World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Check for updates

Cloud security in practice: A technical guide to confidentiality, integrity, and availability at scale

Vivek Madan *

Director, IT Security Risk and Compliance, Fortinet Inc., California, USA.

World Journal of Advanced Research and Reviews, 2025, 26(02), 2165-2171

Publication history: Received on 14 April 2025; revised on 11 May 2025; accepted on 13 May 2025

Article DOI: https://doi.org/10.30574/wjarr.2025.26.2.1904

Abstract

Cloud computing has revolutionized how businesses deploy and scale IT infrastructure. However, this shift introduces significant security challenges that require well-architected security techniques across the cloud ecosystem. This paper presents comprehensive techniques to ensure confidentiality, integrity, and availability of data and systems in cloud environments. Covered topics include data encryption, secure storage, key management, logging and monitoring, virtual private cloud (VPC) security, container security, DAST and SAST scanning, baseline imaging, configuration management, and change control practices. These are mapped to CSA's Cloud Controls Matrix (CCM) and CAIQ v4.0 domains to demonstrate holistic cloud risk management. Real-world examples, missteps, and best practices are discussed

Keywords: Cloud Security; Data Encryption; CSA; CAIQ; Cloud Controls Matrix; Zero Trust; Compliance

1. Introduction

Cloud computing offers unmatched scalability, flexibility, and cost-efficiency, but it also introduces complex security challenges. As organizations shift critical workloads to the cloud, they must adopt robust and structured security techniques to safeguard data, ensure compliance, and maintain resilience. This paper explores proven strategies aligned with the Cloud Security Alliance's CAIQ framework and highlights technical controls across governance, data, identity, infrastructure, application, and compliance domains.

2. Security Techniques for Cloud Environments

2.1. Governance, Risk Management, and Compliance

GRC is foundational to cloud security governance. Organizations must align cloud operations with business objectives, risk tolerance, and regulatory mandates. Key practices include defining cloud-specific governance structures, embedding risk ownership, and implementing compliance frameworks such as ISO 27001, NIST SP 800-53, and CSA CCM. Workflow automation platforms like RSA Archer or ServiceNow should be used to manage control documentation, policy exceptions, and audit trails.

Security controls should be continuously monitored and mapped to regulatory requirements using a compliance matrix. Dev SecOps integration ensures policy enforcement and compliance validation throughout CI/CD pipelines. Common gaps include relying on spreadsheets for risk assessments, neglecting third-party governance, or treating compliance as a one-time event. Mature organizations operationalize GRC by aligning it with engineering and DevOps cycles, using KRIs and dashboards to track real-time risk.

* Corresponding author: Vivek Madan

2.2. Data Security and Privacy

Data security begins with classification and extends through encryption, storage control, and lifecycle management. Data at rest must be encrypted using AES-256, and in transit with TLS 1.2 or higher. Metadata and snapshots must also be secured. Privacy regulations like GDPR and HIPAA mandate data minimization, access transparency, and deletion rights.

Tools like AWS Macie and Microsoft Purview support discovery and labeling of sensitive data across cloud repositories. Encryption key rotation, access logging, and masking techniques like tokenization or format-preserving encryption should be applied in production and non-production environments alike. Organizations often fail to classify data consistently, store long-term backups insecurely, or ignore shadow IT data stores. A data-centric security strategy ensures resilience against breaches and regulatory violations.

2.3. Identity and Access Management (IAM)

IAM governs who can access what, when, and under what conditions. Implement Role-Based Access Control (RBAC) or Attribute-Based Access Control (ABAC) to enforce least privilege principles. Federated identity via SAML or OIDC supports Single Sign-On (SSO) and centralized policy enforcement. Privileged account access must always require Multifactor Authentication (MFA).

IAM policies should be managed using infrastructure-as-code, version-controlled, and peer-reviewed. Temporary privilege elevation with approval workflows reduces attack surface. Tools like AWS IAM Access Analyzer or Azure AD Conditional Access help detect overprivileged accounts or unusual access patterns. Mistakes include leaving wildcard permissions ("*"), not revoking access after offboarding, and hardcoding credentials. Secret managers like AWS Secrets Manager or Vault mitigate these risks by securely storing credentials and tokens.

2.4. Infrastructure and Virtualization Security

This domain covers protection of virtual machines, storage, and network layers. Use hardened base images with CIS benchmarks. Segment cloud workloads using VPCs, subnetting, security groups, and network ACLs. Isolate production and development traffic with firewalls and gateway controls.

Infrastructure-as-Code (IaC) tools like Terraform or CloudFormation enforce consistency and enable automated validation. Monitor runtime behavior using Cloud Workload Protection Platforms (CWPPs) or Cloud-Native Application Protection Platform (CNAPP) such as FortiCNAPP, Prisma Cloud, Wiz, or Aqua. Tagging assets, automating patching, and performing drift detection are critical to operational integrity. Top risks include publicly exposed S3 buckets, unpatched hypervisors, flat network topologies, and absent egress controls. Secure infrastructure is the backbone of resilient cloud computing.

2.5. Interoperability and Portability

Cloud systems should be designed to avoid lock-in and promote operational agility across providers. Containerization via Docker and orchestration using Kubernetes decouple applications from infrastructure. Infrastructure-as-Code (IaC) and GitOps practices standardize deployments across platforms, improving portability.

APIs must follow open standards and be thoroughly documented. Cloud-neutral solutions like Azure Arc, and HashiCorp Terraform modules facilitate hybrid and multi-cloud interoperability. Avoiding reliance on proprietary services like AWS Lambda Layers or Azure AD B2C ensures flexibility. Maintain consistent architecture documentation and cross-cloud disaster recovery plans to uphold continuity in the face of regulatory shifts or provider outages.

2.6. Application and Interface Security (AIS)

AIS involves securing APIs, web applications, and software supply chains. Embed security from design through deployment via a Secure Software Development Lifecycle (SSDLC). Incorporate threat modeling, code reviews, and Static and Dynamic Application Security Testing (SAST/DAST). Use Software Composition Analysis (SCA) to scan dependencies.

Authentication mechanisms like OAuth 2.0 and granular authorization scopes must be enforced for all APIs. Web Application Firewalls (WAFs) and API gateways help mitigate injection, DoS, and credential abuse attacks. Enforce input validation, avoid debug endpoints in production, and never store secrets in frontend code. With the rise of supply chain attacks, validate container images and SBOMs before pushing to production.

2.7. Security Incident Management, E-Disc and Cloud Forensics

An effective incident response strategy is vital in dynamic cloud environments. Develop a cloud-specific incident response plan (IRP) outlining roles, escalation paths, and playbooks. Integrate cloud-native tools like AWS GuardDuty, FortiCNAPP, CloudTrail, and Azure Sentinel with centralized SIEM/SOAR platforms for threat detection and automated remediation such as FortiSIEM Cloud.

Regularly simulate scenarios via tabletop exercises or chaos engineering tools. Securely archive forensic data such as logs, packet captures, and snapshots for post-incident analysis. Define metrics like MTTD and MTTR to track effectiveness. Common shortcomings include lack of logging coverage, unretained evidence, and delayed response due to lack of clarity or tooling gaps.

2.8. Threat and Vulnerability Management (TVM)

TVM is essential for identifying, prioritizing, and remediating risks across virtual machines, APIs, containers, and SaaS platforms. Run vulnerability scans regularly using tools like Qualys, Nessus, or native services like AWS Inspector. Prioritize patching using exploitability scores, not just CVSS ratings.

Container images should be scanned via Clair, Trivy, or Prisma before deployment. Integrate vulnerability management into CI/CD pipelines to shift left. Maintain a Software Bill of Materials (SBOM) and track third-party libraries using SCA tools. Enforce remediation SLAs based on business criticality. Avoid over-reliance on monthly scans and ensure misconfiguration assessments complement vulnerability reviews for full coverage.

2.9. Human Resources Security

Human element remains a crucial factor in cloud security. Begin with pre-employment background screening, and continue with role-based security training throughout employment. Implement access provisioning workflows tightly coupled with HR systems such as Workday or SuccessFactors to enforce immediate access revocation upon termination.

Conduct periodic access reviews, particularly for privileged users. Employ behavior monitoring via User and Entity Behavior Analytics (UEBA) to detect insider threats. Regular phishing simulations and contextual learning reinforce vigilance. Common issues include over-provisioned accounts at onboarding, delayed offboarding, and insufficient training on cloud-specific threat vectors like cloud phishing, MFA fatigue attacks, and improper data sharing.

2.10. Universal Endpoint Management (UEM)

UEM ensures that all devices accessing cloud systems comply with security baselines. Centralized tools like Microsoft Intune, Jamf, or Kandji enforce consistent policies across mobile, desktop, and virtual endpoints. Policies should mandate full disk encryption, secure boot, auto-patching, and real-time antivirus protections.

Implement posture-aware conditional access controls based on geolocation, device compliance, and login behavior. Segment corporate and personal data on mobile devices using containers or sandboxing techniques. Lack of visibility into unmanaged devices or tolerance of outdated OS versions presents significant security risks. Endpoint Detection and Response (EDR) tools such as FortiEDR, should integrate with SIEM to correlate alerts across infrastructure.

2.11. Datacenter Security

Though cloud abstracts physical infrastructure, data center security remains vital, especially in hybrid or private cloud deployments. Ensure physical access controls such as biometric authentication, surveillance, and visitor logs. Validate that your cloud service provider (CSP) complies with standards like ISO/IEC 27001, SOC 2 Type II, and TIA-942.

Conduct risk assessments for colocation or on-prem data centers including threats like natural disasters, insider access, or power failures. Ensure redundancy via backup power and multipath connectivity. CSP transparency around their supply chain, data replication, and access logging is critical. Zero-trust physical security must complement virtual security.

2.12. Logging and Monitoring

Effective logging and monitoring is critical for detecting anomalies, ensuring compliance, and supporting forensic investigations in the cloud. Enable native cloud logging services like AWS CloudTrail, Azure Monitor, and Google Cloud Audit Logs across all regions and services. Integrate these logs into centralized SIEM platforms such as FortiSIEM, Splunk, Elastic, or Sentinel.

Logs should be immutable, encrypted, and retained per regulatory requirements. Use log analyzers and behavior analytics to detect lateral movement, privilege escalation, or unusual API usage. Implement alerting thresholds for critical actions (e.g., IAM changes, firewall updates). Ensure logs are timestamped accurately and synchronized via NTP. Common gaps include insufficient log coverage, lack of correlation rules, and unmonitored third-party SaaS integrations.

2.13. Business Continuity Management, and Op Resilience

Cloud-based resilience requires architecture that supports high availability, fault tolerance, and rapid recovery. Leverage multi-zone or multi-region architectures and define business-aligned Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).

Automate disaster recovery processes using tools like AWS CloudEndure or Azure Site Recovery. Use IaC to replicate infrastructure configurations across regions. Store backups in isolated accounts or regions to prevent data loss from cascading failures. Perform routine failover drills, chaos testing, and audit trail validation. Overlooked issues include co-located backups with production workloads, lack of cross-region DNS failover, and outdated DR playbooks.

2.14. Audit and Assurance

Audit readiness in the cloud involves continuous control monitoring, centralized evidence collection, and stakeholder accountability. Use compliance automation platforms like Drata, Vanta, or Lacework to map cloud controls to frameworks like ISO 27001, SOC 2, and HIPAA.

All audit logs should be stored immutably, with clear timestamps and source attribution. Implement dashboards showing control status, audit trails, and remediation progress. Perform internal mock audits quarterly to uncover gaps before external engagements. Failures often stem from decentralized evidence, unclear roles, or manual control validation.

2.15. Supply Chain Management, Transparency, and Accountability

Security of cloud supply chains requires visibility into all dependencies, including APIs, libraries, and SaaS tools. Maintain a Software Bill of Materials (SBOM) for all products, updated through automated scans like Syft or CycloneDX.

Third-party vendors should undergo due diligence through questionnaires (e.g., CAIQ-Lite), and contracts must define breach notification and audit rights. Monitor vendor risk continuously using platforms like OneTrust or SecurityScorecard. Transitive risks from upstream providers or open-source maintainers should be factored into overall enterprise risk posture.

2.16. Change Control and Configuration Management

Enforce rigorous configuration management using IaC pipelines, peer reviews, and automatic drift detection tools like AWS Config or Azure Policy. Track all configuration changes with ticket IDs and version control.

Critical changes must pass CAB approval and include rollback plans. Use tagging standards to document ownership and cost centers. Prohibit direct console modifications to production systems unless emergency changes are documented post-facto. Lack of configuration control often results in downtime, compliance violations, and shadow infrastructure.

2.17. Cryptography, Encryption, and Key Management

Encrypt all data using AES-256 for rest and TLS 1.2+ for transit. Keys should be rotated periodically and stored using secure KMS or HSM-backed services. Implement envelope encryption to decouple key material from data storage.

Use role-based policies to restrict access to keys. Log every cryptographic operation for audit purposes. Avoid storing keys in the same cloud region as encrypted data. Comply with NIST SP 800-57 and FIPS 140-3 for enterprise-grade key management practices.

3. Common Cloud Security Mistakes

3.1. Misconfigured Storage Buckets

One of the most common and dangerous cloud security oversights is the misconfiguration of storage buckets, such as AWS S3 or Azure Blob Storage. Often, organizations inadvertently leave these storage buckets publicly accessible, either due to default settings, lack of awareness, or human error during deployment. Such misconfigurations can expose sensitive data, including customer records, proprietary code, or configuration files to the open internet, allowing attackers to access or exfiltrate it without any authentication. Mitigating this requires robust configuration management practices, regular audits, use of least privilege access controls, and automation tools that can scan for and remediate publicly exposed storage resources.

3.2. Overprivileged IAM Roles

Identity and Access Management (IAM) missteps, particularly overprivileged roles, are another critical risk area in cloud environments. Granting users or services broader permissions than they actually need increases the attack surface and can lead to privilege escalation, lateral movement, and data compromise if credentials are stolen or abused. For example, a developer with admin rights in production could unintentionally (or maliciously) modify critical infrastructure. Following the principle of least privilege, enforcing role-based access control (RBAC), and conducting periodic IAM reviews can significantly reduce this risk. Many cloud providers also offer tools like AWS IAM Access Analyzer to identify and flag excessive permissions.

3.3. Lack of Encryption

Failing to encrypt data in the cloud, whether at rest or in transit exposes organizations to unnecessary risks. Encryption acts as a final safeguard, ensuring that even if data is intercepted or accessed by unauthorized users, it remains unreadable without the proper keys. Unfortunately, some teams rely solely on cloud provider defaults or neglect encrypting metadata and backup files, leaving gaps in their protection. Best practices include enabling TLS/SSL for all data in transit, using AES-256 for data at rest, and managing encryption keys securely through cloud-native Key Management Services (KMS). Regulatory frameworks like HIPAA, GDPR, and PCI-DSS also mandate strong encryption protocols to protect sensitive data.

3.4. Poor Key Management

Encryption is only as strong as the key management behind it. Poor key management practices such as hardcoding keys into source code, not rotating them regularly, or storing them in the same location as the encrypted data—can render encryption useless. Threat actors often scan public code repositories like GitHub to find leaked secrets and keys. To mitigate this, organizations should adopt centralized key management solutions, enforce strict access controls, and enable automatic key rotation policies. Leveraging cloud-native tools like AWS KMS or Azure Key Vault ensures integration with broader security policies while reducing the likelihood of key exposure.

3.5. Insecure CI/CD Pipelines

Continuous Integration and Continuous Deployment (CI/CD) pipelines are integral to modern cloud-native application development, but they can also become major security liabilities if not properly secured. Common mistakes include storing secrets in plaintext, inadequate access control, and skipping security testing stages. Attackers can exploit weak points in the pipeline to inject malicious code or compromise infrastructure. To secure CI/CD environments, secrets should be stored in vaults, tools like SAST (Static Application Security Testing) and DAST (Dynamic Application Security Testing) should be integrated into the pipeline, and pipelines should be audited regularly. Additionally, using ephemeral build environments and enforcing strong authentication for CI/CD tools enhances overall security.

3.6. Shadow IT

Shadow IT refers to the use of cloud services, applications, or infrastructure without formal approval or oversight from the organization's IT or security teams. Employees may spin up cloud resources or use third-party SaaS applications to boost productivity, unaware of the security risks. These unmonitored assets can become weak points, lacking proper encryption, monitoring, or compliance with corporate policies leading to data leakage or regulatory violations. Addressing shadow IT involves raising employee awareness, implementing strong cloud access governance (CASB), and using discovery tools to identify and bring rogue applications under formal security control.

3.7. Insufficient Logging and Monitoring

Without adequate logging and monitoring, organizations operate in the dark unable to detect, respond to, or investigate security incidents effectively. In cloud environments, where dynamic workloads and ephemeral infrastructure are common, visibility is critical. Many organizations fail to enable native logging tools like AWS CloudTrail, Azure Monitor, or Google Cloud Audit Logs, or they do not centralize logs for correlation and alerting. Effective cloud security monitoring requires real-time log collection, correlation through SIEM solutions, anomaly detection using behavioral analytics, and robust incident response plans. Logging should cover authentication events, access to critical resources, and changes to cloud infrastructure.

4. Case Studies of Cloud Security Failures

4.1. Case Study 1: Capital One Breach (2019)

A misconfigured Web Application Firewall allowed unauthorized access to S3 buckets affecting over 100 million users. Root causes included poor IAM role design and firewall misconfiguration.

4.2. Case Study 2: Accenture Cloud Leakage (2021)

Accenture exposed confidential data through unsecured S3 buckets, underlining the need for consistent cloud configurations.

4.3. Case Study 3: Toyota Source Code Exposure (2022)

A third-party GitHub repository exposed T-Connect app source code and secrets, reflecting weak software supply chain security.

5. Conclusion

CSA's CAIQ framework provides a comprehensive structure for cloud security. Aligning technical safeguards to these domains ensures measurable maturity, regulatory compliance, and operational resilience for modern enterprises leveraging the cloud.

Compliance with ethical standards

Acknowledgments

The author thanks CSA community for their ongoing contributions to cloud security best practices.

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Cloud Security Alliance, “Cloud Controls Matrix v4.0,” [Online]. Available: https://cloudsecurityalliance.org/research/cloud-controls-matrix

[2] Amazon Web Services, “AWS Security Best Practices,” [White Paper], [Online]. Available: https://docs.aws.amazon.com/whitepapers/latest/security-best-practices/security-best-practices.pdf

[3] National Institute of Standards and Technology, “Security and Privacy Controls for Information Systems and Organizations (SP 800-53 Rev. 5),” Sep. 2020. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

[4] OWASP Foundation, “OWASP Application Security Verification Standard 4.0.3,” Mar. 2021. [Online]. Available: https://owasp.org/www-project-application-security-verification-standard/

[5] C. Kanaracus, “The Capital One Hack: Everything You Need to Know,” CSO Online, 2019. [Online]. Available: https://www.csoonline.com/article/3441229/the-capital-one-hack-everything-you-need-to-know.html

[6] T. Spring, "Accenture Data Leak Spotlights Cloud Misconfiguration Danger," Threatpost, Aug. 2021. [Online]. Available: https://threatpost.com/accenture-data-leak-cloud/168624/

[7] K. Subramanian, "Toyota Customer Data Exposed Due to GitHub Leak," SecurityWeek, Oct. 2022. [Online]. Available: https://www.securityweek.com/toyota-customer-data-exposed-due-to-github-leak/

[8] IBM X-Force, "Cloud Misconfiguration Report 2023," IBM Security Research (Simulated), 2023.

Authors Short Biography

Vivek Madan is an award-winning cybersecurity leader with over 16 years of experience in IT security, governance, risk, and compliance. He currently serves as the Director of IT Security Risk and Compliance at Fortinet Inc., a global cybersecurity leader securing over 660,000 organizations worldwide.

Vivek specializes in designing enterprise-grade security frameworks, automating third-party risk management, and driving compliance with standards such as ISO/IEC 27001, NIST SP 800-53/800-161, SOC 2, HIPAA, and TISAX. He has led the development of AI-driven trust portals, implemented supply chain risk governance aligned with NIST guidelines, and reduced organizational vulnerabilities through cloud-native automation.

Recognized with the 2025 Titan Gold Award for Cybersecurity – Risk Management, Vivek actively contributes to the cybersecurity community through publications, conference talks, and peer reviews. His work focuses on strengthening digital trust, enabling secure innovation, and shaping the future of cloud and AI security.