Compliance Auditing in the Cloud

- Continuous real-time compliance status
- Slice-specific compliance
- ISO 2700 series
- Virtualization/isolation mechanisms and network products compliance
- Baseline compliance
- HIPAA-compliant slice
- ISO 26262-compliant slice
- FedRAMP-compliant slice

Charting the Future of Innovation
More and more companies are moving their applications and data to the cloud, and many have started offering cloud services to their customers as well. But how can they ensure that their cloud solutions are secure?

Security compliance auditing is an assessment of the extent to which a subject (a cloud services provider or CSP, in this case) conforms to security-related requirements. At a minimum, a CSP must be able to deploy tenants’ applications, store their data securely and ensure compliance with multiple regulations and standards.

Many industry sectors – healthcare and utilities, for example – are highly regulated and have to meet stringent data privacy and protection requirements. To serve these types of companies, cloud providers must be able to prove their alignment with the latest standards and regulations such as the Health Insurance Portability and Accountability Act (HIPAA), the Payment Card Industry Data Security Standard (PCI DSS) and the Federal Risk and Authorization Management Program (FedRAMP). Without the right set of tools in place, cloud characteristics such as elasticity, dynamicity and multi-tenancy make proving compliance with such standards both challenging and costly.

Regulations such as HIPAA and PCI DSS define auditing and proving compliance with industry standards and regulations as shared responsibilities. To address users’ compliance-related needs, cloud providers must demonstrate evidence of compliance with regulatory requirements across industry segments.

Figure 1 illustrates the cloud security compliance landscape. Providers that can offer tenants credible, trustworthy compliance information on relevant requirements at any time, in a cost-efficient manner, stand to gain a significant competitive advantage.

Auditing security compliance typically involves the manual inspection of regularly generated reports, reviewing system logs, and conducting penetration tests.
audit reports and logs, and possibly dynamic tests conducted at runtime. However, applying such techniques in the cloud would be time consuming and costly owing to cloud characteristics.

For instance, to prove network isolation, all layers such as cloud management as well as the virtual network, overlay network, real network (non-virtual), and physical network have to be verified. The results of each verification process on the layers are correlated to avoid any gaps. Current practices such as design document verification, network traffic injection and penetration testing don’t work in an environment where tenants share resources, and network parameters change quickly and dynamically.

Operators and cloud providers therefore need a new set of automated tools and techniques that can manage security and compliance, protect consumers’ assets, and enable security-related services – in a continuous and cost-effective fashion. In telecom context, the European Telecommunications Standards Institute (ETSI) has proposed an architecture for continuous security monitoring and lifecycle management for network function virtualization to satisfy security requirements at both the operator and consumer level [1].

The ways in which evidence of compliance is provided in the cloud marketplace vary widely at present. It is problematic for a tenant to evaluate cloud providers’ capabilities and to understand which party is responsible for what from a compliance perspective. Trust between tenants and their providers is often based on legal texts and disclaimers that can be difficult to comprehend. There is clearly room for improvement, as evidenced by the European Union’s call for closer adherence to privacy regulations by global CSPs.

**Compliance standards in the cloud**

To ensure compliance with different security frameworks in the cloud, there are two main types of standards: vertical and horizontal. Horizontal standards are generic standards that are applicable to many industries. Vertical standards are applicable to specific industries. Several standards (horizontal and vertical) have been supplemented

---

**Terms and abbreviations**

- **AICPA** – American Institute of Certified Public Accountants
- **AWS** – Amazon Web Services
- **CCM** – Cloud Controls Matrix
- **CCS** – Control Compliance Suite/Services
- **CSA** – Cloud Security Alliance
- **ETSI** – European Telecommunications Standards Institute
- **FedRAMP** – Federal Risk and Authorization Management Program
- **GRC** – governance, risk management and compliance
- **HIPAA** – Health Insurance Portability and Accountability Act of 1996
- **IaaS** – infrastructure as a service
- **ISO 27001** – specification for an Information Security Management System (ISMS)
- **ISO 27018** – code of practice for protection of personal data
- **NIST** – Network Information Security & Technology
- **NIST SP** – Network Information Security & Technology Special Publication
- **NoSQL** – not only Structured Query Language
- **PaaS** – platform as a service
- **PCI DSS** – Payment Card Industry Data Security Standard
- **SaaS** – software as a service
- **SIEM** – security information and event management
- **SOC 1, 2, 3** – Service Organization Controls type 1, 2, 3 report
- **SQL** – Structured Query Language
- **V&V** – verification and validation
- **VM** – virtual machine
- **CPRIoEth** – CPRI over Ethernet
to guide certification handling in the cloud computing domain.

Besides the establishment of horizontal and vertical standards by standardization bodies, other organizations and informal groups such as the Cloud Security Alliance (CSA) address standardization issues related to cloud computing and work on promoting best practices and reaching a consensus on ways to provide security assurance in the cloud. For example, the CSA’s cloud security governance, risk management and compliance (GRC) stack [2] supports cloud tenants and cloud providers to increase their mutual trust and demonstrate compliance capabilities.

**Current auditing tools**
The auditee – in this case the cloud provider or consumer – is required to produce compliance reports to prove that their security measures are protecting their assets from being compromised. Additionally, regulatory bodies require the auditee to retain log data for long periods of time, making it possible for auditors to analyze audit trails and logs. To this end, the auditee can use different types of tools to manage and maintain a holistic view of the security of its environment.

Several open source and commercial tools, including security information and event management (SIEM) and GRC tools, that enable generation of compliance reports on a periodic and/or on-demand basis, exist in the market. Figure 2 illustrates the main input, output and functionality of an SIEM tool.

In addition to SIEM functionality, GRC [3] tools deliver the core assessment technologies to enable security and compliance programs and support IT operations in the data center.
They enable information security managers to address IT governance, risk and compliance issues by helping them to prevent and respond to non-compliance of security controls while taking into account tolerated risk.

**Enterprise class tools**

With the advent of the cloud, the makers of several enterprise class tools have proposed integration of their solutions into the cloud environment. While many enterprise-class SIEM engines rely exclusively on correlation to analyze audit data, a new generation of cloud-specific tools includes log search engines and advanced analytics to process the large amount of data and gain security intelligence and knowledge. Nonetheless, most of these tools have been designed to work in enterprise environments whose characteristics differ significantly from the cloud.

**Open source projects**

Due to the increasing importance of auditing and monitoring in the cloud, open source projects have been created as part of existing cloud management software. For example, OpenStack Congress aims to offer governance and compliance assurance by providing policy as a service. It targets IaaS and does not cover any PaaS or SaaS deployment. Specifically, it allows declare, audit and enforce policies in heterogeneous cloud environments.

A drawback of OpenStack Congress is that it does not allow a full verification through all layers – verification is limited to the information provided by OpenStack services. An elastic stack based on open source tools is another option. This alternative consists of a data search stack that encompasses several components, namely: Kibana for data visualization; Elasticsearch for searching, analyzing and storing data; as well as Beats and

---

**Figure 2**

Summary of main SIEM input, output and functionality

---

**Standards and regulations**

CCM
ISO 27002/17
HIPAA
NIST
PCI-DSS

**Contextual data**

Threat intelligence
Identity and access management
Asset inventories
Vulnerabilities databases
Business workflow
Risk management

**Raw audit data**

Logs
Events
Flows

**INPUT**

**AUDITING**

**OUTPUT**

**SIEM**

Log and context data collection
Normalization and categorization
Data retention
Rule/correlation engine
Compliance V&V
Visualization and reporting
Notification/alerting

**Data collection & processing**

**Compliance assessment**

**Use cases**

Compliance reporting
Real-time security monitoring
Incident investigation
Historical analysis
Policy review and process improvement

**Figure 2**

Summary of main SIEM input, output and functionality
Logstash for data collection from various sources in different formats.

When comparing commercial tools with these open source projects, a notable benefit of commercial tools is that they have most of the audit process ready to use out-of-the-box.

Cloud-based services offered by cloud providers

Some cloud IaaS providers are currently proposing partial solutions to help consumers verify that their applications are handled in conformance with their security policies. For instance, AWS offers dynamic customizable compliance checking of cloud resources using AWS configuration rules. Other tools have also been proposed, such as Inspector by Amazon, which is an automated security assessment service that finds security or compliance issues on applications launched within AWS instances.

Cloud-specific tools

Cloud-specific tools such as Catbird Secure offer policy compliance automation and monitoring solutions for private and hybrid cloud environments and focus on software-defined security. Another example is RiskVision Continuous Compliance Service (CCS), an on-demand service allowing providers to gain visibility into their cloud risk exposure and to manage compliance.

Challenges and implementation gaps

A number of challenges make techniques for auditing conventional IT systems unsuitable for use in a cloud environment without significant adaptation. While several common concerns arise when auditing in both domains, a cloud security audit must address unique problems.

Compliance responsibility

Cloud applications run in different deployment models (IaaS, PaaS, or SaaS) and on different types of cloud (public, private or hybrid). This rich set of combinations leads to a complex control dependency and complicates the responsibilities of different actors. The reliance on the CSP varies according to the deployment and type of cloud.

For example, in a public IaaS, the hardware and virtual layers are managed by the CSP while the application layer is managed by the tenant. Therefore, there is limited reliance on CSP in IaaS, but most reliance on CSP in SaaS. Thus, it is necessary to define a clear model for the shared responsibility of compliance management.

The massive size of the cloud

The large scale of cloud environments – with the increased number of virtual resources and sources of data – has a direct impact on the size of audit trails and logs. Given the huge amount of data held in them, efficient collection, manipulation and storage techniques are required. Conventional tools were not conceived for large-scale data – they use off-the-shelf fixed-schema SQL databases with a centralized system for the analysis of audit trails. The scale and performance limitations of this type of architecture represent a single point of failure. Auditing and compliance verification tools for the cloud must be designed from scratch to process a very large quantity of data while meeting performance requirements.

The rapidity and dynamicity of cloud services

The speed of events and operations in the cloud constantly changes logs and configuration data. For example, each time a new virtual machine (VM) is created or migrated, new data is generated that may change the compliance status. This is becoming more complex as cloud providers are moving toward more real-time programmable controls by using software-defined networks and NFV in their cloud data centers. One of the major issues in conventional solutions is that they are conceived to execute in a quasi-static environment where auditing is generally performed periodically and remains valid until the next period. They mainly verify a snapshot of the security state at the time of the audit. This is not sufficient in the cloud, where audit and compliance assurance is required each time the infrastructure changes to assess whether these changes give rise to security gaps or infrastructure misuse.
If an audit and compliance assessment tool cannot cope with the high rate of configuration changes for large data centers, it is not fit for the task. Changes in the cloud require the ability to automatically collect data to present near-real-time visibility about compliance to tenants and auditors alike.

Multi-tenancy in the cloud
Audit trails and logs are currently being generated for different actors (tenants, users, cloud provider and so on) on shared physical and virtual layers without a clear separation between them. This approach cannot address all the needs rising from complex use cases such as when a cloud broker leases virtual resources to a third party. Furthermore, it may not be possible for auditing tools to monitor the full stack from the hardware layer up to the application layer because of potential compromise of the privacy of other tenants and of the confidentiality of sensitive information concerning the cloud infrastructure. This is why some providers (particularly SaaS ones) restrict vulnerability assessments and penetration testing, while others limit availability of audit logs and activity monitoring. Most conventional tools are simply not designed to support multi-tenant environments. Therefore, different accessibility schemas must be put in place to give the right access to the common logs for different tenants based on the roles and privileges of different actors.

Privacy protection and GRC support
A CSP with a multi-tenant environment is forbidden to reveal details or metadata that would compromise tenants’ privacy or security. Nor is it allowed to disclose any sensitive information to a third party and it must protect against attackers accessing any significant information about the tenants. At the same time, mandated auditors need to access useful and complete information to provide evidence of compliance. In addition, tenants need to receive the right assurances from the CSP and the auditors or perform their own compliance audit of their setting in the cloud, independently of the cloud provider. Therefore, auditing tools should allow for securely outsourcing anonymized logs and audit trails to different interested entities without sacrificing privacy and sensitive information for an evidence-based audit and GRC approach in the cloud.

Trust and integrity of audit data
Audited data is often considered to be inherently reliable. But before being presented to the auditor, the original pieces of data will have been passed from the source to the presentation layer via communication interfaces and processed by dynamic software instances. The degree of trust in such a chain is hard to evaluate. Many cloud solutions enable an assessment of the trustworthiness of the hardware platform and bootstrapping of the virtual machines, and safeguard the integrity of log files at rest and in transit. However, audit data would not necessarily be approved as evidence in court if the data integrity had been compromised during any step of the process. The integrity of the audit data source, of the data collector and of the log server should be attestable, assuming that appropriate controls are in place for securing the audit data itself and that there is proof of mutual authentication between the processing elements with an accepted security strength.
Achieving truly effective auditing in the cloud

In light of the challenges to creating an effective auditing approach in the cloud using the conventional techniques, it is useful to highlight some of the key characteristics of an effective cloud auditing solution.

Continuous monitoring and high automation for compliance

As the cloud is inherently elastic and dynamic, an effective auditing framework must be augmented by continuous compliance and monitoring features [1]. This is not only necessary to maintain compliance but also to improve overall security. It must also provide a high level of automation to cope with quick and transparent changes in collaboration with the cloud management system. Automation is necessary to collect the right information in near real-time and from the right source. Additionally, to enforce an evidence-based compliance verification in a multi-tenant environment, the CSP’s should expose information gathered from trusted monitored sources in an open standard format while protecting tenants’ privacy by using, for example, anonymization of traces and audit trails for the auditors’ and tenants’ benefit. Therefore, moving towards a continuous automated compliance verification model that provides complete compliance visibility to the tenants is key to reducing and limiting exposure to risks related to compliance and security breaches.

Building auditing capabilities into the cloud infrastructure

It is much more effective and cost-efficient to build intrinsic auditing capabilities into the cloud infrastructure than to attempt to retrofit existing auditing approaches to the cloud environment. To provide various actors with the necessary audit trails without violating user and tenant privacy, the cloud infrastructure could implement labeling mechanisms to trace the logs to their target tenants. Tackling logs and audit trails in the cloud as opposed to a classical centralized log server in an enterprise environment requires a distributed log collection and retrieval mechanism. Building accountability and traceability into the cloud infrastructure is the best way to provide an efficient and effective auditing solution.

Using analytics for compliance verification

While conventional audit systems specialize in detecting known threats, providing support for identifying unknown threats is a new trend in auditing that is highly relevant to the cloud. Owing to the great quantity of audit data and logs in large data centers, the use of big data analytics based on data mining, machine learning and behavioral monitoring techniques for cloud auditing tools and SIEMs is increasing. In the same vein, storing raw audit data requires new database architecture and technology (such as NoSQL) or support of flat file databases. For the sake of scalability, new deployment options are being considered to move from centralized audit analyses to distributed ones. Analytics must be further explored and improved to tackle cloud-specific characteristics and their actual potential must be investigated in real-world deployments.

Modular compliance approach

Many cloud applications are deployed for highly regulated industries with different compliance needs such as PCI/DSS, HIPAA, ISO 27017 and ISO 27001. These compliance frameworks correspond to different security requirements, which in turn necessitate a large set of controls that must be put in place in the cloud infrastructure.
There are, however, many commonalities between the requirements of all these frameworks in terms of data storage obfuscation, data storage integrity and access control, for example. Therefore, a baseline security requirement needs to be defined to cover the major common requirements. This baseline should be augmented dynamically in the cloud to provide support for different compliance frameworks. Consequently, an efficient auditing approach should be modular, supporting the common denominator requirements as a baseline security requirement and adding different control modules to support specific security frameworks. The CSA CCM compliance matrix is a good starting point for aggregating the major common security requirements.

**Application to 5G**

5G networks are expected to play a central role in providing a common backbone for information exchange between various applications that belong to different industry segments, which would mean that the security of these applications would depend on the security of the 5G network [4]. This would result in the need to certify 5G networks against all (or at least parts of) the security standards that are related to the served verticals. Implementing isolated network slices for different types of applications would ease compliance assurance by confining certification efforts to each single slice against the appropriate subset of the security requirements. **Figure 3** shows one way this could be accomplished.

**Conclusion**

The cloud has become a standard in modern computing, and companies in many industry verticals are moving their data to it. Therefore, security assurance, auditing and compliance in the cloud is gaining momentum. Unfortunately, several challenges related to the particular specificities of cloud are limiting the potential benefit of applying current auditing practices and tools.

---

**Figure 3**

Application to 5G security compliance auditing
Moving toward a continuous automated compliance verification model that provides tenants with complete compliance visibility is key to reducing and limiting exposure to security-related risk. An effective and efficient cloud auditing solution must:

- support large-scale cloud environments
- offer a high level of automation
- allow for near-real-time compliance visibility without compromising stakeholders’ privacy and the confidentiality of sensitive data
- fully support multi-tenancy
- provide modular compliance verification to address several standards.

In light of these requirements, new auditing solutions adapted to the cloud environment must be proposed.

**Further reading**


**References:**


Yosr Jarraya  
◆ joined Ericsson in 2016 as a security researcher after a two-year postdoctoral fellowship with the company. She holds a Ph.D. in electrical and computer engineering from Concordia University in Montreal, Canada. In the past six years she has produced more than 25 research papers on topics including SDN, security, software and the cloud.

Ari Pietikäinen  
◆ is a senior security specialist. He joined Ericsson in 1990 and has worked in the security domain since 2003, most recently with cloud, NFV and IoT security topics. He holds an M.Sc. from Helsinki University of Technology in Espoo, Finland.

Jukka Ylitalo  
◆ is a chief security architect who joined Ericsson in 2001. He has contributed to security standardization work and published several scientific articles during his career. He holds an M.Sc. and a D.Sc. Tech. from Helsinki University of Technology in Espoo, Finland.

Mads Becker Jørgensen  
◆ is a strategic product manager whose work focuses on the cloud and data platforms area. He has more than 15 years of experience as an information security professional in both the public and private sectors. His current research interests are within secure identity and holistic security.

Chiadi Obi  
◆ joined Ericsson in 2015 as a principal consultant in global IT and cloud services. He has over 19 years of experience centering around information security, the cloud as well as adjacent platforms such as the IoT, with a keen focus on strategy, compliance, governance and privacy aspects. He holds an M.Sc. in information security from Colorado University in the USA as well as industry-driven designations such as the CISSP, CISM and CRISC. He has also authored white papers on cloud and IoT security.

Satyakam Nanda  
◆ joined Ericsson in 2010 where he worked as a principal consultant in global IT & cloud services until 2017. Over the past two decades, he has served in various leadership roles in consulting, product design, operations and product management driving security strategy and execution for critical infrastructure protection. He holds dual masters’ degrees in software engineering and business management from the University of Texas in Dallas, USA.

Giovanni Zanetti  
◆ joined Ericsson in 2010 as a senior security consultant in the IT & Cloud regional unit. His work focuses on security compliance design. He holds an M.Sc. in industrial engineering from Milan University, Italy, as well as CISSP and ISO 27001-22301 Lead Auditor certifications.

Makan Pourzandi  
◆ is a researcher who joined Ericsson in 1999. He holds a Ph.D. in computer science from the University of Lyon, France. An inventor with 28 US patents granted or pending, he has also produced more than 50 research papers.