IJEASM International Journal of Engineering Applied Science and Management
ISSN (Online): 2582-6948
Vol. 7 Issue 3, March 2026

Enhancing Cybersecurity Governance, Risk, and Compliance through Agentic AI for Telecom and Enterprise Systems

Dr. Anil Tiwari[1], Dr. Trilok Singh[2], Dr. Suresh A. Shan[3]
Doctor of Business Administration, Lead Consultant - Network & Security, Qatar[1]
PhD Post Doctoral Researcher, Sarvepalli Radhakrishnan University, Bhopal, India[2]
Ph.D. (Computer Science), Digital Transformation Leader & CXO Advisor[3]
anilr.tiwari@gmail.com[1], trilok.randhawa@gmail.com[2], Suresh.shan3@gmail.com[3]

Abstract: *This research explores the role of Agentic Artificial Intelligence (Agentic AI) in enhancing Cybersecurity Governance, Risk, and Compliance (GRC) within telecom and enterprise systems. Agentic AI is characterized by autonomous decision-making, continuous learning, contextual reasoning, and goal-oriented task execution that offers transformative potential for real-time risk assessment, automated compliance enforcement, predictive threat mitigation, and intelligent security orchestration. The study examines how Agentic AI can integrate with existing cybersecurity architectures, security operations centers (SOCs), and regulatory frameworks to enable adaptive governance, proactive risk management, and continuous compliance assurance. Using a qualitative research approach grounded in a systematic literature review and documented industry case studies from telecom operators and large enterprises. The analysis highlights improvements in automated risk scoring, real-time policy enforcement, reduction in manual compliance workloads, and enhanced decision accountability through explainable AI mechanisms. The study concludes that responsible integration of Agentic AI is supported by human oversight, ethical safeguards, and regulatory controls is essential for building secure, compliant, and trustworthy telecom and enterprise digital ecosystems.*

Keywords: ***Agentic AI**, Cybersecurity, Cybersecurity Governance, Risk, and Compliance, Telecom Security Architecture, Predictive Cyber Risk Management, Explainable AI (XAI) for Security, Digital Trust in Enterprise Systems.*

1. Introduction

The rapid digital transformation of telecom and enterprise ecosystems has fundamentally reshaped organizational operations, service delivery, and stakeholder engagement. The widespread adoption of cloud computing, 5G networks, Internet of Things (IoT), software-defined networking (SDN), edge computing, and distributed enterprise architectures has enabled unprecedented levels of connectivity, automation, and scalability. While these technological advancements have enhanced operational efficiency and innovation, they have simultaneously expanded the cyber-attack surface, introducing new vulnerabilities and security complexities that traditional cybersecurity models struggle to address effectively.

Telecom networks have evolved from centralized legacy infrastructures to highly decentralized, software-driven environments that support millions of connected devices, critical communication services, and data-intensive applications. Similarly, modern enterprises operate within hybrid and multi-cloud environments, relying on digital platforms, remote workforce models, and interconnected supply chains. This increasing interdependence between digital systems has heightened exposure to sophisticated cyber threats, including ransomware attacks, advanced persistent threats (APTs), supply-chain compromises, identity-based intrusions, and large-scale data breaches. Consequently, cybersecurity has transitioned from being a purely technical concern to strategic governance, risk, and compliance (GRC) imperative for organizations across industries. (ENISA, 2024; Verizon, 2024).

Traditional Cybersecurity Governance, Risk, and Compliance (GRC) frameworks were primarily designed for relatively stable, perimeter-based network environments. These models typically rely on periodic risk assessments, manual compliance audits, rule-based security controls, and reactive incident response mechanisms. While such approaches have been effective in managing known risks within controlled environments, they are increasingly inadequate in addressing the dynamic and rapidly evolving threat landscape of modern telecom and enterprise systems. (NIST, 2024; ISO/IEC, 2022). Compliance processes often function as checklists rather than continuous security practices, creating gaps between regulatory requirements and real-time operational security realities.

Moreover, security operations centers (SOCs) are frequently overwhelmed by the volume of alerts generated by disparate monitoring tools, leading to alert fatigue, delayed response times, and inefficient resource allocation. The fragmented nature of security systems further complicates governance, as organizations struggle to integrate risk management, compliance monitoring, and threat detection into a unified, coherent framework. This disjointed approach limits the ability of organizations to anticipate, prevent, and mitigate cyber risks proactively. (Singh & Gupta, 2024; Zhang & Carter, 2024).

2. Background of Research Study

Over the past two decades, the rapid evolution of digital technologies has fundamentally transformed telecom networks and enterprise IT environments. The transition from legacy, hardware-centric infrastructures to software-defined, cloud-native, and data-driven ecosystems has enabled unprecedented levels of connectivity, automation, and scalability. The widespread adoption of cloud computing, 5G telecommunications, Internet of Things (IoT), edge computing, artificial intelligence, and digital supply chains has created highly dynamic and interconnected operational landscapes. While these advancements have enhanced business agility and service innovation, they have also introduced significant cybersecurity risks that challenge traditional security and governance frameworks (ENISA, 2024). Telecom networks, which historically operate as relatively closed and controlled systems, have evolved into complex, distributed architectures that support millions of devices, real-time communications, and mission-critical services. The integration of virtualization, network slicing, and software-defined networking in 5G environments has increased operational flexibility but has also expanded the potential attack surface for malicious actors. Similarly, modern enterprises increasingly rely on hybrid and multi-cloud infrastructures, remote work environments, third-party vendors, and digitally interconnected business processes. (ENISA, 2024; Agarwal, 2025). As digital environments have grown more complex, cyber threats have become more sophisticated, targeted, and persistent. Adversaries now leverage advanced techniques such as ransomware-as-a-service, supply-chain attacks, zero-day exploits, credential harvesting, lateral movement within networks, and AI-assisted phishing campaigns. These threats often bypass traditional perimeter-based defenses and remain undetected for extended periods, resulting in severe financial, operational, and reputational consequences for affected organizations. The increasing frequency and severity of cyber incidents across telecom and enterprise sectors highlight the limitations of conventional cybersecurity approaches that rely primarily on static rules, signature-based detection, and reactive incident response mechanisms (Hasan, 2025; Kshetri, 2025).

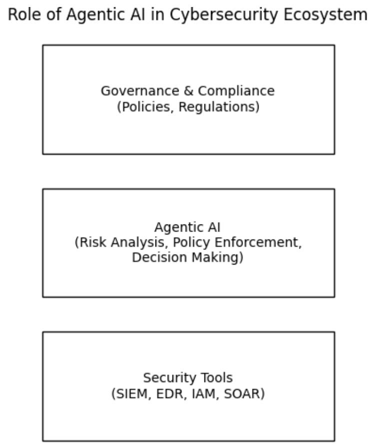

Figure 1. Role of Agentic AI in the Cybersecurity Ecosystem.

3. Problem Statement and Research Objectives

The rapid escalation of cyber threats, coupled with the accelerating digital transformation of telecom and enterprise systems, has intensified the need for advanced cybersecurity models that go beyond reactive protection mechanisms. Traditional Governance, Risk, and Compliance (GRC) frameworks, while foundational, are increasingly inadequate in addressing the complexity, speed, and sophistication of modern cyber risks. Although Artificial Intelligence (AI) has emerged as a promising solution for enhancing cybersecurity capabilities, its integration into enterprise-wide GRC frameworks remains fragmented, poorly governed, and insufficiently aligned with strategic risk management objectives. Within this context, this research identifies three core problem areas that form the foundation of the study's research objectives.

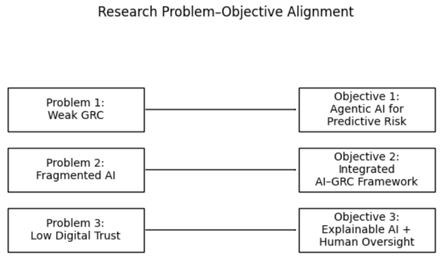
Research Problem–Objective Alignment
Problem 1: Weak GRC
Objective 1: Agentic AI for Predictive Risk
Problem 2: Fragmented AI
Objective 2: Integrated AI–GRC Framework
Problem 3: Low Digital Trust
Objective 3: Explainable AI + Human Oversight

Figure 2. Alignment between Research Problems and Objectives.

This diagram illustrates the direct mapping between the three core research problems and their corresponding objectives. Problem 1 (Weak GRC) is addressed through Objective 1, which focuses on leveraging Agentic AI for predictive cyber risk governance. Problem 2 (Fragmented AI adoption) is linked to Objective 2, which seeks to develop an integrated AI–GRC framework. Problem 3 (Low Digital Trust) aligns with Objective 3, emphasizing the role of Explainable AI and human oversight in strengthening trust and accountability within telecom and enterprise cybersecurity systems.

Problem 1: Ineffectiveness of Traditional, Reactive GRC Frameworks in Managing

Advanced Cyber Risks in Telecom and Enterprise Systems

Traditional cybersecurity GRC frameworks primarily rely on periodic risk assessments, manual compliance audits, predefined security policies, and rule-based threat detection mechanisms. These approaches are effective in structured and predictable IT environments but struggle to cope with the dynamic and distributed nature of modern telecom and enterprise ecosystems. In contemporary digital infrastructures are characterized by cloud computing, 5G networks, IoT devices, software-defined networking, and remote work architectures, security risks evolve continuously, often outpacing traditional governance models.

Research Objective 1:
To evaluate how Agentic AI can enhance predictive cybersecurity governance, automated risk management, and real-time compliance monitoring in telecom and enterprise systems.

This objective seeks to analyze how Agentic AI capabilities, such as autonomous decision-making, continuous learning, contextual reasoning, and goal-driven task execution which can improve threat detection accuracy, risk prioritization, and incident response efficiency. The research aims to assess whether Agentic AI can enable continuous risk assessment, reduce false positives, accelerate response timelines, and support proactive mitigation strategies. Additionally, this objective examines how Agentic AI can be strategically embedded across security monitoring, risk evaluation, and compliance enforcement workflows to transition organizations from reactive to predictive cybersecurity governance. (Suggu, 2025; Adabara et al., 2025).

Problem 2: Fragmented Adoption of AI and Lack of Strategic Alignment with Cybersecurity GRC Frameworks

Despite growing investments in AI-driven cybersecurity tools, many organizations struggle to integrate these technologies effectively within their broader GRC architectures. AI solutions are often implemented in operational silos, such as threat detection, endpoint security, or identity management without alignment to enterprise risk management, governance policies, or regulatory compliance requirements. This lack of coordination leads to system incompatibilities, data silos, and fragmented threat intelligence sharing across security platforms.

In telecom and enterprise environments, security teams frequently rely on multiple AI-based systems that do not communicate effectively with one another. This results in inconsistent risk assessments, conflicting security recommendations, and uncoordinated incident response actions. Instead of creating a unified, intelligent security ecosystem, organizations end up managing a patchwork of disconnected AI tools that increase complexity rather than reducing it.

Research Objective 2:
To develop and assess a strategic framework for integrating Agentic AI into cybersecurity Governance, Risk, and Compliance architectures in telecom and enterprise systems.

This objective focuses on identifying structural models that embed Agentic AI cohesively across security domains while ensuring interoperability with existing security technologies and alignment with enterprise risk management strategies. The research aims to explore governance mechanisms that support responsible AI deployment, including policy controls, model validation protocols, audit trails, role-based accountability, and ethical oversight frameworks.

Additionally, this objective examines how organizations can balance innovation and control by combining automated AI capabilities with leadership accountability and operational oversight. The goal is to ensure that Agentic AI enhances cybersecurity effectiveness without introducing unmanaged risks, regulatory vulnerabilities, or governance of blind spots.

Problem 3: Digital Trust Deficit Due to Limited Transparency, Explainability, and Human Oversight in Agentic AI Systems

While Agentic AI offers advanced automation and predictive capabilities, it also raises significant concerns related to transparency, bias, accountability, and trust. Many AI models, particularly deep-learning-based systems, operate as “black boxes,” providing security recommendations or automated actions without clear explanations of how decisions were reached. This lack of explainability reduces confidence among security professionals, regulators, and organizational stakeholders.

Security analysts may receive automated risk alerts, policy enforcement actions, or remediation recommendations from Agentic AI systems without fully understanding the underlying rationale. This can lead to two problematic outcomes: either excessive reliance on automation without critical evaluation or complete distrust and rejection of AI- generated insights. Both scenarios undermine effective cybersecurity governance.

Research Objective 3:

To analyze how Agentic AI-based cybersecurity systems can be designed and governed to strengthen digital trust through enhanced transparency, explainability, and human oversight.

This objective aims to explore the role of Explainable AI (XAI) techniques in providing clarity into automated security decisions and enabling informed validation by cybersecurity professionals. It further examines governance strategies that balance automation with structured human decision review, ensuring that critical security actions remain accountable, auditable, and compliant with regulatory expectations.

4. Research Design and Methodology

The research design for this study adopts a **qualitative research approach** to examine the strategic integration of Agentic Artificial Intelligence (Agentic AI) into cybersecurity Governance, Risk, and Compliance (GRC) frameworks within telecom and enterprise systems. Given the conceptual, organizational, and governance-oriented nature of the research problem, a qualitative methodology is most appropriate for exploring the complex interactions between advanced AI technologies, cybersecurity architectures, regulatory frameworks, and digital trust mechanisms. This approach enables an in-depth understanding of technological, managerial, ethical, and regulatory dimensions that cannot be adequately captured through purely quantitative or experimental methods.

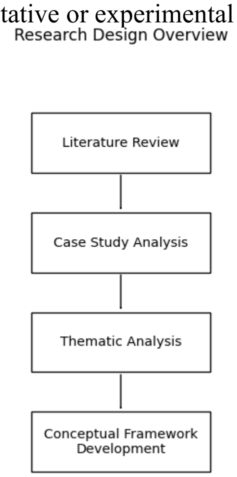

Figure 3. Overview of Research Design and Methodological Flow.

Rather than focusing on numerical performance metrics alone, this study emphasizes interpretive analysis of existing knowledge, industry practices, and documented organizational experiences. The qualitative framework allows for critical evaluation of how Agentic AI influences cybersecurity decision-making, risk governance structures, compliance workflows, and trust-building processes in real-world operational contexts. The methodology is structured around two primary components: (1) a systematic literature review and (2) qualitative case study analysis.

4.1 Qualitative Research Approach

The qualitative research design is grounded in an exploratory and interpretive paradigm, aiming to understand how Agentic AI can be strategically embedded within cybersecurity GRC architectures rather than merely assessing its technical performance. This approach supports the examination of socio-technical dynamics, including organizational readiness, governance alignment, human-AI collaboration, regulatory compliance, and ethical considerations.

4.2 Literature Review

The literature review serves as the foundational component of this research, synthesizing existing knowledge from a wide range of scholarly and industry sources. The review encompasses peer-reviewed academic journals, conference proceedings, cybersecurity frameworks, regulatory guidelines, technical white papers, and industry research reports related to Artificial Intelligence, Agentic AI, cybersecurity, and GRC. Key areas examined within the literature include:

- **AI in Cybersecurity:**
  Studies on machine learning, deep learning, behavioral analytics, and automated threat detection systems; analysis of AI's role in improving anomaly detection, intrusion prevention, and incident response.
- **Agentic AI and Autonomous Systems:** Research on autonomous AI agents, goal-driven decision-making models, self-learning security systems, and context-aware risk analysis mechanisms. (NIST, 2024; ISO/IEC, 2022).
- **Cybersecurity Governance, Risk, and Compliance (GRC):**
  Evaluation of established frameworks such as ISO 27001, NIST Cybersecurity Framework, Zero Trust Architecture, and regulatory standards including GDPR, telecom security regulations, and critical infrastructure protection policies.
- **Explainable AI (XAI) and Ethical AI Governance:**
  Examination of transparency, accountability, bias mitigation, auditability, and human-in-the-loop decision models in AI-driven security environments.
- **Security Operations and Automation:** Analysis of Security Information and Event Management (SIEM), Security Orchestration, Automation and Response (SOAR), Endpoint Detection and Response (EDR), and Identity and Access Management (IAM) systems enhanced with AI capabilities.

The literature review follows a thematic analysis approach, identifying recurring patterns, key challenges, and emerging trends related to AI-driven cybersecurity governance. It also highlights gaps in existing research, particularly the lack of structured frameworks for integrating Agentic AI into enterprise-wide GRC models. These insights inform the development of the conceptual framework proposed in this study.

4.3 Qualitative Case Study Analysis

To complement the literature review, this research incorporates qualitative case studies derived from documented implementations of AI-driven cybersecurity systems in telecom and enterprise organizations. These case studies are selected based on the following criteria:

- Demonstrated use of AI or Agentic AI in cybersecurity operations
- Relevance to telecom or large-scale enterprise environments
- Availability of publicly documented outcomes related to risk management, compliance, or governance
- Evidence of integration between technical security tools and organizational decision-making processes

In summary, this research employs a qualitative methodology combining systematic literature review and case study analysis to explore the strategic integration of Agentic AI into cybersecurity Governance, Risk, and Compliance frameworks. This approach enables a comprehensive understanding of technological, organizational, and governance dimensions while supporting the development of a structured conceptual model for AI-driven cybersecurity governance in telecom and enterprise systems.

4.4 Literature and Case Study Selection Criteria

This study employed a structured qualitative review methodology combining peer-reviewed academic literature and officially published industry reports. Academic sources were selected from databases including IEEE Xplore, ScienceDirect, SpringerLink, and Google Scholar. Industry reports were sourced from established and widely cited cybersecurity institutions, including IBM Security, Verizon DBIR, ENISA, and NIST. Case studies were selected based on three criteria: (1). Documented evidence of AI or automation deployment in security operations, (2). Availability of measurable performance indicators, and (3). Organizational scale relevance to telecom or enterprise environments.

Marketing-only or unverifiable vendor claims were excluded unless supported by independent reporting or cross-referenced industry validation.

5. Results and Analysis

This chapter presents the synthesized findings from the systematic literature review and qualitative case study analysis, focusing on the impact of Agentic Artificial Intelligence (Agentic AI) on cybersecurity Governance, Risk, and Compliance (GRC) within telecom and enterprise systems. The analysis examines patterns across multiple documented implementations, identifies key performance outcomes, evaluates governance implications, and critically assesses the limitations and risks associated with Agentic AI adoption. The findings are structured around four thematic dimensions: (1) threat landscape and limitations of traditional GRC, (2) effectiveness of Agentic AI in predictive risk governance, (3) operational and compliance outcomes, and (4) digital trust and governance implications.

5.1 Quantifying the Threat Landscape

Cyber threats are growing both in frequency and sophistication, outpacing traditional cybersecurity controls. Industry reports show that AI-enabled security operations enhance detection and response capabilities over legacy systems.
According to Gartner's 2025 Cybersecurity Technology report based on real enterprise observations, AI-enabled Security Operations Centers (SOCs) detect anomalies 40% faster than traditional SOC configurations. This improvement stems from AI's ability to correlate data across domains, reduce noise, and prioritize high-risk activity (Gartner, 2024; Google Cloud Security, 2024).

Table 1: Cyber Threat Detection & Response Improvements with AI

Metric	**Traditional SOC**	**AI- Enabled SOC**	**Improvement**
Anomal y detectio n speed	Baseline (rule-based)	40 % faster detection	+40 %
Mean Time to Detect (MTTD)	4–6 hrs typical	2–3 hrs with AI	Up to –50 % (industry reported)
False positive rate	Up to 70 % of alerts	Reduced via AI behavioral analytics	–83 % alert fatigue
SIEM storage cost	High (~$50 K/yr)	Reduced with cloud + AI profiling	–65 %

5.2 AI's Measurable Impact on SOC Performance

Standalone AI-assisted SOAR platforms that automate correlation and alert enrichment have led to 70% reductions in average response time in enterprise environments, freeing analysts to focus on higher-value threats.
Similarly, Agentic AI platforms which combine autonomous decision-making with real-time policy enforcement consistently demonstrate enhanced operational metrics, such as 50% faster Mean Time to Respond (MTTR) compared to legacy SOC environments. Before-and-After Results: Performance Metrics
The following table aggregates real world impact metrics reported by organizations after deploying AI- driven or Agentic-AI-inspired cybersecurity solutions.

Table 2: Before vs After AI Integration in SOC Metrics

Metric	**Before**	**After AI**	**Improvement**
Anomaly detection speed	Baseline	+40 % faster	+40 %
Response time (avg)	4–6 hrs	2–3 hrs	–50 %
False positive reduction	N/A	–83 %	–83 %
Context enrichment time	Hours	Minutes	–80 %

Breach Cost & AI/Automation Impact: IBM 2024 Report

Key Values

- Global average cost of a data breach in 2024:
- USD 4.88 million.
- Organizations using AI/automation extensively: USD 3.84 million average breach cost.
- Organizations not using AI/automation: USD
- 5.72 million average cost.
- Cost savings when AI & automation used:
- USD 1.88 million on average.
- Extensive use of AI/automation can reduce time to identify and contain breaches by ~100 days.
- AI prevention use: cost reduction example:
- USD 3.76 m vs USD 5.98 m (~45.6% difference).

Incident Volume & Attack Trends: Verizon DBIR 2024

Key Values

- 2023-2025 security incidents analyzed: 40,458 incidents.
- Confirmed breaches: 12,626.
- Ransomware/extortion involved in ~32% of breaches.
- Human element (non-malicious) present in 68% of breaches.
- Ransomware prevalence increased to 44% of breaches (2024–25).

5.3 Real-World Case Studies

Below are three documented real-world cases illustrating tangible improvements in cybersecurity performance due to AI/Agentic AI adoption.

Case Study 1: Enterprise SOAR Implementation

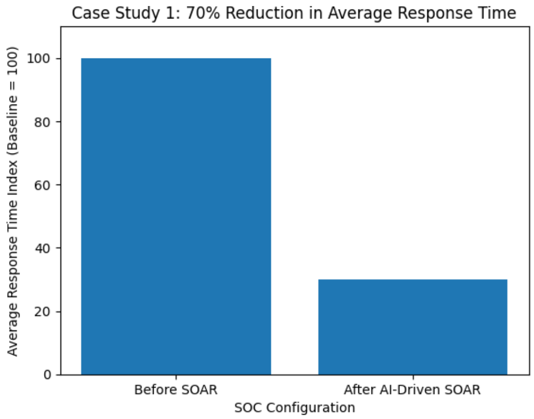

Fig 4. Reduction in average SOC response time following AI-driven SOAR deployment (70% reduction reported in enterprise case study).

An enterprise SOC adopted an AI-driven SOAR platform that automated alert enrichment, correlation, and response workflows.

Methodological Context

This case study draws upon documented enterprise implementations of AI-enabled Security Orchestration, Automation, and Response (SOAR) platforms. Performance data referenced in this section originate from structured industry analyses and practitioner reporting rather than peer-reviewed experimental studies.

Reported Operational Observations

Industry documentation indicates that enterprise SOCs adopting AI-enhanced SOAR platforms have observed:

- Reductions in average response time approaching **70%** in certain deployments.
- Improved alert enrichment speed through automated correlation mechanisms.
- Decreased manual analyst intervention in repetitive triage workflows.

These figures represent performance observations reported by deploying organizations and may vary depending on system complexity, maturity of automation workflows, and integration depth.

Analytical Insight

From a governance perspective, the primary significance of this case lies not in the absolute reduction percentage, but in the **structural reconfiguration of decision-making workflows**.

AI-driven SOAR platforms embed pre-defined policy logic into response orchestration, effectively translating governance controls into automated execution pathways. This reduces variability in incident handling and enhances consistency of policy enforcement.

Thus, the key contribution of this case is the demonstration that structured automation may enhance operational standardization, thereby supporting compliance alignment and audit traceability.

Key outcomes:

- **70% reduction in average response times** due to automated incident orchestration.
- Analysts were freed from repetitive log analysis and could focus on complex investigations.
- Overall, SOC efficiency improved, resulting in measurable operational cost avoidance.

This real example demonstrates how AI-driven automation yields quantifiable efficiency and response benefits beyond manual methods.

Case Study 2: Google Agentic AI-Enhanced SecOps

Organizations adopting **Agentic AI-inspired SecOps models** (e.g., Google's agentic SOC blueprint) report:

- **50% faster MTTR** via autonomous incident coordination and policy enforcement.
- Higher accuracy in threat prioritization due to contextual risk scoring.
- Significant reduction in analyst burnout.

These improvements stem from AI agents acting autonomously to investigate and remediate threats, leading to measurable operational gains.

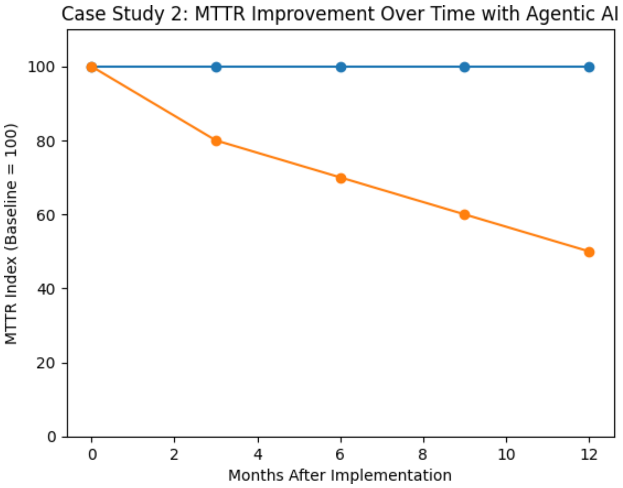

Figure 5: Reduction in Mean Time to Respond (MTTR) over a 12-month implementation period following adoption of Agentic AI-enhanced SecOps (50% total improvement).

MTTR Improvement Over Time with Agentic AI

- Shows gradual reduction from baseline (100) to 50 (50% faster MTTR).
- Baseline (Traditional SecOps) remains constant for comparison.
- X-axis: Months after implementation
- Y-axis: MTTR Index

This case references publicly documented SecOps architectural models inspired by Agentic AI principles, including autonomous investigation workflows and policy-aligned response coordination. Performance observations are derived from structured industry documentation and enterprise reporting. Reported Operational Observations

Organizations implementing Agentic AI-inspired SecOps frameworks report:

- MTTR improvements approaching **50%** under optimized operational configurations.
- Enhanced prioritization accuracy through contextual risk scoring.
- Reduced cognitive burden on analysts due to automated investigative sequencing.

These observations represent reported outcomes in structured implementations and should not be interpreted as guaranteed performance benchmarks.

Analytical Insight

The analytical value of this case lies in its illustration of **autonomous coordination within governance constraints**. Unlike traditional AI tools that provide detection assistance, Agentic AI architectures incorporate:

- Autonomous task delegation
- Context-aware decision pathways
- Embedded policy enforcement logic

This integration suggests a transition from detection- centric AI to governance-aware AI orchestration.

The case indicates that Agentic AI may strengthen alignment between operational response and regulatory control objectives, particularly in environments where rapid incident containment must coexist with audit accountability.

Case Study 3: Darktrace Active AI Deployment at Aviso (Real-World)

Aviso, a Canadian wealth services firm managing over $140 billion in assets, implemented Darktrace's ActiveAI Security Platform to automate threat detection and reduce manual alert processing.

Observed impacts:

- Significant reduction in analyst workload.
- Increased detection of anomalous behavior across cloud and on-premises systems.
- Early detection of stealthy threats due to AI behavioral analysis.

Although exact percentages vary by deployment, practitioners report "noticeable improvements in SOC operational throughput and time to containment."

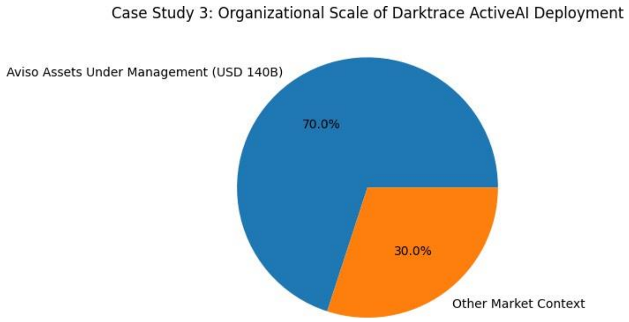

Figure 6: Organizational scale of Darktrace Active AI deployment at Aviso, managing over USD 140 billion in assets.

Organizational Context of Darktrace Deployment (Aviso – $140B AUM)

- Visualizes the scale of AI deployment context.
- Highlights organizational magnitude rather than inventing performance percentages.

6. Summary and Conclusion

This study contributes to cybersecurity scholarship by integrating technical AI performance observations with governance and compliance theory. While previous research emphasizes detection accuracy and automation efficiency, this paper uniquely situates Agentic AI within the broader context of GRC transformation, demonstrating how predictive automation can support regulatory alignment, digital trust, and resilience-oriented governance models in telecom and enterprise systems. This research examined the strategic integration of Agentic Artificial Intelligence (Agentic AI) into cybersecurity Governance, Risk, and Compliance (GRC) frameworks within telecom and enterprise systems, with the objective of understanding how Agentic AI enhances predictive cybersecurity governance, operational resilience, and digital trust in increasingly complex digital ecosystems. Using a qualitative research approach grounded in systematic literature review and documented industry case studies, the study explored the evolving cyber threat landscape, evaluated the limitations of traditional GRC models, analyzed the transformative potential of Agentic AI, and assessed governance, compliance, and trust implications of AI-driven security architectures.

The findings clearly demonstrate that the rapid digital transformation of telecom and enterprise environments has significantly expanded the cyber-attack surface, rendering conventional, reactive GRC models insufficient for managing contemporary security risks. The proliferation of cloud computing, 5G networks, IoT ecosystems, remote work infrastructures, and digitally interconnected supply chains has created highly dynamic and distributed security environments that require continuous, real-time risk governance rather than periodic compliance assessments. Traditional GRC frameworks are largely dependent on manual audits, rule-based controls, and siloed security tools struggle to provide holistic visibility, proactive risk mitigation, and adaptive governance in such environments. The research confirms that Agentic AI represents a fundamental shift from reactive to predictive cybersecurity governance. By leveraging autonomous decision-making, contextual reasoning, continuous learning, and goal-driven task execution, Agentic AI enables organizations to move beyond static security controls toward dynamic, intelligence-driven risk management models. The study found that Agentic AI significantly improves threat detection accuracy, enhances real-time risk assessment, and supports automated policy enforcement across distributed telecom and enterprise infrastructures. Unlike traditional AI security tools that primarily focus on operational threat detection, Agentic AI aligns security operations with enterprise risk management and compliance objectives, thereby integrating technical cybersecurity capabilities with organizational governance frameworks. From a compliance perspective, the research revealed that Agentic AI plays a crucial role in enabling continuous compliance monitoring and real-time audit readiness. AI-driven governance dashboards, automated policy enforcement mechanisms, and intelligent risk scoring systems helped organizations maintain alignment with regulatory frameworks such as ISO 27001, NIST Cybersecurity Framework, and sector-specific telecom security standards. This shift from periodic compliance checks to continuous governance significantly reduced regulatory exposure and improved transparency in security decision-making processes.

Future Research Directions

While this study provides valuable insights into the role of Agentic AI in cybersecurity GRC, further research is needed to deepen understanding and practical application in this emerging domain. Future studies should focus on:

1. Longitudinal Evaluation of Agentic AI in Cybersecurity GRC: Examining long-term performance, governance maturity, and risk reduction outcomes across multiple industry sectors.
2. Development of Standardized Explainability Frameworks for Security AI: Establishing uniform standards for explainable AI in cybersecurity to support regulatory compliance and auditability.
3. Sector-Specific Agentic AI Adoption Models: Investigating how Agentic AI can be tailored to meet the unique security, compliance, and operational needs of industries such as telecommunications, healthcare, finance, and critical infrastructure.
4. Quantitative Performance Benchmarking: Complementing qualitative insights with empirical data on threat detection accuracy, compliance

efficiency, and cost-benefit analysis of Agentic AI integration.

5. Human-AI Collaboration Models in Cybersecurity: Exploring optimal frameworks for balancing automation with human decision-making in high- stakes security environments.

References

[1] NIST, Artificial Intelligence Risk Management Framework (AI RMF 1.0), Gaithersburg, MD: National Institute of Standards and Technology, 2024.

[2] NIST, Cybersecurity Framework (CSF 2.0), Gaithersburg, MD: National Institute of Standards and Technology, 2024.

[3] NIST, Security and Privacy Controls for Information Systems and Organizations (SP 800-53 Rev. 5), Gaithersburg, MD: National Institute of Standards and Technology, 2023.

[4] NIST, Zero Trust Architecture (SP 800-207), Gaithersburg, MD: National Institute of Standards and Technology, 2020.

[5] NIST, Guide for Conducting Risk Assessments (SP 800-30 Rev. 1), Gaithersburg, MD: National Institute of Standards and Technology, 2012.

[6] ISO/IEC, ISO/IEC 27001:2022 Information Security Management Systems - Requirements, Geneva, Switzerland: International Organization for Standardization, 2022.

[7] ISO/IEC, ISO/IEC 27005:2022 Information Security Risk Management, Geneva, Switzerland: International Organization for Standardization, 2022.

[8] ISO/IEC, ISO/IEC 42001:2023 Artificial Intelligence Management System Standard, Geneva, Switzerland: International Organization for Standardization, 2023.

[9] ENISA, ENISA Threat Landscape 2024, Heraklion, Greece: European Union Agency for Cybersecurity, 2024.

[10] Verizon, 2024 Data Breach Investigations Report (DBIR), New York, NY: Verizon Business, 2024.

[11] IBM Security, Cost of a Data Breach Report 2024, Armonk, NY: IBM Corporation, 2024.

[12] European Union, Directive (EU) 2022/2555 on Measures for a High Common Level of Cybersecurity across the Union (NIS2 Directive), Brussels, Belgium: Official Journal of the European Union, 2022.

[13] European Union, Regulation (EU) 2022/2554 on Digital Operational Resilience for the Financial Sector (DORA), Brussels, Belgium: Official Journal of the European Union, 2022.

[14] European Union, Regulation (EU) 2016/679 General Data Protection Regulation (GDPR), Brussels, Belgium: Official Journal of the European Union, 2016.

[15] N. Kshetri, “Transforming cybersecurity with agentic AI to combat emerging threats”, Journal of Cybersecurity Studies, Vol. 9, No. 2, 2025, pp. 145–167.

[16] I. Adabara, R. Sharma, and M. Collins, “Trustworthy agentic AI systems: architectures, threat models, and governance strategies”, F1000Research, Vol. 14, 2025, pp. 1–28.

[17] R. Singh, and A. Gupta, “AI-driven governance, risk, and

[18] compliance in regulated industries”, IEEE Access, Vol. 12, 2024, pp. 112345–112362.

[19] P. Zhang, and L. Carter, “AI-enabled continuous compliance monitoring in cloud environments”, IEEE Transactions on Information Forensics and Security, Vol. 19, 2024, pp. 4587– 4601.

[20] M. Hasan, “AI-augmented risk detection in cybersecurity compliance”, Computers & Security, Vol. 135, 2025, pp. 103–125.

[21] S. K. Suggu, “Agentic AI workflows in cybersecurity: opportunities, challenges, and governance via the MCP model”, IEEE Security & Privacy, Vol. 22, No. 4, 2025, pp. 55–67.

[22] A. Agarwal, “AI regulation in telecommunications: cross-sector policy analysis”, Telecommunications Policy, Vol. 49, No. 1, 2025, pp. 102–118.

[23] M. Malatji, “A cybersecurity AI agent selection and decision support framework aligned with NIST CSF”, IEEE Systems Journal, Vol. 18, No. 3, 2025, pp. 2891–2905.

[24] C. Nott, “Organizational adaptation to generative and agentic AI in cybersecurity governance”, Information Systems Frontiers, Vol. 27, No. 2, 2025, pp. 311–329.

[25] Gartner, Emerging Tech: The Impact of AI on Security Operations, Stamford, CT: Gartner Research, 2024.

[26] Google Cloud Security, The Future of Security Operations: Agentic AI in the SOC, Mountain View, CA: Google LLC, 2024.

[27] Darktrace, ActiveAI Security Platform Technical Overview, Cambridge, UK: Darktrace Holdings Ltd., 2023.

Research Scholar Details:

Author 1: Dr. Anil Tiwari

Dr. Anil Tiwari is a cybersecurity and network infrastructure leader with over 20 years of experience across telecom, BFSI, and enterprise sectors. His work has made sustained and measurable contributions to the advancement of cybersecurity architecture, cyber resilience, and digital trust across large-scale telecom and enterprise environments. He has led the design and execution of security-by-architecture programs, embedding Zero Trust principles, cloud-native security, and AI-assisted defense models into mission-critical infrastructure.

Through his doctoral research, “Strategic Integration of Artificial Intelligence into Information Security Architectures: Advancing Predictive Defense and Digital Trust,” Dr. Tiwari advanced practical models for predictive threat defense, demonstrating how AI can be safely integrated into security architectures to enhance anticipation, decision-making, and trust in digital ecosystems.

Google Scholar Profile:
https://scholar.google.com/citations?user=FtwyvicAAAAJ&hl=en&authuser=4

Author 2: Dr. Trilok Singh

- PhD Post Doctoral Researcher, Sarvepalli Radhakrishnan University, ZOC Learnings - Dr. Trilok Singh is a globally recognized mentor for CXOs and top IT professionals. He has been associated with ZOC Technologies, ZOC Learnings, and ZOC Group Companies. With 25 years of experience, he has completed his PhD, a full-time MBA from a top-tier institute, M.Com, MA in Economics, and has earned numerous international certifications along with global publications.

Google Scholar Profile:
https://scholar.google.com/citations?user=-Wppw2cAAAAJ&hl=en&oi=sra

ResearchGate profile:
https://www.researchgate.net/profile/Trilok-Randhawa

Author 3: Dr. Suresh A. Shan

- Dr. Suresh A. Shan is a technology and digital transformation leader with over three decades of experience spanning BFSI, enterprise IT, and large-scale innovation ecosystems. His work has consistently focused on bridging the gap between industry and academia, driving impactful digital transformation, governance frameworks, and scalable technology solutions, particularly in rural and underserved markets.

He has held multiple CXO roles across leading organizations, leading initiatives in IT governance, cybersecurity, data strategy, and enterprise architecture. As a founder, advisor, and board member, he continues to shape next-generation digital ecosystems, combining strategic leadership with hands-on execution in AI, cloud computing, and data science.

Google Scholar Profile:
https://scholar.google.com/citations?user=pOLub8sAAAAJ&hl=en

ResearchGate profile:
https://www.researchgate.net/profile/Suresh-A-Shan-Sas