sonraí SECURITY

INDUSTRY REPORT

# Financial Services Guide To Identity and Data Governance Across the Public Cloud

From global banks to payment platforms and emerging FinTech startups, innovate faster while staying continuously secure and compliant in the cloud.

Financial service organizations such as FinTech startups, online payment platforms to global banks have to modernize and transform to meet the increasing demand for improved delivery of their financial services. However, this digital transformation is new territory and comes with significant risks; for example, compliance requirements according to corporate standards, local government regulations, and industry related standards. With technological advancements at an all-time high, developers are shifting their focus to cloud service innovation.

Additionally, by shifting it then becomes essential to protect sensitive data such as identifiable customer information. These challenges make security and compliance a necessary element during digital transformation that involves the adoption of the cloud.

Sonrai Dig seeks to help financial companies protect their public cloud environments from actions such as breached identity and faulty governance, policy violations, and misconfiguration. As a financial institution, it is critical that your customers are well informed and comfortable with this shift, that there is tangible evidence of compliance to auditors and assessors, and that there are well-defined governance standards. With **Sonrai Dig**, you will be able to achieve continuous compliance and security, allowing your developers to focus on more groundbreaking innovations to meet your company's goals.

Adopting cloud technology for your organization while mitigating the potential risks can be an overwhelming task. For example, you need to understand how compliance in the financial service industry translates to the public cloud to shift left effectively. You also need to learn how to map directives back to an extensive set of cloud services while using software defined configurations without violating policy. Also, you need to ensure continuous and consistent compliance in the public cloud's transient and dynamic world. Though daunting, complete integration of your financial institution into the public cloud is possible. The first step is to understand and embrace the workings of cloud-native frameworks.

"100% of the fintech enterprises had some security or privacy issues associated with web apps, APIs, and subdomains."

## What are Cloud-Native Frameworks?

The foundation of cloud governance, when it comes to financial service organizations, involves three frameworks, namely, Centre for Internet Security (CIS) Benchmarks, Cloud Security Alliance Cloud Controls Matrix (CSA CCM), and SOC 2. Cloud-native frameworks are about how applications are created and not where they are created. The frameworks empower organizations to build and run applica-tions in private, hybrid, and public clouds.

## Center for Internet Security (CIS) Benchmarks

**CIS benchmarks** work to help you secure platforms, such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP). They are endorsed by IT governing bodies and security systems, and they work to safeguard your organization from cyber threats and potential security breaches. While operating platforms, you need to create a secure baseline configuration. Each framework offers different foundations and interaction options within the cloud, with cloud providers, and third party data stores. For example, CIS benchmarks published a new benchmark in 2018, specifically for security workloads on GCP. It contains recommendations regarding cloud security across identity and management, networking, monitoring storage, containers, and compute. It is important to note that the CIS benchmarks are specific to a set of cloud services and do not offer guidance for the ever-growing vast collection of the services provided by various cloud services.

## Cloud Security Alliance Cloud Controls Matrix

Cloud Security Alliance Cloud Controls Matrix (**CSA CCM**) provides cloud-native frameworks with specific and simplified details of the security principles and concepts. Its recommendations apply to other compliance standards and help various organizations meet their requirements under the stipulated regulations. CSA CCM provides detailed frameworks to the Cloud Security Alliance guidance in sixteen domains.

For example, Human resources, application and interface, data security and information lifecycle management, mobile security, threat, and vulnerability management, implementation and interface security, and data center security, just to mention a few. This framework relays information surrounding security in the cloud industry, such as security control requirements, identification, and reduction of vulnerabilities and security threats in the cloud, standardization of operations and security risk management, the normalization of security expectations, various cloud terminologies and taxonomy, and necessary security measures implementation.

CSA CCM is one of the more robust frameworks. For example, if you follow its guidance and achieve compliance in one sector, it has the power to offer validation to prove you are compliant with numerous related frameworks. It is a favorite among many users because it is well-documented, easily accessible, and can be held as a standard of measure for financial service institutions, such as banks for efficient accountability.

## Service Organization Control (SOC2) Report

The **SOC 2** report was developed by the American Institute CPAs, for proper mapping of cloud controls. It focuses on your organization's non-financial reporting controls and how they interact with processing, security, integrity, privacy, and confidentiality. SOC 2 works to measure five critical controls known as **CIA Triad** plus privacy, which are essentially controls related to IT and data service providers:

### 1 Privacy

To manage and limit the collection and use of customer's personal information which is critical in any financial service organization

### 2 Availability

To gauge the reliability and easy access to systems, services, and information for the clientfor any potential risks. The lockdown system comes with inbuilt alarm systems that send out an alarm if triggered by unexpected or sudden activity

### 3 Security

To ensure the protection of systems and prevent data access from unauthorized users

### 4 Processing integrity

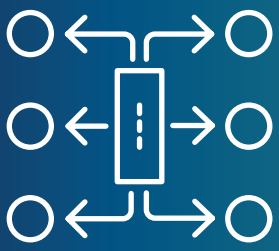
To gauge the accuracy and validity of your organization's data processing systems

### 5 Confidentiality

To ensure the protection of confidential data of both the organization and the client

Having identified the workings of the cloud through a deeper understanding of the various cloud-native frameworks, and how to transform and integrate your organization into the cloud, you need to manage risks and modernize your environment.  Lack of compliance with the security regulations could have your organization facing significant penalties which are time-consuming and costly.

# You can achieve high levels of security and compliance



## Create A Roadmap To Compliance

There are three key building blocks to compliance, namely, systems, frameworks, and cultures. You can achieve complete automation by using these three elements to engineer cloud operations.

**Systems.** Implement cloud-native frameworks that address the challenges arising from automation of the public cloud.

**Frameworks.** Incorporate the three structures mentioned above and use them as a foundation for your cloud governance strategy and by selecting the right framework you can enjoy a strong foundation with easy to understand guidance.

**Cultures.** Modify the traditional view of IT departments that sees them operate as silos and instead adjust it to a 'trust but verify' which will allow you to enjoy the advantages of the public cloud. This may also include creating awareness amongst your teams.

# De-Risk Your Cloud By Securing And Locking Down Your Data

As you choose to shift to cloud operations, a primary concern is the security of your data, business architecture, and compliance. Your developers are tasked with the feat of developing fast, secure, and flexible applications that offer financial services to your clients without any risk of data exposure. These risks are not to be taken lightly. The financial industry is a favorite for hackers for obvious reasons. Also, it is one of the most regulated and scrutinized industries due to the sensitivity of data it deals with and the critical nature of financial systems.

Some of the regulations in place to protect consumers include; Gramm-Leach-Bliley acts, Sarbanes-Oxley, Payment Card Industry Data Security Standard (PCI DSS), and the most recent the General Data Protection Regulation (GDPR). Contrary to popular belief, the issue of information security is not just specific to the IT department. The legal and reputational ramifications from a data breach could adversely affect an organization, for example, loss of trust from clients, severe fines, and sometimes complete destruction of an organization.

Sonrai Dig provides your organization with the agility of the cloud without compromising security or compliance. It de-risks your cloud by finding possible holes, helping you fix them, and preventing these problems from occurring again even before they occur. It does so by monitoring your resources, data, and microservices, monitoring your database services to get real-time feedback on the health state of your public cloud, looking for object stores and public buckets, and monitoring access to these resources and stores. While working with **Sonrai Dig** to de-risk your cloud, the goals are to:

- Eliminate identity risks in your cloud by getting and maintaining least privilege
- Lock down your most important data to avoid mistaken data exposure
- Integrate your security, audit, DevOps teams, and IAM to shift left effectively
- Fix occurring problems and prevent them from occurring in the first place

## Get To And Maintain The Principle Of Least Privilege

Regulation of the principle of least privilege involves determining what is sufficient permissions. Sonrai Dig uses advanced analytics to monitor the various identities and data relationships closely. It ensures that identities only receive minimum permissions to meet their goals and avoids any risk of excessive privilege. Regular presentation of detailed graphs also allows you to visualize all the identity to data relationships, making for easier management of the organization. Effective regulation of least privilege helps reduce errors such as privilege escalations, toxic combinations, and separation of duties. The principle of least privilege works to ensure there are no security threats from within the company either by accident or on purpose.

## Shift Left To Integrate Teams

Sonrai Dig provides collaborative arrangements early enough in the data management process, which helps companies develop efficient systems from the very beginning. A useful tool is the Swimlanes, which organize the clouds by access rights and teams. Swimlanes ensure that the right information reaches the right units for prompt responses and timely remediation.

## Remediate And Prevent Issues

Sonrai Dig offers a well-structured platform that works to prevent data issues and achieve a high-performance structure for your organization's public cloud. An identified issue is escalated to the right bot or team immediately.

## Locking Down Crown Jewel Data

The goal of Sonrai Dig is to reduce the blast radii of any potential security concern significantly. It does this by finding solutions, classifying them, and de-risking your financial organization's crown jewel data. The crown jewel data is locked down with an impenetrable system that comes with an inbuilt alarm system that sends out a signal in case of any unexpected or sudden activity.



sonraí SECURITY

# How Can Sonrai Dig Help?

Sonrai Dig offers a platform that works to place prevention rules across your company's cloud to ensure they are met. The goal is to fix risks found in your cloud environment even before they cause any damage and close them down. The cloud allows your teams to push varying workloads to the system, and though this increases efficiency, it also opens your systems up to numerous challenges. To remedy this, Sonrai Dig places checks that automatically eliminate any risks. By using out of the box automation, your frameworks are flexible enough to allow you to add custom bots. The bot activity is continually audited to ensure compliance and workflow is monitored to give you control over escalations that might otherwise cause alert fatigue.

## Benefits of Using Sonrai Dig

### Financial  Service organizations benefit from Sonrai Dig

#### Increase Security

Sonrai Dig continuous access monitoring prevents security breaches. The Sonrai Dig data and identity-centric security approach finds, classifies, minimizes access, and continuously monitors all Crown Jewel data in structured and unstructured stores.

#### Reduce Risk

Sonrai Dig eliminates risk, other solutions cannot see. Patented graph analytics, superior integrations, and intelligent collection find identity, data, and network risks impossible to see without Sonrai Dig.  Automation eliminates the risk.

#### Maximize efficiency

Sonrai Dig increases innovation velocity while reducing costs. Swimlanes, role-based access, DevOps workflows, and automation ensures security while increasing DevOps team agility.  Customizable objectives simplify playbooks while solution breadth eliminates redundant tooling.

#### Enforce compliance

Sonrai Dig is the most complete compliance platform. With over 1000 control policies and 30 frameworks spanning data, identity, cloud-platform and container compliance mandates Sonrai Dig is the most comprehensive cloud and security continuous compliance platform.



sonraí SECURITY

## Manage CSPM

Sonrai Dig allows you to effectively utilize the speed and agility of cloud technology to monitor the cloud and container infrastructure.  At the same time, the system enforces the strength of your compliance posture and cloud security. The automation of remediation and detection of cloud misconfigurations gives you real-time insight into errors that could violate policy or breach security. It also helps increase profitability, productivity, and innovation while significantly reducing risk

## Continuously Audit

Sonrai security recognizes that to maintain efficiency, companies should regularly conduct internal audits because they help identify possible non-compliance issues before external auditors. However, lack of time and sufficient resources are constant reasons given to excuse lacking to perform internal audits. Sonrai Security helps remedy this making the audit process less time-consuming. Additionally, through automation Sonrai Security provides reports and evidence of compliance, significantly cutting down the auditor's hours and consequently saving money for your organization since most external auditors charge on a per-hourly basis.

## Delivery of Complete Risk Models

When dealing with data in the cloud, it is essential to monitor and identify all the ways it has been and can be accessed to deploy security measures such as data and identity governance properly. Sonrai Dig eliminates risk, other solutions cannot see. Patented graph analytics, superior integrations, and intelligent collection find identity, data, and network risks impossible to see without Sonrai Dig.  Automation eliminates the risk.

# See Our Platform in Action

Sonrai offers a demo for financial service organizations to correctly identify holes such as; escalations, separation of duty, excessive privilege, and possible risks across the roles and compute instances within your cloud. Our demo helps show you how to identify what has access to your data, what is accessing your data, what could access your data, and what changes have occurred.

REQUEST A DEMO

SEE THE PLATFORM

Contact us today to get your free demo and be that much closer to achieving best-in-class cloud security.



sonraí SECURITY

# Sonrai Can Help Your Financial Service Organization Today

Sonrai Security provides a platform designed to focus on data and identity governance within public clouds.

It shows you the potential risks that may arise from the data and identity relationship, such as ways your data can be accessed, or how it has been obtained in the past. Sonrai helps de-risk your cloud through a complete risk model that addresses activity movement across clouds, cloud providers and third-party data stores, and identity and data relationships.

Cloud technology provides a wide array of advantages for the healthcare and life sciences industry. It is an essential tool for achieving greater heights in healthcare innovations regarding treatment, research, cures, health services, and medical devices. However, the complexity of an ever-changing cloud environment can pose serious challenges when it comes to ensuring compliance and data security putting your organization at a higher risk. Data management in the healthcare industry is critical due to the sensitive nature of the systems and data involved. It requires you to manage your resources, compute, processes, and teams to better protect your organization's infrastructure.

## Learn More

See how we identify holes such as excessive privilege, escalations, separation of duty, and potential risks that may arise from the identities, permissions, and data exchange within and across clouds.

### Contact Us


sonraísecurity.com
info@sonraísecurity.com
646.389.2262




01212021_KS