International Journal of Scientific Research in Computer Science, Engineering and Information Technology

ISSN : 2456-3307 OPEN ACCESS

Available Online at : www.ijsrcseit.com

doi : https://doi.org/10.32628/CSEIT251112368

Zero Trust and Cloud Identity: Building a Resilient Security Framework

Naga Yeswanth Reddy Guntaka

CDW Technologies LLC, USA

ARTICLEINFO

Article History:

Accepted : 23 Feb 2025

Published: 25 Feb 2025

Publication Issue

Volume 11, Issue 1

January-February-2025

Page Number

3450-3460

ABSTRACT

This article explores the implementation of Zero Trust Architecture (ZTA) and cloud identity solutions in building resilient security frameworks for modern enterprises. As traditional perimeter-based security models become inadequate, organizations are shifting towards identity-centric approaches that incorporate continuous verification and least privilege access principles. It examines the evolution of identity management, emphasizing the transformation towards decentralized identity systems and their integration with established security frameworks. Through analysis of current standards and best practices, including NIST guidelines and industry frameworks, the article presents comprehensive strategies for implementing Zero Trust principles alongside modern Identity and Access Management (IAM) solutions. It encompasses critical components such as identity governance, role-based access control, micro-segmentation, and automated policy enforcement. The article also addresses implementation challenges, providing a phased approach for organizations transitioning to Zero Trust Architecture while maintaining operational efficiency. Additionally, the article explores emerging trends and preparation strategies, offering insights into

Copyright © 2025 The Author(s) : This is an open access article under the CC BY license (http://creativecommons.org/licenses/by/4.0/)

future considerations for maintaining robust security postures in an evolving threat landscape.

Keywords: Zero Trust Architecture, Cloud Identity Management, Decentralized Identity, Security Framework Implementation, Cyber Security Governance

Introduction

In today's rapidly evolving threat landscape, traditional perimeter-based security models have become inadequate for protecting modern enterprises. The expanding digital ecosystem, coupled with sophisticated cyber threats, has prompted organizations to reevaluate their security strategies. According to Gartner's analysis of government and public sector cybersecurity trends, Zero Trust adoption has become a strategic imperative for organizations seeking to protect their digital assets and maintain operational resilience in an increasingly complex threat environment [1]. This shift represents a fundamental change in how organizations approach security, moving from traditional perimeter-based models to more comprehensive, identity-centric frameworks.

The convergence of cloud computing, remote work, and decentralized identity management has fundamentally transformed organizational security requirements. Traditional security boundaries have dissolved as enterprises embrace hybrid work models and cloud-first strategies. This transformation has created new attack surfaces and vulnerabilities that conventional security measures struggle to address effectively. IBM Security's comprehensive analysis of enterprise security paradigms demonstrates that organizations implementing mature Zero Trust frameworks show significantly improved security postures and operational efficiency in managing modern cyber threats [2]. Their research emphasizes the critical importance of adopting adaptive security frameworks that can evolve with emerging threats while supporting dynamic business operations.

As organizations continue to navigate the complexities of digital transformation, the integration of Zero Trust principles with cloud identity solutions has emerged as a cornerstone of modern security architecture. This approach represents a fundamental shift from implicit trust based on network location to explicit verification based on identity and context. The framework encompasses comprehensive identity and access management integration, sophisticated role-based access control mechanisms, continuous authentication processes, and automated policy enforcement. These components work in concert to create a robust security posture that adapts to evolving threats while maintaining operational efficiency.

This article explores the intricacies of building a resilient security framework through the integration of Zero Trust principles with modern cloud identity solutions. It examines the architectural components, implementation strategies, and operational considerations necessary for successful deployment. The discussion encompasses identity governance, access management, continuous authentication mechanisms, and policy automation, providing organizations with a comprehensive understanding of how to enhance their security posture in today's dynamic threat landscape.

The Evolution of Identity Management

2.1. Decentralized Identity: A Paradigm Shift

The emergence of decentralized identity represents a fundamental transformation in digital identity management, marking a significant departure from traditional centralized architectures. The NIST Digital

Identity Guidelines (SP 800-63-3) establish comprehensive frameworks for identity proofing, authentication, and federation, providing a foundation for understanding how decentralized identity systems can enhance security while maintaining privacy [3]. These guidelines emphasize the importance of identity assurance levels and authentication mechanisms that align with modern digital service delivery requirements.

The W3C Decentralized Identifiers (DIDs) specification defines a new approach to digital identity management that enables verifiable, self-sovereign digital identities [4]. Unlike traditional centralized systems, DIDs leverage distributed systems to create persistent identifiers that remain under the identity owner's control. This specification introduces key concepts such as DID methods, DID documents, and verification methods that form the technical foundation for decentralized identity systems. The architecture enables identity owners to prove control over their identifiers without relying on centralized registries or certificate authorities.

The integration of NIST's identity guidelines with DID implementations creates a robust framework for modern identity management. NIST's emphasis on identity assurance levels (IALs), authenticator assurance levels (AALs), and federation assurance levels (FALs) provides a structured approach to implementing decentralized identity solutions that meet specific security and privacy requirements. These guidelines, combined with the technical capabilities of DIDs, enable organizations to implement authentication mechanisms that support both security and user autonomy.

The W3C DID specification's support for different DID methods allows flexibility in implementation while maintaining interoperability. This enables organizations to choose appropriate technological foundations for their identity systems while ensuring compatibility with broader identity ecosystems. The specification's emphasis on decentralized identifier resolution and verification provides mechanisms for reliable identity verification without creating new security vulnerabilities or privacy concerns.

Leading platforms are implementing these standards to create more secure and user-centric identity solutions. By adhering to NIST guidelines for digital identity while leveraging the capabilities defined in the W3C DID specification, these implementations enable robust identity verification while giving users greater control over their identity information.

Identity Management Characteristics	Traditional Centralized Systems	Decentralized Identity Systems
Identity Control	Organizational Control	User Control
Authentication Method	Centralized Authentication	Self-Sovereign Authentication
Infrastructure Dependency	Certificate Authorities	Distributed Systems
Identity Verification	Centralized Registries	Decentralized Verification
Implementation Flexibility	Limited	Multiple DID Methods
Privacy Control	Organization Managed	User Managed
Security Assurance Levels	Single Level	IAL, AAL, FAL Framework
Identity Persistence	Organization Dependent	Persistent Identifiers
Ecosystem Compatibility	Platform Specific	Interoperable
Vulnerability Points	Single Point of Failure	Distributed Risk

Table 1: Evolution of Identity Management: Key Implementation Characteristics [3, 4]

Understanding Identity Governance and Access Management

3.1. Identity Governance

Identity governance represents the cornerstone of modern security architecture, aligning directly with NIST's Risk Management Framework (RMF). NIST SP 800-37r2 emphasizes the importance of governance through a structured approach that includes preparing organizations, categorizing systems, implementing controls, and conducting ongoing assessments [5]. This framework establishes a risk-based approach to security and privacy control selection, integrating security and risk management activities into the system development lifecycle. The RMF's seven-step process provides organizations with a comprehensive methodology for managing security and privacy risks to systems, individuals, and organizations.

The implementation of identity governance requires careful consideration of organizational risk tolerance and mission priorities, as outlined in the NIST framework. This includes establishing clear lines of responsibility, defining risk management roles, and implementing continuous monitoring strategies. The framework emphasizes the importance of developing and maintaining an organization-wide risk management strategy that includes the identification of mission and business functions, risk tolerance determinations, and risk responses.

3.2. Access Management

Access management implementation aligns closely with Domain 12 of the Cloud Security Alliance's Security Guidance v4.0, which provides detailed recommendations for identity and access management in cloud computing environments [6]. The CSA guidance emphasizes the critical nature of identity as the new perimeter in cloud security, highlighting the importance of federation, strong authentication, and dynamic authorization controls. This includes implementing robust identity management practices across cloud service models (IaaS, PaaS, and SaaS) while maintaining consistency with existing identity governance frameworks.

The CSA framework specifically addresses the challenges of managing identities and access controls in distributed cloud environments. It emphasizes the importance of implementing identity governance and provisioning, authentication, authorization, and identity federation. These components work together to create a comprehensive approach to managing access in complex, multi-cloud environments while maintaining security and compliance requirements.

Organizations implementing these frameworks must consider both the technical and operational aspects of identity and access management. The integration of NIST's risk management principles with CSA's cloud-specific guidance enables organizations to develop comprehensive governance strategies that address both traditional and cloud-based identity management challenges. This includes establishing automated workflows for access reviews, implementing strong authentication mechanisms, and maintaining detailed audit trails for compliance purposes.

Component Category	Identity Governance Elements	Access Management Elements
Primary Framework	NIST Risk Management Framework	CSA Security Guidance
Core Focus	Risk-based Security Controls	Identity-based Perimeter Security
Key Activities	System Categorization	Federation Management
	Control Implementation	Authentication Services
	Continuous Assessment	Authorization Controls
	Risk Response Management	Identity Provisioning
Implementation Scope	Organization-wide Strategy	Cloud Service Models
Control Types	Security Controls	Dynamic Access Controls

Component Category	Identity Governance Elements	Access Management Elements
	Privacy Controls	Federation Controls
	Risk Controls	Authorization Controls
Monitoring Approach	Continuous Monitoring	Real-time Authentication
Documentation Requirements	Risk Assessment Reports	Audit Trails
Workflow Type	Risk Management Workflows	Access Review Workflows
Environment Coverage	Traditional Systems	Multi-cloud Environments

Table 2: Identity and Access Management Framework Components in Cloud Environments [5, 6]

Core Zero Trust Principles

The implementation of Zero Trust architecture fundamentally shifts security from static, network-based perimeters to focusing on resources, assets, and users. NIST SP 800-207 defines Zero Trust (ZT) as a collection of concepts designed to minimize uncertainty in enforcing accurate, per-request access decisions in information systems and services, establishing that no implicit trust should be granted to assets or user accounts based solely on their physical or network location [7]. This architectural approach requires authentication and authorization of every user, device, and network flow as essential components of the security decision process, fundamentally changing how organizations approach security [7].

4.1. Role-Based Access Control (RBAC)

Role-Based Access Control provides the foundation for modern access management strategies. NIST SP 800-162 establishes RBAC as a mechanism that assigns access rights and permissions based on organizational roles, incorporating three primary rules: role assignment, role authorization, and permission authorization [8]. This specification emphasizes that RBAC becomes particularly crucial in large organizations where managing individual user permissions would be impractical, offering a structured approach to access control that aligns with organizational hierarchies [8].

The integration of RBAC with Attribute Based Access Control (ABAC) creates a more comprehensive security framework. According to NIST SP 800-162, this hybrid approach enables organizations to consider both role-based permissions and additional attributes such as time, location, and resource sensitivity when making access decisions [8]. The specification outlines implementation strategies that allow organizations to maintain role-based controls while incorporating attribute-based rules for enhanced security granularity [8].

4.2. Least Privilege Implementation

The principle of least privilege forms a cornerstone of Zero Trust Architecture implementation. NIST SP 800-207 emphasizes that access to resources should be granted only for the minimum time and level necessary to complete authorized tasks, requiring continuous monitoring and assessment of access requirements [7]. This framework stipulates that least privilege must be implemented through policy enforcement points (PEP) and policy decision points (PDP), working in concert to evaluate access requests against established policies [7].

4.3. Zero Trust Architecture Components

The core components of Zero Trust Architecture, as defined by NIST SP 800-207, create a comprehensive security framework [7]. The Policy Engine (PE) and Policy Administrator (PA) work together to make and enforce access decisions based on enterprise policy and external data sources, while Policy Enforcement Points (PEPs) enable, monitor, and terminate connections between subjects and enterprise resources [7].

NIST SP 800-207 specifies that all resource access must be determined by dynamic policy, including the

observable state of client identity, application, and requesting asset [7]. The Continuous Diagnostics and Mitigation (CDM) System plays a crucial role by collecting data about enterprise assets' current state and applying updates to configuration and software components, ensuring that security posture remains current and effective [7].

The implementation of these components requires careful consideration of organizational requirements and security objectives. As outlined in NIST SP 800-162, successful deployment depends on proper alignment between access control mechanisms and business processes, ensuring that security controls support rather than hinder operational efficiency [8]. This integration enables organizations to maintain strong security posture while supporting business agility and user productivity.

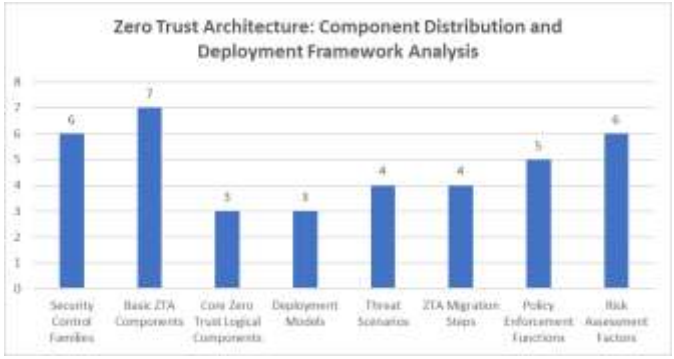

Fig 1: Quantitative Analysis of Zero Trust Architecture Components and Implementation Metrics from NIST SP 800-207 [7]

IAM Integration in Zero Trust Architecture

The integration of Identity and Access Management (IAM) within Zero Trust Architecture requires a comprehensive approach to security that aligns with NIST's established frameworks. As defined in NIST SP 800-207, the Zero Trust Architecture (ZTA) requires continuous monitoring and validation of the security configuration and posture of all owned and associated assets [7]. This framework emphasizes that IAM components must integrate seamlessly with policy enforcement points (PEP) and policy decision points (PDP) to maintain effective security controls.

5.1. Continuous Authentication

Authentication in Zero Trust environments must align with the digital identity assurance levels defined in NIST SP 800-63B [9]. The framework establishes three Authentication Assurance Levels (AALs) that provide increasing levels of assurance that an authenticator is bound to a specific identity. AAL1 provides some assurance, AAL2 provides high confidence, and AAL3 provides very high confidence in the asserted identity [9]. In Zero Trust implementations, these authentication mechanisms must be continuously evaluated throughout user sessions, not just at initial access.

NIST SP 800-207 emphasizes that authentication decisions must incorporate multiple factors, including device identity, user identity, and application identity [7]. This multi-faceted approach to authentication aligns with NIST SP 800-63B's requirements for multi-factor authentication at higher assurance levels, ensuring robust identity verification throughout the authentication lifecycle [9].

5.2. Micro-Segmentation Support

The implementation of micro-segmentation in Zero Trust Architecture requires careful consideration of both network architecture and identity management components. NIST SP 800-207 defines specific requirements for enterprise resource protection through micro-perimeters and resource isolation [7]. These micro-perimeters must be enforced through a combination of identity-based security controls and network segmentation policies.

As specified in NIST SP 800-207, micro-segmentation strategies must incorporate dynamic access controls that can adapt to changing threat landscapes [7]. This includes implementing granular access policies that consider both identity attributes and environmental factors when making access decisions. The integration of identity management with micro-segmentation enables organizations to maintain precise control over resource access while supporting business agility.

5.3. Automated Policy Enforcement

Policy enforcement in Zero Trust environments must align with both architectural requirements and digital identity guidelines. NIST SP 800-207 specifies that policy enforcement points must be capable of making and enforcing access decisions in real time [7]. This requires automated systems that can evaluate multiple factors, including identity assurance levels as defined in NIST SP 800-63B [9].

The framework for automated policy enforcement must incorporate the identity proofing and authentication requirements specified in NIST SP 800-63B, ensuring that access decisions are based on appropriate levels of identity assurance [9]. This includes implementing controls for credential management, authenticator assurance levels, and federation requirements as defined in the digital identity guidelines.

Implementation Strategy for Zero Trust Architecture

The implementation of Zero Trust Architecture requires a carefully planned, phased approach that aligns with established industry frameworks. The National Cybersecurity Center of Excellence (NCCoE) at NIST provides comprehensive guidance for implementing Zero Trust Architecture, emphasizing the importance of a structured approach that addresses both technical and operational considerations [10]. This implementation framework focuses on demonstrating Zero Trust security concepts across an enterprise environment while maintaining business operations.

6.1. Phase 1: Foundation Building

The initial phase of Zero Trust implementation must establish core architectural components as defined by NCCoE's implementation guide [10]. This phase begins with a thorough assessment of existing infrastructure and security capabilities, followed by the deployment of foundational Zero Trust components. Organizations should focus on implementing essential security capabilities including enterprise identity management, asset management, and network segmentation strategies.

The Reference Architecture Model for Industry 4.0 (RAMI 4.0) emphasizes the importance of establishing clear architectural layers during initial implementation [11]. This includes defining the integration of business processes, functional descriptions, and information flows that support secure operations. The framework specifies that organizations must establish baseline security controls that align with both operational requirements and security objectives.

6.2. Phase 2: Enhancement

During the enhancement phase, organizations should focus on implementing advanced Zero Trust capabilities as outlined in the NCCoE implementation guide [10]. This includes deploying enhanced authentication mechanisms, establishing comprehensive asset visibility, and implementing dynamic policy enforcement capabilities. The NCCoE framework emphasizes the importance of integrating security components across the enterprise environment to create a cohesive security architecture.

RAMI 4.0 provides guidance for enhancing security controls through the integration of communication and information layers [11]. This includes implementing secure communication protocols, establishing data flow controls, and deploying monitoring capabilities that support security operations. The framework emphasizes the importance of maintaining interoperability while enhancing security controls.

6.3. Phase 3: Optimization

The optimization phase focuses on refining and enhancing implemented security controls based on operational experience and emerging requirements. The NCCoE implementation guide emphasizes the importance of continuous evaluation and improvement of Zero Trust implementations [10]. This includes analyzing security metrics, identifying areas for enhancement, and implementing additional

security controls as needed to address emerging threats.

According to RAMI 4.0, organizations should focus on optimizing the integration between business processes and security controls during this phase [11]. This includes fine-tuning security policies based on operational requirements, implementing advanced analytics capabilities, and establishing continuous improvement processes that enable adaptation to evolving security challenges.

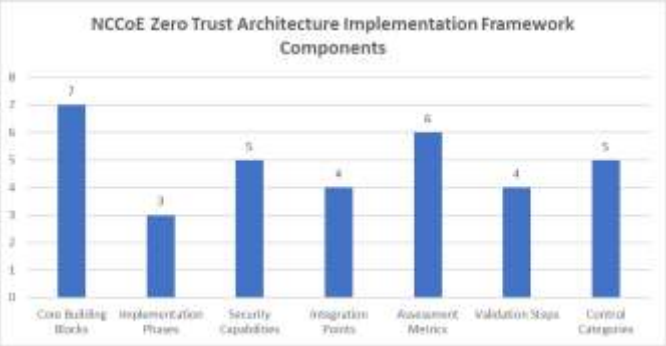

Fig 2: Quantitative Analysis of Zero Trust Implementation Building Blocks [10]

Best Practices for Success

The implementation of Zero Trust Architecture must align with established cybersecurity frameworks and control guidelines. The NIST Framework for Improving Critical Infrastructure Cybersecurity establishes five core functions: Identify, Protect, Detect, Respond, and Recover, which provide a strategic view of managing cybersecurity risk [12]. This Framework Core offers a comprehensive approach to security implementation that addresses both technical and organizational aspects of cybersecurity risk management.

7.1. Technical Implementation

Technical implementation must follow the security control baselines established in NIST SP 800-53 Revision 5, which provides a comprehensive catalog of security and privacy controls for information systems [13]. The framework emphasizes implementing controls across multiple families, including Access Control (AC), Audit and Accountability (AU), and System and Communications Protection (SC), ensuring a defense-in-depth approach to security.

According to NIST SP 800-53 Rev 5, organizations must implement continuous monitoring strategies that incorporate automation and real-time analysis capabilities [13]. The Continuous Monitoring (CM) family of controls specifies requirements for implementing automated mechanisms to maintain awareness of threats and vulnerabilities. These controls must be integrated with incident response capabilities defined in the Incident Response (IR) control family, ensuring rapid detection and response to security events.

The Framework Core emphasizes the importance of protective technology and detection processes [12]. Organizations must implement technical controls that enable anomaly detection, system monitoring, and automated alerts. This includes deploying security information and event management (SIEM) systems that can correlate security events and trigger appropriate response procedures based on predefined rules and algorithms.

7.2. Organizational Alignment

The organizational aspects of security implementation must align with the Governance and Risk Assessment categories of the NIST Cybersecurity Framework [12]. This includes establishing organizational security policies that clearly define roles, responsibilities, and security requirements. The Framework emphasizes the importance of risk management strategies that consider business context, resources, and risk tolerances when implementing security controls.

NIST SP 800-53 Rev 5 provides specific guidance for organizational controls through the Planning (PL) and Program Management (PM) control families [13]. These controls emphasize the importance of developing comprehensive security plans, establishing governance structures, and maintaining documentation of security controls. Organizations must implement processes for regular assessment and

updates of security controls to address emerging threats and changing business requirements.

The Framework Core's Protect function emphasizes awareness and training programs as essential components of organizational security [12]. Organizations must develop and maintain comprehensive training programs that ensure all stakeholders understand their roles in maintaining security. This includes establishing clear procedures for security operations, incident response, and continuous improvement of security controls.

Future Considerations

The evolution of Zero Trust Architecture must anticipate and adapt to emerging technological trends and security challenges. According to Salesforce's security framework for emerging technologies, organizations must focus on three key areas: cloud security, mobile security, and IoT security when preparing for future technological adoption [14]. This comprehensive approach ensures that security strategies remain effective as technology landscapes evolve.

8.1. Emerging Trends

The National Cyber Security Strategy emphasizes the critical importance of strengthening the security of digital payment systems, protecting critical information infrastructure, and building a robust cybersecurity products and services ecosystem [15]. This strategic framework identifies key technological trends that will shape the future of cybersecurity implementation.

Salesforce's emerging technology guidelines highlight the increasing importance of securing cloud-native applications and services [14]. The framework emphasizes that organizations must adapt their security approaches to address the unique challenges presented by cloud computing, including data protection, access control, and compliance requirements. This includes implementing advanced security controls that can effectively protect cloud-based resources while maintaining operational efficiency.

The National Cyber Security Strategy identifies artificial intelligence, blockchain, and quantum computing as transformative technologies that will significantly impact cybersecurity practices [15]. Organizations must prepare for the integration of these technologies while ensuring appropriate security controls are maintained. The strategy emphasizes the need for developing indigenous capabilities and promoting research and innovation in cybersecurity.

8.2. Preparation Strategies

To address these emerging challenges, organizations must develop comprehensive preparation strategies that align with established security frameworks. Salesforce's security considerations emphasize the importance of implementing secure development practices and maintaining robust security testing processes throughout the technology lifecycle [14]. This includes establishing clear security requirements for new technologies and ensuring appropriate controls are implemented during development and deployment.

The National Cyber Security Strategy outlines several key preparation areas, including capacity building, skill development, and the creation of sectoral Computer Emergency Response Teams (CERTs) [15]. Organizations must focus on developing public-private partnerships and fostering innovation in cybersecurity to address emerging challenges effectively.

The strategy emphasizes the importance of creating a strong cybersecurity framework that can adapt to evolving threats [15]. This includes developing mechanisms for threat intelligence sharing, establishing cybersecurity audit frameworks, and creating standardized testing and certification for cybersecurity products. Organizations must also focus on developing human resources with appropriate cybersecurity skills through training and capacity-building programs.

Salesforce's framework emphasizes the importance of maintaining security awareness and implementing continuous monitoring capabilities [14]. Organizations must establish processes for regular security assessments and updates to ensure that security controls remain effective as technology evolves. This includes implementing automated security testing tools and maintaining comprehensive security documentation.

Conclusion

The successful implementation of Zero Trust Architecture represents a fundamental shift in enterprise security strategy, requiring careful integration of modern identity management solutions with comprehensive security controls. Organizations must balance technical excellence with operational requirements while maintaining flexibility to address emerging threats and technological advances. The implementation journey demands a structured approach, incorporating identity governance, access management, and continuous monitoring capabilities while ensuring alignment with established security frameworks and industry standards. As the threat landscape continues to evolve, organizations must maintain adaptive security postures through continuous learning, regular assessment, and strategic implementation of emerging technologies. The transformation to Zero Trust Architecture, while challenging, provides organizations with the foundation needed to protect digital assets and maintain operational resilience in an increasingly complex security environment.

References

[1]. Gartner, "Implementing Zero Trust Security in the Public Sector," Gartner Research. Available: https://www.gartner.com/en/industries/government-public-sector/topics/zero-trust

[2]. IBM Security, "Cost of a Data Breach Report 2024," IBM Report. Available: https://www.ibm.com/downloads/documents/us-en/107a02e94948f4ec

[3]. National Institute of Standards and Technology, "Digital Identity Guidelines," National Institute of Standards and Technology Documentation, 2023. Available: https://pages.nist.gov/800-63-3/

[4]. Manu Sporny et al., "Decentralized Identifiers (DIDs) v1.0," W3C Documentation, 2022. Available: https://www.w3.org/TR/did-1.0/

[5]. National Institute of Standards and Technology, "Risk Management Framework for Information Systems and Organizations," NIST Special Publication 800-37, 2018. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf

[6]. Cloud Security Alliance, "Security Guidance for Critical Areas of Focus in Cloud Computing v4.0," Cloud Security Alliance Report, 2017. Available: https://cloudsecurityalliance.org/artifacts/security-guidance-v4#

[7]. Scott Rose et al., "Zero Trust Architecture," NIST Special Publication 800-207, 2020. Available: https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-207.pdf

[8]. Vincent C. Hu et al., "Guide to Attribute-Based Access Control (ABAC) Definition and Considerations," NIST Special Publication 800-162, 2014. Available: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-162.pdf

[9]. Paul A. Grassi et al., "Digital Identity Guidelines: Authentication and Lifecycle Management," NIST Special Publication 800-63B, 2017. Available: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-63b.pdf

[10]. National Institute of Standards and Technology, "Implementing a Zero Trust Architecture," NCCoE, Available:

https://www.nccoe.nist.gov/projects/implementing-zero-trust-architecture

[11]. Dr. Karsten Schweichhart, "Reference Architectural Model Industry 4.0 (RAMI 4.0)," European Commission. Available: https://ec.europa.eu/futurium/en/system/files/ged/a2-schweichhart-reference_architectural_model_industrie_4.0_rami_4.0.pdf

[12]. National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity," National Institute of Standards and Technology Version 1.1, 2018. Available: https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf

[13]. National Institute of Standards and Technology, "Security and Privacy Controls for Information Systems and Organizations," NIST SP 800-53 Rev. 5, 2020. Available: https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

[14]. Salesforce, "Security Considerations for Emerging Technologies," Salesrorce. Available: https://trailhead.salesforce.com/content/learn/modules/security-considerations-for-emerging-technologies

[15]. Drishti IAS, "National Cyber Security Strategy Analysis," Drishti IAS. Available: https://www.drishtiias.com/daily-news-analysis/national-cyber-security-strategy-1