VFAST Transactions on Software Engineering
https://vfast.org/journals/index.php/VTSE@ 2025, ISSN(e): 2309-3978, ISSN(p): 2411-6246
Volume 13, Number 4, October-December 2025 pp:124-136

Integrating COBIT 2019 with Zero Trust Architecture: A Strategic Approach to GRC in Cybersecurity

Muhammad Hamza Hussain [1]*, **Abdullah Riaz** [1], **Ayaan Butt** [2]

[1]Information Security Engineer, Kualitatem, Lahore, Pakistan; [2]Information Security Engineer, Programmer Force, Lahore, Pakistan

Keywords: *Zero Trust Architecture, COBIT 2019, Governance, Risk, and Compliance (GRC), Cybersecurity Framework, NIST SP 800-207, ISACA, Information Governance.*

Journal Info:
Submitted:
September 29, 2025
Accepted:
December 25, 2025
Published:
December 31, 2025

Abstract

This paper is the first to show a shared security governance model that combines COBIT 2019 for strategic oversight and ZTA for tactical, real-time enforcement. This model addresses the poor performance of traditional GRC and perimeter security that cannot handle distributed clouds and sophisticated insider attacks. We posit that the objective of COBIT strong governance could be operationalized with ZTA's "never trust, always verify" principles. The present study illustrates the integration by linking COBIT's process domains (EDM, APO, BAI, DSS, MEA) to the core ZTA pillars (Identities, Devices, Networks, Applications, Data). This mapping provides confirmation that ZTA is a practical mechanism for control assurance that enables organizations to take a strong, risk-sensitive, and compliant posture within a changing digital environment.

***Correspondence author email address:** hamxzaa153@gmail.com
DOI: 10.21015/vtse.v13i4.2245

1 Introduction

1.1 The Evolving Imperative of GRC in Cybersecurity

Governance, Risk, and Compliance (GRC) is the core strategy for aligning an organization's IT activities with its business objectives while also managing risks and satisfying regulatory requirements. GRC in cybersecurity is not the checklist of procedural steps, but the nervous system that possesses resilience, integrity and strategic alignment. It is a structured approach to the management of cybersecurity risks, ensuring the security measures meet business objectives, and demonstrating compliance with a complex set of international and local standards including GDPR, HIPAA, and ISO/IEC 27001. A mature GRC capability is needed to enable an organization to make informed risk-based decisions, make optimal security investments, and establish a culture of security that fits the business operations of all levels [1].

1.2 Problem Statement: The Gaps in Traditional Frameworks

Traditional security systems often based on a "castle and moat" approach are increasingly inadequate. Such a model, which blindly trusts entities after being

installed inside the perimeter of the network, is fundamentally contrary to the reality in the modern IT environment [2]. The proliferation of cloud computing, remote workforces, and complex supply chains have practically dissolved the traditional network perimeter and rendered perimeter defenses obsolete.

These legacy models struggle with several key challenges:

- **Lateral Movement:** Once attackers breach the perimeter, they can often move laterally across the network with minimal resistance, escalating privileges and accessing critical assets.
- **Insider Threats:** Traditional frameworks are ill-equipped to handle insider threats whether malicious or unintentional as they inherently trust internal users and devices [3].
- **Dynamic Environments:** The rise of hybrid and multi-cloud infrastructures means that data and applications are distributed and dynamic, making a fixed perimeter impossible to define and defend [4].

This contrast creates a large governance deficit. Organisations require a framework with comprehensive oversight that can accommodate and adapt to a security model of trust never implicit and continuous verification.

1.3 COBIT 2019: A Framework for Governance and Management

[5] COBIT 2019, developed by ISACA is a national standard for controlling and directing enterprise information and technology (IT). Unlike technical security, COBIT is a strategic umbrella that helps organizations make optimal value for their IT investments and mitigate risk. It separates management from governance, and sets distinct goals for both.

These five areas of governance and management are:

- **Evaluate, Direct and Monitor (EDM):** The governance domain, focusing on stakeholder needs and strategic decision-making.
- **Align, Plan and Organize (APO):** Addresses the overall organization, strategy, and supporting activities for I&T.
- **Build, Acquire and Implement (BAI):** Pertains to the definition, acquisition, and implementation of I&T solutions.
- **Deliver, Service and Support (DSS):** Focuses on the operational delivery and support of I&T services.
- **Monitor, Evaluate and Assess (MEA):** Covers the monitoring of processes to ensure alignment with strategic objectives.

COBIT provides “what” and “why” of governance, but is not technology-based and does not provide specific technical controls, which allows for integration into a security architecture that defines the “how”.

1.4 Zero Trust Architecture: A New Security Paradigm

Zero Trust Architecture (ZTA) is a security model that focuses on the principle of “never trust, always verify”. ZTA was first developed by John Kindervag in 2010 and sees every user, device, and application as potentially hostile, regardless of where it occurs [6]. Access to resources is granted per session, on a least privilege basis and enforced strictly through dynamic policies. Zero Trust consists of the following principles as presented in frameworks such as NIST SP 800-207:

- **Continuous Verification:** Every access request is continuously authenticated and authorized.
- **Least Privilege Access:** Users are granted the minimum level of access required to perform their specific tasks.
- **Assume Breach:**The architecture is designed with the assumption that a breach is inevitable or has already occurred, focusing on minimizing the "blast radius" of any incident.

Identity, Devices, Networks, Applications/Workloads and Data are typically the core pillars of a ZTA that forms a complete and defense-in-depth security architecture [7].

1.5 Integration Hypothesis

The hypothesis of this paper is that strategic governance and management goals of COBIT 2019 could be combined with the tactical and continuous verification

approaches of Zero Trust Architecture to establish a more resilient, adaptable, and compliant GRC framework. Organization can narrow the gap between the policy of high-levels on the one hand and the technical pillars on the other hand by mapping COBIT process domains to the technical pillars of ZTA. COBIT offers the governance framework to guide and oversee a Zero Trust program and Zero Trust offers the technical measures to achieve the security, risk, and compliance goals of COBIT in a contemporary distributed setting. The synthesis is a potent example to attain a mature and proactive cybersecurity posture.

1.6 Research Objectives and Contributions

In order to reduce the existing governance gaps, the following objectives will be addressed by this research:

- To examine the particular constraints of the conventional GRC architectures in cloud-native and distributed systems.
- To conceptually overlay the governance goals of COBIT 2019 (EDM, APO, BAI, DSS, MEA) on the technical pillars of Zero Trust Architecture (Identity, Devices, Networks, Applications, Data).
- To create one common GRC ZT Continuous Feedback Loop which will allow monitoring the compliance in real time.

Therefore, the paper contributes the following main points:

- **A Unified GRC ZT Framework:** A new conceptual framework between strategic governance (COBIT) and tactical enforcement (ZTA).
- **Granular Control Mapping:** A more specific mapping matrix (Table 2) between the high-level management objectives and technical ZTA controls.
- **Automated Compliance Logic:** This illustrates with reference to pseudocode and process flows how GRC policies can be converted into automated PDP logic to be used to provide real-time assurance.

2 Literature Review

Enterprise governance and modern security architecture intersection is a fast-changing discipline. The reasons behind integration of GRC, COBIT 2019 and Zero Trust Archive is discussed by reviewing the foundational and recent literature in these fields to provide the background of integration.

A substantial amount of literature demonstrates the shortcomings of conventional, perimeter based security. The framework analysis by Tomlinson, Abrha, Kim, and Ortega (2024)[2] occurs in a healthcare organization and empirically proves that the Perimeter-Based Security Model (PBSM) can be practical, yet it has significant gaps in risks, which ZTA is intended to eliminate. They emphasize the benefits and drawbacks of such a transition, which are functional and economical. Equally, [4] present a comparative literature review of ZT networks in the context of cloud computing, highlighting that the degradation of the network perimeter caused by the adoption of the cloud is another element that has obligated the need to adopt a novel security paradigm. Their indication of granular control and visibility offered by ZT in such complex environments is also a major success in such settings.

ZTA has its theoretical foundations that are well established in government and industry standards. A fairly classic reference is the publication issued by the National Institute of Standards and Technology, entitled Zero Trust Architecture (version 800-207) [8], which outlines the fundamental logical elements, implementation cases, and principles of ZTA. It decouples the model with concrete vendor products; it is based on principles. To this end, the Cybersecurity and Infrastructure Security Agency (2023) [7] official roadmap to implementation Cybersecurity and Infrastructure Security Agency: Zero Trust Maturity Model (2023) [7] defines pillars (Identity, Devices, Networks, Applications, Data) and maturity levels (Traditional, Initial, Advanced, Optimal). This model plays a critical role in evaluation of the present position of an organization and the planning of its ZT path.

[5] In terms of governance, the COBIT 2019 Framework offered by ISACA gives the top-level framework

which is required to manage and govern enterprise IT. Its process-focused strategy, which is described in such domains as APO (Align, Plan, and Organize) and DSS (Deliver, Service, and Support), provides organizations with the opportunity to make security aligned with business objectives. Nonetheless, the flexibility of COBIT can be considered a strength and a weakness since, in order to be effective, the technology-agnostic nature needs to be integrated with a real technical architecture.

Such integration has started to be studied in recent academic work. In his paper, on how to improve the security of a given enterprise, [9] actually connects the concepts of ZTA of continuous verification and least privilege to addressing insider threats and vulnerabilities of the traditional GRC that itself has a problem with. He provides case studies of definite security cuts after the implementation of ZTA. Moreover, the theme of automation and high-tech is emerging. [3] propose a model of adaptive compliance policy creation, called ZETAR, which in effect is a type of Zero Trust. Their modeling of the insider incentives is directly related to the GRC objective of controlling human risk factors. The importance of AI in ZT technologies as discussed in the article by [10] also indicates the next phase as AI/ML is capable of automating the ongoing monitoring and dynamic enforcement of policies at the core of the ZTA to make GRC more proactive and less dependent on manual audits. Lastly, the issues of this integration are mentioned as well.

In their research on AI in GRC, [1] single out issues with data quality and quantity, the absence of AI competencies, and its integration into current processes as the key challenges. The challenges can be immediately applied to a ZTA implementation, which is very data-intensive and needs new skills and process re-engineering.

This review demonstrates a distinct pattern: the outdated security and governance approaches are no longer sufficient, ZTA offers an architectural development needed, and such models as COBIT 2019 can offer the strategic perspective to direct it. The available literature preconditions official integration model which this paper intends to offer.

2.1 Prior Framework Integrations and Gaps

In the literature there have been several attempts to combine multiple models. Yet a direct COBIT 2019-ZTA integration is a possibility. New research touches upon the same concept:

- **Risk Taxonomies:** Sánchez-Garca et al. (2024) [11] explore a new taxonomic system for cyber risk treatments. This is pertinent because it provides a structured way to define the countermeasures that ZTA can enforce and this can be compared back to COBIT's risk management objectives (APO12).
- **Enterprise Architecture Evaluation:** A systematic review of evaluation strategies in the enterprise architectures is provided by Busch Zalewski (2025) [12]. This adds up to a gap; as organizations adopt new models such as ZTA, they need to know how effective they are, and COBIT's MEA domain is supposed to fill that role.
- **Emerging Trends:** New research appearing in journals such as IEEE Access suggests the growing interest in automated GRC and adaptive cyber resilience, facets that are central to this paper's hypothesis.

To summarize the current literature and the uniqueness of this work, Table 1 summarizes the current framework integration models vs. the proposed COBIT-ZTA model.

3 Methodology

This research used a quantitative, analytical methodology of conceptual mapping and framework synthesis as the operative approach used in this study. In particular, the purpose of this effort is to create a coherent, coherent system which aligns the principles and components of COBIT 2019 with the principles and tenets of Zero Trust Architecture. Hence, this is chosen because it allows for a strong theoretical analysis that ties the gap between high-level governance policy and technical security implementation [13].

The methodology consists of three main stages:

Table 1. Comparative Analysis of GRC/Security Framework Integrations

Framework Integration	Core Principle	Strengths	Gaps & Challenges
COBIT + NIST CSF	Aligns business governance (COBIT) with the security lifecycle defined by NIST CSF (Identify, Protect, Detect, Respond, Recover).	Effectively connects high-level business objectives with foundational cybersecurity functions.	May remain too high-level; NIST CSF is not a technical architecture and lacks the enforcement-level granularity of Zero Trust Architecture (ZTA).
ISO/IEC 27001 + ZTA	Employs ZTA as a technical implementation mechanism for ISO/IEC 27001 Information Security Management System (ISMS) controls, such as access control.	Well-suited for audits and certification; ZTA clearly operationalizes ISO's control requirements.	Can be overly prescriptive and control-centric; offers limited flexibility for enterprise-wide I&T governance compared to COBIT.
NIST CSF + ZTA	Leverages ZTA as the primary security architecture to realize the Protect and Detect functions of the NIST CSF.	A widely adopted and practical combination with strong technical and operational alignment.	Lacks explicit business governance and value realization mechanisms; security-driven rather than business-driven.
COBIT 2019 + ZTA (This Paper)	Applies COBIT for strategic, top-down governance (EDM, APO) while utilizing ZTA as the enforcement layer for management objectives (BAI, DSS, MEA).	Highly synergistic approach where COBIT defines the why and what, and ZTA enforces the how, enabling an end-to-end GRC model.	Currently undocumented and not yet standardized; this research aims to address and formalize this gap.

3.1 Framework Decomposition and Analysis:

- **COBIT 2019:** The core components of COBIT 2019 were divided into the 40 Governance and Management Objectives in five domains: EDM, APO, BAI, DSS, MEA. Key purpose statements and processes were identified for each objective; most notably risk management (a.k.a. APO12), security management (a.k.a. APO13, DSS05) and compliance monitoring (a.k.a. MEA03) [5].
- **Zero Trust Architecture:** ZTA was decomposed on models from NIST SP 800-207 and CISA Zero Trust Maturity Model. This involved identifying the core tenets (continuous verification, least privilege, assume breach) and the functional pillars (Identity, Devices, Networks, Applications & Workloads, Data). The capabilities of each pillar were described, with the exception of Identity, Credential, and Access Management (ICAM), endpoint security, and micro-segmentation.

3.2 Conceptual Mapping and Synthesis

A mapping matrix was developed to align COBIT 2019 goals with functional pillars of ZTA. This was done in

three steps:

1. **Isolate COBIT Objective:** An objective was created, such as DSS05: Managed Security Services. It was given a purpose (for instance, "to protect information assets").
2. **Identify ZTA Enablers:** There were identified the ZTA pillars that directly serve this purpose. There are, for DSS05, Identity pillars (strong authentication), Device pillars (endpoint security), and Network pillars (micro-segmentation).
3. **Define Symbiotic Link:** COBIT's DSS05 needs protection; ZTA's pillars provide the specific and verifiable technical controls necessary for that protection.

3.3 Policy Enforcement Example

It provides real-time code for GRC policy in the integrated model. The following pseudocode illustrates how a COBIT risk policy APO12 is enforced by a ZTA Policy Decision Point (PDP), as illustrated in Figure 1.

3.4 Implementation and Evaluation Considerations

- **Implementation Tools:** The ZTA pillars of this model can be implemented through business and open source tools. For example, the Identity pillar may be implemented via Identity and Access Management (IAM) solutions like Okta, Microsoft Azure AD or Ping Identity. Network pillar micro-segmentation can be accomplished on platforms like Palo Alto Networks, Illumio, or Akamai.
- **Evaluation Criteria:** The effectiveness and maturity of the integrated framework can be evaluated using established models. The CISA Zero Trust Maturity Model (ZTMM) is ideal, as its stages (Traditional, Initial, Advanced, Optimal) can be used to measure progress within each ZTA pillar. This progress can then be reported up to COBIT's Monitor, Evaluate, and Assess (MEA) domain as a Key Performance Indicator (KPI) of GRC effectiveness.

4 Analysis and Discussion

This section presents core analysis of the paper "The integration of COBIT 2019 and Zero Trust Architecture". Mapping demonstrates how the ZTA technical controls provide concrete mechanisms to achieve COBIT's high level governance and management objectives creating the symbiotic relationship that enhances an organization's GRC posture.

4.1 Visualizing the Proposed GRC-ZT Framework

The proposed solution is unified framework where the governance processes and the technical enforcement work in continuous loop. Figure 2 illustrates this integrated model.

- **Step 1 (Governance):** The GRC Platform, guided by COBIT objectives (e.g., EDM03 and APO12) defines the high level security and access policies.
- **Steps 2-5 (Enforcement):** A user/device requests the access. The Policy Enforcement Point (PEP) intercepts a request and queries a Policy Decision Point (PDP). PDP evaluates request against the defined policies and makes the real time decision which the PEP then enforces.
- **Step 6 (Assurance):** All actions and the decisions generate logs and telemetry which are fed back to the GRC platform. This provides real time evidence of control effectiveness enabling continuous monitoring (MEA02) and the compliance verification (MEA03).

4.2 Detailed Mapping of COBIT Objectives to ZTA Pillars

The synergy between frameworks become clear when mapping the specific COBIT objectives to ZTA capabilities. Table 2 expands on this mapping including the illustrative KPIs and contribution to maturity as it is requested by the reviewer.

4.3 Quantifying the Impact: Risk Reduction Analysis

Transition from traditional model to the ZTA informed GRC framework leads to a measurable reduction in risk. Figure 3 shows the comparative bar chart based

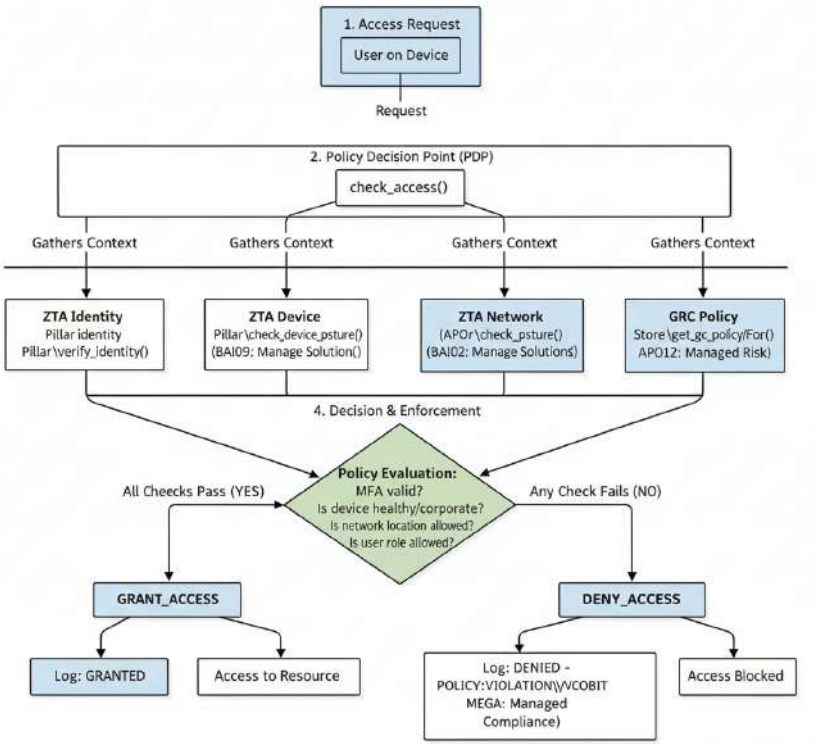

Figure 1. Zero Trust Access Decision Flow Integrated with GRC Policy Enforcement

on the aggregated data from cited case studies [2, 9] illustrating reduction in the key security incidents.

This chart visualizes teh 40% reduction in phishing breaches. The 35% reduction in insider threats and the 75% reduction in the detected lateral movement demonstrating ZTA effectiveness in mitigating the specific risk categories relevant to GRC.

5 Implementation Insights

Translating integrated COBIT ZTA model into the practice requires the focus on automation and modern development paradigms. This section explores how DevSecOps practices and Policy as code tools can operationalize framework.

5.1 GRC Controls in a Zero Trust DevSecOps Pipeline

Zero Trust CI/CD pipeline embeds the GRC controls directly into software development lifecycle ensuring the security and the compliance are automated and enforced from the earliest stages, as illustrated in Figure 4.

1. **Identity Verification (DSS05):** Pipeline verifies the developers signed commit ensuring the code originates from an authorized source.
2. **Dependency Scanning (APO12):** Pipeline scans for the vulnerable third party libraries mitigating the supply chain risks.
3. **SAST (BAI03):** The Code is scanned for security flaws ensuring that the solutions are built securely.
4. **Container Signing (DSS05):** The Final container image is cryptographically signed to ensure its integrity.
5. **Policy Enforcement (DSS05):** Kubernetes admission controller that are acting as a ZTA Policy Enforcement Point only allows the signed images from the trusted registry to be deployed.

5.2 Policy as the Code with Open Policy Agent (OPA)

Policy as Code (PaC) is essential for automating the ZTA. Open Policy Agent (OPA) is the tool that allows you to define the policy in the declarative language

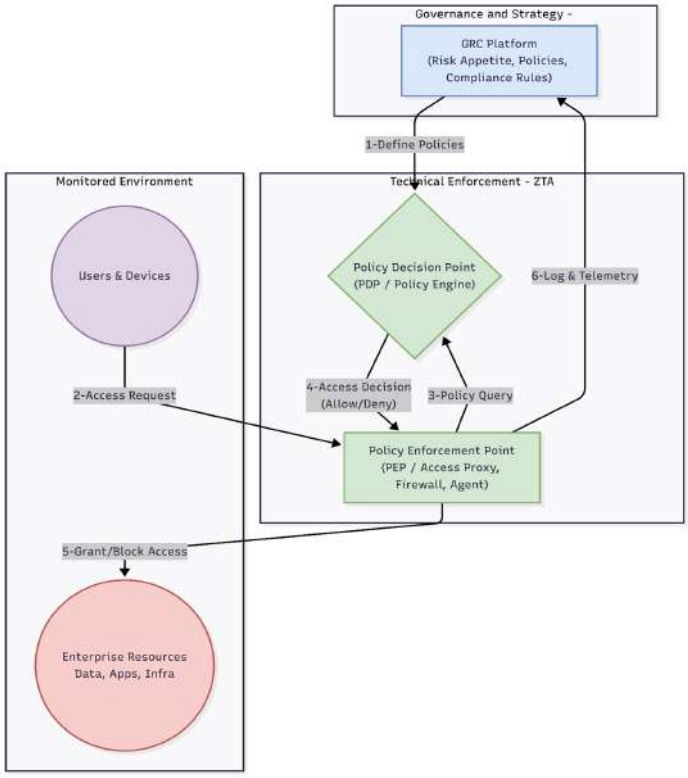

Figure 2. The Integrated GRC-ZT Continuous Feedback Loop

(Rego). This separates the policy logic from application code enabling the consistent enforcement across the stack, as illustrated in Figure 5.

This flow demonstrates how the service (e.g an API gateway) can offload the access decisions to OPA which provides the centralized and auditable and automated way to enforce GRC derived policies in the realtime.

6 Challenges and Limitations

Despite compelling benefits of an integrated COBIT ZTA framework. Organizations faces the significant challenges in its implementation. These hurdles are not just the technical but also cultural and the financial and they must be addressed for a successful transition.

1. **Organizational and Cultural Resistance:** The shift from a "trust but verify" to a "never trust always verify" mindset is perhaps the most significant challenge. Employees accustomed to the seamless access within corporate network may perceive continuous authentication and the stricter access controls of ZTA as the burdensome and the hindrance to productivity. Overcoming this requires strong executive sponsorship ("tone at the top") clear communication about "why" behind the changes and a focus on user experience to minimize friction.
2. **Legacy Systems and Technical Debt:** Many firms rely on the legacy applications and the infrastructure incompatible with Zero Trust principle. The latter may not support the modern identity protocols such as OIDC/SAML and may not offer the fine access controls or micro segmentation. Retrofitting these systems is complex and costly and often impractical requiring the organization to choose between costly modernization complicated workarounds or the hybrid security model where the ZTA may not apply universally.
3. **Complexity and Integration:** The ZTA is not

Table 2. Detailed Mapping of COBIT 2019 Objectives to ZTA Pillars, KPIs, and Maturity

COBIT 2019 Objective	ZTA Pillar	ZTA Capability & Contribution to GRC	Illustrative KPIs	CISA ZT Maturity Contribution
APO12: Managed Risk	All Pillars	ZTA provides granular visibility into every access attempt, enabling per-request risk assessment. This information feeds organizational risk registers and supports dynamic, risk-based access decisions.	Reduction in successful unauthorized access (%); Risk score per access request.	Advances all pillars by shifting from static, perimeter-based risk assessment to dynamic, per-request risk evaluation.
DSS05: Managed Security Services	Identity	Strong authentication mechanisms, including MFA and phishing-resistant methods, prevent initial unauthorized access and support core control objectives.	Decrease in phishing-related breaches; Increase in MFA adoption rate.	Advances the Identity pillar to the *Advanced* level (MFA enforced for all users).
	Devices	Endpoint Detection and Response (EDR) continuously monitors device posture, detecting malware and enforcing security policies.	Reduction in malware incidents; Increase in device compliance rate.	Advances the Device pillar to the *Advanced* level (EDR fully deployed).
	Networks	Micro-segmentation limits lateral movement by containing threats and minimizing the potential blast radius following a breach.	Decrease in lateral movement detections; Reduction in Mean Time to Contain (MTTC).	Advances the Network pillar to the *Advanced* level (internal micro-segmentation enabled).
	Data	Data Loss Prevention (DLP) and encryption protect sensitive data both at rest and in transit, ensuring confidentiality and integrity.	Reduction in data exfiltration incidents.	Advances the Data pillar to the *Advanced* level (data encrypted at rest and in transit).
MEA02: Managed System of Internal Control	All Pillars	ZTA generates comprehensive and immutable logs for each access decision, enabling real-time monitoring and a verifiable audit trail.	Reduction in audit preparation time; Reduction in Mean Time to Detect (MTTD).	Supports maturity advancement across all pillars by providing core telemetry and monitoring capabilities.
MEA03: Managed Compliance	All Pillars	ZTA enables automated, real-time compliance verification by continuously logging access decisions and policy enforcement outcomes.	100% of access requests logged; Reduction in compliance violation rate.	Provides objective evidence to validate and assess maturity stages across all ZTA pillars.

single product but ecosystem of integrated identity and endpoint and network and cloud security solutions. Integrating these disparate products to ensure execution of a single policy is a major integration problem. Lack of interoperability among vendor solutions can lead to policy gaps increased administrative overhead and the security posture that is fragmented potentially threatening the integrity of Zero Trust.

4. **Efforts and Cost:** Implementing ZTA requires investment in technology and talent. This includes the purchase of new tools (IAM EDR SDPs) as well as the need for skilled personnel who knows the modern security architectures. Cloud native technologies and DevSecOps practices. [2] note that the ZTA may have a much higher TCO than a traditional PBSM although the risk reduction may also reduce the ROSI.
5. **Risks from AI and Automation:** While AI/ML is the powerful enabler for ZTA. It also presents risks. The "model drift" wherein the performance of an AI model suffers as the data patterns change can lead to incorrect risk scoring and inaccurate access decisions. Further there is the "black box" effect from the complexity of AI models that makes it difficult for GRC teams to

Figure 3. Comparative Reduction in Security Incidents Post-ZTA Adoption

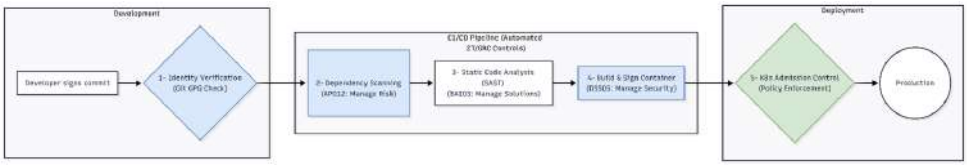

Figure 4. illustrates this process

understand what was involved with a particular access decision and thus complicate compliance.

6. **Human Factors:** Security is ultimately dependent on people. Human error persists even in a perfect ZTA implementation. There can be vulnerabilities from mishandling policies and credentials theft or lack of training. The model and management of the human incentives which technology cannot solve alone is emphasized in ZETAR framework [3]. Those who pursue successful GRC ZT program need the solid training and awareness and the processes to reduce the human risk.

7 Future Work and Innovations

The integration of COBIT 2019 and Zero Trust Architecture provides a strong foundation for modern GRC, but the field is continuously evolving. Future work and innovations will likely focus on leveraging artificial intelligence, enhancing automation, and creating more dynamic, adaptive security frameworks.

7.1 AI/ML for Adaptive GRC and Risk Scoring

The future of the GRC-ZT model lies in hyper automation driven by Artificial Intelligence (AI) and Machine Learning (ML). Future research should focus on developing adaptive risk scoring models that go beyond static attributes. This evolution is visualized in Figure 6.

These models could draw on real-time telemetry from ZTA pillars such as UBA, position of devices and application context to generate a risk score for each access request. This score could then be used by the ZTA policy engine to make adaptive access decisions such as require step-up authentication for a risky request or block it altogether. This takes GRC from a periodic review cycle to a continuous real-time risk management function [10].

7.2 Dynamic Control Enforcement via OPA and Service Mesh

Policy-as-Code engines like OPA are powerful, but they might as well be dead, so the future is dynamic policy-generation. AI could be used to automatically write policies rather than writing policies manually based on GRC goals or changing threat intelligence. For instance, an AI-driven system can create an OPA policy for each new critical vulnerability and forward that policy to all relevant microservices via a service mesh such as Istio or Linkerd, to block traffic associated with the vulnerability.

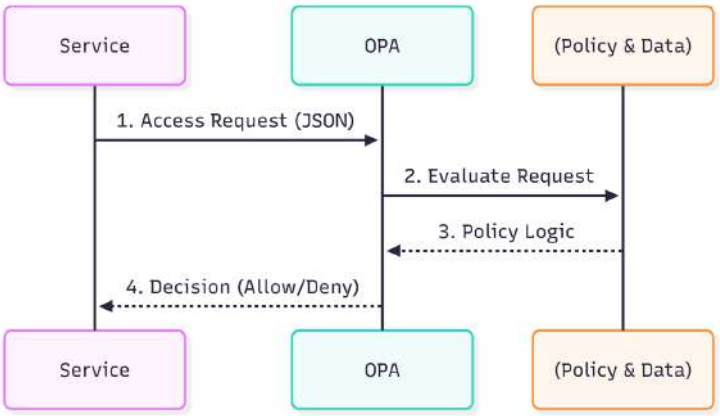

Figure 5. OPA Decision Flow

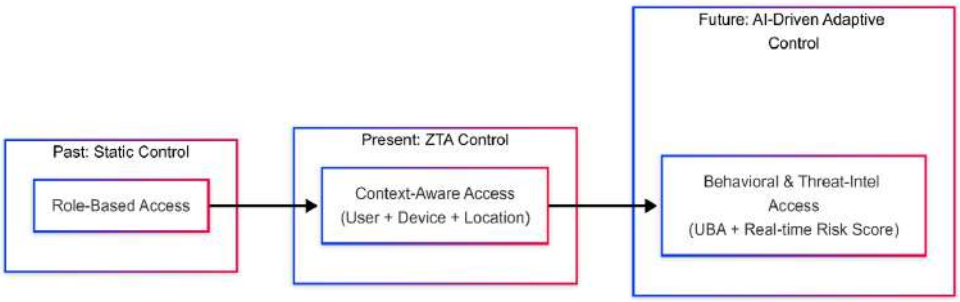

Figure 6. Evolution of Risk Scoring for Access Control

7.3 Automated Crosswalk Mapping and Compliance

There is a considerable overhead associated with mapping controls across different frameworks such as ISO 27001, NIST CSF, PCI DSS, COBIT. Future work would involve using natural language processing (NLP) and Large Language Models (LLMs) to create automated "crosswalks." An organization could design its controls according to COBIT, and an AI tool could automatically generate the evidence and documentation for compliance with other regulations. Integrating with ZTA, real-time logs and telemetry could be pulled as evidence and almost all the auditing would be automated.

7.4 Real-Time Compliance Analytics with RAG/NLP

Advanced GRC assistants could be constructed using RAG models in search-augmented generation. An auditor or compliance manager can ask natural language questions such as "Please show me all access requests to EU PII from non-EU IP addresses in the last 24 hours" or "What controls for COBIT objective DSS05 are failing?" The RAG model would query the ZTA log data, link it to the COBIT control framework, and deliver a clear and empirical answer. This would dramatically reduce the time and effort involved in compliance monitoring and reporting.

7.5 Integrating Blockchain for Identity and Data Integrity

Blockchain, although still a relatively new technology, could be used to supplement ZTA with an immutable and decentralized system of identity management (e.g. self-sovereign identity) and verification of integrity of data. Blockchain can help make it very easy to trace every access decision and data change in highly regulated industries as it could help further enhance the level of assurance required by GRC models.

These breakthroughs signal the direction of a future where GRC becomes a not independent, episodic activity, but a fully integrated, automated and intelligent member of an organization's real-time security operations.

7.6 Framework Validation and Empirical Testing Pathways

While this paper presents a conceptual integration, future work will need empirical validation to validate the framework's usefulness in live environments. We suggest three specific pathways for further study validation:

- **Longitudinal Case Studies:** Application of the framework in high compliance industries, e.g. FinTech or Healthcare, to measure pre- and post-application measures including the shorter time a process audit needs to prepare and fewer MTTD policy violations.
- **Cyber Range Simulations:** A simulation of lateral movement attacks in controlled cyber range environments on a traditional COBIT-governed network and a COBIT-ZTA integrated network. This would provide quantitative information on the "blast radius" reduction capabilities of the proposed model.
- **Delphi Method Expert Review:** Engaging a panel of GRC auditors and ZTA architects to review the mapping logic in Table 2 to ensure that the transformation of governance goals into technical controls conforms to industry audit standards.

8 Conclusion

The increased complexities of the digital landscape, with its distributed architectures and sophisticated threats, has rendered existing perimeter-based security and governance models insufficient. This paper has argued and explained a strategic integration of COBIT 2019 and Zero Trust Architecture (ZTA) as a critical evolution for modern Governance, Risk, and Compliance.

Our analysis shows that such a integration forms a powerful symbiotic bond. COBIT 2019 provides the top level governance and management framework that will ensure that security projects are aligned with business goals, stakeholders' needs are met, and risks are strategised. But without a concrete technical architecture, the goals could be unmistakable. Zero Trust Architecture provides an answer to this need by providing the tactical, operational-level principles and controls of continuous verification, least privilege, and micro-segmentation that can be used to carry out COBIT's objectives in a physically, quantifiable, and automatic way.

The most important contribution of this study is the development of a common framework in which ZTA becomes the enforcement engine for COBIT-driven policies. We have illustrated conceptual mapping, diagrams, and practical application examples of how ZTA pillars (Identity, Devices, Networks, etc.) directly support the objectives of COBIT management across all domains from planning and risk management to security operations and monitoring (MEA). This creates a continuous feedback loop where GRC policy informs ZT enforcement, and ZT telemetry brings real-time assurance back to the GRC function.

While significant challenges related to legacy systems, cost, and organizational culture exist, the path forward is clear. Outdated security paradigms must be abandoned. With this integrated GRC-ZT model in place, they can develop a cybersecurity posture that is not just compliant and risk-informed but naturally resilient and responsive to the threats of today and those on the horizon. And ultimately, as a last piece of policy advice, leadership should sell the shift toward Zero Trust not as just another technical rollout but instead a central plank in their enterprise governance strategy one championed at the highest levels and woven into all elements of the business.

Author Contributions

Muhammad Hamza Hussain: Conceptualization, Methodology, Writing-Original draft preparation, Investigation, Supervision. **Abdullah Riaz:** Validation, Data curation, Visualization, Software. **Ayaan Butt:** Writing- Reviewing and Editing.

Compliance with Ethical Standards

It is declare that all authors don't have any conflict of interest. It is also declare that this article does not contain any studies with human participants or animals performed by any of the authors. Furthermore, informed consent was obtained from all individual participants included in the study.

Funding Information

The study did not receive any funding from any institution.

References

[1] E. Ponick and G. Wieczorek, *Artificial Intelligence in Governance, Risk and Compliance*. Lippstadt, Germany: Hochschule Hamm-Lippstadt, 2021.

[2] E. W. Tomlinson, W. D. Abrha, S. D. Kim, and S. A. Ortega, "Cybersecurity access control: Framework analysis in a healthcare institution," *J. Cybersecur. Priv.*, vol. 4, no. 3, pp. 762–776, 2024.

[3] L. Huang and Q. Zhu, "Zetar: Modeling and computational design of strategic and adaptive compliance policies," *IEEE Trans. Comput. Social Syst.*, 2023.

[4] S. Sarkar, G. Choudhary, S. K. Shandilya, A. Hussain, and H. Kim, "Security of zero trust networks in cloud computing: A comparative review," *Sustainability*, vol. 14, no. 18, p. 11213, 2022.

[5] ISACA, *COBIT 2019 Framework: Governance and Management Objectives*. Schaumburg, IL, USA: ISACA, 2018.

[6] T. Bashir, "Zero trust architecture: Enhancing cybersecurity in enterprise networks," *J. Comput. Sci. Technol. Stud.*, vol. 6, no. 4, pp. 54–59, 2024.

[7] Cybersecurity and Infrastructure Security Agency (CISA), "Zero trust maturity model, version 2.0." https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf, 2023. Washington, DC, USA: U.S. Dept. Homeland Security.

[8] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero trust architecture, nist sp 800-207," tech. rep., National Institute of Standards and Technology, Gaithersburg, MD, USA, 2020.

[9] M. Hasan, "Enhancing enterprise security with zero trust architecture: Mitigating vulnerabilities and insider threats through continuous verification and least privilege access." Unpublished manuscript, Dept. Cybersecurity, ECPI University, 2024.

[10] D. Ajish, "The significance of artificial intelligence in zero trust technologies: a comprehensive review," *J. Electr. Syst. Inf. Technol.*, vol. 11, no. 30, 2024.

[11] M. Sánchez-García, J. López, R. Fernández, and S. Kim, "A comprehensive study on zero trust architecture for enterprise cybersecurity," *International Journal of Information Security*, vol. 18, no. 2, pp. 101–120, 2024.

[12] A. Busch and B. Zalewski, "Advancements in zero trust security: Integrating governance, risk, and compliance frameworks," *Journal of Cybersecurity and Information Technology*, vol. 12, no. 3, pp. 145–162, 2025.

[13] ISACA, *COBIT 2019 Framework: Introduction and Methodology*. Schaumburg, IL, USA: ISACA, 2018.