Comparative analysis of cybersecurity in leading cloud platforms based on the NIST framework

Порівняльний аналіз кібербезпеки провідних хмарних платформ за фреймворком NIST

Vitalii Molnar
Postgraduate student of Department of Information Security, e-mail: vitalii.v.molnar@lpnu.ua, ORCID: 0009-0001-3183-0117

Dmytro Sabodashko
Doctor of Philosophy, Senior Lecturer of Department of Information Security, e-mail: dmytro.v.sabodashko@lpnu.ua, ORCID: 0000-0003-1675-0976

Lviv Polytechnic National University, Lviv, Ukraine

Віталій Молнар
аспірант кафедри захисту інформації, e-mail: vitalii.v.molnar@lpnu.ua, ORCID: 0009-0001-3183-0117

Дмитро Сабодашко
доктор філософії, старший викладач кафедри захисту інформації, e-mail: dmytro.v.sabodashko@lpnu.ua, ORCID: 0000-0003-1675-0976

Національний університет «Львівська політехніка», м. Львів, Україна

Received: November 15, 2024 | Revised: December 22, 2024 | Accepted: December 31, 2024

DOI: 10.33445/sds.2024.14.6.8

Purpose: To examine the cybersecurity capabilities of three leading cloud platforms—AWS, Azure, and GCP—according to the five core functions of the NIST Cybersecurity Framework: identify, protect, detect, respond, and recover.

Method: A comparative approach was used, covering the analysis of the tools and services of each platform for the implementation of NIST functions.

Findings: The analysis demonstrated the strengths and weaknesses of AWS, Azure, and GCP in terms of identity, protection, detection, response, and recovery capabilities, highlighting the most effective tools for each.

Theoretical implications: The study deepens the understanding of cybersecurity strategies based on the NIST framework and can serve as a basis for further research in the direction of optimizing protection in cloud environments.

Practical implications: The obtained results provide valuable recommendations for improving cloud security practices through informed choice of cloud services and security strategies.

Value: The study offers a structured approach to assessing the cybersecurity of cloud platforms, highlighting each provider's ability to address different aspects of cybersecurity.

Future research: Future research may focus on the impact of emerging technologies such as artificial intelligence and machine learning on improving the effectiveness of cybersecurity in cloud environments.

Paper type: Conceptual research.

Мета роботи: Дослідити засоби забезпечення кібербезпеки трьох провідних хмарних платформ — AWS, Azure та GCP — відповідно до п'яти основних функцій фреймворку кібербезпеки NIST: ідентифікація, захист, виявлення, реагування та відновлення.

Метод: Використано порівняльний підхід, що охоплює аналіз інструментів та сервісів кожної платформи для реалізації функцій NIST.

Результати дослідження: Аналіз продемонстрував сильні та слабкі сторони AWS, Azure і GCP щодо функцій ідентифікації, захисту, виявлення, реагування та відновлення, підкреслюючи найефективніші інструменти для кожної з них.

Теоретичні цінність дослідження: Дослідження поглиблює розуміння стратегій кібербезпеки на основі фреймворку NIST та може слугувати основою для подальших досліджень у напрямку оптимізації захисту у хмарних середовищах.

Практичні цінність дослідження: Отримані результати надають цінні рекомендації для вдосконалення практик хмарної безпеки через обґрунтований вибір хмарних сервісів і стратегій безпеки.

Цінність дослідження: Дослідження пропонує структурований підхід до оцінки кібербезпеки хмарних платформ, висвітлюючи здатність кожного провайдера вирішувати різні аспекти кібербезпеки.

Майбутні дослідження: Майбутні дослідження можуть зосередитися на впливі новітніх технологій, таких як штучний інтелект і машинне навчання, на підвищення ефективності кібербезпеки у хмарних середовищах.

Тип статті: Концептуальне дослідження.

Key words: cloud computing, cloud services, cloud security, cybersecurity, NIST framework.

Ключові слова: хмарні обчислення, хмарні сервіси, хмарна безпека, кібербезпека, фреймворк NIST.

Introduction

The changing world of cloud computing technology advancements are taking place at a pace leading to the vital selection of an ideal cloud platform, for businesses especially focusing on data security and reliability as top priorities. As companies continue to shift their activities to cloud the significance of cybersecurity measures has gained prominence with the evolution of cyber threats making safeguarding cloud infrastructures a critical concern.

This article provides a comprehensive comparison of the three leading cloud platforms: Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP). The primary focus lies on the platforms' security services, analyzed through the lens of the Five Functions of Cloud

Security: Identify, Protect, Detect, Respond, and Recover, as outlined in the National Institute of Standards (NIST) and Technology's "Framework for Improving Critical Infrastructure Cybersecurity" [1]. Each platform offers unique capabilities to address these critical aspects of cloud security, providing entities with tools to safeguard their data, applications, and operations.

By analyzing the security offerings of AWS, Azure, and GCP, this article aims to assist in determining which platform best aligns with specific security objectives and risk tolerance. In an era of increasingly sophisticated cyber threats, cloud service providers must offer not only robust defenses but also the necessary tools for proactive threat detection, swift incident response, and comprehensive data recovery. AWS, Azure, and GCP provide extensive suites of security tools, but their effectiveness can vary based on specific needs and priorities.

This study examines the complex framework of cloud security by detailing the features of each platform in the areas of identification, protection, detection, response, and remediation. The goal is to empower readers with the knowledge needed to make strategic decisions aligned with their security objectives, maximizing the benefits of AWS, Azure, and GCP while effectively managing cybersecurity risks.

As shown in Figure 1, the cloud computing industry is dominated by three major players: AWS, Azure, and GCP [3]. Each provider offers a comprehensive suite of services, including storage, computers, managed databases, and AI tools, designed to meet diverse needs and budgets.

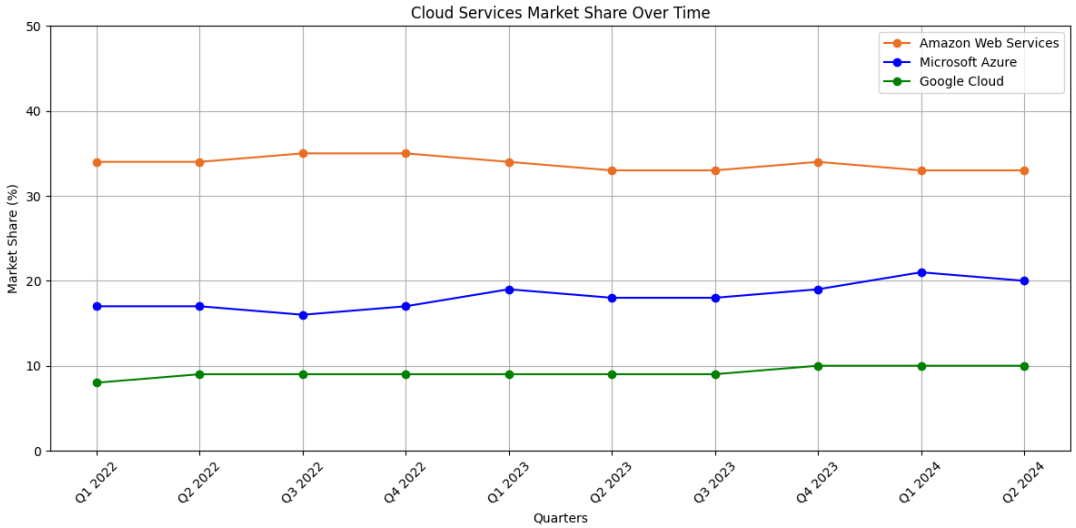

Figure 1 – Cloud Services Market Share Over Time

AWS, as a pioneer in cloud computing, maintains the largest market share due to its extensive portfolio of mature, feature-rich services, providing unparalleled flexibility for scalable solutions. Azure is favored by organizations already integrated into the Windows ecosystem, benefiting from seamless integration with tools like Office 365 and Dynamics 365. GCP is known for its advanced AI and machine learning capabilities, attracting innovative companies focused on data-driven services and cloud-native development.

Understanding the unique strengths of each platform is essential for making informed decisions, as selecting the right cloud provider is critical for a secure, resilient, and successful cloud journey.

Theoretical Foundations of Research

The digital landscape is shifting, with businesses migrating at an accelerating pace to the cloud. From nimble startups to established enterprises, organizations of all sizes are leveraging the unparalleled scalability, agility, and cost-efficiency offered by cloud services [2]. This paradigm shift, however, brings with it a critical new imperative: robust cybersecurity.

Storing sensitive data and running mission-critical applications in the cloud expose entities to new vulnerabilities. In this interconnected environment, data breaches have the potential to inflict devastating damage, compromising both intellectual property and customer trust. The consequences of a data breach can include financial losses, regulatory non-compliance, and irreparable reputational damage.

As a result, safeguarding the cloud must be embedded into the core of any cloud adoption strategy. By prioritizing strong cybersecurity practices, organizations can unlock the full potential of cloud computing while ensuring that their data and applications remain shielded from the growing array of cyber threats [4].

Problem Statement

Despite the advantages of cloud computing, significant challenges persist in securing these environments. A core complexity is the shared responsibility model, which delineates security duties between the cloud provider and the customer [5]. This division necessitates clear collaboration and a thorough understanding of each party's responsibilities in securing specific aspects of the cloud stack.

Key challenges include navigating complex data privacy and regulatory compliance requirements, such as GDPR and CCPA, which mandate that data must be stored, processed, and secured according to evolving regulations. Furthermore, the dynamic nature of cloud services demands constant vigilance; misconfigurations or weak access controls can expose systems to significant risks, underscoring the need for continuous monitoring and timely security updates. Additionally, the multi-tenant nature of cloud platforms necessitates stringent access controls and data isolation to mitigate cross-tenant risks.

To strengthen cloud security, it is essential to adopt best practices, leverage advanced cloud security tools, and promote a culture of continuous security awareness. This proactive approach supports a resilient defense against the constantly evolving landscape of cyber threats.

Research Methodology

This section outlines the research methodology used in this study, centered on the NIST Cybersecurity Framework, which provides a comprehensive approach to enhancing cloud security. As illustrated in Figure 2, the NIST Cybersecurity Framework is structured around five core functions—Identify, Protect, Detect, Respond, and Recover—each comprising specific categories designed to enhance cybersecurity measures and resilience.

The Identify function focuses on understanding and managing cybersecurity risks by recognizing the assets, systems, and data that require protection, thus establishing a foundation for risk management. In the Protect function, organizations implement safeguards to ensure the continuity of critical services, utilizing measures such as access controls and data encryption to mitigate potential cybersecurity threats.

The Detect function emphasizes continuous monitoring and anomaly detection, enabling organizations to promptly identify and respond to cybersecurity incidents within a dynamic threat landscape. Following this, the Respond function highlights the importance of having a structured approach to incident response, encompassing planning, communication strategies, and coordination with stakeholders to minimize the impact of incidents.

Finally, the Recover function outlines the necessary activities to restore impaired capabilities or services after an incident, focusing on recovery planning and process improvements to enhance future resilience [6].

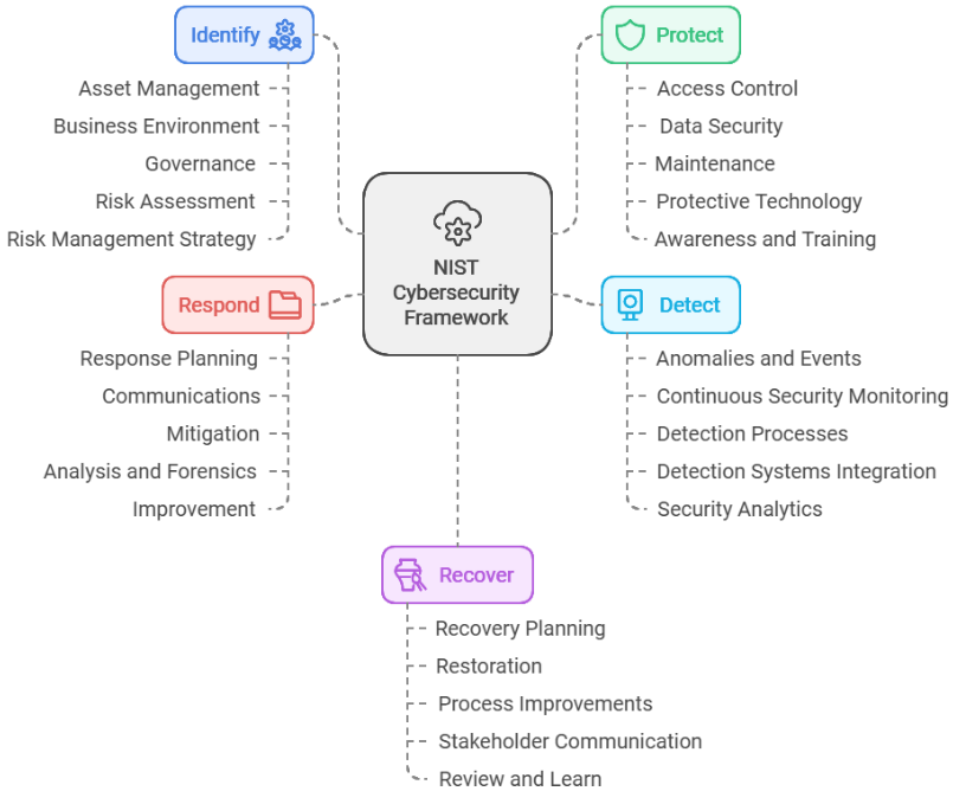

Figure 2 – Overview of the NIST Cybersecurity Framework, illustrating its five core functions and associated categories

This framework serves as a guide for navigating cloud security. Subsequent sections will explore the specifics of each function and how AWS, Azure, and GCP address them.

Results and Discussion

Identify function

The Identify function serves as the cornerstone of effective cloud security. It establishes a foundational understanding necessary for managing cybersecurity risks. This function addresses the diverse nature of these risks related to systems, people, assets, data, and capabilities. According to the NIST Cybersecurity Framework, the activities within the Identify function are essential for effectively utilizing the entire framework [1]. By grasping the business context and understanding the resources that support critical functions, stakeholders can strategically approach cybersecurity risk management, allowing them to prioritize efforts in line with their unique risk profiles and business objectives.

This function encompasses several key outcome categories that enhance cybersecurity posture. Asset management involves identifying and understanding the value of diverse assets within the ecosystem. A comprehensive understanding of the business environment is critical for contextualizing cybersecurity risks, taking into account industry trends and regulatory requirements. Governance ensures that cybersecurity policies, processes, and controls align with objectives. Conducting thorough risk assessments enables stakeholders to quantify potential threats and vulnerabilities, facilitating informed decision-making. Lastly, developing a robust risk management strategy empowers stakeholders to proactively address and mitigate cybersecurity risks in alignment with broader business strategy.

Table 1 compares the cloud services provided by AWS, Azure, and GCP concerning the Identify function, highlighting their respective tools and capabilities.

Table 1 – Cloud Service Comparison for the Identify function

Category	AWS	Azure	GCP
Asset Management	AWS Config	Azure Resource Manager	Google Cloud Asset Inventory
Business Environment	AWS Organizations	Azure Policy	Google Cloud Resource Manager
Governance	AWS Organizations	Azure Policy	Google Cloud Resource Manager
Risk Assessment	Amazon Inspector	Azure Security Center	Google Cloud Security Command Center
Risk Management Strategy	AWS Security Hub	Azure Security Center	Google Cloud Security Command Center

Focused Comparison of Each Category in the Identify function:

Each cloud provider offers distinct capabilities that enhance the Identify function. AWS Config allows for continuous monitoring and assessment of resource configurations, ensuring visibility into asset relationships and compliance [7]. Azure Resource Manager simplifies the management of resources through templates, promoting consistent governance across cloud environments [8]. In contrast, Google Cloud Asset Inventory maintains an up-to-date inventory of assets, aiding compliance and security assessments [9].

Regarding risk assessment, Amazon Inspector automates security evaluations, identifying vulnerabilities in applications running on AWS [10]. Azure Security Center provides continuous security posture assessments across hybrid environments, while Google Cloud Security Command Center integrates security data, offering insights to prioritize remediation efforts effectively [11, 12].

For governance, tools like AWS Organizations enable centralized management across multiple accounts, whereas Azure Policy enforces compliance rules to ensure adherence to corporate standards. Google Cloud Resource Manager similarly facilitates hierarchical policy application [13, 14, 15].

By utilizing these tools, users can establish a robust foundation for understanding and managing cybersecurity risks. This foundational insight allows for informed decision-making and effective risk management strategies tailored to unique operational contexts and security requirements, ultimately strengthening the overall security posture.

Protect function

The Protect Function, as outlined by the NIST Cybersecurity Framework, is vital for enhancing cybersecurity defenses. Its primary objective is to develop and implement safeguards that ensure the continuous and secure delivery of essential services, thereby limiting the impact of cybersecurity incidents and maintaining critical operations [1]. By establishing a solid framework for protection, significant improvements in overall cybersecurity posture can be achieved.

This function encompasses several key categories. Effective identity management and access control are essential for ensuring that only authorized personnel can access critical systems and data; techniques like multi-factor authentication help mitigate unauthorized access risks. Given the significant role of human behavior in cybersecurity, awareness and training are crucial; educating employees on security risks and best practices equips them to recognize and respond to potential threats effectively [16].

Data security is another foundational aspect, involving the implementation of encryption, data classification, and adherence to compliance standards such as GDPR and HIPAA to maintain confidentiality, integrity, and availability of sensitive information. Additionally, establishing clear information protection processes and procedures ensures consistent cybersecurity practices [11]. Regular maintenance of systems and infrastructure is critical for identifying and addressing

vulnerabilities, keeping systems updated, and patching weaknesses. Finally, the deployment of protective technologies, including firewalls, antivirus software, and intrusion detection systems, actively defends against cybersecurity threats, solidifying the protective measures

The Table 2 below highlights each provider's offerings within the Protect function, showcasing essential services that contribute to a strong, adaptive cybersecurity posture.

Table 2 – Cloud Service Comparison for the Protect function

Category	AWS	Azure	GCP
Identity Management and Access Control	AWS IAM	Azure Active Directory (AAD)	Google Cloud IAM
Awareness and Training	AWS Training and Certification	Microsoft Learn, Azure Security Center	Google Cloud Training, Cloud Security Command Center
Data Security	AWS KMS, Amazon VPC, AWS Certificate Manager	Azure Disk Encryption, Azure Storage Service Encryption, Azure Information Protection	Google Cloud KMS, Encryption at Rest by Default, DLP Tools
Information Protection Processes and Procedures	AWS Config, AWS Trusted Advisor	Azure Policy, Azure Blueprints, Azure Security Center	Google Cloud Security Command Center, Cloud Audit Logs
Maintenance	AWS Systems Manager, AWS Trusted Advisor	Azure Automation, Azure Update Management, Azure Advisor	Google Cloud Operations Suite, Recommendations
Protective Technology	AWS WAF, AWS Shield, AWS Firewall Manager	Azure Firewall, Azure DDoS Protection, Azure Security Center	Google Cloud Armor, Cloud Security Command Center

Focused Comparison of Each Category in the Protect function:

In the realm of identity management and access control, AWS Identity and Access Management (IAM), Azure Active Directory, and Google Cloud IAM offer robust solutions, with AWS IAM particularly excelling in customizable permissions that cater well to large-scale environments [17, 18, 19].

For awareness and training, AWS Training and Certification provides extensive resources tailored to different skill levels, making it a favored option for those seeking in-depth, role-specific security training [21].

When it comes to data security, Google Cloud stands out with its automatic encryption at rest across all data, facilitating compliance for industries with strict regulations, whereas Azure and AWS provide more selective encryption services [21]. In the area of information protection processes and procedures, Azure's Security Center and Policy tools offer seamless integration with its ecosystem, enabling efficient implementation of security policies [22, 23].

Maintenance is well-supported by Azure's Update Management system, which automates patching and is particularly beneficial in hybrid environments [234]. Meanwhile, AWS provides insightful maintenance guidance through Trusted Advisor, and Google Cloud offers Recommendations to assist users [25, 27]. Lastly, AWS distinguishes itself with a comprehensive suite of protective technologies, such as AWS WAF and Shield, which are tailored for advanced protection in complex, multi-tenant applications [27, 28].

In summary, the Protect function serves as a critical foundation for enhancing cybersecurity defenses. By implementing comprehensive identity management, data security, and awareness

training, risks can be mitigated, and operational integrity can be maintained in the face of evolving threats.

Detect Function

The Detect function is essential within the NIST Cybersecurity Framework, focusing on the timely identification of cybersecurity events. It encompasses several critical elements that must be implemented to ensure effective threat detection [1].

A key aspect of the Detect function is the identification of anomalies and events. Establishing a baseline of normal activity helps in recognizing unusual patterns or behaviors that could signal potential threats. This requires continuous monitoring using tools such as Intrusion Detection Systems (IDS) and Security Information and Event Management (SIEM) systems.

Ongoing continuous monitoring is crucial for maintaining the effectiveness of security controls. This involves real-time assessments to quickly identify potential issues, ensuring that controls are functioning as intended through regular updates and maintenance.

Developing robust detection processes is also important. Systematic procedures for monitoring, analyzing, and responding to alerts from security tools are essential for effective cybersecurity event management. By implementing these elements, it becomes possible to enhance the capability to detect and respond to potential threats swiftly.

Table 3 – Cloud Service Comparison for the Detect function

Category	AWS Features	Azure Features	GCP Features
Anomalies and Events	GuardDuty, Macie, CloudTrail	Security Center	Security Command Center, Pub/Sub
Security Continuous Monitoring	CloudWatch (Logs, Config, Inspector)	Azure Monitor, Security Center	Monitoring, Logging, Config Management
Detection Processes	Security Hub, CloudWatch Events	Sentinel, Logic Apps	Security Command Center, Functions

Focused Comparison of Each Category in the Detect function:

In terms of anomalies and events, AWS provides GuardDuty, which leverages machine learning for advanced threat detection [7]. Azure's Security Center offers a unified security management platform, while Google Cloud Platform (GCP) features the Security Command Center, delivering comprehensive security insights [11, 12].

For security continuous monitoring, AWS CloudWatch enables thorough monitoring and logging, whereas Azure Monitor provides full-stack observability [29, 30]. GCP combines centralized monitoring and logging with effective configuration management to ensure security measures are consistently maintained [31].

When it comes to detection processes, AWS Security Hub consolidates security management, while Azure Sentinel offers cloud-native Security Information and Event Management (SIEM) capabilities [32, 33]. GCP's Security Command Center also provides extensive security insights, enhanced by robust event-handling tools [12].

Overall, the Detect function significantly enhances cybersecurity posture by enabling the timely detection of potential threats. Each cloud provider offers unique features that allow for tailored detection strategies to meet specific needs.

Respond Function

The Respond function is a vital element of the NIST Cybersecurity Framework, aimed at effectively addressing detected cybersecurity incidents. Its primary objective is to contain the impact of these incidents, mitigate their effects, and enhance overall response capabilities. To achieve this, the function includes key activities such as response planning, communication, analysis, mitigation, and continuous improvement [1].

Response planning involves developing and implementing effective plans for handling cybersecurity incidents, which include documented procedures, communication strategies, and coordination mechanisms. Effective communication is crucial during an incident to ensure timely and accurate sharing of information both within the organization and with external stakeholders.

A thorough analysis of the incident is necessary to understand its nature, scope, and impact. This entails collecting and analyzing incident-related data to inform decision-making and response activities. Mitigation efforts focus on containing the incident's impact, which may involve isolating affected systems, applying patches, or implementing other measures to prevent further harm.

Finally, improvements are made by learning from the incident, which includes updating response plans, refining processes, and enhancing capabilities to better prepare for future incidents.

Below, Table 4 outlines the specific capabilities and resources offered by AWS, Azure, and GCP within each category of the Respond function. This comparison illustrates how these cloud providers equip users with the necessary tools and processes to enhance incident response efforts.

Table 4 – Cloud Service Comparison for the Respond function

Category	AWS	Azure	GCP
Response Planning	AWS Incident Response	Azure Incident Response	Google Cloud Incident Response
Communications	Amazon SNS (Simple Notification Service)	Azure Notification Hubs	Google Cloud Pub/Sub
Analysis	Amazon CloudWatch Logs	Azure Monitor, Azure Log Analytics	Google Cloud Logging
Mitigation	AWS WAF, AWS Shield	Azure Application Gateway WAF	Google Cloud Armor, Google Cloud CDN
Improvements	AWS CloudTrail, AWS Config	Azure Policy, Azure Security Center	Google Cloud Security Command Center

Focused Comparison of Each Category in the Respond function:

In the context of incident response, each cloud provider offers tailored resources to enhance the Respond function. AWS and GCP provide comprehensive guidelines for incident response, while Azure emphasizes aligning plans with its environment [34, 35, 36].

Effective communication during an incident is critical. AWS facilitates notifications through its Simple Notification Service, Azure supports push notifications for various applications via Notification Hubs, and GCP enables event-driven communication with its Pub/Sub service [37, 38, 39].

For incident analysis, AWS utilizes CloudWatch Logs for log analysis, while Azure combines Azure Monitor and Log Analytics to handle telemetry data. GCP's Cloud Logging also plays a crucial role in understanding and troubleshooting its environments.

Mitigation involves specific tools tailored for different scenarios. AWS offers Web Application Firewall (WAF) and Shield for web application and DDoS protection, while Azure provides similar capabilities through its Application Gateway WAF. GCP leverages Cloud Armor and its Content Delivery Network (CDN) for effective threat mitigation [37, 38].

To foster improvements, AWS and GCP use CloudTrail and Security Command Center, respectively, to track and enhance their security posture. Meanwhile, Azure employs its Policy and Security Center to enforce organizational standards.

Incorporating the Respond function into cybersecurity practices significantly enhances the ability to detect, respond to, and recover from incidents. This proactive approach improves overall cybersecurity resilience, enabling more effective protection of critical infrastructure and sensitive information.

Recover Function

The Recover function is a critical component of the NIST Cybersecurity Framework, focusing on activities that develop and implement resilience plans while restoring capabilities or services affected by cybersecurity incidents. Its primary goal is to minimize the impact of such incidents and ensure a timely return to normal operations, emphasizing preparedness and the ability to recover swiftly and effectively [1].

Key aspects of the Recover function include recovery planning, which involves creating well-defined strategies, plans, and procedures for timely recovery. This process outlines roles and responsibilities and establishes recovery time objectives (RTO) and recovery point objectives (RPO) to facilitate an efficient recovery process. Continuous improvement in recovery capabilities is essential; plans should be regularly reviewed and updated based on lessons learned from past incidents, changes in the threat landscape, and advancements in technology [39].

Effective communication is vital during and after a cybersecurity incident. Establishing clear communication plans and mechanisms ensures that relevant stakeholders are promptly informed, fostering trust and coordinated recovery efforts. This includes both internal communication among teams and external communication with customers, partners, and regulators.

Incorporating the Recover function into a cybersecurity strategy enhances its overall resilience. Regular recovery exercises and simulations should be conducted to test recovery plans, revealing gaps and providing insights for improvement. Establishing a culture of continuous learning and improvement empowers employees to actively contribute to enhancing recovery capabilities, leading to more effective plans and procedures.

Table 5 – Cloud Service Comparison for the Recover Function

Category	AWS	Azure	GCP
Recovery Planning	AWS Backup, AWS Disaster Recovery	Azure Site Recovery	Google Cloud Backup, Google Cloud DR
Improvements	AWS Config, AWS CloudTrail	Azure Security Center, Azure Policy	Google Cloud Security Command Center
Communications	Amazon SNS	Azure Notification Hubs	Google Cloud Pub/Sub

In the context of Recovery Planning, AWS Incident Response and Google Cloud Incident Response offer comprehensive recovery strategies tailored to various scenarios [40, 41]. Meanwhile, Azure Incident Response emphasizes integration with the Azure environment to support seamless recovery [42].

Regarding Improvements, AWS CloudTrail and Azure Policy focus on enforcing policies that support continuous improvement, whereas Google Cloud Security Command Center enhances security visibility, which informs and strengthens recovery enhancements.

For Communications, AWS utilizes Simple Notification Service (SNS) for alerts, Azure employs Notification Hubs for scalable notifications, and Google Cloud leverages Pub/Sub for event-driven messaging during recovery efforts.

By utilizing the specific tools and features of AWS, Azure, and GCP within the Recover Function, effective recovery strategies can be developed. Each cloud provider offers distinct advantages, facilitating a quick return to normal operations while reducing the impact of cybersecurity incidents.

Conclusion

The rapid evolution of cybersecurity threats necessitates a proactive and comprehensive approach to risk management, particularly within cloud environments. This article examined the NIST Cybersecurity Framework, emphasizing the importance of its five core functions—Identify, Protect, Detect, Respond, and Recover. By assessing the capabilities of major cloud service providers—AWS, Azure, and GCP—users can strategically leverage their offerings to enhance their cybersecurity posture.

Comparative analysis reveals that while each cloud provider offers robust tools and services across the framework's functions, their strengths differ. AWS excels in customizable identity management and protective technologies, Azure integrates seamlessly with Microsoft-centric environments, and GCP leads in automated encryption and data security. It is essential to consider specific needs, regulatory requirements, and existing IT ecosystems when selecting a cloud provider.

Furthermore, integrating these cloud services into a comprehensive cybersecurity strategy is crucial for resilience against potential incidents. By adopting best practices from the framework and utilizing the strengths of leading cloud platforms, a robust cybersecurity strategy can be crafted to address current threats and anticipate future challenges. Ultimately, a well-defined cybersecurity framework is essential for protecting critical infrastructure and sensitive information, fostering trust among stakeholders, and maintaining operational continuity in an increasingly complex digital landscape.

Funding

This study received no specific financial support.

Competing interests

The authors declare that they have no competing interests.

References

1. NIST. (2018). Framework for Improving Critical Infrastructure Cybersecurity. Retrieved from: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
2. Alam, Md & Pandey, Manjusha & Rautaray, Siddharth. (2015). A Comprehensive Survey on Cloud Computing. International Journal of Information Technology and Computer Science. 7. 68-79. https://doi.org/10.5815/ijitcs.2015.02.09/
3. Synergy Research Group. (2023). Cloud service providers market share at the beginning of 2023. Retrieved from: https://www.srgresearch.com/articles/cloud-spending-growth-rate-slows-but-q4-still-up-by-10-billion-from-2021-microsoft-gains-market-share
4. M.S. Salek and S.M. Khan. (2021). A Review on Cybersecurity of Cloud Computing for Supporting Connected Vehicle Applications. https://doi.org/10.1109/JIOT.2022.3152477
5. Jai Sisodia & Mohammed Khan. (2022). Understanding the Shared Responsibilities Model in Cloud Services. Retrieved from: https://www.isaca.org/resources/isaca-journal/issues/2022/volume-3/understanding-the-shared-responsibilities-model-in-cloud-services
6. NIST. (2010). Contingency Planning Guide for Federal Information Systems. https://doi.org/10.6028/NIST.SP.800-34r1/
7. Amazon GuardDuty. (n.d.). Official AWS Documentation [Website]. Retrieved from: https://aws.amazon.com/guardduty/
8. Azure Resource Manager. (n.d.). Official Microsoft Documentation [Website]. Retrieved from: https://learn.microsoft.com/en-us/azure/azure-resource-manager/
9. Google Cloud Asset Inventory. (n.d.). Official Google Cloud Documentation [Website]. Retrieved from: https://cloud.google.com/asset-inventory/docs
10. Amazon Inspector. (n.d.). Official AWS Documentation [Website]. Retrieved from: https://docs.aws.amazon.com/inspector/

11. Azure Security Center. (n.d.). Official Microsoft Documentation [Website]. Retrieved from: https://learn.microsoft.com/en-us/shows/azure-friday/azure-security-center
12. Google Cloud Security Command Center. (n.d.). Official Google Cloud Documentation [Website]. Retrieved from: https://cloud.google.com/security-command-center/docs
13. AWS Organizations. (n.d.). Official AWS Documentation [Website]. Retrieved from: https://docs.aws.amazon.com/organizations/
14. Azure Policy. (n.d.). Official Microsoft Documentation [Website]. Retrieved from: https://learn.microsoft.com/en-us/azure/governance/policy/
15. Google Cloud Resource Manager. (n.d.). Official Google Cloud Documentation [Website]. Retrieved from: https://cloud.google.com/resource-manager/docs
16. Negussie, D. (2023). Importance of cybersecurity awareness training for employees in business. A journal of Gujarat University, 2, 104-107. http://dx.doi.org/10.47413/vidya.v2i2.206
17. AWS IAM. (n.d.). Official AWS Documentation [Website]. Retrieved from: https://aws.amazon.com/iam/
18. Azure Active Directory. (n.d.). Official Microsoft Documentation [Website]. Retrieved from: https://learn.microsoft.com/en-us/azure/active-directory/
19. Google Cloud IAM. (n.d.). Official Google Cloud Documentation [Website]. Retrieved from: https://cloud.google.com/iam/
20. AWS Training and Certification. (n.d.). Official AWS Training and Certification Website [Website]. Retrieved from: https://aws.training/
21. Google Cloud Data Encryption. (n.d.). Official Google Cloud Documentation [Website]. Retrieved from: https://cloud.google.com/security/encryption
22. Azure Security Center. (n.d.). Official Microsoft Documentation [Website]. Retrieved from: https://learn.microsoft.com/en-us/shows/azure-friday/azure-security-center
23. Azure Policy. (n.d.). Official Microsoft Documentation [Website]. Retrieved from: https://learn.microsoft.com/en-us/azure/governance/policy/
24. Azure Update Management. (n.d.). Official Microsoft Documentation [Website]. Retrieved from: https://learn.microsoft.com/en-us/azure/update-manager/overview
25. AWS Trusted Advisor. (n.d.). Official AWS Documentation [Website]. Retrieved from: https://aws.amazon.com/premiumsupport/technology/trusted-advisor/
26. Google Cloud Recommendations. (n.d.). Official Google Cloud Documentation [Website]. Retrieved from: https://cloud.google.com/recommendations/
27. AWS WAF. (n.d.). Official AWS Documentation [Website]. Retrieved from: https://docs.aws.amazon.com/waf/
28. AWS Shield. (n.d.). Official AWS Documentation [Website]. Retrieved from: https://docs.aws.amazon.com/shield/
29. AWS CloudWatch. (n.d.). Official AWS Documentation [Website]. Retrieved from: https://aws.amazon.com/cloudwatch/
30. Azure Monitor. (n.d.). Official Microsoft Documentation [Website]. Retrieved from: https://learn.microsoft.com/en-us/azure/azure-monitor/
31. Google Cloud Operations Suite. (n.d.). Official Google Cloud Documentation [Website]. Retrieved from: https://cloud.google.com/products/operations
32. AWS Security Hub. (n.d.). Official AWS Documentation [Website]. Retrieved from: https://docs.aws.amazon.com/securityhub/
33. Azure Sentinel. (n.d.). Official Microsoft Documentation [Website]. Retrieved from: https://learn.microsoft.com/en-us/azure/sentinel/
34. AWS Simple Notification Service (SNS). (n.d.). Official AWS Documentation [Website]. Retrieved from: https://aws.amazon.com/sns/
35. Azure Notification Hubs. (n.d.). Official Microsoft Documentation [Website]. Retrieved from: https://azure.microsoft.com/en-us/products/notification-hubs/
36. Google Cloud Pub/Sub. (n.d.). Official Google Cloud Documentation [Website]. Retrieved from: https://cloud.google.com/pubsub/
37. Google Cloud Armor. (n.d.). Official Google Cloud Documentation [Website]. Retrieved from: https://cloud.google.com/armor/

38. Google Cloud CDN. (n.d.). Official Google Cloud Documentation [Website]. Retrieved from: https://cloud.google.com/cdn/
39. Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions [Journal article]. Information Fusion, 97, 101804. https://doi.org/10.1016/j.inffus.2023.101804
40. AWS Incident Response. (n.d.). AWS Documentation [Website]. Retrieved from: https://docs.aws.amazon.com/whitepapers/latest/aws-security-incident-response-guide/aws-security-incident-response-guide.html
41. Google Cloud Incident Response. (n.d.). Google Cloud Documentation [Website]. Retrieved from: https://cloud.google.com/security/resources/datasheets/incident-response-services
42. Azure Incident Response. (n.d.). Official Microsoft Documentation [Website]. Retrieved from: https://learn.microsoft.com/en-us/security/benchmark/azure/security-control-incident-response

Список використаних джерел

1. NIST. (2018). Framework for Improving Critical Infrastructure Cybersecurity. Retrieved from: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
2. Alam, Md & Pandey, Manjusha & Rautaray, Siddharth. (2015). A Comprehensive Survey on Cloud Computing. International Journal of Information Technology and Computer Science. 7. 68-79. https://doi.org/10.5815/ijitcs.2015.02.09/
3. Synergy Research Group. (2023). Cloud service providers market share at the beginning of 2023. Retrieved from: https://www.srgresearch.com/articles/cloud-spending-growth-rate-slows-but-q4-still-up-by-10-billion-from-2021-microsoft-gains-market-share
4. M.S. Salek and S.M. Khan. (2021). A Review on Cybersecurity of Cloud Computing for Supporting Connected Vehicle Applications. https://doi.org/10.1109/JIOT.2022.3152477
5. Jai Sisodia & Mohammed Khan. (2022). Understanding the Shared Responsibilities Model in Cloud Services. Retrieved from: https://www.isaca.org/resources/isaca-journal/issues/2022/volume-3/understanding-the-shared-responsibilities-model-in-cloud-services
6. NIST. (2010). Contingency Planning Guide for Federal Information Systems. https://doi.org/10.6028/NIST.SP.800-34r1/
7. Amazon GuardDuty. (n.d.). Official AWS Documentation [Website]. Retrieved from: https://aws.amazon.com/guardduty/
8. Azure Resource Manager. (n.d.). Official Microsoft Documentation [Website]. Retrieved from: https://learn.microsoft.com/en-us/azure/azure-resource-manager/
9. Google Cloud Asset Inventory. (n.d.). Official Google Cloud Documentation [Website]. Retrieved from: https://cloud.google.com/asset-inventory/docs
10. Amazon Inspector. (n.d.). Official AWS Documentation [Website]. Retrieved from: https://docs.aws.amazon.com/inspector/
11. Azure Security Center. (n.d.). Official Microsoft Documentation [Website]. Retrieved from: https://learn.microsoft.com/en-us/shows/azure-friday/azure-security-center
12. Google Cloud Security Command Center. (n.d.). Official Google Cloud Documentation [Website]. Retrieved from: https://cloud.google.com/security-command-center/docs
13. AWS Organizations. (n.d.). Official AWS Documentation [Website]. Retrieved from: https://docs.aws.amazon.com/organizations/
14. Azure Policy. (n.d.). Official Microsoft Documentation [Website]. Retrieved from: https://learn.microsoft.com/en-us/azure/governance/policy/
15. Google Cloud Resource Manager. (n.d.). Official Google Cloud Documentation [Website]. Retrieved from: https://cloud.google.com/resource-manager/docs
16. Negussie, D. (2023). Importance of cybersecurity awareness training for employees in business. A journal of Gujarat University, 2, 104-107. http://dx.doi.org/10.47413/vidya.v2i2.206
17. AWS IAM. (n.d.). Official AWS Documentation [Website]. Retrieved from: https://aws.amazon.com/iam/
18. Azure Active Directory. (n.d.). Official Microsoft Documentation [Website]. Retrieved from: https://learn.microsoft.com/en-us/azure/active-directory/

19. Google Cloud IAM. (n.d.). Official Google Cloud Documentation [Website]. Retrieved from: https://cloud.google.com/iam/
20. AWS Training and Certification. (n.d.). Official AWS Training and Certification Website [Website]. Retrieved from: https://aws.training/
21. Google Cloud Data Encryption. (n.d.). Official Google Cloud Documentation [Website]. Retrieved from: https://cloud.google.com/security/encryption
22. Azure Security Center. (n.d.). Official Microsoft Documentation [Website]. Retrieved from: https://learn.microsoft.com/en-us/shows/azure-friday/azure-security-center
23. Azure Policy. (n.d.). Official Microsoft Documentation [Website]. Retrieved from: https://learn.microsoft.com/en-us/azure/governance/policy/
24. Azure Update Management. (n.d.). Official Microsoft Documentation [Website]. Retrieved from: https://learn.microsoft.com/en-us/azure/update-manager/overview
25. AWS Trusted Advisor. (n.d.). Official AWS Documentation [Website]. Retrieved from: https://aws.amazon.com/premiumsupport/technology/trusted-advisor/
26. Google Cloud Recommendations. (n.d.). Official Google Cloud Documentation [Website]. Retrieved from: https://cloud.google.com/recommendations/
27. AWS WAF. (n.d.). Official AWS Documentation [Website]. Retrieved from: https://docs.aws.amazon.com/waf/
28. AWS Shield. (n.d.). Official AWS Documentation [Website]. Retrieved from: https://docs.aws.amazon.com/shield/
29. AWS CloudWatch. (n.d.). Official AWS Documentation [Website]. Retrieved from: https://aws.amazon.com/cloudwatch/
30. Azure Monitor. (n.d.). Official Microsoft Documentation [Website]. Retrieved from: https://learn.microsoft.com/en-us/azure/azure-monitor/
31. Google Cloud Operations Suite. (n.d.). Official Google Cloud Documentation [Website]. Retrieved from: https://cloud.google.com/products/operations
32. AWS Security Hub. (n.d.). Official AWS Documentation [Website]. Retrieved from: https://docs.aws.amazon.com/securityhub/
33. Azure Sentinel. (n.d.). Official Microsoft Documentation [Website]. Retrieved from: https://learn.microsoft.com/en-us/azure/sentinel/
34. AWS Simple Notification Service (SNS). (n.d.). Official AWS Documentation [Website]. Retrieved from: https://aws.amazon.com/sns/
35. Azure Notification Hubs. (n.d.). Official Microsoft Documentation [Website]. Retrieved from: https://azure.microsoft.com/en-us/products/notification-hubs/
36. Google Cloud Pub/Sub. (n.d.). Official Google Cloud Documentation [Website]. Retrieved from: https://cloud.google.com/pubsub/
37. Google Cloud Armor. (n.d.). Official Google Cloud Documentation [Website]. Retrieved from: https://cloud.google.com/armor/
38. Google Cloud CDN. (n.d.). Official Google Cloud Documentation [Website]. Retrieved from: https://cloud.google.com/cdn/
39. Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions [Journal article]. Information Fusion, 97, 101804. https://doi.org/10.1016/j.inffus.2023.101804
40. AWS Incident Response. (n.d.). AWS Documentation [Website]. Retrieved from: https://docs.aws.amazon.com/whitepapers/latest/aws-security-incident-response-guide/aws-security-incident-response-guide.html
41. Google Cloud Incident Response. (n.d.). Google Cloud Documentation [Website]. Retrieved from: https://cloud.google.com/security/resources/datasheets/incident-response-services
42. Azure Incident Response. (n.d.). Official Microsoft Documentation [Website]. Retrieved from: https://learn.microsoft.com/en-us/security/benchmark/azure/security-control-incident-response