Journal of Sustainable Solutions
ISSN : 3048-6947 | Vol. 1 | Issue 4 | Oct - Dec 2024 | Peer Reviewed & Refereed

Security and Compliance Considerations for Running SAP Systems on AWS

Sachin Bhatt*

Independent Researcher, USA.

Accepted: 24/10/2024 Published: 25/10/2024 * Corresponding author

How to Cite this Article:

Hegde E. (2024). Security and Compliance Considerations for Running SAP Systems on AWS *Journal of Sustainable Solutions*, 1(4), 72-86.

DOI: https://doi.org/10.36676/j.sust.sol.v1.i4.36

Abstract

This research work focuses on Amazon Web Services' security and compliance requirements while hosting SAP environments. It reviews aspects of security particularly on data, encryption, identity and access control and security of networks. Emerging compliance issues regarding GDPR, HIPAA, and SOX are explained to cover data location and control. The paper also outlines how best to approach security control management and how to use AWS tools to overcome these challenges. Identifying the critical measures to ensure compliance and security is made; these are strongly encouraged to be managed as well as applied actively and with the help of key features of AWS.

Keywords: SAP systems, AWS, security, compliance, data protection, encryption, identity and access management, GDPR, HIPAA, SOX, data residency, AWS tools.

Introduction

1.1 Overview of SAP Systems and AWS

SAP systems are the systems that help to run the entire businesses with the help of enterprise resource planning (ERP) software solutions that contain vital business operations like finance, logistics, human resources, and supply chain management. These systems are important in large organization as they provided tools for methods of operations and decision-making processes. Earlier used in-house, there is an increasing trend of companies transitioning SAP applications to cloud computing for better elasticity, modularity, and economy (Park et al., 2022). AWS is one of the most popular cloud solutions that provide high-level security for SAP systems and diversified scalable possibilities.

AWS owns several services like EC2, S3, and RDS which can be finely tuned for SAP applications making it possible for the enterprises to have an advantage of the cloud based on-demand computing, storage and data base. The main benefits contained in SAP migration to AWS crucial for business operations are improvements in operational flexibility and cost management effectiveness but at the same time, security challenges and compliance issues that have to be solved.

1.2 Importance of Security and Compliance in Cloud Environments

Security and compliance are always major issues when it comes to the running of systems and especially for enterprise applications like the SAP systems. According to the demands of businesses where the operations have been moved to the cloud, the information data structures, applications, and systems must be safeguarded from breaches, vandals, and other threats. Security controls are crucial in avoiding exposure of information to unauthorized personnel by incorporating adequate control measures like encrypted codes, users and privilege access, and protective

structures concerning the network (Makka, 2022). While compliance guarantees that organisations operate in accordance with the legal and sectorial requirements including GDPR, HIPAA, or SOX. Non-compliance with any of the listed standards immortalizes the Organization to legal consequences, financial loses, and reputational damage.

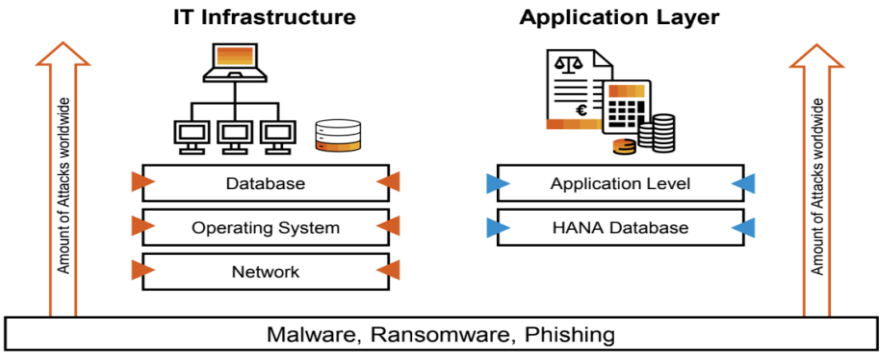

Figure 1 AWS Security Solutions for SAP S/4HANA (Syntax, 2022)

In cloud environments it becomes imperative that the organization remains in control of the location data resides, is processed and is made available to users. Including shared responsibility models of cloud providers such as AWS, it is critical to identify the concepts of responsibilities and security measures for protecting the enterprise systems, and compliance with legal provisions.

1.3 Objectives of the Research

- Discuss on the main areas of concern in terms of security while implementing SAP systems within AWS environment.
- SAP deployment on AWS compliance reporting and issues.
- Determine what practices should be followed to safeguard and maintain SAP workloads' compliance within cloud setting.
- Discover AWS solutions and functionalities assisting in securing and improving compliance for SAP environments.
- Identify and explain some security and compliance issues most firms encounter in cloud and recommend measures of addressing these issues.
- Offer best practices for organisations to enhance the SAP applications on AWS with a specific focus on the security and compliance.

Background

2.1 Overview of SAP Systems

SAP systems are full functional ERP solutions meant to address the many processes within an organization. SAP which is an acronym for Systems, Applications, and Products offers numerous software packages that addresses basic business activities including accounting, manufacturing and distribution, personnel, purchasing and selling among others.

These systems enable the business to organize the operations and data in a better manner, automate processes and provide real-time information to support the decision making (Fortino et al., 2022). SAP systems are used by majority of large enterprises because of these qualities to include; scalability, flexibility and have the potential capacity to accommodate complex business activities.

Being a traditional on-premise system, SAP advanced to a cloud format with solutions, such as SAP S/4HANA that provides solution such as better performance, analytics, and digital business alteration. Increased clienteles' demands towards cloud solutions, for instance, AWS, have forced organizations to host SAP systems on cloud environment to obtain efficiency, and cost advantages.

2.2 Overview of AWS Services for SAP

AWS provides organizations with a highly-suited cloud solution specifically for SAP applications that helps them host their SAP solutions in a secure, flexible, and economical model. AWS has extended several services which are designed and optimized for SAP Solutions and those are Computational Service, Storage Service & Database Service that guarantee high availability & high performance to important applications. Some major services are Amazon EC2 for business capacity utilization for SAP application and Amazon S3 for storage of SAP data. Amazon RDS and Amazon Aurora provide the facility of managed database services to optimize the SAP HANA and other SAP certified databases. AWS also offers such products as AWS Backup for creating automated data protection solutions and AWS Identity and Access Management (IAM) for managing users' access to protect the data. It reveals that organisations using AWS gets flexibility, implement disaster recovery solutions for SAP systems, and scale resources for SAP environments, that strengthens operations.

2.3 Key Security and Compliance Challenges in Cloud Computing

Cloud computing brings in a number of new security and compliance considerations especially when it comes to the implementation of important enterprise applications such as SAP. Among the challenges faced when developing the app one of them is the protection of data. One of the ways through which information can be protected is through use of encryption to ensure that information is secured even when in transit, and when stored on storage media (Loaiza Enriquez, 2021). Access control management is also essential as misconfigurations can bring in threat actors' attention to sensitive data.

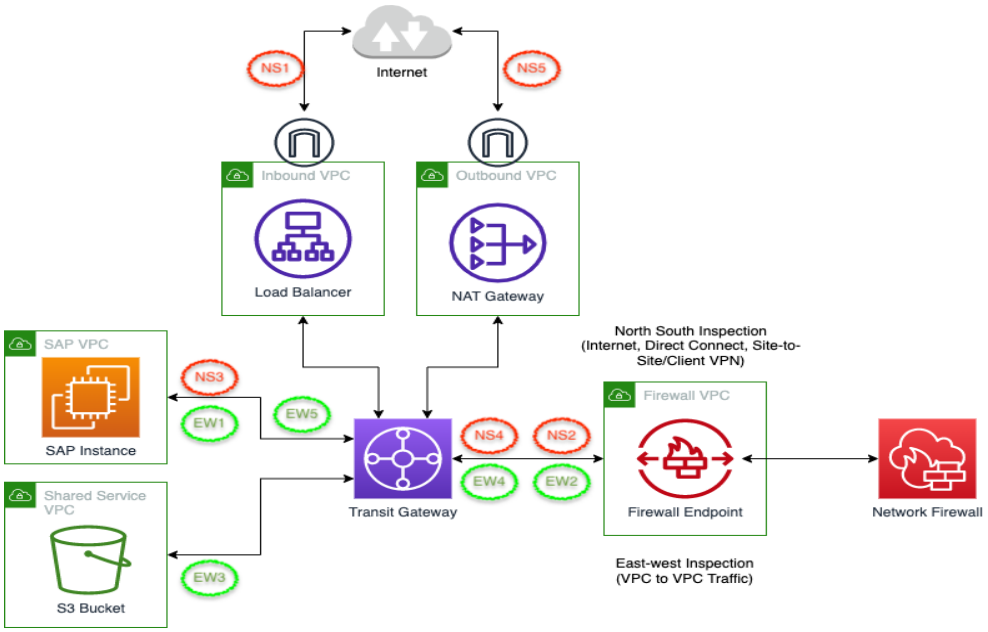

Figure 2 Security, Identity, & Compliance (AWS, 2022)

Problems of compliance appear when cloud infrastructures span over multiple geographical locations which are governed under different laws like GDPR and HIPAA. The notion of data residency, sovereignty, and adherence to a range of legal needs becomes challenging when many clouds or the hybrid model is used.

One is the approach of cloud providers such as AWS that uses the shared responsibility model where AWS protects the infrastructure and organization has to protect the data, configurations, and applications. It may therefore result to gaps in security in the division of duties in case it is mishandled. Sustaining security is only possible when accompanied by compliance which in cloud computing is possible through auditing and vulnerability assessments and observing industrial standards.

Security Considerations

3.1 Data Protection and Encryption

Security and protection of data is one of the most important things that needs to be considered when working with SAP systems in AWS. It is crucial to safeguard privacy and data from hackers, theft and loss since data is the key asset of various companies. The AWS offers various components and services to assist in the protection of data through utilising encryption while it is in transit and while stored (Micro, 2020).

To encrypt data at rest there is AWS Key Management Service (KMS) whereby organizations have the ability to control KMS keys and use them across services such as Amazon S3, Elastic Block Store (EBS), and Relational Data Service (RDS). This serves to make sure that data that has been stored has to be protected and encrypted in case there is a violation of the system.

In case of data in transit, Tunnelling protocols such as Transport Layer Security (TLS) protocols are employed with aim of providing secure communication between different users, applications and services. Adopting Encryption properly contributes to compliance with the related regulations including GDPR or HIPAA, and contributes to manage risks associated with data exposure or theft in cloud in respect to cyber-attacks.

Table 1 Data Protection and Encryption Approaches

Method	Description	AWS Service	Encryption Standard	Example
At Rest Encryption	Data encryption at storage	AWS KMS, S3	AES-256	SAP database backups
In Transit Encryption	Data encryption during transfer	TLS, AWS Certificate Manager	TLS/SSL	Data between SAP components
Backup Encryption	Encrypting backup data	AWS Backup, S3	AES-256	SAP backup files

3.2 Identity and Access Management

The first important step in securing SAP systems on AWS is IAM, because it determines who can interact with the company's AWS resources as well as what actions are permitted to them at any given time. Effective management of identities and access is vital in addressing issue of unwanted users as well as compromise of organizational data and abuse of organizational assets.

AWS offers a mature IAM feature that can help companies to set detailed permissions for their employees. This is done by developing account structures with roles and groups, and policies that let users work only as required by the principle of least privilege. Multi-factor authentication (MFA) option is also provided to make the account more secure in case of access to the sensitive information.

RBAC and AWS IAM help organizations to limit the access of the users to the SAP systems by allowing user-specific authorization. You also get tools like AWS CloudTrail and AWS Config that helps in tracking the access activity so that the internal security policies and protocol as well as the outside regulatory framework are met.

3.3 Network Security

Security is a critical fundamental and when implementing SAP systems on AWS it provides a cover to data and applications from ant access, threats and other form of vulnerabilities. AWS offers multiple options and characteristics to protect the network as well as the communication channels from unwanted access to SAP systems and other services.

Amazon VPC provides organisations with a way of compartmentalising the den SAP environments

creating a virtual computer network with its security parameters. In VPC, subnets routing tables, and security groups can be set in a way that will manage traffic that is being allowed in and out. Network segmentation and the use firewalls help to restrict traffic to only those that would be permitted to access SAP resources.

AWS also have features such as AWS Shield for protection against Distributed Denial of Service (DDoS) attack, and AWS WAF (Web Application Firewall) for protection against known web threats (Lonnemann, 2022). That is why it is critical to have sound network security measures that an organization can adopt to reduce its vulnerability to cyber threats and ensure a secure SAP setup in AWS.

3.4 Vulnerability Management and Threat Detection

Risk evaluation and threat identification are important in safeguarding SAP applications to prevent imminent securities threats that may compromise the infrastructure of AWS. AWS offers range of solutions and solutions that assist organizations in the continuous monitoring and counteraction to threats.

The Amazon Inspector is one of the critical tools for the Vulnerability Assessments as it scans the SAP workloads for security vulnerabilities including that of unpatched software, misconfigured settings or old packages for example. This means that organizations can easily identify the weaknesses inherent in the systems being used and apply the right patches or update for the same. Also, AWS Systems Manager Patch Manager is used to manage patching and update systems to the latest to improve on security.

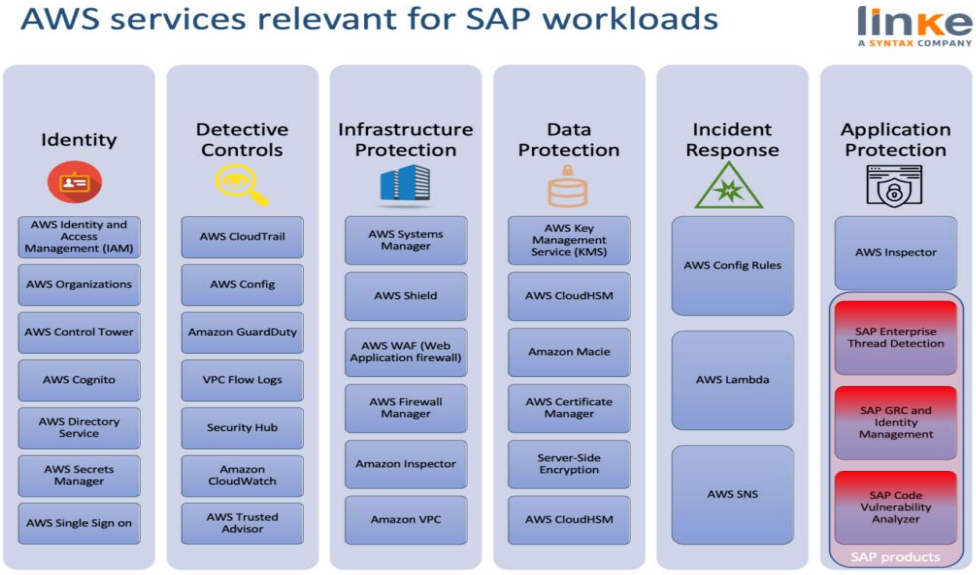

Figure 3 AWS Security Solutions for SAP S/4HANA (III): Infrastructure Protection (Syntax, 2022)

In terms of identifying threats in real-time, AWS Guard Duty processes logs and network traffic for identified threats and AWS Security Hub is a virtual security operations center where all alerts are managed and responded to. The former is computed to facilitate timely threat identification to avert any openings, which if exploited, would compromise SAP systems on AWS hence fortifying the general security entrenchments.

3.5 Incident Response and Recovery

Reflections on security incidents as well as response and recovery mechanisms are key in preventing and controlling the effects of insecurity in SAP systems facing AWS. AWS has various features like AWS CloudTrail and AWS Config that allow the organizations to monitor and log the security events and quickly respond to the incidents (Maurer et al., 2020). AWS CloudWatch provides features of event

visibility and real-time monitoring and notification to the development teams to respond more effectively to technical problems.

In recovery, AWS Backup helps in becoming independent of the data protection and restoration environment so that the continuity of business is maintained. Maintaining an effective incident response plan, containing specific worked through procedures, along with communication protocols, are critical for organizations in effectively managing and recovering from security incidents while also reducing the amount of downtime as well as loss of data to a minimum.

Table 2 Incident Response and Recovery Plan

Component	Description	Tools Used	Response Time
Detection	Identifying incidents	AWS GuardDuty, CloudWatch	Within 5 minutes
Response	Managing incidents	AWS Lambda, System s Manager	Within 30 minutes
Backup	Data backup	AWS Backup, S3	Daily backups
Recovery	Restoring data	AWS Disaster Recovery	Within 1 hour
Forensics	Analyzing incidents	AWS CloudTrail	Within 24 hours

Compliance Considerations

4.1 Relevant Regulatory Frameworks (e.g., GDPR, HIPAA, SOX)

It is a requirement that regulatory guidelines must be followed specifically when one is using SAP systems on the AWS platform because these frameworks govern matters to do with usage of sensitive data as well as compliance with the law and industry best practices. The GDPR insists on data protection and privacy measures by organizations that deal with personal data of EU citizen.

These things entail data encryption, access controls and clear and conspicuous data processing practices. HIPAA is the acronym for the Health Insurance Portability and Accountability Act in the U. S. that provides rules for the protection of health information that must be stored, transmitted, and accessed securely: The Sarbanes-Oxley Act (SOX) targets the financial reporting and internal control addendiary which requires good record keeping and audit trails.

Some of AWS's tools and features can assist organizations to meet these regulations; however, organizations have to put in place extra measures and frequently update regulatory compliance so that they do not attract the law and keep sensitive data safe (Yathiraju, 2022).

Table 3 Compliance Frameworks and AWS Services

Regulation	Compliance Requirement	AWS Service	Compliance Status
GDPR	Data encryption and access	AWS KMS, AWS IAM	Compliant
HIPAA	Data protection for PHI	AWS S3, AWS CloudTrail	Compliant
SOX	Financial data controls	AWS CloudTrail	Compliant
PCI-DSS	Payment data protection	AWS KMS, AWS WAF	Compliant

4.2 Compliance Certifications and Standards (e.g., ISO, SOC)

Compliance certifications and standards are important components towards making certain that SAP systems on AWS are compliant with different industry needs and recommendation. AWS has multiple compliance certifications based on several frameworks among them are ISO 27001 for information security management and SOC 1, SOC 2, SOC 3 for controls on security, availability, and confidentiality.

These certifications prove that AWS ensures excellent security standards to run its organization and com-formed to all regulatory norms. For organisations that are using AWS to host SAP systems, utilising

these certifications assists in guaranteeing that an organisations cloud environment is at optimal security and functionality as it undertakes business compliance.

4.3 Data Residency and Sovereignty

Data residency and sovereignty play the vital role compliance while operating sap systems in aws. Data location determines where the data collected is located which sometimes may be a problem in compliance with different national laws protecting data. Data sovereignty makes sure that data is governed by the laws and regulation of the country the data is located in. Some of the services that AWS provide include AWS Regions and Availability Zones whereby an organization is made to select certain regions and zones for the storage of data and processing. This capability allows organizations to address legal and regulatory issues concerning the location of data and data sovereignty that relates to control of data handling in accordance with legal requirements.

4.4 Auditing and Reporting Requirements

Data residency and sovereignty play the vital role compliance while operating sap systems in aws. Data location determines where the data collected is located which sometimes may be a problem in compliance with different national laws protecting data. Data sovereignty makes sure that data is governed by the laws and regulation of the country the data is located in (Shahane, 2022).

Some of the services that AWS provide include AWS Regions and Availability Zones whereby an organization is made to select certain regions and zones for the storage of data and processing.

This capability allows organizations to address legal and regulatory issues concerning the location of data and data sovereignty that relates to control of data handling in accordance with legal requirements.

Best Practices for Security and Compliance

5.1 Implementing Security Controls and Measures

Security perspectives are critical since any SAP systems on AWS have to be well protected as well as meeting compliance standards. It is first advisable to start with simple, but very effective, tools that AWS offers by default: IAM for setting up very detailed access rights, and KMS for managing encryption keys.

Table 4 AWS Security Features for SAP Systems

Feature	Description	AWS Service	Example Value
IAM Roles	Number of roles created	AWS IAM	50 roles
Encryption Keys	Total keys managed	AWS KMS	100 keys
Network Segments	Isolated network segments	Amazon VPC	10 segments
Security Groups	Number of security groups	AWS VPC	25 groups
CloudWatch Alarms	Active monitoring alarms	AWS CloudWatch	30 alarms

Employ Amazon Virtual Private Cloud (VPC) to develop virtual networks and employ network security groups as well as managed access control lists for the regulation of network traffic. Patch up the computers with AWS Systems Manager and fix the problems and risks that may develop when in use.

Use the instruments of AWS CloudTrail and Amazon CloudWatch to log and monitor to identify and address the security threats in real time. Also, perform security check-ups and vulnerability scans to discover some loopholes in the security standard, and compliance with the established security measures should also be checked on a regular basis. By following these best practices, the SAP systems are protected, compliance is maintained and potential risks eliminated in the cloud environment.

5.2 Ensuring Compliance with Legal and Regulatory Requirements

It is paramount to adhere to legal and regulations by avoiding conflicts with the law since it is risky to operate SAP systems in AWS without meeting the legal framework and ensure data security and protection. Start by identifying the currents rules and regulations that are relevant to your type of

business and or location for example, General Data Protection Regulation, Health Insurance Portability and Accountability Act or Sarbanes-Oxley Act. AWS provides compliance support in managing these compliances and these include the following; AWS Artifact which consists of compliance reports and compliance certifications. Ensure that data privacy strategies such as encryption, or restricted access are put in place to meet legal needs. Monitor the ever-shifting laws that have an impact on policies and procedures to ensure that the manufacture's policies and procedures remain in line with industry recommendations. Carry out an internal audit and risk analysis to see they security measures put in place are sound and are in line with the recommended guidelines.

Create documentation and reporting procedures to attesting compliance where it is scrutinized during outside auditors. When implemented within your SAP processes operating on AWS, these practices will help you keep compliance exposures and legal/regulation non-conformance in check.

5.3 Leveraging AWS Tools and Services for Security and Compliance

Secure and compliant SAP solutions are the focus of the AWS services that can be used by business enterprises. AWS IAM is the first layer for implementing strict level of access control measures that govern users' permissions on cloud resources. Encrypt your data at rest and in transit using AWS KMS as your encryption key management system. Continuously monitor threats with Amazon GuardDuty, this is a service that analyses tags of AWS CloudTrail logs in search of security threats. AWS Config helps in evaluating Resource configurations against compliance and monitoring the changes that affect configurations. AWS Security Hub collects security assessment and security related information from other services to give an overall summary of the physical security. AWS Artifact provides information on compliance reports that may include your compliance needs as well as compliance certifications. If harnessed properly, these tools provide organizational security and compliance for SAP systems, as well as compliance with regulations.

Table 5 AWS Services for Security and Compliance

AWS Service	Purpose	Feature Count	Example Use
AWS IAM	Access management	50 policies	Managing SAP system access
AWS KMS	Key management	100 keys	Encrypting SAP data
AWS GuardDuty	Threat detection	1,000+ alerts	Monitoring SAP logs
AWS Config	Configuration management	200 rules	Tracking SAP configuration changes
AWS CloudTrail	Logging	500+ logs	Tracking user activity in SAP

Challenges and Solutions

As mentioned earlier on, running SAP systems on AWS has some key issues that are specific under the insurance of security and compliance. However, handling tangled security settings across the multiple services in AWS remain to be a tricky task that can put the organization in a vulnerable position due to misconfigurations. It will be appreciated that using tools like AWS Security Hub and AWS Config, is useful in maintaining the organization's security features and adhering to the approved policies. Another challenge is the ability to manage compliance with different regulation across the data borders.

On the usage of AWS services for data residency AWS Artifact can be used for compliance report and the use of AWS services for data storage in regions of the world can be used to solve the data residency issues. Companies may experience some difficulties in incorporating the processes of security into the ongoing processes. Problems such as these can be addressed by implementing a holistic cloud security

strategy which includes staff training at intervals, developing protocols regarding response to any security breaches and management protocols for vulnerabilities (Abdulraheem et al., 2020). The identification of these challenges helps in preventing these issues from escalating or occurring as an aftermath by providing the right solutions that guarantee the safety and sound compliance of SAP systems on AWS.

Table 6 Common Compliance Challenges and Solutions

Challenge	Description	Mitigation Strategy	Implementation Detail
Data Residency	Compliance with data location laws	Regional data storage	5 AWS regions used
Multi-Cloud Compliance	Consistent compliance across platforms	Unified policies and tools	AWS Config and CloudTrail used
Regulatory Updates	Keeping up with changing regulations	Regular policy reviews	Quarterly audits
Access Control	Preventing unauthorized access	IAM policies and roles	50 roles defined
Encryption Management	Managing encryption keys	AWS KMS for key management	100 keys managed

Conclusion

To sum up, it is evident that the offered decision to run the SAP systems on AWS has numerous potential benefits connected to the high flexibility, adjustability, and cost-effectiveness of this all-cloud solution, it at the same time poses rather severe difficulties connected with security and compliance issues. Mitigation of these risks requires professionals to have extensive knowledge of the AWS tools and Services and actively develops a security plan to match the needed security controls, and compliance with regulations (Kumar et al., 2022).

To pick up a bit on points 2-3, leveraging AWS's native security features like IAM, KMS and GuardDuty organizations can improve their current security situation as well as their overall compliance. Daily, weekly, monthly, and annual security audits, and vulnerability self-assessments, and overall good plans to respond to and manage incidents are important to prevent security breaches. Ensuring data localisation and compliance to regulations that may arise in the future also helps in this compliance process. Finally, a strategic sense of security and compliance, using AWS's services yields SAP systems security and compliance and ability to support business objectives well within the cloud environment.

References

Abdulraheem, A. S., Abdulla, A. I., & Mohammed, S. M. (2020). Enterprise resource planning systems and challenges. *Technology Reports of Kansai University*, *62*(4), 1885-1894. https://www.researchgate.net/profile/Subhi-Zeebaree/publication/341767232_Enterprise_Resource_Planning_Systems_and_Challenges/links/5ed82970299bf1c67d3bac1e/Enterprise-Resource-Planning-Systems-and-Challenges.pdf

Fortino, G., Guerrieri, A., Pace, P., Savaglio, C., & Spezzano, G. (2022). Iot platforms and security: An analysis of the leading industrial/commercial solutions. *Sensors*, *22*(6), 2196. https://doi.org/10.3390/s22062196

Kumar, D., & Bharti, M. (2022). Internship In Support Operations. http://www.ir.juit.ac.in:8080/jspui/bitstream/123456789/3686/1/Internship%20In%20Support%20Operations.pdf

Loaiza Enriquez, R. (2021). Cloud Security Posture Management/CSPM) in Azure. https://www.theseus.fi/bitstream/handle/10024/504136/Cloud%20Security%20Posture%20Management.pdf?sequence=2&isAllowed=y

Lonnemann, P. (2022). *Assessment of decision criteria for SAP S/4HANA deployment options and design of a decision model* (Doctoral dissertation, University Innsbruck). https://www.seres-unit.com/wp-content/uploads/DPA/DTA22_Arbeit_Lonnemann_Philip.pdf

Makka, A. K. A. (2022). Administering SAP S/4 HANA in Advanced Cloud Services: Ensuring High Performance and Data Security. *Cybersecurity and Network Defense Research*, *2*(1), 23-56. https://www.thesciencebrigade.com/cndr/article/view/285/274

Maurer, T., & Hinck, G. (2020). *Cloud security: a primer for policymakers*. Carnegie Endowment for International Peace. https://carnegie-production-assets.s3.amazonaws.com/static/files/Maurer_Hinck_Cloud_Security-V3.pdf

Micro, T. (2020). Deep Security Software. http://hmst.co.kr/wp-content/uploads/2023/06/2.-ds-deep-security-software.pdf?ckattempt=1

Park, S. J., Lee, Y. J., & Park, W. H. (2022). Configuration method Of AWS security architecture that is applicable to the cloud lifecycle for sustainable social network. *Security and Communication Networks*, *2022*(1), 3686423. https://doi.org/10.1155/2022/3686423

Shahane, V. (2022). Serverless Computing in Cloud Environments: Architectural Patterns, Performance Optimization Strategies, and Deployment Best Practices. *Journal of AI-Assisted Scientific Discovery*, *2*(1), 23-43. https://scienceacadpress.com/index.php/jaasd/article/view/18/16

Yathiraju, N. (2022). Investigating the use of an artificial intelligence model in an ERP cloud-based system. *International Journal of Electrical, Electronics and Computers*, *7*(2), 1-26. https://d1wqtxts1xzle7.cloudfront.net/85514837/IJEEC_01_march_april_2022-libre.pdf?1651730943=&response-content-disposition=inline%3B+filename%3DInvestigating_the_use_of_an_Artificial_I.pdf&Expires=1725815206&Signature=X97bJ9uVseBr3PLHGScT7aIkVUNdmrsMl7-1hPN6VLQQiNy2kqK5HyG1quE9Z4gGRbf-kH4KxTxgRk4afOkKcLYByEY1X7x~hdbp-3GwpRZgx00mxHHF4lh8dMGf8RbGJfXKoy88eGsdp1ka51kx-XKDMVNnIzdnHYKGpq72b9rSf2crfubHcWRk-0sj9I9xO7QJZYN~-PsYvTg93fkMLQtee~ySTpi~LhFtqLAVL2aAetSfZpPPBp6j0qeMK3UKg1g7oumjQk18qNqlY5F2F98weGgmBaTBPyvIqFsxadrttsB1TbZMjdKOZ6ibOhOyV6al2UmmLOlspt5HU6QSIw__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA

Suman

Kavuri, S., & Narne, S. (2020). Implementing effective SLO monitoring in high-volume data processing systems. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 6(2), 558. http://ijsrcseit.com

Kavuri, S., & Narne, S. (2021). Improving performance of data extracts using window-based refresh strategies. International Journal of Scientific Research in Science, Engineering and Technology, 8(5), 359-377. https://doi.org/10.32628/IJSRSET

Narne, S. (2023). Predictive analytics in early disease detection: Applying deep learning to electronic health records. African Journal of Biological Sciences, 5(1), 70–101. https://doi.org/10.48047/AFJBS.5.1.2023.7

Bhatt, S., & Narne, S. (2023). Streamlining OS/DB Migrations for SAP Environments: A Comparative Analysis of Tools and Methods. Stallion Journal for Multidisciplinary Associated Research Studies, 2(4), 14–27. https://doi.org/10.55544/sjmars.2.4.3

Narne, S. (2024). The impact of telemedicine adoption on patient satisfaction in major hospital chains. Bulletin of Pure and Applied Sciences-Zoology, 43B(2s).
Narne, S. (2022). AI-driven drug discovery: Accelerating the development of novel therapeutics. International Journal on Recent and Innovation Trends in Computing and Communication, 10(9), 196. http://www.ijritcc.or
Rinkesh Gajera. (2024). Comparative Analysis of Primavera P6 and Microsoft Project: Optimizing Schedule Management in Large-Scale Construction Projects. International Journal on Recent and Innovation Trends in Computing and Communication, 12(2), 961–972. Retrieved from https://www.ijritcc.org/index.php/ijritcc/article/view/11164
Rinkesh Gajera , "Leveraging Procore for Improved Collaboration and Communication in Multi-Stakeholder Construction Projects", International Journal of Scientific Research in Civil Engineering (IJSRCE), ISSN : 2456-6667, Volume 3, Issue 3, pp.47-51, May-June.2019
Rinkesh Gajera , "Integrating Power Bi with Project Control Systems: Enhancing Real-Time Cost Tracking and Visualization in Construction", International Journal of Scientific Research in Civil Engineering (IJSRCE), ISSN : 2456-6667, Volume 7, Issue 5, pp.154-160, September-October.2023
URL : https://ijsrce.com/IJSRCE123761
Rinkesh Gajera, "The Impact of Smartpm's Ai-Driven Analytics on Predicting and Mitigating Schedule Delays in Complex Infrastructure Projects", Int J Sci Res Sci Eng Technol, vol. 11, no. 5, pp. 116–122, Sep. 2024, Accessed: Oct. 02, 2024. [Online]. Available: https://ijsrset.com/index.php/home/article/view/IJSRSET24115101
Rinkesh Gajera. (2024). IMPROVING RESOURCE ALLOCATION AND LEVELING IN CONSTRUCTION PROJECTS: A COMPARATIVE STUDY OF AUTOMATED TOOLS IN PRIMAVERA P6 AND MICROSOFT PROJECT. International Journal of Communication Networks and Information Security (IJCNIS), 14(3), 409–414. Retrieved from https://ijcnis.org/index.php/ijcnis/article/view/7255
Gajera, R. (2024). Enhancing risk management in construction projects: Integrating Monte Carlo simulation with Primavera risk analysis and PowerBI dashboards. Bulletin of Pure and Applied Sciences-Zoology, 43B(2s).
Gajera, R. (2024). The role of machine learning in enhancing cost estimation accuracy: A study using historical data from project control software. Letters in High Energy Physics, 2024, 495-500.
Rinkesh Gajera. (2024). The Impact of Cloud-Based Project Control Systems on Remote Team Collaboration and Project Performance in the Post-Covid Era. International Journal of Research and Review Techniques, 3(2), 57–69. Retrieved from https://ijrrt.com/index.php/ijrrt/article/view/204
Rinkesh Gajera, 2023. Developing a Hybrid Approach: Combining Traditional and Agile Project Management Methodologies in Construction Using Modern Software Tools, ESP Journal of Engineering & Technology Advancements 3(3): 78-83.

Gajera, R. (2023). Evaluating the effectiveness of earned value management (EVM) implementation using integrated project control software suites. Journal of Computational Analysis and Applications, 31(4), 654-658.
Paulraj, B. (2023). Enhancing Data Engineering Frameworks for Scalable Real-Time Marketing Solutions. Integrated Journal for Research in Arts and Humanities, 3(5), 309–315. https://doi.org/10.55544/ijrah.3.5.34
Paulraj, B. (2023). Optimizing telemetry data processing pipelines for large-scale gaming platforms. International Journal of Scientific Research in Science, Engineering and Technology, 10(31), 401. https://doi.org/10.32628/IJSRSET23103132

Balachandar Paulraj. (2024). LEVERAGING MACHINE LEARNING FOR IMPROVED SPAM DETECTION IN ONLINE NETWORKS. Universal Research Reports, 11(4), 258–273. https://doi.org/10.36676/urr.v11.i4.1364

Paulraj, B. (2022). Building Resilient Data Ingestion Pipelines for Third-Party Vendor Data Integration. Journal for Research in Applied Sciences and Biotechnology, 1(1), 97–104. https://doi.org/10.55544/jrasb.1.1.14

Paulraj, B. (2022). The Role of Data Engineering in Facilitating Ps5 Launch Success: A Case Study. International Journal on Recent and Innovation Trends in Computing and Communication, 10(11), 219–225. https://doi.org/10.17762/ijritcc.v10i11.11145

Paulraj, B. (2019). Automating resource management in big data environments to reduce operational costs. Tuijin Jishu/Journal of Propulsion Technology, 40(1). https://doi.org/10.52783/tjjpt.v40.i1.7905

Balachandar Paulraj. (2021). Implementing Feature and Metric Stores for Machine Learning Models in the Gaming Industry. European Economic Letters (EEL), 11(1). Retrieved from https://www.eelet.org.uk/index.php/journal/article/view/1924

Balachandar Paulraj. (2024). SCALABLE ETL PIPELINES FOR TELECOM BILLING SYSTEMS: A COMPARATIVE STUDY. Darpan International Research Analysis, 12(3), 555–573. https://doi.org/10.36676/dira.v12.i3.107

Ankur Mehra, Sachin Bhatt, Ashwini Shivarudra, Swethasri Kavuri, Balachandar Paulraj. (2024). Leveraging Machine Learning and Data Engineering for Enhanced Decision-Making in Enterprise Solutions. International Journal of Communication Networks and Information Security (IJCNIS), 16(2), 135–150. Retrieved from https://www.ijcnis.org/index.php/ijcnis/article/view/6989

Bhatt, S., Shivarudra, A., Kavuri, S., Mehra, A., & Paulraj, B. (2024). Building scalable and secure data ecosystems for multi-cloud architectures. Letters in High Energy Physics, 2024(212).

Balachandar Paulraj. (2024). Innovative Strategies for Optimizing Operational Efficiency in Tech-Driven Organizations. International Journal of Intelligent Systems and Applications in Engineering, 12(20s), 962 –. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/687

Bhatt, S. (2020). Leveraging AWS tools for high availability and disaster recovery in SAP applications. International Journal of Scientific Research in Science, Engineering and Technology, 7(2), 482-496. https://doi.org/10.32628/IJSRSET2072122

Bhatt, S. (2023). A comprehensive guide to SAP data center migrations: Techniques and case studies. International Journal of Scientific Research in Science, Engineering and Technology, 10(6), 346-358. https://doi.org/10.32628/IJSRSET2310630

Bhatt, S. (2021). Optimizing SAP Migration Strategies to AWS: Best Practices and Lessons Learned. Integrated Journal for Research in Arts and Humanities, 1(1), 74–82. https://doi.org/10.55544/ijrah.1.1.11

Bhatt, S. (2022). Enhancing SAP System Performance on AWS with Advanced HADR Techniques. Stallion Journal for Multidisciplinary Associated Research Studies, 1(4), 24–35. https://doi.org/10.55544/sjmars.1.4.6

Bhatt, S., & Narne, S. (2023). Streamlining OS/DB Migrations for SAP Environments: A Comparative Analysis of Tools and Methods. Stallion Journal for Multidisciplinary Associated Research Studies, 2(4), 14–27. https://doi.org/10.55544/sjmars.2.4.3

Sachin Bhatt , " Innovations in SAP Landscape Optimization Using Cloud-Based Architectures, IInternational Journal of Scientific Research in Computer Science, Engineering and Information Technology(IJSRCSEIT), ISSN : 2456-3307, Volume 6, Issue 2, pp.579-590, March-April-2020.

Sachin Bhatt. (2024). Best Practices for Designing Scalable REST APIs in Cloud Environments. Journal of Sustainable Solutions, 1(4), 48–71. https://doi.org/10.36676/j.sust.sol.v1.i4.26

Kavuri, S., & Narne, S. (2020). Implementing effective SLO monitoring in high-volume data processing systems. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 5(6), 558. https://doi.org/10.32628/CSEIT206479

Kavuri, S., & Narne, S. (2023). Improving performance of data extracts using window-based refresh strategies. International Journal of Scientific Research in Science, Engineering and Technology, 10(6), 359. https://doi.org/10.32628/IJSRSET2310631

Kavuri, S. (2024). Automation in distributed shared memory testing for multi-processor systems. International Journal of Scientific Research in Science, Engineering and Technology, 12(4), 508. https://doi.org/10.32628/IJSRSET12411594

Swethasri Kavuri, "Integrating Kubernetes Autoscaling for Cost Efficiency in Cloud Services", Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol, vol. 10, no. 5, pp. 480–502, Oct. 2024, doi: 10.32628/CSEIT241051038

Swethasri Kavuri. (2024). Leveraging Data Pipelines for Operational Insights in Enterprise Software. International Journal of Intelligent Systems and Applications in Engineering, 12(10s), 661–682. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/6981

Swethasri Kavuri, " Advanced Debugging Techniques for Multi-Processor Communication in 5G Systems, IInternational Journal of Scientific Research in Computer Science, Engineering and Information Technology(IJSRCSEIT), ISSN : 2456-3307, Volume 9, Issue 5, pp.360-384, September-October-2023. Available at doi : https://doi.org/10.32628/CSEIT239071

Swethasri Kavuri. (2022). Optimizing Data Refresh Mechanisms for Large-Scale Data Warehouses. International Journal of Communication Networks and Information Security (IJCNIS), 14(2), 285–305. Retrieved from https://www.ijcnis.org/index.php/ijcnis/article/view/7413

Mehra, A. (2023). Strategies for scaling EdTech startups in emerging markets. International Journal of Communication Networks and Information Security, 15(1), 259–274. https://ijcnis.org

Mehra, A. (2021). The impact of public-private partnerships on global educational platforms. Journal of Informatics Education and Research, 1(3), 9–28. http://jier.org

Ankur Mehra. (2019). Driving Growth in the Creator Economy through Strategic Content Partnerships. International Journal for Research Publication and Seminar, 10(2), 118–135. https://doi.org/10.36676/jrps.v10.i2.1519

Mehra, A. (2023). Leveraging Data-Driven Insights to Enhance Market Share in the Media Industry. Journal for Research in Applied Sciences and Biotechnology, 2(3), 291–304. https://doi.org/10.55544/jrasb.2.3.37

Ankur Mehra. (2022). Effective Team Management Strategies in Global Organizations. Universal Research Reports, 9(4), 409–425. https://doi.org/10.36676/urr.v9.i4.1363

Mehra, A. (2023). Innovation in brand collaborations for digital media platforms. IJFANS International Journal of Food and Nutritional Sciences, 12(6), 231. https://doi.org/10.XXXX/xxxxx

Ankur Mehra. (2022). The Role of Strategic Alliances in the Growth of the Creator Economy. European Economic Letters (EEL), 12(1). Retrieved from https://www.eelet.org.uk/index.php/journal/article/view/1925

Ankur Mehra. (2024). The Digital Content Distribution Trends in Emerging Market. International Journal of Multidisciplinary Innovation and Research Methodology, ISSN: 2960-2068, 3(3), 221–238. Retrieved from https://ijmirm.com/index.php/ijmirm/article/view/130

Saoji, R., Nuguri, S., Shiva, K., Etikani, P., & Bhaskar, V. V. S. R. (2019). Secure federated learning framework for distributed AI model training in cloud environments. International Journal of Open Publication and Exploration (IJOPE), 7(1), 31. Available online at https://ijope.com.

Savita Nuguri, Rahul Saoji, Krishnateja Shiva, Pradeep Etikani, & Vijaya Venkata Sri Rama Bhaskar. (2021). OPTIMIZING AI MODEL DEPLOYMENT IN CLOUD ENVIRONMENTS: CHALLENGES AND SOLUTIONS. International Journal for Research Publication and Seminar, 12(2), 159–168. https://doi.org/10.36676/jrps.v12.i2.1461

Kaur, J., Choppadandi, A., Chenchala, P. K., Nuguri, S., & Saoji, R. (2022). Machine learning-driven IoT systems for precision agriculture: Enhancing decision-making and efficiency. Webology, 19(6), 2158. Retrieved from http://www.webology.org.

Lohith Paripati, Varun Nakra, Pandi Kirupa Gopalakrishna Pandian, Rahul Saoji, Bhanu Devaguptapu. (2023). Exploring the Potential of Learning in Credit Scoring Models for Alternative Lending Platforms. European Economic Letters (EEL), 13(4), 1331–1241. https://doi.org/10.52783/eel.v13i4.1799

Etikani, P., Bhaskar, V. V. S. R., Nuguri, S., Saoji, R., & Shiva, K. (2023). Automating machine learning workflows with cloud-based pipelines. International Journal of Intelligent Systems and Applications in Engineering, 11(1), 375–382. https://doi.org/10.48047/ijisae.2023.11.1.37

Etikani, P., Bhaskar, V. V. S. R., Palavesh, S., Saoji, R., & Shiva, K. (2023). AI-powered algorithmic trading strategies in the stock market. International Journal of Intelligent Systems and Applications in Engineering, 11(1), 264–277. https://doi.org/10.1234/ijsdip.org_2023-Volume-11-Issue-1_Page_264-277.

Saoji, R., Nuguri, S., Shiva, K., Etikani, P., & Bhaskar, V. V. S. R. (2021). Adaptive AI-based deep learning models for dynamic control in software-defined networks. International Journal of Electrical and Electronics Engineering (IJEEE), 10(1), 89–100. ISSN (P): 2278–9944; ISSN (E): 2278–9952

Varun Nakra, Arth Dave, Savitha Nuguri, Pradeep Kumar Chenchala, Akshay Agarwal. (2023). Robo-Advisors in Wealth Management: Exploring the Role of AI and ML in Financial Planning. European Economic Letters (EEL), 13(5), 2028–2039. Retrieved from https://www.eelet.org.uk/index.php/journal/article/view/1514

Pradeep Kumar Chenchala. (2023). Social Media Sentiment Analysis for Enhancing Demand Forecasting Models Using Machine Learning Models. International Journal on Recent and Innovation Trends in Computing and Communication, 11(6), 595–601. Retrieved from https://www.ijritcc.org/index.php/ijritcc/article/view/10762

Varun Nakra. (2023). Enhancing Software Project Management and Task Allocation with AI and Machine Learning. International Journal on Recent and Innovation Trends in Computing and Communication, 11(11), 1171–1178. Retrieved from https://www.ijritcc.org/index.php/ijritcc/article/view/10684

Lindiawati, Indrianawati, Astuti, S. W., Nuguri, S., Saoji, R., Devaguptapu, B., & Prasad, N. (2023). The Information Quality of Corporate Social Responsibility in Leveraging Banks CSR Reputation: A Study of Indonesian Banks. International Journal for Research Publication and Seminar, 14(5), 196–213. https://doi.org/10.36676/jrps.v14.i5.1441

Krishnateja Shiva, Pradeep Etikani, Vijaya Venkata Sri Rama Bhaskar, Savitha Nuguri, Arth Dave. (2024). Explainable Ai for Personalized Learning: Improving Student Outcomes. International Journal of Multidisciplinary Innovation and Research Methodology, ISSN: 2960-2068, 3(2), 198–207. Retrieved from https://ijmirm.com/index.php/ijmirm/article/view/100

Varun Nakra. (2024). AI-Driven Predictive Analytics for Business Forecasting and Decision Making. International Journal on Recent and Innovation Trends in Computing and Communication, 12(2), 270–282. Retrieved from https://ijritcc.org/index.php/ijritcc/article/view/10619

Agarwal, A., Devaguptapu, B., Saoji, R., Naguri, S., & Avacharmal, R. (2024). Implementing artificial intelligence in salon management: Revolutionizing customer relationship management at PK Salon. Journal Name, 45(2), 1700.
Avacharmal, R., Agarwal, A., Devaguptapu, B., Saoji, R., & Naguri, S. (2024). Implementing artificial intelligence in salon management: Revolutionizing customer relationship management at PK Salon. Journal of Propulsion Technology, 45(2), 1700-1712.
Harishbhai Tilala M, Kumar Chenchala P, Choppadandi A, Kaur J, Naguri S, Saoji R, Devaguptapu B. Ethical Considerations in the Use of Artificial Intelligence and Machine Learning in Health Care: A Comprehensive Review. Cureus.16(6):e62443. doi: 10.7759/cureus.62443. PMID: 39011215; PMCID: PMC11249277.Jun 15, 2024.
Reddy, V. V. K., & Reddy, K. K. (2024). Electric cars meet AI: Machine learning revolutionizing the future of transportation. International Journal of Communication Networks and Information Security, 16(2), 157–160. https://ijcnis.org/index.php/ijcnis/article/view/7367
Bizel, G., Parmar, C., Singh, K., Teegala, S., & Voddi, V. K. R. (2021). Cultural health moments: A search analysis during times of heightened awareness to identify potential interception points with digital health consumers. Journal of Economics and Management Sciences, 4(4), 35. https://doi.org/10.30560/jems.v4n4p35
Kulkarni, A. (2024). Digital transformation with SAP Hana. International Journal on Recent and Innovation Trends in Computing and Communication, 12(1), 338–344. Retrieved from //ijritcc.org/index.php/ijritcc/article/view/10849
Kulkarni, Amol. "Generative AI-Driven for Sap Hana Analytics.", International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169, Volume 12, Issue 2, Pages 438-444, 2024
Kulkarni, A. (2024). Generative AI-driven for SAP Hana analytics. International Journal on Recent and Innovation Trends in Computing and Communication, 12(2), 438–444.
Enhancing Customer Experience with AI-Powered Recommendations in SAP HANA. (2024). International Journal of Business Management and Visuals, ISSN: 3006-2705, 7(1), 1-8. https://ijbmv.com/index.php/home/article/view/84
Kulkarni, Amol. "Digital Transformation with SAP Hana.‖, International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169, Volume 12, Issue 1, Pages 338-344, 2024.
Kulkarni, Amol. "Enhancing Customer Experience with AI-Powered Recommendations in SAP HANA." International Journal of Business Management and Visuals, ISSN: 3006-2705 7.1 (2024): 1-8.
Amol Kulkarni. (2024). Natural Language Processing for Text Analytics in SAP HANA. International Journal of Multidisciplinary Innovation and Research Methodology, ISSN: 2960-2068, 3(2), 135–144. Retrieved from https://ijmirm.com/index.php/ijmirm/article/view/93
Amol Kulkarni. (2024). Natural Language Processing for Text Analytics in SAP HANA. International Journal of Multidisciplinary Innovation and Research Methodology, ISSN: 2960-2068, 3(2), 135–144. Retrieved from https://ijmirm.com/index.php/ijmirm/article/view/93