Trends in Cloud Security and Compliance: Historic Challenges and Current Innovations

Arham Darky

Akintunde Eyisanmi

Alex Marzella

DePaul University

IS 460: Enterprise Cloud Computing

Kumail Razvi

June 11, 2025

Abstract

This paper examines the historical implementations of security and compliance in cloud computing and describes how these past strategies have changed over time. The successes and failures of early standards in security and compliance will be deconstructed to demonstrate how they influenced current security and compliance practices in cloud computing. Our research also covers the legislative history of cloud computing to demonstrate how emerging legal precedent influenced public perception of what safe and compliant cloud computing looks like. After establishing the historical and contemporary context of cloud security, this paper will also examine prospective future developments in the realm of cloud computing in an effort to theorize how security and compliance will change or stay the same in the future. This paper's examinations of security and compliance practices will give consideration to the unique challenges faced by cloud computing security over traditional means of security and compliance.

Early Legislation of Cloud Computing Technology

A common saying among construction workers is that “Every rule is written in blood”, meaning that workplace rules are often created as reactions to incidents that could have been prevented. This saying is also true of many things related to security and compliance in the world of cloud computing. When one thinks of security compliance in regards to cloud computing, the typical things that come to mind might be technology such as data encryption or legislative regulatory requirements such as GDPR. These modern contemporary standards and practices of cloud computing are influenced by years of historical development that showed the necessity for those solutions. When cloud computing technology was first evolving there was, compared to the current era, less of a matured understanding of what the ethical security responsibilities of a cloud service provider were. Compared to the relatively sanitized experience offered today, this time period could be described as the “Wild West” of the internet. The things one thinks of when choosing a safe and secure enterprise cloud solution might not have been as large of a consideration in the past because the culture of cloud computing was still in its infancy. This formative time period for cloud computing is reflected in a general lack of legal legislation, which at the time had yet to establish a clear precedent for cloud compliance standards. There wasn’t yet precedent to answer the question of “Is my data safe with my cloud service provider who may be operating an illegal business?”.

One example of a precedent being set can be seen in the company MEGA, formerly MegaUpload. MegaUpload was established in 2005 and was, in addition to various other services, primarily a cloud based file storage provider. The site was at the time “Estimated to be the 13th most frequently visited website on the internet” (Johnston 2012). Despite being legally registered in Hong Kong, the company's assets and domain names were seized by US authorities

in 2012. In addition to shutting down all services run by MegaUpload, the founders of the company were also arrested and extradited (Johnston, 2012). The reason MegaUpload was targeted by US authorities is because the United States Department of Justice alleged that MegaUpload operated uniquely relative to other cloud storage platforms by encouraging users to host pirated content. As a result of the seizure of MegaUpload, cloud storage services offered by MegaUpload were shut down for “150 million registered users” (Johnston, 2012) and access to content hosted by MegaUpload was lost.

This incident regarding MegaUpload raised several concerns over security and compliance in cloud computing. When choosing a safe solution for a cloud service provider it is important to consider where your data is being stored and which country’s laws apply to your data. In the case of MegaUpload, their service despite being Hong Kong based was alleged to have violated laws within the United States and was therefore subjected to international law. Because MegaUpload users trusted a company which was not legally compliant, these users lost access to data which they believed to be secure. Despite previous warnings present in MegaUpload’s terms of service that users should “Keep copies of any files they uploaded", this loss of data was nonetheless seen as a violation of MegaUpload’s responsibility as a cloud storage platform. In the current era of cloud computing there is a greater understanding of the extent that the law applies to cloud service platforms. At the time of the MegaUpload case it was previously hypothesized that a new law such as the Stop Online Piracy act would need to be codified to properly prosecute platforms like MegaUpload (Greenwald, 2012). The United States ability to shut down a website without a trial was also not yet widely known at this time. However, despite the Stop Online Piracy Act never being signed into law, prosecutors were able to use existing legislation to shut down MegaUpload before any legal verdict was reached. When

MegaUpload was seized consumers were “Shocked when they learned that the power of the U.S. Government to seize and shut down websites based solely on accusations, with no trial -- is a power the U.S. Government already possesses” (Greenwald, 2012). This legal action set a clear precedent moving forward to cloud service providers for the legal standards with which they should operate their business. It also informed consumers on the importance of choosing platforms that provide solutions to issues related to business continuity and disaster recovery to ensure the security of their data in the event of a site shutdown.

The Evolution of Cloud Computing and Compliance Challenges

Building on the lessons learned from early incidents like MegaUpload, the cloud computing industry began to mature and develop more sophisticated approaches to security and compliance. The "Wild West" era of cloud services gradually gave way to a more structured environment where formal standards and frameworks became essential for business operations.

Cloud computing evolved through three distinct service models that cater to different organizational needs and risk tolerance levels. Infrastructure as a Service (IaaS) provides the fundamental building blocks, virtual machines, storage, and networking, giving organizations complete control over their technology stack. Platform as a Service (PaaS) offers development platforms and tools, enabling developers to focus on creating applications rather than managing underlying infrastructure. Software as a Service (SaaS) delivers complete applications through web browsers, eliminating the need for local installation and maintenance.

As businesses increasingly moved their most sensitive data and critical operations to the cloud, the need for robust governance frameworks became apparent. The early lessons about legal jurisdiction, business continuity, and data sovereignty highlighted the inadequacy of traditional security approaches for cloud environments.

Recognizing these challenges, industry leaders developed foundational standards that would shape modern cloud security. ISO/IEC 27001 emerged as one of the most comprehensive frameworks, providing organizations with a systematic approach to managing sensitive information through Information Security Management Systems (ISMS). This standard transformed security from reactive firefighting to proactive risk management through its Plan-Do-Check-Act cycle, ensuring that security measures evolve with changing threats and business requirements.

The Service Organization Control 2 (SOC 2) standard, developed by the American Institute of Certified Public Accountants (AICPA), addressed specific concerns about outsourcing critical functions to third-party providers. SOC 2 focuses on five fundamental trust service principles: security, availability, processing integrity, confidentiality, and privacy (A-LIGN, 2024). Its flexibility allows organizations to tailor their approach based on specific services and customer needs, a cloud storage company might prioritize confidentiality and security, while a software platform might emphasize availability and processing integrity.

The Cloud Security Alliance (CSA) STAR certification added another layer of cloud-specific assurance, building upon existing frameworks to address the unique challenges of cloud computing environments (Cloud Security Alliance, 2023). Unlike traditional security frameworks that were adapted for cloud use, CSA STAR was designed specifically for cloud services, addressing risks and scenarios that general-purpose standards might not fully consider.

Critical Gaps in Modern Compliance Frameworks

While these foundational standards established important baselines for cloud security, the rapid evolution of technology and business practices has revealed significant limitations in

current approaches. The reality facing organizations today is far more complex than what early compliance frameworks anticipated.

The first major challenge is managing multiple compliance requirements simultaneously. Healthcare technology companies, for example, must juggle HIPAA for patient data protection, SOC 2 for cloud services, ISO/IEC 27001 for overall security management, and numerous other regional and industry-specific requirements. Each standard has its own audit cycles, documentation requirements, and control frameworks, often creating conflicts or redundancies that waste resources without improving security.

Multi-cloud strategies present another significant challenge. Most organizations today use multiple cloud providers, Amazon Web Services for some services, Microsoft Azure for others, and Google Cloud for specific applications. While this approach avoids vendor lock-in and allows companies to choose optimal tools for each task, it creates consistency challenges for security policies and compliance reporting across different platforms (Al-Doghman et al., 2023).

Emerging technologies like artificial intelligence, blockchain, and edge computing introduce entirely new categories of risks that existing frameworks weren't designed to address. AI systems raise questions about algorithmic bias and data privacy in machine learning models. Blockchain technologies challenge traditional notions of data control and modification. Edge computing distributes data processing across countless devices that may be difficult to monitor and protect (da Silva et al., 2018).

Perhaps most significantly, current compliance research tends to adopt generalist approaches that ignore industry-specific challenges. Healthcare organizations must navigate patient privacy regulations and medical device security requirements. Financial services face real-time fraud detection and anti-money laundering compliance demands. Manufacturing

companies entering Industry 4.0 must protect both traditional IT systems and operational technology that controls physical processes (Al-Doghman et al., 2023).

The gap between universal standards and sector-specific needs forces organizations to adapt general frameworks without sufficient guidance on maintaining security effectiveness while meeting industry-specific requirements. What's needed is a fundamental shift toward integrated approaches that recognize the complexity of modern technology environments and provide adaptive frameworks that work across diverse cloud platforms while addressing unique industry challenges and emerging technologies.

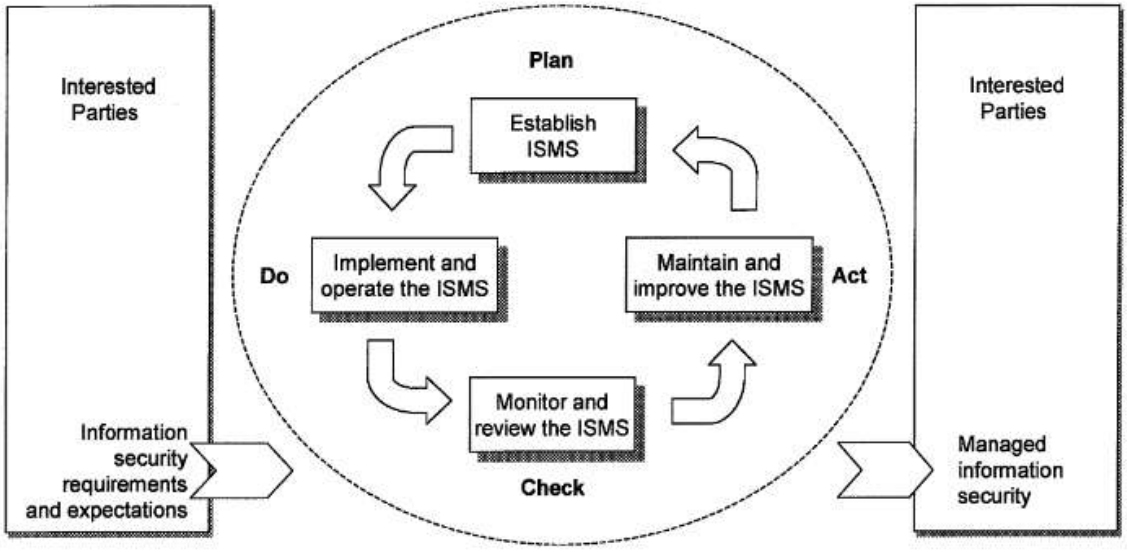
Integrating Existing Knowledge for Early Success

Security and compliance standards for traditional means of computing had been battle-tested and developed for years before cloud computing was a commonplace mainstream technology. As cloud computing matured, it had the benefit of this early security and compliance foundation that it could build itself on top of. Many of these foundational security and compliance standards integrated by cloud computing technologies are still adhered today.
One example of an early security standard still in use today is ISO/IEC 27001. ISO is a security standard that was first published in 2005 by the International Organization for Standardization and International Electrotechnical Commission. The intention behind ISO was to create clear and uniform guidelines of best IT security practices that businesses could implement at all levels in the corporate hierarchy. The process approach for the ISO/IEC 27001 standards was to encourage security specialists to emphasize the importance of “Understanding an organization's information security requirements and the need to establish policy and objectives for information security" (ISO, 2005). In an effort to accomplish this the ISO implements what they call a “Plan-Do-Act” model which is used as a thesis on how all information security processes are

formulated. The “Plan-Do-Act” model breaks security compliance down into four main stages. The four main stages of the ISO model are Plan (Establishing the ISMS), Do (Implement and operate the ISMS), Check (Monitor and review ISMS), and Act (Maintain and improve the ISMS). These four steps cascade down to the intention behind every other security standard defined in the ISO/IEC standards.

Figure 1

ISO/IEC 27001 Plan-Do-Act Model



Note. Figure depicting Plan-Do-Act model published in first version of the ISO/IEC standards, 2005

In addition to formalizing a set of best security practices, corporations can also become officially certified as a way for consumers to recognize that the business adheres to the ISO/IEC best security practices. Certification is conducted by various different approved regulatory bodies. ISO certification is conducted in two stages to verify that the applicant adheres to the

standards outlined in the ISO/IEC publication, and follow up audits and reviews are conducted to maintain the certification (ISO, 2005). A notable early adopter of ISO/IEC standards is Amazon Web Service. In 2010 Amazon Web Services announced in a blog post that they officially completed ISO/IEC certification. Amazon mentioned that “This is a comprehensive international standard and one that should be of special interest to customers from an information security perspective.” (Barr, 2010) and remarked how this certification should “Give users a lot of confidence in the strength and maturity of Amazon’s operating practices and procedures over information security.” (Barr, 2010). After first becoming ISO certified in 2010, Amazon continued to maintain their ISO certification to the present day. Maintaining this certification required Amazon to be compliant with all newly published versions of the ISO/IEC 27001, which had revised versions published in 2013 and later 2022. Amazon’s enduring commitment to maintaining ISO/IEC 27001 certification from 2010 to now shows the success of ISO/IEC 27001 as a security standard. The persistence of the ISO/IEC 27001 security standards demonstrates their utility because if these standards weren’t effective corporations would have stopped internally supporting them long ago. Security and compliance standards which were developed years before cloud computing was a mainstream technology gave cloud computing a head start in the field of security and compliance. Because cloud computing had access from inception to practices that earlier forms of computing lacked, cloud computing providers were able to avoid the pitfalls that afflicted others due to the relative immaturity of the field .

Technical and Process Controls in Modern Cloud Security

Today's cloud security landscape looks dramatically different from the chaotic early days when companies like MegaUpload operated with minimal oversight. What we see now is a

mature ecosystem built on hard-learned lessons, where organizations have developed sophisticated strategies that blend cutting-edge technology with proven management practices.

The technical foundation of modern cloud security starts with encryption, which has essentially become non-negotiable. Organizations encrypt data both when it's stored and when it's moving between systems, typically using Advanced Encryption Standard (AES) with 256-bit keys. What's particularly exciting is the emergence of homomorphic encryption, which allows companies to perform computations on encrypted data without ever having to decrypt it (Al-Doghman et al., 2023). This represents a significant leap forward from the vulnerable data storage practices that plagued early cloud services like MegaUpload.

Identity and Access Management (IAM) has evolved far beyond the simple username-password combinations that once dominated the internet. Today's IAM systems embrace the zero-trust philosophy, which essentially means "trust no one until proven otherwise." Every user and device must continuously verify their identity and authorization, regardless of whether they accessed the system safely yesterday. This approach directly tackles the access control weaknesses that made early cloud services vulnerable to both internal threats and external attacks.

Network security has adapted to the reality that cloud computing means data and applications are distributed across multiple locations and platforms. Technologies like micro-segmentation create individual security bubbles around different applications and data sets, so even if attackers breach one area, they can't easily move to others. Virtual private clouds (VPCs) provide additional isolation, ensuring that even in shared cloud environments, each organization's data remains separate and protected.

On the process side, organizations have learned that technology alone isn't enough. Regular security audits have become standard practice, following the systematic Plan-Do-Check-Act approach established by ISO/IEC 27001 (ISO, 2005). Rather than waiting for problems to surface, companies now actively hunt for vulnerabilities before they become serious threats. Continuous monitoring has replaced the old periodic check-ups, with security teams analyzing real-time data streams from user activities, system events, and network traffic. This proactive stance contrasts sharply with the reactive approach of early cloud computing, where security issues were often discovered only after substantial damage had already occurred. The MegaUpload incident, where 150 million users lost access to their data overnight, serves as a powerful reminder of why robust incident response procedures and business continuity planning are now considered essential rather than optional (Johnston, 2012).

Technical and Process Controls in Modern Cloud Security

The sheer complexity of managing security across multiple cloud platforms has pushed organizations toward automation tools that can handle tasks no human team could manage manually. These aren't just fancy add-ons anymore; they've become essential for any organization serious about cloud security.

Cloud Security Posture Management (CSPM) tools have become the watchdogs of cloud security, constantly scanning configurations to catch problems before they become breaches. What makes CSPM particularly valuable is its ability to work consistently across different cloud platforms, addressing one of the biggest headaches in multi-cloud strategies (Al-Doghman et al., 2023). These tools continuously monitor cloud resources against security standards, automatically flagging when something doesn't match approved configurations. Given how

quickly cloud resources can be created, modified, or destroyed, this real-time oversight has become indispensable.

Security Information and Event Management (SIEM) systems have undergone a dramatic transformation, evolving from simple log collectors into intelligent analysis platforms powered by machine learning. Modern SIEM platforms learn what normal behavior looks like in an organization and can spot anomalies that might indicate security threats. They can connect the dots between events happening across multiple cloud platforms and traditional on-premises systems, giving security teams a comprehensive view of their entire environment. The integration of artificial intelligence has been a game-changer, dramatically reducing the number of false alarms that used to overwhelm security analysts.

Extended Detection and Response (XDR) platforms represent the next step in this evolution, providing integrated threat detection and response capabilities that work across endpoints, networks, and cloud environments. XDR solutions help solve the fragmentation problem that many organizations face when managing security across diverse technology stacks.

What really makes these tools effective isn't their individual capabilities but how they work together as part of integrated security frameworks. Organizations are moving away from rigid, checklist-based compliance toward more flexible, risk-based approaches that can adapt as threats evolve. Automated compliance monitoring tools can now assess compliance against multiple standards simultaneously, whether that's SOC 2, ISO/IEC 27001, or industry-specific requirements, significantly reducing administrative burden while improving accuracy (A-LIGN, 2024). As cloud computing continues evolving with artificial intelligence and edge computing, these security strategies are being tested and refined to address entirely new categories of risk (da

Silva et al., 2018). The foundation built by established standards like ISO/IEC 27001, combined with cloud-specific frameworks like CSA STAR, provides a solid base for tackling these emerging challenges (Cloud Security Alliance, 2023).

Enterprise Case Studies

In order to have a comprehensive understanding of security and compliance,we need to examine them in real-world and large-scale production environments. Thus, we will analyze Netflix, Amazon to shed light on common problems and best practices.

Netflix: Chaos Engineering Approach

With over 260 million subscribers worldwide, Netflix was an early adopter of a complete cloud infrastructure. For a company of this scale, continuous regulatory compliance such as PCI-DSS (for payments) and GDPR (for viewers in the EU) are vital to Netflix's survival (Izrailevsky & Tseitlin, 2011). The defining security practice at Netflix is chaos engineering, where they deliberately introduce failures and errors into their live production environment to test if they can handle failures and determine the strength of their security measures. Tools such as Chaos Monkey (which randomly stops running instances) and Security Monkey (which continuously scans for policy violations) run daily in their AWS infrastructure (Basiri et al., 2016).

According to an internal study, Netflix discovered with their chaos engineering approach to test identity management and encryption key changes, they could detect misconfiguration and setup errors 38% faster (Basiri et al., 2016). This outcome demonstrates the significance of checking compliance in advance rather than investigating only after a problem has occurred.

Amazon Web Services: Compliance Management

Despite being a cloud provider, AWS is also a significant user of its own infrastructure. In order to pass its annual compliance checks such as SOC2 and ISO 27001 audits, AWS has an automated system that collects compliance information within its service pipeline. For instance, whenever a new EC2 instance is launched, AWS Config rules automatically verifies if its settings follow the Center for Internet Security (CIS) protocols; if not the instance is blocked from going live in the production network (AWS, 2023). A significant innovation by AWS is Nitro Enclaves, a technology that uses hardware virtualization to create isolated computing environments which allows customers to work confidential tasks with enhanced security (Sabt et al., 2015).

In order to manage compliance, AWS uses Audit Manager, a tool that automatically links the live status of its resources to the documentation of 35 different compliance frameworks such as FedRAMP and GDPR,etc. By automating the process of gathering compliance evidence, AWS enables its customers to achieve certifications faster and reduces the need for manual spreadsheet tracking (Hashizume et al., 2013).

These cases despite being from different industries and having different approaches to security and compliance, they all heavily use automation, and use real-time data to track compliance. This collectively proves that compliance and security can be advantageous to a business success rather than obstacles to deployment.

Best Practices and Future Directions

As cloud computing continues to evolve, organizations must proactively identify future security risks and adopt strong security and compliance measures. The following best practices provide guidance for organizations to navigate the growing challenges of security and compliance adherence.

Zero Trust Security Model: Putting Identity First

Organizations should adopt a zero-trust security approach, where every request whether internal or external must be authorized, authenticated and encrypted (Gilman & Barth, 2017). This can be achieved by enforcing multi-factor authentication for all console and API interactions, using tools such as AWS IAM Roles Anywhere for workload identities and utilizing temporary, just-in-time credentials rather than long-term secrets. Service mesh technologies such as AWS App Mesh provides mutual TLS and detailed policy enforcement for internal networks, which reduces the reliance on security focused at the network's edge.

AI for Automated Security Threat Detection

To improve security systems, machine-learning models are used to analyze network logs, endpoint data, and users' behaviour in order to detect unusual activities that traditional systems do not detect. Services such as Amazon GuardDuty and Microsoft Defender for Cloud utilize machine-learning to spot things like stolen credentials, uncommon API calls and data being taken out of the system.

However, for AI threat detection to be effective, the models must have good training data and automatically respond to machine-learning alerts, for example, quarantining a hacked user account (AWS, 2023).

Building Resilience and Disaster Recovery Planning

In order to achieve cloud resilience, organizations should adopt strong disaster recovery and business continuity plans. This includes multi-region deployments, routinely performing disaster-recovery drills and employing immutable data backups to prevent ransomware and data tampering (AWS, 2023).

It is important for organizations to regularly conduct mock trial scenarios that test their disaster recovery plan by simulating cyber-attacks, data loss incidents and cloud provider failures. In addition, innovations such as Google Cloud's Dual-Run provides solutions for resilience against the risks associated with vendor lock-in by enabling enterprises to run operations across multiple cloud platforms.

Ultimately, adopting these best practices will allow organizations to satisfy current and future compliance and security requirements while gaining competitive advantage through strong, secure and resilient cloud environments.

Conclusion

This research has examined how the security and compliance of cloud computing has evolved over time, providing insights into both historical and current developments. The historical analysis of MegaUpload showed how early regulatory interventions set new standards that transformed the expectations and responsibilities of organizations concerning cloud security and compliance.

The case studies of Netflix and Amazon Web Services (AWS) highlighted practical applications of how security practices are being used. Netflix's innovative use of chaos engineering demonstrated security resilience by intentionally injecting faults into their system, while AWS's strategy of automating compliance in real-time demonstrated how to effectively manage compliance demands.

Moreover, this research identified best practices for organizations to adopt such as zero-trust security, strict authentication and identity management, and artificial intelligence for rapid threat detection. Disaster recovery and business continuity plans such as multi-region setups and secure backups are also essential for continuous operation and compliance.

Lastly, for organizations to protect their data and systems from future risks, they must continuously adapt to emerging standards and proactively manage threats. By adhering to the best practices, organizations will not only be more secure but gain competitive advantage from their strong compliance.

References

Amazon Web Services. (2023). *AWS security services overview* [White paper]. Amazon Web Services, Inc. https://docs.aws.amazon.com/whitepapers/latest/aws-overview/security-services.html

Basiri, A., Casale, G., García López, P., Klein, C., Moser, L., & Tordsson, J. (2016). Chaos engineering. *IEEE Software, 33*(3), 35–41. https://doi.org/10.1109/MS.2016.68

Gilman, E., & Barth, A. (2017). *Zero-trust networks: Building secure systems in untrusted networks*. O'Reilly Media.

Barr, J. (2010, November 16). *AWS receives ISO 27001 certification | Amazon Web Services*. Amazon Web Services. https://aws.amazon.com/blogs/aws/aws-receives-iso-27001-certification/

Greenwald, G. (2012, January 21). Two lessons from the Megaupload seizure. *Salon*. https://www.salon.com/2012/01/21/two_lessons_from_the_megaupload_seizure/

Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013). An analysis of security issues for cloud computing. *Journal of Internet Services and Applications, 4*(1), 5. https://doi.org/10.1186/1869-0238-4-5

ISO. (2005). International Standard. ISO. computer software, Geneva.

Johnston, K. (2012, January 20). FBI seeks extradition of internet "pirate." *The Sydney Morning Herald*. https://www.smh.com.au/technology/fbi-seeks-extradition-of-internet-pirate-20120120-1qacn.html

Sabt, M., Achemlal, M., & Bouabdallah, A. (2015). Trusted execution environment: What it is and what it is not. In *Proceedings of the 2015 IEEE Trustcom/BigDataSE/ISPA* (pp. 57–64). IEEE. https://doi.org/10.1109/Trustcom.2015.357

A-LIGN. (2024). What is SOC 2? Complete guide to audits and compliance. https://www.a-lign.com/articles/what-is-soc-2-complete-guide-audits-and-compliance

Al-Doghman, F., Al-Mashaqbeh, I., & Abuzneid, A. (2023). Compliance and regulatory challenges in cloud computing: A sector-wise analysis. ResearchGate. https://www.researchgate.net/publication/382265359

Cloud Security Alliance. (2023). SOC 2 and ISO certifications vs. CSA STAR. https://cloudsecurityalliance.org/blog/2023/09/18/soc-2-and-iso-certifications-vs-csa-star

da Silva, E. S., Costa, A. P. C. S., & de Souza, J. T. (2018). Research gaps and trends in cloud computing: A systematic mapping study. ResearchGate. https://www.researchgate.net/publication/322590617

A-LIGN. (2024). SOC 2 compliance guide: Understanding the five trust service principles. A-LIGN Security & Compliance Solutions.

Al-Doghman, F., Chaczko, Z., Ajayan, A. R., & Klempous, R. (2023). A review of cloud security challenges and solutions. Journal of Cloud Computing, 12(1), 1-24.

Barr, J. (2010, November 11). AWS achieves ISO 27001 certification. Amazon Web Services Blog. https://aws.amazon.com/blogs/aws/aws-achieves-iso-27001-certification/

Cloud Security Alliance. (2023). Security, trust, assurance, and risk (STAR) certification. Cloud Security Alliance.

da Silva, G. C., Rose, L. M., & Calinescu, R. (2018). A systematic review of cloud lock-in solutions. In 2018 IEEE 5th International Conference on Cloud Computing and Intelligence Systems (pp. 147-152). IEEE.

Greenwald, G. (2012, January 19). The internet and the government's power to shut it down. The Guardian. https://www.theguardian.com/commentisfree/2012/jan/19/internet-government-power-shut-down

International Organization for Standardization. (2005). ISO/IEC 27001:2005 Information technology — Security techniques — Information security management systems — Requirements. ISO.

Johnston, C. (2012, January 20). Megaupload shut down by FBI as owner arrested. Ars Technica. https://arstechnica.com/tech-policy/2012/01/megaupload-shut-down-by-fbi-as-owner-arrested/