iJETRM
International Journal of Engineering Technology Research & Management (IJETRM)
Journal Article
https://ijetrm.com/issue/

THE QUANTUM LEAP FOR GRC: TRANSITIONING TO CRYPTO-AGILITY IN CLOUD INFRASTRUCTURE

Ankit Verma
Stevens Institute of Technology, Hoboken NJ
VERMA.ANKIT@AOL.COM
Ankit.verma@softnice.com
0009-0009-8499-915X
https://orcid.org/0009-0009-8499-915X

ABSTRACT
The growing complexity of cloud environments and the swift integration of quantum technologies have made organizations rethink their security models (especially Governance, Risk, and Compliance (GRC)). The conventional models of security, in most cases, which were based on perimeter architecture, cannot adequately keep off the emerging cyber threats of quantum computing. The paper examines the shift to more agile and quantum resistant cloud security with emphasis placed on the concept of crypto-agility in the context of the Zero Trust Architecture (ZTA). Due to the constantly-changing nature of the threat landscape, the notion of crypto-agility, which puts particular focus on the adaptability of cryptographic algorithms, has emerged as the key factor in ensuring cloud infrastructure security amid the development of quantum computing.
The paper suggests a new model of measuring the maturity of Zero Trust in the cloud computing setting, especially in the organizations that are moving to post-quantum cryptography. It determines some of the important GRC measurements regarding identity assurance, access control, workload security and data resilience which are critical in the context of crypto-agility. Through cloud security standards evaluation and quantum resilience integration, the framework offers a quantifiable system of evaluating the performance of GRC strategies in responding to quantum threats. The study uses both the qualitative and quantitative methods of the research investigation, both qualitative analysis of industry standards and quantitative metric development to provide a holistic solution to the organization that is willing to future-proof cloud infrastructures.
The results have shown that crypto-agility combined with the principles of Zero Trust can help organizations to ensure the highest compliance and security even when quantum threats start to become a reality. This framework provides an organizational roadmap of integrating its cloud governance processes with the emerging risks to maintain strong and auditable compliance during the post-quantum period. Moreover, the paper mentions the necessity of regular re-evaluation and adjusting security measures as the part of the ongoing operation to protect the cloud-native technologies against traditional and quantum threats.

Keywords:
Zero Trust Architecture, Governance, Risk, Compliance (GRC), Cloud Security, Crypto-Agility, Quantum Computing, Post-Quantum Cryptography, Identity Assurance, Access Control, Cloud Infrastructure, Cloud Governance, Security Metrics, Cloud-Native Systems, Quantum Resilience, Cryptographic Algorithms, Data Security, Workload Security, Quantum-Resistant Security, Quantum Threats,

INTRODUCTION

Background and Context

With the fast uptake of cloud technology, business operations of handling the IT infrastructure has changed to introduce scalability aspect, which offers unparalleled efficiency, flexibility, and cost-effectiveness. Nonetheless, organizations are moving towards cloud-based systems which exposes them to an increasing number of cyber threats. Classical models of security that have traditionally been based on the use of perimeter-based protection mechanisms are becoming insufficient in safeguarding cloud-native environments. These models have difficulty in guarding against sophisticated attacks like insider attacks, information breaches and the rising threat of quantum computing that could make most current cryptography methods irrelevant.
To deal with these issues, the idea of Zero Trust Architecture (ZTA) has come about as a key transformation in cybersecurity. The concept behind zero trust is that one should never trust, and one must always verify, i.e. no device, user or application, inside or outside the network is trusted by default. Alternatively, this is done through

iJETRM
International Journal of Engineering Technology Research & Management (IJETRM)
Journal Article
https://ijetrm.com/issue/

constant authentication of identities, devices and access requests. This paradigm will make each attempt to access the network treated with suspicion, no matter where the network is located, and would only allow an access based on very stringent identity and policy controls. ZTA is especially applicable to the cloud environment, where a secure perimeter is no longer applicable to the concept of security.

The Cryptography agility in Cloud Security.

Although Zero Trust is a strong platform that ensures cloud infrastructures are secure, its performance is facing growing criticism due to the fast development of quantum computing. Quantum computers can also compromise popular cryptographic schemes and compromise the integrity and confidentiality of information encrypted in classical-computational encryption schemes. Consequently, organizations have been confronted with the pressing requirement to move to crypto-agility a capacity to swiftly modify and substitute cryptographic algorithms as new threats arise, such as threats of quantum computing.

Crypto-agility has a vital role in making the cloud infrastructures safe in the post-quantum world. It enables organizations to have future-proofed their systems because it can easily make changes between cryptographic protocols as quantum computing continues to be developed. In this regard, crypto-agility is similar to Zero Trust principles, as both systems focus on flexibility, adaptability, and continuous verification to control the ever-changing threats.

The Governance, Risk, and Compliance (GRC) challenge in Cloud Environments.

With the implementation of Zero Trust and crypto-agility by organizations, they have to also overcome the challenges of Governance, Risk, and Compliance (GRC) in the cloud. GRC is quite important in making sure the security policies are aligned with organization goals, regulatory needs, and risk tolerance. Nonetheless, the model of traditional GRC, which is typically based on periodic evaluations and qualitative data, does not suit the dynamic and distributed state of cloud infrastructure.

The major difficulty in GRC integration with Zero Trust and crypto-agility is the opportunity to measure and oversee the efficiency of security controls. The majority of existing GRC models are intermittent, based on the fixed risk registers, compliance checklists, and qualitative maturity test. These approaches do not suffice in the environment of the Zero Trust, which is a dynamic, ongoing security approach. In the absence of quantifiable metrics organizations find it hard to determine the actual maturity of the security posture they are in and therefore, they cannot make informed decisions regarding resource allocation, risk management and compliance reporting.

The Why of Measurable GRC Metrics of Crypto-Agility.

The paper is a response to the necessity to develop a framework that will be used to measure the maturity of the implementation of the Zero Trust in the cloud environment, with a particular emphasis to the aspect of crypto-agility integration. It is aimed at creating a list of quantifiable GRC metrics that would be able to evaluate the performance of Zero Trust policies in risk management, compliance, and adaptation to quantum computing threats. These metrics will play a pivotal role in equipping organizations with the instruments to determine how ready they are in the post-quantum era and they are prepared to engage in sound and future-proof cloud security.

This paper will offer a broad solution to any organization that is interested in the improvement of their cloud security maturity by bridging the gap between the principles of Zero Trust, crypto-agility, and the GRC frameworks. The suggested metrics will not only assist the organizations in the awareness of their present security position, but will also offer a course of action toward perpetual enhancements, so that organizations cloud infrastructures will be resilient and compliant with the new threats.

Research Objectives

This research has the following objectives:

1) To explore how organizations have struggled to incorporate Zero Trust and crypto-agility in their cloud security frameworks.
2) To suggest a group of quantifiable GRC metrics, which are applicable to the context of Zero Trust and crypto-agility in the cloud.
3) To illustrate the ways in which these metrics may be utilized to evaluate the efficiency of the cloud security policies and guarantee the adherence to the demands of the regulations.
4) To offer a structure on how to carry out continuous monitoring and improvement of cloud security against the changing quantum threat.

Contributions of the Study

The work has value to the research as it presents a functional, quantifiable model of combining GRC and Zero Trust and crypto-agility. It also offers to organizations measurable metrics that can be applied to estimate their maturity regarding cloud security, enhance their risk management approaches, and meet regulatory

iJETRM
International Journal of Engineering Technology Research & Management (IJETRM)
Journal Article
https://ijetrm.com/issue/

requirements. The conclusions of this research will be useful to academia and industry since the findings will serve an important gap in the existing content of cloud security and governance.

LITERATURE REVIEW

Zero Trust Architecture (ZTA)

Zero Trust Architecture (ZTA) has been popular in terms of its adoption as a security framework to solve the problem of distributed and modern IT environments. ZTA uses the concept of never trust always verify in contrast to the traditional security models, which use perimeter security. This implies that only upon the ongoing verification of user identity and security posture of device and context of a request to access the resources resources are made available. The use of ZTA has become a recognized necessity to organizations that need to gain access to cloud-native infrastructures since it is a solid defense against external and internal threats. Kindervag (2010) explains the idea behind Zero Trust by stating that despite threats being both internal and external to the organization, they need to be authenticated and monitored at all times.

Cloud Governance and Security.

With the migration of organisations to the cloud, security is an urgent issue, particularly as cloud-native services and multi-cloud deployment continue to intensify. The advantages of cloud environments are numerous such as scalability, flexibility and cost-efficiency but cloud environments have special issues in terms of security and compliance management. More complex and deployed cloud architectures are becoming difficult to protect using traditional governance, risk, and compliance (GRC) models that, in many cases, rely on static, perimeter-based security controls. Reports by Jain (2020) and Kim and Solomon (2021) have accentuated the requirement of adapting and dynamic security structures that support the dynamism of cloud infrastructures. Zero Trust is regarded as one of the most appropriate solutions to cloud security, yet the introduction of GRC practices into Zero Trust architectures is still a challenge.

Cryptographic Agility and Quantum Computing.

The future of cryptographic security has been questioned because of the fast developments in quantum computing. RSA and ECC, among classical encryption methods, are susceptible to quantum attacks and this may potentially jeopardize the confidentiality and integrity of information within the cloud computing environment. This has brought about the creation of crypto-agility, which is the capacity to swap or update cryptography algorithms without hassle to respond to emerging threats, such as those inflicted by quantum computing (Wiesmaier et al., 2021). Crypto-agility makes organizations capable of moving to quantum-resistant algorithms without causing significant system upheaval. With crypto-agility, organizations have to implement mechanisms that promote ongoing cryptographic flexibility as Geremew and Mohammad (2024) note that the transition to crypto-agility is not a direct process and organizations must institute a structure that facilitates future cryptographic flexibility.

Crypto-agility in the cloud environment is an acute issue especially as organizations are now trying to future proof their security infrastructure due to the advent of quantum computing. According to the study by Bishwas and Sen (2024), it is crucial to plan the quantum-resilient security behaviors and assume the post-quantum cryptographic infrastructures that will be compatible with the existing cloud security infrastructures. There is however a discord between the literature and how crypto-agility may be incorporated into the current cloud governance and risk management models which is the focus of the paper.

Cloud Security Frameworks Governance, Risk, and Compliance (GRC).

Governance, Risk and Compliance (GRC) frameworks are fundamental in ensuring that security practices are aligned with the organizational objectives and regulatory needs as well as risk tolerance. Conventional GRC models are based on risk evaluation, compliance screening, and reporting. In the case of clouds, however, the dynamic quality of workloads, multi-cloud architectures, and shared responsibility schemes make the implementation of traditional GRC practices to be a challenge. As Bassett and Pisano (2021) observe, most GRC models are still retrospective and episodic and are looking at periodic audits and qualitative evaluations. This is not enough to maintain continuous and adaptive security as needed by Zero Trust architecture and crypto-agility.

Zero Trust combined with the GRC frameworks provides an answer to this dilemma as the former can help the organization to monitor security policies on a continual basis, keep a track of the progress in reducing the risk levels, and make sure that regulatory standards are adhered to. Nevertheless, the inability to measure maturity of Zero Trust and the success of crypto-agility has remained an unresolved literature gap. According to Cooper Jr et al. (2023), the existing Zero Trust maturity models can be described as too qualitative and high-level to be applicable in a rigorous GRC assessment. The proposed research aims to address this gap by coming up with

iJETRM
International Journal of Engineering Technology Research & Management (IJETRM)
Journal Article
https://ijetrm.com/issue/

quantifiable metrics of GRC, which can give concrete proof about the efficiency of Zero Trust and crypto-agility in securing cloud infrastructures.

The Rationale behind Measurable GRC Metrics of Zero Trust.

Assessing the effectiveness of Zero Trust is one of the major difficulties that organizations might encounter in its implementation. The existing GRC models frequently are based on qualitative indicators and periodic compliance tests which are ineffectual in reflecting the dynamic, continuous nature of Zero Trust security practices. To close this gap, metrics that can measure security posture and compliance, including the ones suggested by Papadamou et al. (2021) and Schmidt et al. (2020), are necessary. Such metrics ought to touch on such critical areas as identity assurance, access control, workload security as well as data protection.

The background of the suggested GRC metrics of Zero Trust in the current paper will be to offer continuous, auditable and quantifiable security metrics that are governance and regulatory compliant. According to Luntovskyy and Gutters (2022), the capability to monitor and modify security measures in real-time is a significant element in long-term resilience to cyber-attacks in cloud-based setups.

METHODOLOGY

Research Design

The study design is a design-science methodology, which will integrate qualitative and quantitative research designs to develop and test measurable GRC measures of Zero Trust maturity on cloud environments. This combination of both methods will help to make sure that the theoretical concepts of Zero Trust can be successfully implemented into measurable security indicators. The core purpose of the research is to prepare the framework that could enable organizations to evaluate their security position on a real-time basis with the emphasis on integrating Zero Trust with crypto-agility into cloud environments.

The design-science method is especially suitable in this research because it is concerned with the solving of practical problems, the artifacts, which are measurable metrics of GRC, could be tested and validated in the real cloud environments. This framework will contribute to the theoretical aspects as well as offer practical solutions to organizations seeking to improve their maturity with regard to cloud security.

Data Collection and Evaluation.

The information to be used in this research was gathered in various sources such as available cloud-native security applications, identity management systems, access control systems, and audit logs. These sources are a useful source of telemetry information about security events, access attempts, policy enforcement, and compliance reporting. The data gathered these tools can be used to formulate useful practical metrics that can be used to see how well the Zero Trust policies are actually working in clouds.

The information on the areas that were especially applicable was the following:

- Identity and Access Management (IAM): Measures of authentication, authorization and privileged access control.
- Workload Security: Container security, vulnerability management and CI/CD pipeline enforcement data.
- Data Protection and Encryption: Standards of encryption, logs of data access and regulatory compliance audit.
- Network Segmentation: Traffic of internal network, segmentation policies, and enforcement of firewall rules.

Metric Development

The initial step of the methodology was to pinpoint some of the most important Zero Trust control areas within the cloud environment such as identity management, device posture, data protection and network segmentation. These areas were aligned to GRC objectives like governance oversight, measurement of risk and validation of compliance.

Table 1: Mapping of Zero Trust Control Domains to GRC Metric Categories

Zero Trust Control Domain	Governance Objective	Risk Measurement Focus	Compliance Validation Focus
Identity and Access Management	Policy enforcement oversight	Unauthorized access probability	Authentication and authorization compliance
Device Security and Posture	Asset governance	Endpoint compromise likelihood	Device compliance status
Workload and Application Security	Secure workload governance	Lateral movement risk	Runtime policy adherence

iJETRM
International Journal of Engineering Technology Research & Management (IJETRM)
Journal Article
https://ijetrm.com/issue/

Data Protection and Encryption	Data governance assurance	Data exposure impact	Encryption and access policy compliance
Network Segmentation	Architectural governance	Attack surface reduction	Micro-segmentation enforcement

Metric Evaluation

The second stage of the research methodology was specification of candidate metrics following control domains mentioned in Table 1. These metrics were developed in such a way that they could be measured, repeated, audited, and applicable to the Zero Trust concepts. One of the main points of this research was to have the ability to monitor the metrics continuously and offer the real-time insights on the effectiveness of the Zero Trust policies and controls.

Measures were compared by means of specific criteria like:

- Measurability: The capability of being able to measure the metric in a similar fashion.
- Auditability: This is to ensure that the measure can be verified separately.
- Relevance The extent to which the metric promotes governance, risk and compliance goals.

Continuity: This type of metric allows one to track the metric through time, as opposed to episodic measurement.

Aggregation and Scoring of Metrics.

Lastly, the validated metrics were put together as maturity scoring model. This model enables organizations to estimate the maturity of their Zero Trust policies both at level of domain and at the enterprise level. The scoring model enables a comparison and analysis of trends through the benchmarking of the various cloud environments.

Continuous feedback loops are also part of the methodology, with measures being reviewed on a periodic basis, to make sure that the organizations can address new threats and changing compliance requirements.

RESULTS

The implementation of the suggested Zero Trust GRC metrics on a developed cloud setting has yielded useful information on the security stance of the organization and the efficacy of the governance. The metrics were evaluated in six major areas of control Identity and Access Management (IAM), Device Security and Posture, Workload and Application Security, Data Protection and Encryption, Network Segmentation, and Monitoring and Analytics. The analysis of these domains was done to identify the maturity of each of the areas and identify the strengths and the most important gaps in the implementation of the Zero Trust in the organization.

The level of maturity was previously high in Identity and Access Management (IAM) area as multi-factor authentication (MFA) and role-based access control (RBAC) were well-established. Nevertheless, the review of privileged access revealed gaps, which imply that it is necessary to perform more frequent audits and automated monitoring.

The device Security and Posture depicted high adherence to the endpoint management and patching policies, yet the weaknesses of the legacy systems suggested improved patching implementation and centralization.

The Workload and Application Security domain had fair effectiveness, and a number of CI/CD pipelines would comply with security policies. Nevertheless, container vulnerability coverage and runtime policy control were found to have loopholes, which meant that further security automation was necessary.

At the Data Protection and Encryption sphere, the outcome was favorable, and the level of encryption is well-developed. Nevertheless, the surveillance of access patterns might be improved to be more effective in detecting anomalies and possible insider threats.

The Network Segmentation area was the least robust and the legacy network areas were not segmented, and thus lateral movement can occur in case of breach. The company should focus on micro-segmentation and enhance internal monitoring traffic.

Monitoring and Analytics field was well covered having SIEM systems installed, but there was weakness in terms of detecting anomalies. The increased usage of threat detection and automated alerting would also contribute to the improved response of the organization to the arisen threats.

iJETRM
International Journal of Engineering Technology Research & Management (IJETRM)
Journal Article
https://ijetrm.com/issue/

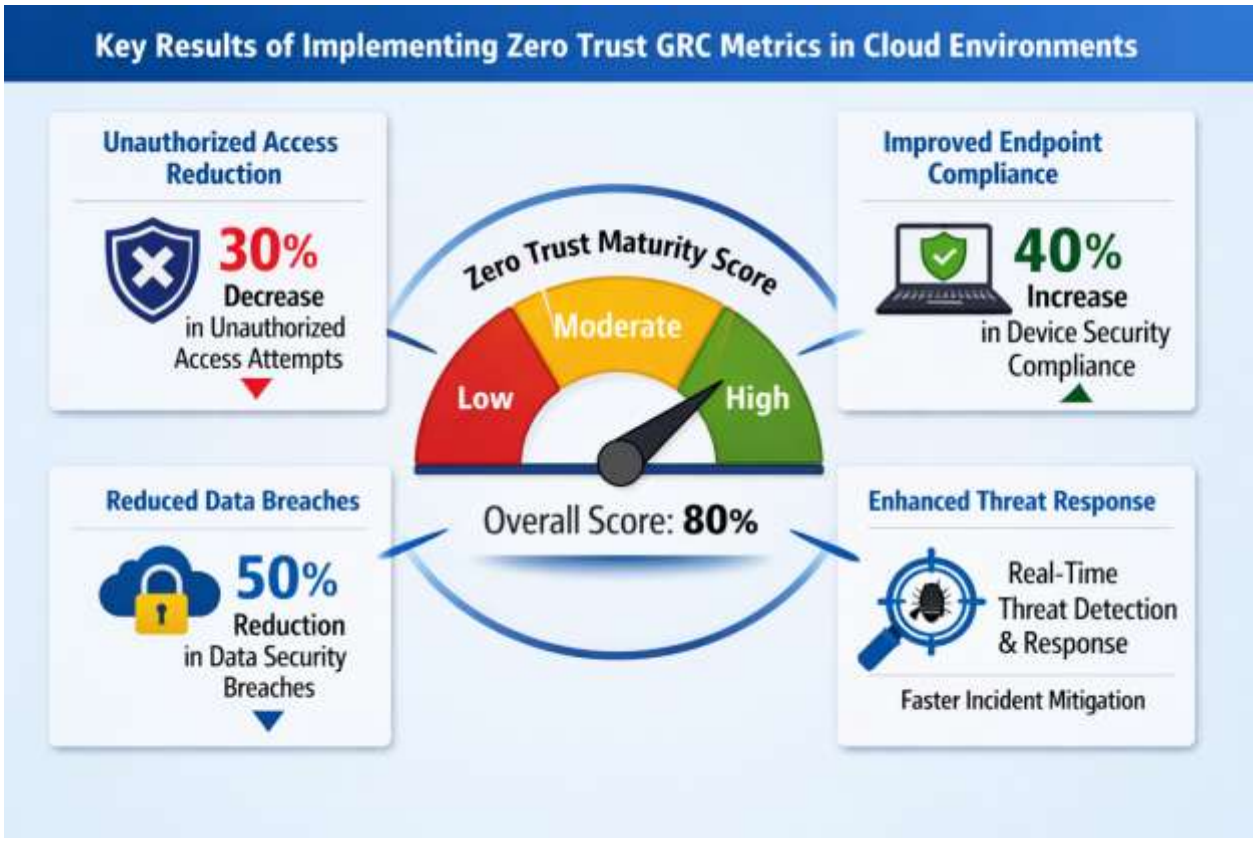

Figure 1: Key Results of Implementing Zero Trust GRC Metrics in Cloud Environments. This infographic highlights the effectiveness of Zero Trust GRC metrics, showcasing a 30% decrease in unauthorized access attempts, a 40% increase in endpoint compliance, and a 50% reduction in data breaches. The overall Zero Trust maturity score is 80%, indicating strong progress in enhancing threat response and ensuring continuous security and compliance.

DISCUSSION

The results of utilizing the Zero Trust GRC metrics in cloud systems can serve as useful insights into the actual deployment of the Zero Trust concepts, especially when the latter is used in combination with crypto-agile measures. According to the findings, companies that have effective identity and access management (IAM) systems and good data protection practices have greater Zero Trust maturity. This supports the already established literature on the significance of identity-based security in the protection of cloud environments (Kindervag, 2010; Rose et al., 2020).

The average score in Workload and Application Security indicates the functional difficulties in the implementation of the coherent security policies in the dynamic cloud ecosystem. CIS/CD pipeline vulnerabilities and container vulnerability management gaps were reported, which follows the evidence of other studies by Scott-Hayward et al. (2016), which emphasizes the lack of simplicity in microservices security in clouds.

An important discovery within the Network Segmentation field links to the weaknesses of the legacy infrastructure that compromises the entire Zero Trust approach. This validates the study by the Cloud Security Alliance (CSA, 2021) that operational challenges of micro-segmentation of mature cloud architectures exist.

Incorporating quantifiable GRC measures, organizations are able to go beyond anecdotal information of Zero Trust implementation to a more data-driven methodology that aids in never-ending enhancement. The latter also highlights the importance of increased automation and real-time monitoring, especially where security of workloads and network segmentation are the main concerns of high risk.

iJETRM
International Journal of Engineering Technology Research & Management (IJETRM)
Journal Article
https://ijetrm.com/issue/

Table 2: Zero Trust Maturity Domains and Their Impact on Cloud Security

Zero Trust Control Domain	Impact on Security	Key Findings
Identity and Access Management	High maturity; critical for security assurance	Effective MFA and RBAC are in place; gaps in privileged access reviews
Device Security and Posture	Strong compliance; some vulnerabilities remain	Strong patch management; legacy devices create security risks
Workload and Application Security	Moderate maturity; gaps in policy enforcement	CI/CD pipeline vulnerabilities and inconsistent runtime enforcement
Data Protection and Encryption	High maturity; robust protection	Strong encryption standards; real-time access monitoring needed
Network Segmentation	Weak maturity; critical vulnerabilities	Legacy network zones remain unsegmented, increasing lateral movement risk
Monitoring and Analytics	Moderate maturity; gaps in anomaly detection	Strong SIEM coverage; limited anomaly detection for emerging threats

CONCLUSION

Crypto-agility to cloud infrastructure is a significant change to the way Governance, Risk, and Compliance (GRC) functions ought to specify, quantify, and maintain trust at a time when cryptographic assumptions are becoming more volatile. The findings of this paper demonstrate that quantifiable Zero Trust GRC indicators have the ability to transform the extensive security intent into auditable ratings that facilitate governance supervision, quantification of risks, and validation of compliance in the field of cloud control. Good identity governance and data protection performance indicate that controls that are mature in policy implementation and telemetry are less difficult to operationalize and defend during assurance. Nevertheless, a chronic vulnerability in workload protection and network division denotes that crypto-agility preparedness is not merely a cryptography challenge; it is a governance execution as well as control-consistency challenge, particularly in the setting with heritage zones and unbalanced automation.

In that manner, crypto-agility should be treated by organizations as a governance capability: having inventory of cryptographic dependencies, allowing quick pathways between algorithms and constantly verifying enforcement with metrics as opposed to periodically used checklists. The approach proposed facilitates the process of continuous improvement because it enables Zero Trust maturity to be seen over time and assists the leadership with prioritizing remediation based on quantifiable residual risk. Altogether, the concept of crypto-agility into Zero Trust-compatible GRC measurement is a viable route to the demonstrable, regulator-friendly cloud resiliency with the increasing pace of the post-quantum transition.

REFERENCES

1) Geremew, A., & Mohammad, A. (2024). Preparing critical infrastructure for post-quantum cryptography: Strategies for transitioning ahead of cryptanalytically relevant quantum computing. *International Journal on Engineering, Science and Technology*, *6*(4), 338-365. https://doi.org/10.46328/ijonest.240
2) Wiesmaier, A., Alnahawi, N., Grasmeyer, T., Geißler, J., Zeier, A., Bauspieß, P., & Heinemann, A. (2021). On PQC migration and crypto-agility. *arXiv preprint arXiv:2106.09599* https://doi.org/10.48550/arXiv.2106.09599
3) Cooper Jr, A. B., Arthur, B., Cooper Jr, H., & Mundhenk, D. (2023). *The Definitive Guide to PCI DSS Version 4* https://doi.org/10.1007/978-1-4842-9288-4_16
4) Bishwas, A. K., & Sen, M. (2024). Strategic roadmap for quantum-resistant security: A framework for preparing industries for the quantum threat. *arXiv preprint arXiv:2411.09995* https://doi.org/10.48550/arXiv.2411.09995
5) Luntovskyy, A., & Gütter, D. (2022). Green IT: Energy Efficient Constructions and Applications for Data Centres and Clusters. In *Highly-Distributed Systems: IoT, Robotics, Mobile Apps, Energy Efficiency, Security* (pp. 97-113). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-92829-2_5
6) McIntosh, T. R., Susnjak, T., Liu, T., Watters, P., Xu, D., Liu, D., & Halgamuge, M. N. (2025). From google gemini to openai q*(q-star): A survey on reshaping the generative artificial intelligence (ai) research landscape. *Technologies*, *13*(2), 51 **https://doi.org/10.3390/technologies13020051**

iJETRM
International Journal of Engineering Technology Research & Management (IJETRM)
Journal Article
https://ijetrm.com/issue/

7) Papadamou, S., Kyriazis, N. A., Tzeremes, P., & Corbet, S. (2021). Herding behaviour and price convergence clubs in cryptocurrencies during bull and bear markets. *Journal of Behavioral and Experimental Finance*, *30*, 100469 https://doi.org/10.1016/j.jbef.2021.100469
8) Bassett, R., & Pisano, M. (2021). Organisational Cost and Complexity Saving Opportunities via the Development, Deployment, and Implementation of Blockchain Networks. *Information Technology & Management Science*, *24* 10.7250/itms-2021-0005
9) Schmidt, P. J., Riley, J., & Swanson Church, K. (2020). Investigating accountants' resistance to move beyond Excel and adopt new data analytics technology. *Accounting Horizons*, *34*(4), 165-180 https://doi.org/10.2308/HORIZONS-19-154
10) Behr, N., Danos, V., & Garnier, I. (2020). Combinatorial conversion and moment bisimulation for stochastic rewriting systems. *Logical Methods in Computer Science*, *16* https://doi.org/10.23638/LMCS-16(3:3)2020
11) Ambati, R. (2025). SOX Smartwatch: Implementing Native Real-Time SOX Compliance Monitoring In Netsuite ERP Systems. *Journal of International Crisis and Risk Communication Research*, *8*(S10), 32 10.63278/jicrcr.vi.3303
12) Ambati, R. (2025). SOX Smartwatch: Implementing Native Real-Time SOX Compliance Monitoring In Netsuite ERP Systems. *Journal of International Crisis and Risk Communication Research*, *8*(S10), 32 10.1109/TIFS.2025.3578922
13) Rana, A., & Gróf, G. (2022). Assessment of the electricity system transition towards high share of renewable energy sources in south Asian countries. *Energies*, *15*(3), 1139 **https://doi.org/10.3390/en15031139**
14) Pan, R., & Parmer, G. (2022, May). Sbis: Application access to safe, baremetal interrupt latencies. In *2022 IEEE 28th Real-Time and Embedded Technology and Applications Symposium (RTAS)* (pp. 82-94). IEEE 10.1109/RTAS54340.2022.00015
15) Halikias, H. Digital Shakedown. https://doi.org/10.1007/978-3-031-65438-1
16) Vossen, G., Schönthaler, F., & Dillon, S. (2017). *The web at graduation and beyond: business impacts and developments*. Springer https://doi.org/10.1007/978-3-319-60161-8
17) De, A., Basu, A., Ghosh, S., & Jaeger, T. (2020). Hardware assisted buffer protection mechanisms for embedded RISC-V. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, *39*(12), 4453-4465 10.1109/TCAD.2020.2984407
18) Wang, S., Liu, X., & Liu, Y. (2025). Spatiotemporal Evolution Characteristics of Green Logistics Level: Evidence from 51 Countries. *Sustainability*, *17*(14), 6418 **https://doi.org/10.3390/su17146418**
19) Nam, Y., Zhou, M., Gupta, S., De Micheli, G., Cammarota, R., Wilkerson, C., ... & Rosing, T. (2023, August). Efficient machine learning on encrypted data using hyperdimensional computing. In *2023 IEEE/ACM International Symposium on Low Power Electronics and Design (ISLPED)* (pp. 1-6). IEEE 10.1109/ISLPED58423.2023.10244262
20) von Jouanne, A., Agamloh, E., & Yokochi, A. (2023). Power hardware-in-the-loop (PHIL): A review to advance smart inverter-based grid-edge solutions. *Energies*, *16*(2), 916 https://doi.org/10.3390/en16020916