual audits operate without continuous assurance for extended periods, during which control failures may occur undetected (Majdalawieh, Sahraoui, & Barkhi, 2012). When auditors eventually discover compliance breaches or control deficiencies, the issues may have persisted for months, potentially causing regulatory violations, financial losses, or reputational damage. Baldwin, Beres, and Shiu (2007) emphasized that risk and governance processes require continuous attention rather than periodic intervention. The authors noted that traditional assurance models fail to account for the dynamic nature of organizational operations, where business processes, system configurations, and risk exposures change continuously. A control that functioned effectively during the previous audit may have degraded or failed shortly thereafter, yet the organization remains unaware until the next scheduled assessment.

2.2 Fragmentation and Silo-Based Approaches

Chinenye (2013) identified fragmentation as a critical weakness in traditional GRC frameworks. Organizations typically maintain separate compliance programs for financial regulations, information security standards, operational risk management, and industry-specific requirements. Each program operates with distinct methodologies, separate technology platforms, and independent reporting structures. This fragmentation generates several problems: First, it creates redundant control activities where multiple teams independently verify similar controls without coordination or information sharing. Second, it produces inconsistent risk assessments as different teams apply varying methodologies and criteria to evaluate similar risk exposures. Third, it obscures enterprise-wide risk visibility because no single function maintains a comprehensive view of organizational compliance status across all domains (Chinenye, 2013). Governatori and Sadiq (2009) described the journey to business process compliance as inherently complex due to the multiplicity of regulatory requirements and the difficulty of mapping these requirements to operational processes. The authors noted that organizations often struggle to maintain accurate inventories of applicable regulations, understand their specific obligations, and ensure consistent implementation across business units.

2.3 Resource Intensity and Cost Inefficiency

Traditional audit approaches require substantial human resources to manually review documentation, test controls, interview personnel, and compile findings. Teeter and Brennan (2008) observed that IT audits, in particular, consume significant time and effort due to the technical complexity of systems and the volume of transactions requiring examination. The manual nature of these activities limits audit scope, as resource constraints prevent comprehensive testing of all controls and transactions. Moreover, the episodic nature of audits creates workload spikes that strain organizational resources. Audit preparation demands intensive effort from operational personnel who must compile evidence, respond to inquiries, and address findings, often disrupting normal business activities (Kehlenbeck, Sandner, & Breitner, 2010). These resource demands escalate as regulatory complexity increases and organizations face audits from multiple regulatory bodies, external auditors, and internal audit functions.

2.4 Reactive Rather Than Proactive Posture

Periodic audits fundamentally position organizations in reactive rather than proactive compliance stances. Audits identify problems that have already occurred rather than preventing issues before they materialize (Birukou, D'Andrea, Leymann, et al., 2010). By the time auditors detect a control deficiency or compliance breach, the organization has already experienced the associated risks and may face regulatory penalties or operational consequences. This reactive orientation contrasts sharply with the proactive risk management that modern governance frameworks advocate. Organizations require the capability to identify emerging risks, detect control degradation, and respond to compliance threats before they escalate into significant problems (Chinenye, 2013). Periodic audits, by their nature, cannot provide this forward-looking perspective or enable timely intervention.

3. Continuous Assurance: Conceptual Foundations

3.1 Defining Continuous Monitoring and Continuous Auditing

Continuous monitoring and continuous auditing represent related but distinct concepts within the continuous assurance paradigm. Dempsey et al. (2011) defined information security continuous monitoring (ISCM) as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. The authors emphasized that continuous monitoring provides real-time or near-real-time assessment of security controls, enabling organizations to respond rapidly to emerging threats. Majdalawieh et al. (2012) distinguished between continuous monitoring, which focuses on observing system states and transactions, and continuous auditing, which emphasizes automated testing

of controls and compliance with established criteria. The authors proposed an intra/inter process continuous auditing (IIPCA) framework that integrates continuous audit capabilities within enterprise systems, enabling simultaneous monitoring of process execution and control effectiveness. Continuous assurance encompasses both monitoring and auditing functions, providing ongoing verification that organizational controls operate effectively and that activities comply with established policies, regulations, and standards (Teeter & Brennan, 2008). Unlike periodic audits that provide point-in-time snapshots, continuous assurance delivers persistent visibility into compliance status, enabling organizations to detect and respond to issues as they emerge.

3.2 Integrated Governance Framework

Chinenye (2013) proposed a conceptual framework for integrated governance that unifies risk management, information security, and regulatory compliance into a cohesive system. The framework addresses the fragmentation that characterizes traditional GRC approaches by establishing common processes, shared data repositories, and coordinated control activities across previously siloed domains. The integrated governance framework rests on several key principles. First, it recognizes that risk, security, and compliance represent interconnected rather than independent concerns. A security vulnerability constitutes a risk exposure that may also create regulatory compliance implications. Second, it advocates for unified risk intelligence that aggregates information from all governance domains into a comprehensive organizational risk profile. Third, it emphasizes coordinated control implementation where a single control may address multiple regulatory requirements or risk exposures, eliminating redundancy and ensuring consistency (Chinenye, 2013). Spies (2011) extended this concept to cloud computing environments, proposing rule-enhanced domain models for cloud security governance, risk, and compliance management. The author argued that effective GRC in distributed computing environments requires formalized representation of compliance requirements, automated rule enforcement, and integrated monitoring across infrastructure, platform, and application layers.

3.3 Technology Enablers for Continuous Assurance

The operationalization of continuous assurance depends upon several technological capabilities. First, real-time data integration enables GRC systems to access current information from operational systems, security tools, and business applications (Chuprunov, 2013). Rather than waiting for periodic data extracts, continuous monitoring systems maintain persistent connections to source systems, capturing transactions, configuration changes, and security events as they occur. Second, automated control testing replaces manual audit procedures with programmatic evaluation of control effectiveness. Automated tests can execute

continuously or at frequent intervals, evaluating whether controls operate as designed and identifying exceptions that require investigation (Teeter & Brennan, 2008). Third, intelligent analytics apply statistical models, pattern recognition, and anomaly detection to identify unusual activities, emerging risks, or potential compliance breaches that may not trigger traditional rule-based alerts (Kehlenbeck et al., 2010). Fourth, workflow automation orchestrates remediation activities when continuous monitoring detects control failures or compliance exceptions. Rather than simply generating alerts, advanced GRC platforms can automatically initiate corrective workflows, assign remediation tasks, and track resolution progress (Adya & Deshpande, 2011). Finally, integrated reporting consolidates information from multiple governance domains into unified dashboards and reports that provide comprehensive visibility into organizational compliance status (Courtney & De Angelis, 2007).

4. GRC Automation Technologies and Architectures

4.1 Enterprise GRC Platforms

Enterprise GRC platforms provide integrated technology solutions that consolidate governance, risk, and compliance functions into unified systems. Chuprunov (2013) examined GRC automation in SAP environments, describing how enterprise resource planning (ERP) systems can embed compliance monitoring and control testing within operational processes. By integrating GRC functionality directly into business applications, organizations achieve real-time visibility into compliance status without requiring separate audit systems or manual data collection. Modern GRC platforms typically incorporate several core modules. Risk management modules maintain risk registers, facilitate risk assessments, and track mitigation activities. Compliance management modules map regulatory requirements to organizational controls, monitor compliance status, and manage regulatory reporting. Policy management modules centralize policy documentation, track policy acknowledgments, and enforce policy compliance. Audit management modules plan audit activities, document findings, and track remediation (Adya & Deshpande, 2011).

4.2 Continuous Monitoring Architectures

Dempsey et al. (2011) described comprehensive architectures for information security continuous monitoring that extend beyond traditional security information and event management (SIEM) systems. The authors outlined a layered approach encompassing asset management, configuration management, vulnerability management, security control monitoring, and threat intelligence integration. This architecture provides multiple perspectives on organizational security posture, enabling correlation of information across layers to identify complex threats or systemic weaknesses. Marques, Santos, and Santos (2015) proposed architectures for monitoring organizational transactions in enterprise information systems using

continuous auditing. Their approach employs event-driven architectures where business transactions trigger automated audit rules that evaluate compliance with established criteria. Exceptions generate alerts for investigation while compliant transactions proceed without intervention, enabling comprehensive coverage without impeding operational efficiency.

4.3 Service-Oriented and Cloud-Based GRC

The evolution toward service-oriented architectures and cloud computing introduces new dimensions to GRC automation. Birukou et al. (2010) presented an integrated solution for runtime compliance governance in service-oriented architecture (SOA) environments. Their approach monitors service invocations, evaluates compliance with service-level agreements and regulatory requirements, and enforces compliance policies through automated controls embedded within the service infrastructure. Bhagat (2011) addressed cloud computing governance, cybersecurity, risk, and compliance, proposing business rule systems adapted for cloud environments. The author emphasized that cloud computing's distributed nature, shared responsibility models, and dynamic resource allocation require GRC approaches that differ from traditional on-premises systems. Cloud-based GRC solutions must account for multi-tenancy, data location requirements, and the division of control responsibilities between cloud providers and customers. Kokash (2014) explored integrating compliance management in service-driven computing, developing conceptual models and automation techniques for distributed service environments. The author argued that service-oriented systems require continuous compliance verification because service compositions may change dynamically, and individual services may be provided by external parties whose compliance status the organization cannot directly control.

4.4 Business Process Compliance Management

Elgammal and Turetken (2015) proposed lifecycle business process compliance management using semantically-enabled frameworks. Their approach recognizes that compliance requirements must be considered throughout the business process lifecycle, from design through execution and optimization. Semantic technologies enable formal representation of compliance requirements, automated checking of process designs against regulatory constraints, and runtime monitoring of process executions for compliance violations. Governatori and Sadiq (2009) described the journey to business process compliance as requiring multiple capabilities: identifying applicable regulations, interpreting regulatory requirements, translating requirements into enforceable business rules, implementing controls within process designs, monitoring process executions, and demonstrating compliance through audit trails and reports. The authors

emphasized that automation technologies enable organizations to embed compliance verification within business processes rather than treating compliance as a separate, periodic activity.

5. Comparative Analysis: Traditional vs. Automated GRC

Table 1 presents a comprehensive comparison of traditional periodic audit approaches and automated continuous assurance models across multiple dimensions.

Table 1: Comparison of Traditional Periodic Audits and Continuous Assurance

Dimension	Traditional Periodic Audits	Continuous Assurance (Automated)
Assessment Frequency	Quarterly, annually, or on-demand	Real-time or near-real-time continuous
Detection Timing	Retrospective; issues discovered after occurrence	Immediate; issues detected as they occur
Control Testing	Manual sampling of transactions	Automated testing of all or most transactions
Risk Visibility	Point-in-time snapshots with temporal gaps	Persistent, ongoing visibility
Resource Requirements	High manual effort; periodic workload spikes	Lower manual effort; automated processes
Organizational Integration	Often siloed by compliance domain	Integrated across governance, risk, compliance
Response Capability	Reactive; remediation after audit findings	Proactive; real-time alerts enable rapid response
Coverage Scope	Limited by resource constraints; sampling-based	Comprehensive; can examine all transactions
Compliance Posture	Reactive verification of past compliance	Proactive assurance of ongoing compliance
Cost Structure	High labor costs; episodic expenditures	Technology investment; lower ongoing costs

Audit Trail	Manual documentation; potential gaps	Automated logging; complete audit trails
Regulatory Reporting	Manual compilation; time-intensive	Automated generation; readily available

The comparison reveals fundamental differences in how traditional and automated approaches address governance, risk, and compliance challenges. Continuous assurance provides capabilities that periodic audits cannot match, particularly regarding detection timing, coverage scope, and proactive response.

6. Benefits and Value Realization

6.1 Enhanced Risk Visibility and Decision Support

Continuous monitoring provides organizational leadership with persistent visibility into risk exposures, control effectiveness, and compliance status (Chinenye, 2013). Rather than waiting for periodic audit reports, executives and board members can access real-time dashboards that present current compliance metrics, emerging risks, and control performance indicators. This ongoing visibility enables more informed risk-based decision-making and allows organizations to identify trends, patterns, and systemic issues that may not be apparent in point-in-time audit snapshots (Baldwin et al., 2007).

6.2 Improved Regulatory Compliance and Reduced Violations

Automated GRC systems reduce compliance violations by detecting issues immediately rather than allowing them to persist undetected between audit cycles (Pasic, Bareño, Gallego-Nicasio, et al., 2010). When continuous monitoring identifies a potential compliance breach, automated workflows can trigger immediate remediation activities, preventing minor issues from escalating into significant violations. Additionally, comprehensive audit trails generated by automated systems provide robust evidence of compliance efforts, supporting regulatory examinations and reducing the risk of penalties (Courtney & De Angelis, 2007).

6.3 Cost Reduction and Efficiency Gains

Although GRC automation requires initial technology investments, organizations typically realize substantial cost savings over time. Automated control testing eliminates much of the manual effort associated with traditional audits, reducing labor costs and freeing personnel to focus on higher-value

activities such as risk analysis and strategic planning (Teeter & Brennan, 2008). Integration of previously siloed compliance functions eliminates redundant activities and reduces the total cost of compliance across the organization (Chinenye, 2013).

6.4 Agility and Adaptability

Automated GRC platforms enhance organizational agility by enabling rapid adaptation to regulatory changes, new business initiatives, or emerging risks (Kehlenbeck et al., 2010). When regulations change, organizations can update automated compliance rules and immediately begin monitoring for the new requirements without waiting for the next audit cycle. Similarly, when launching new products, entering new markets, or adopting new technologies, organizations can quickly implement appropriate controls and monitoring to ensure compliance from inception.

Table 2 illustrates the evolution of GRC technologies and their corresponding capabilities across three generations.

Table 2: Evolution of GRC Technologies

Generation	Time Period	Primary Technologies	Key Capabilities	Limitations
First Generation	1990s-2000s	Spreadsheets, document management, basic databases	Manual tracking, document storage, basic reporting	Fragmented, labor-intensive, limited integration, no automation
Second Generation	2000s-2010s	Integrated GRC suites, workflow automation, basic analytics	Centralized repositories, automated workflows, risk registers, compliance mapping	Limited real-time capabilities, primarily reactive, siloed implementations
Third Generation	2010s-2017	Continuous monitoring, advanced analytics, cloud platforms, integrated architectures	Real-time monitoring, predictive analytics, automated control testing, cross-domain integration	Implementation complexity, change management challenges, skills requirements

7. Implementation Challenges and Critical Success Factors

7.1 Organizational Change Management

Transitioning from periodic audits to continuous assurance requires significant organizational change. Personnel accustomed to traditional audit cycles may resist continuous monitoring, perceiving it as intrusive or questioning its necessity (Kehlenbeck et al., 2010). Successful implementations require comprehensive change management programs that communicate the benefits of continuous assurance, address concerns, and provide training to help stakeholders adapt to new processes and technologies.

7.2 Technology Integration Complexity

Implementing continuous monitoring requires integration with numerous source systems across the organization. Choudhary, Antony, Cooper, et al. (2009) described the technical challenges of correlating information from diverse systems with varying data formats, update frequencies, and access protocols. Organizations must invest in robust integration architectures, potentially including enterprise service buses, application programming interfaces (APIs), and data warehouses that consolidate information for GRC analysis.

7.3 Rule Definition and Maintenance

Automated GRC systems depend upon accurate, comprehensive rules that define compliance requirements and control expectations (Governatori & Sadiq, 2009). Developing these rules requires deep understanding of regulatory requirements, business processes, and control objectives. Organizations must establish governance processes for rule development, testing, approval, and maintenance to ensure that automated monitoring remains accurate and relevant as regulations and business conditions evolve.

7.4 Skills and Expertise Requirements

Continuous assurance requires personnel with combined expertise in compliance, technology, data analytics, and business operations (Spies, 2011). Traditional audit teams may lack the technical skills needed to implement and manage automated monitoring systems, while IT personnel may lack the compliance knowledge required to develop appropriate rules and interpret monitoring results. Organizations must invest in training, hire specialized talent, or engage external expertise to build necessary capabilities.

Table 3 presents a benefits realization framework for continuous assurance implementations, illustrating the progression of value delivery over time.

Table 3: Benefits Realization Framework for Continuous Assurance

Implementation Phase	Timeline	Primary Activities	Expected Benefits	Success Metrics
Foundation	Months 0-6	Platform selection, architecture design, initial integration	Process standardization, centralized visibility	Systems integrated, baseline metrics established
Automation	Months 6-12	Rule development, automated testing deployment, workflow implementation	Reduced manual effort, faster issue detection	Percentage of controls automated, detection time reduction
Optimization	Months 12-18	Analytics enhancement, cross-domain integration, predictive capabilities	Proactive risk management, comprehensive coverage	Risk prediction accuracy, coverage percentage
Maturity	Months 18+	Continuous improvement, advanced analytics, strategic integration	Strategic decision support, competitive advantage	Business outcome improvements, ROI achievement

8. Future Directions and Emerging Trends

The evolution of GRC automation continues as emerging technologies create new capabilities and address persistent challenges. Advanced analytics and machine learning enable predictive risk modeling that identifies potential compliance issues before they occur, moving beyond reactive detection to proactive prevention (Kehlenbeck et al., 2010). Artificial intelligence applications in GRC include natural language processing for automated interpretation of regulatory requirements, anomaly detection for identifying unusual patterns that may indicate fraud or control failures, and intelligent automation that can respond to certain compliance exceptions without human intervention. The proliferation of cloud computing, mobile technologies, and Internet of Things (IoT) devices expands the scope and complexity of GRC requirements while simultaneously creating opportunities for enhanced monitoring (Bhagat, 2011). Cloud-based GRC platforms offer scalability, accessibility, and reduced infrastructure requirements, enabling organizations of all sizes to implement sophisticated continuous assurance capabilities. However, cloud adoption also introduces new compliance considerations regarding data sovereignty, shared responsibility models, and third-party risk management. Integration of GRC with broader enterprise risk management and strategic planning processes represents another important direction. Rather than treating compliance as a separate function, leading organizations increasingly view GRC as integral to business strategy, operational

excellence, and value creation (Baldwin et al., 2007). This strategic perspective positions continuous assurance not merely as a compliance tool but as a business enabler that provides confidence to pursue opportunities while managing associated risks appropriately.

9. Conclusion

The transformation from periodic audits to continuous assurance represents a fundamental evolution in organizational governance, risk management, and compliance. Traditional approaches, characterized by episodic audits and fragmented control systems, prove inadequate for the dynamic, complex risk environments that contemporary organizations navigate. The temporal gaps inherent in periodic audits create windows of vulnerability during which control failures and compliance breaches may go undetected. Fragmentation across governance domains generates inefficiencies, inconsistencies, and incomplete risk visibility. Resource-intensive manual processes limit audit scope and position organizations in reactive rather than proactive compliance stances. Chinenye (2013) articulated a compelling vision for integrated governance that unifies risk, security, and regulatory controls into cohesive systems. This conceptual framework provides the theoretical foundation for understanding how automation technologies can operationalize continuous assurance. By leveraging real-time data integration, automated control testing, intelligent analytics, and workflow automation, GRC platforms enable organizations to maintain persistent visibility into compliance status and respond immediately to emerging issues.

The benefits of continuous assurance extend beyond improved compliance to encompass enhanced risk visibility, reduced costs, greater organizational agility, and strategic decision support. However, realizing these benefits requires addressing significant implementation challenges including organizational change management, technology integration complexity, rule development and maintenance, and skills development. Organizations that successfully navigate these challenges position themselves to achieve more effective governance, more efficient compliance operations, and more proactive risk management. As regulatory complexity continues to increase and risk landscapes become more dynamic, the imperative for continuous assurance will only intensify. Organizations that maintain reliance on periodic audits will find themselves increasingly disadvantaged relative to competitors who leverage automation to achieve ongoing compliance verification and real-time risk intelligence. The journey from periodic audits to continuous assurance is not merely a technological upgrade but a fundamental transformation in how organizations conceptualize and operationalize governance, risk, and compliance.

Future research should examine the long-term outcomes of continuous assurance implementations, including quantitative assessments of risk reduction, compliance improvement, and cost savings. Additionally, investigation of optimal integration models between GRC automation and emerging technologies such as artificial intelligence, blockchain, and advanced analytics would provide valuable insights. Understanding how different organizational contexts, regulatory environments, and risk profiles influence continuous assurance effectiveness would help organizations tailor implementations to their specific circumstances. Finally, exploration of the human dimensions of continuous assurance, including skills requirements, organizational culture factors, and change management approaches, would support more successful transformations from traditional to automated GRC models.

References

Adya, A., & Deshpande, G. (2011). Automated governance, risk management, and compliance integration. U.S. Patent Application.

Baldwin, A., Beres, Y., & Shiu, S. (2007). Using assurance models to aid the risk and governance life cycle. *BT Technology Journal*, *25*(1), 232-243.

Bhagat, B. C. (2011). Cloud computing governance, cyber security, risk, and compliance business rules system and method. U.S. Patent Application.

Birukou, A., D'Andrea, V., Leymann, F., Serafinski, J., Silveira, P., Strauch, S., & Tluczek, M. (2010). An integrated solution for runtime compliance governance in SOA. In *Service-Oriented Computing* (pp. 122-136). Springer.

Chinenye, J. (2013). From fragmented compliance to integrated governance: A conceptual framework for unifying risk, security, and regulatory controls. *Scholars Journal of Engineering and Technology*, *1*(4), 238-250.

Choudhary, U., Antony, J. M., Cooper, M. H., Roese, J. J., & Thornton, M. A. (2009). System and method for auditing governance, risk, and compliance using a pluggable correlation architecture. U.S. Patent Application.

Chuprunov, M. (2013). *Auditing and GRC automation in SAP*. Springer.

Courtney, P., & De Angelis, D. (2007). Global compliance management system. U.S. Patent No. 7,216,136.

Dempsey, K., Chawla, N. S., Johnson, A., Johnston, R., Jones, A. C., Orebaugh, A., Scholl, M., & Stine, K. (2011). *Information security continuous monitoring (ISCM) for federal information systems and organizations* (NIST Special Publication 800-137). National Institute of Standards and Technology.

Elgammal, A., & Turetken, O. (2015). Lifecycle business process compliance management: A semantically-enabled framework. In *Proceedings of the 2015 IEEE International Conference on Services Computing* (pp. 91-95). IEEE.

Governatori, G., & Sadiq, S. (2009). The journey to business process compliance. In *Handbook of Research on Business Process Modeling* (pp. 426-454). IGI Global.

Kehlenbeck, M., Sandner, T., & Breitner, M. H. (2010). Managing internal control in changing organizations through business process intelligence and continuous auditing. In *Proceedings of the 16th Americas Conference on Information Systems*. Association for Information Systems.

Kokash, N. (2014). Integrating compliance management in service-driven computing: Conceptual models and automation. In *Fundamentals of Software Engineering* (pp. 186-200). Springer.

Majdalawieh, M., Sahraoui, S., & Barkhi, R. (2012). Intra/inter process continuous auditing (IIPCA), integrating CA within an enterprise system environment. *Business Process Management Journal*, *18*(2), 304-327.

Marques, R. P., Santos, H., & Santos, C. (2015). Monitoring organizational transactions in enterprise information systems with continuous auditing. *Information Systems and e-Business Management*, *13*(4), 611-646.

Pasic, A., Bareño, J., Gallego-Nicasio, B., & Merino, J. (2010). Trust and compliance management models in emerging outsourcing environments. In *Trust Management IV* (pp. 151-166). Springer.

Spies, M. (2011). Rule-enhanced domain models for cloud security governance, risk and compliance management. In *Economics of Grids, Clouds, Systems, and Services* (pp. 169-184). Springer.

Teeter, R. A., & Brennan, G. (2008). Aiding the audit: Using the IT audit as a springboard for continuous controls monitoring. *Journal of Information Systems*, *22*(1), 173-188.