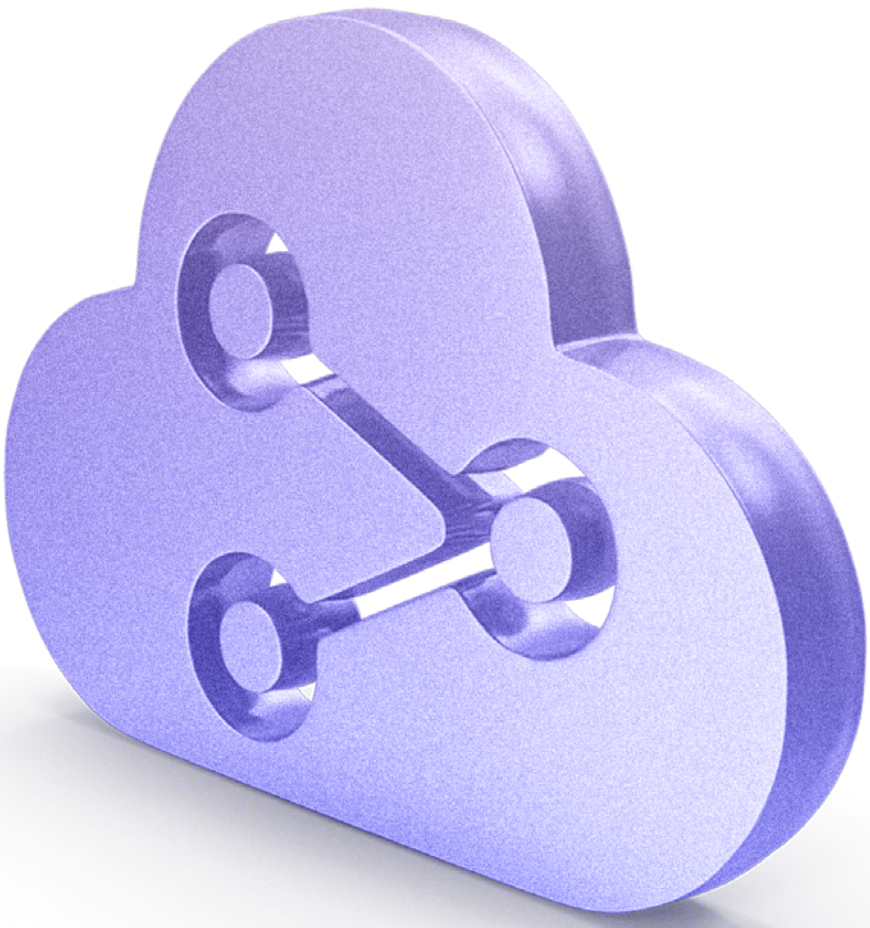
Financial Services Sector Coordinating Council
for Critical Infrastructure Protection and Homeland Security

FS-ISAC

Principles for Financial Institutions' Security and Resilience in Cloud Service Environments



July 2024

This document is the product of the Transparency and Monitoring Secure-by-Default Workstream that the Financial Services Sector Coordinating Council created in response to the release of the US Treasury Department's document, The Financial Services Sector's Adoption of Cloud Services. The participants in the workstream are representatives of financial institutions of all sizes and criticality, led by the Financial Services Information Sharing and Analysis Center (FS-ISAC). The Financial Services Sector Coordinating Council (FSSCC) has engaged major cloud service providers in the development of this paper to encourage greater collaboration.

The principles outlined in this document align to the CRI Cloud Profile version 2.0 (FSSCC Workstream 1) and will inform FSSCC Workstream 2 on outsourcing best practices. The Transparency and Monitoring Secure-by-Default Workstream plans to integrate its work with Fintech Open-Source Foundation's (FINOS) Compliant Financial Infrastructure (CFI) workgroup when its output is complete, which will help financial institutions validate workload settings.

Executive Summary

The exponential growth of cloud services has enabled financial institutions to leverage nascent technology, allowing them to more quickly respond to changing market conditions. Financial services institutions and cloud service providers have collaborated for years to make those services more secure and resilient. This document proposes principles to further that outcome.

The principles described in this document suggest methods to simplify the way financial institutions implement cloud-based workloads – i.e., processes, services, products, or applications that consume cloud-based resources – in closer alignment with financial sector cybersecurity and resilience needs.

On a practical level, these principles embody a proactive approach to safeguarding cloud workloads and simplifying security configurations for cloud service providers (CSPs) and financial services institutions (FIs). As such, it reduces risks, creates efficiency, and increases the resilience of financial services business operations.

The document illustrates the principles in terms of outcomes, i.e., the overall result that the financial institution and cloud service provider desire to achieve. The document describes those security and resilience outcomes, and offers examples that financial institutions of all sizes can scale to suit their enterprise security configurations and requirements.

As the financial sector continues to embrace cloud technologies, these principles support the confidentiality, integrity, and availability of critical financial data and applications in the cloud.

Security by Design is an integral concept to these principles. Security by design is a security assurance approach that uses best programming practices to build security controls – such as automated security baselines and continuous testing – into software and hardware before it goes to market. This approach makes customers' cybersecurity a core aspect, rather than an add-on feature, of a service.

Overview

As financial services institutions rely more on cloud service providers to manage, process, and store data for mission-critical activities, it is essential that CSPs meet the high security and resilience needs of FIs.

In March 2024, the Department of Homeland Security's Cyber Safety Review Board[1] proposed industry-agnostic actions to secure cloud environments. The Transparency and Monitoring Secure-by-Default Workstream proposes two principles that complement those actions but consider the specific needs of FIs (as well as managed service providers and other third-party providers operating on behalf of FIs).

Those principles are:

> **A cloud services "Bill of Materials," a service inter-dependency and resilience model** that combines service transparency, architecture best practices, and more detailed information about how the CSP manages its own internal resilience program specific to each service offered to a FI. This principle helps FIs know their CSPs' service environment and its resilience, learn how to mitigate specific kinds of events (and know which only the CSP can mitigate), and understand the design of their application stack based on known dependencies from one service to another.
>
> **Security by Default/Design: "One Click" Security for cloud workloads,** which implements additional security requirements through FI and CSP collaboration that simplify FI instantiation and consumption of CSP services. One Click Security extends the Security by Default/Design approach by providing a streamlined and user-friendly means of enhancing the security of FIs' cloud workloads. It leverages automation and pre-configured security templates to simplify the complex task of securing cloud resources.

Implementing the Principles in the Document

The following practices are applicable in various financial services cloud implementations and will help FIs and CSPs obtain the most benefit from these principles.

Financial Institutions

> Become familiar with the principles and outcomes provided in this document. Other resources on the topic are available from NIST, ISO, CRI, CSA, CISA, and CIS.
> Decide the features, practices, or controls that are relevant or important to the FI's specific cloud services implementation.

Financial Institutions and Cloud Service Providers

> Discuss these principles and obtain any related CSP-specific information or implementation guidance.
> Understand and agree to the FI's and CSP's shared security responsibilities.
> Draft a standard or customized plan to monitor and manage the FI's and CSP's shared security responsibilities over the life of the relationship.

CSP Service Bill of Materials

Overview

Financial services institutions' operational resilience is both a business and regulatory requirement, and critical to the functioning of society's financial life. It is therefore necessary for FIs to engineer resilience into their products and digital systems.

To operate these systems effectively and reduce risks, FIs must understand the interdependencies and resilience models of all underlying technologies as well as information about their CSP's physical infrastructure, major service dependencies, and failure model testing.

However, modern technology stacks often construct service offerings using multiple independent services. CSPs build their more complex services in this way.

For example, multiple Amazon Web Services (AWS) use AWS Lambda[2] for various functions, so a service availability event impacting Lambda would affect multiple downstream services.

Components of the CSP Service Bill of Materials

> Service Design Data: Information regarding the CSP's architecture and service dependencies

> Service Resilience Data: Information regarding testing under potential service failure scenarios

> Physical Infrastructure Design and Resilience Data: Information regarding the CSP's physical topology and infrastructure

> Solution Implementation: Information regarding the uptime and availability of the CSP infrastructure

It is therefore difficult for CSPs to provide a complete list of all service dependencies for each service they provide to FIs, which impedes FIs from understanding the interconnected risk among services.

The Workstream proposes a CSP Service Bill of Materials to address this issue. The Bill of Materials includes data on service design, resilience, physical infrastructure, and implementation in a proposal that combines service transparency, architecture best practices, and more.

The CSP Service Bill of Materials uses the Shared Resilience Responsibility Model (SRRM) in alignment with the move to shared responsibility between FIs and CSPs. SRRMs are a framework listing a Cloud Service Provider's and user's various responsibilites over an entire cloud environment (such as data, workloads, infrastructure, settings, etc.).

This SRRM unites the components of service design, reliability, FI mitigations, and CSP mitigations to provide FIs a comprehensive understanding of how to build applications and apply best practices that address CSP service failures.

With regards to specific details shared between CSPs and FIs, the recommendation is to start minimally and collaboratively determine the data that will be essential to the design decisions over time.

CSP Service Bill of Materials: Service Design Data

Understanding the design of CSP services – such as its architecture and service dependencies – would help FIs plan risk mitigation strategies. To address design and architecture of services, the Workstream proposes outcomes (and associated examples of the outcomes) connected to resilience, facilitated by CSPs, starting with the services used most within FI workloads.

- **Outcome**
  FIs understand architectural considerations that will impact security and resilience by knowing the major dependencies and service level agreements (SLAs).
  - > Example: FIs know the critical dependent or secondary (ignoring microservices) services and whether they are at the same level of security and SLAs as the primary service. Users understand where data in the architecture may be insecure or where potential single points of failure may be.
  - > Example: FIs have service dependency information for new services as launched.
- **Outcome**
  FIs can make necessary mitigation or architectural decisions to reduce or eliminate failures at the major service level.
  - > Example: FIs can identify global-level service dependencies where an outage in a single service would make another, individual service unavailable.
  - > Example: FIs and CSPs have a mutual understanding regarding events in which the FI cannot mitigate a specific failure scenario and the CSP must manage the failure.
- **Outcome**
  FIs catalog their CSP service usage to maintain accurate application to service mapping.

CSP Service Bill of Materials: Service Resilience Data

Service Resilience Data regards service availability, testing, and the parity (or lack thereof) of services – such as SLAs, log file output, and architecture – across regions. Such data would help FIs understand the significant impacts likely to occur if services become unavailable and prevent incidents or quickly recover when they occur. (Metrics such as capacity or intrusion detections are not in scope for this document.)

The Workstream proposes the following outcomes (and associated examples) connected to resilience, starting with services used most within FI workloads.

- **Outcome**
  FIs understand, and can demonstrate, that CSPs tested the service(s) they are utilizing under various potential failure scenarios, that the services achieve stated service levels, and the FI can address resilience risks of dependent services.
  - > Example: CSPs share the failure scenarios defined, documented, and tested for the primary service, describing how they achieve the stated service levels.
  - > Example: CSPs share the resilience model and anticipated FI impacts for the primary and secondary services in various levels (such as zone, region, etc.).
  - > Example: As part of annual assurance activities conducted by the FI, CSPs provide testing results (conducted by the CSP itself or a third party) for defined failure scenarios to show where the CSP has mitigated the scenario (without sharing proprietary or sensitive information).
  - > Example: CSPs facilitate FIs in creating incident response procedures in developing runbooks and procedures.

- **Outcome**
  CSPs notify FIs when there is a failure of critical functionality of a primary or secondary service(s) (ignoring microservices) and downstream services.
  - > Example: FIs and CSPs detail in advance the target notifications, such as a CSP's storage or IdP services, given the FI's workloads. (This example of that outcome recognizes that the definition of critical varies.)

CSP Service Bill of Materials: Physical Infrastructure Design and Resilience Data

A CSP's physical topology and infrastructure can effect FI workloads. To address physical infrastructure concerns, the Workstream proposes an outcome (and associated examples) connected to resilience for the CSPs.

- **Outcome**
  FIs design a robust architecture that considers physical implementation, as well as the tested failure scenarios.
  - > Example: FIs have information to inform data transfer speeds and disaster scenario considerations, such as physical topology.
  - > Example: FIs have information on additional testing or scenarios necessary to give the FI confidence in its approach.

CSP Service Bill of Materials: Solution Implementation

FIs require substantial amounts of information to be confident that their cloud services deliver effective and sustainable results and that their workloads are executing properly. The Workstream proposes the following outcomes (and associated examples) connected to resilience.

- **Outcome**
  FIs understand planned and unanticipated downtime information, such as notifications.
  - > Example: FIs receive notice when a service outage occurs that will have downstream impacts on other services.
  - > Example: FIs receive proactive notifications when there are major services changes that require FIs to review and adjust the implemented architecture, such as critical dependency changes or fundamental architectural changes.

- **Outcome**
  FIs receive information regularly – such as annually – to keep resilience plans current at a service and physical infrastructure level.
  - > Example: For all services and infrastructures used, FIs receive failure scenarios, resilience modes, and testing strategies. This dataset could be massive, so the recommendation is to start minimally and decide specific datapoints shared over time.

Security by Default/ Design and One Click Security

Overview

As financial institutions increasingly turn to CSPs to host their mission-critical workloads, ensuring security is imperative. Aiming to fortify the security of cloud workloads within the financial sector, this document considers Security by Default/Design and One Click Security as foundational security prerequisites for CSPs' architecture, infrastructure, and processes.

Security by Default/Design in Architecture, Infrastructure, and Processes

Architecture

Security by design begins with the architectural decisions made by CSPs to construct their cloud infrastructure with multi-layered security in mind, encompassing network segmentation, execution isolation, identity and access management (IAM), encryption, and continuous monitoring. These security features should be enabled by default, requiring no additional configuration by FIs.

Infrastructure

The physical and virtual infrastructure supporting cloud services must prioritize security as the foundation. This includes hardware security modules (HSMs), secure boot processes, and robust isolation mechanisms to thwart unauthorized access.

Processes

Security needs to be woven into the intrinsic processes governing the provisioning, management, and scaling of cloud resources available to the financial sector. Automated security validations and checks should be an integral part of these processes to ensure that any deviation adheres to security policies.

The focus is on protecting FI critical assets, including basic and advanced perspectives, aligning to the CRI Profile and other established frameworks. As such, this approach proactively weaves security into the architecture, infrastructure, and processes of cloud services tailored to financial institutions.

The goal is to make financial services-specific workloads safe and secure by default and fundamentally architected for security out of the box.

One Click Security extends the Security by Default/ Design approach to provide financial institutions

with a more streamlined and user-friendly means of enhancing the security of their cloud workloads.

These concepts focus on the problems of today – over time we can judge their effectiveness and identify useful revisions or adjustments.

To simplify the complex task of securing cloud resources, One Click Security leverages pre-configured security templates, automation, and continuous monitoring, as described below.

- **Pre-configured Settings:**
  The goal is a CSP-built repository of pre-configured security settings or policies aligned with industry best practices and compliance requirements. Financial institutions can select from these templates according to their precise requirements.

- **Automation**
  With a "single click" (or wizard to walk through options), FIs can apply their chosen security template to their workloads. This action triggers an automated process that configures security settings, including firewall rules, IAM policies, and encryption parameters, per the selected template.

- **Continuous Compliance and Monitoring**
  One Click Security encompasses continuous monitoring and instantaneous alerts to identify and respond to security incidents and potential threats in real time. Using defaults is a critical step in streamlining the secure use of CSPs, but user education is still important. FIs need to know why the defaults are the way they are and understand the impacts of users' changes. Because recommended settings may drift over time, understanding when the settings were applied and whether they have been altered are critical. FIs and CSPs can discuss a more robust setup – i.e., versioning and other principles – over time.

Common One Click Workloads

To illustrate One Click Security, workloads are listed below that FIs could select when using this model.

> Public facing, three tier website with database

- Scalable with containers?

> Non-public facing, grid computing using VMs

> Non-public facing, grid computing using containers/Kubernetes

> Microservices workload

> Hybrid connected workloads

> Elastic workloads – unpredictable that must scale up/down dependent on usage

> Big data/data analysis

> Disaster recovery

> Virtual desktop infrastructure/remote workstation

> Generative AI

Benefits of Security by Default/Design and One Click Security

Simplicity

Simplifies the intricate task of securing cloud resources, making the cloud safely accessible even to financial institutions with limited security expertise.

Uniformity

Guarantees a uniform and standardized security posture across the organization's cloud workloads, mitigating the risks associated with misconfigurations and vulnerabilities.

Efficiency

Automated security setup saves time and reduces expenses associated with manual configuration and maintenance. Automation also reduces the risk of manual errors, which can cause costly delays.

Rapid Response

Continuous monitoring and automated responses to security incidents enable financial institutions to react promptly to threats, mitigating potential damage.

Default Platform Configuration Considerations

Each configuration outcome in the proposals below includes the linkage to the related CRI Cloud Profile[3] section, e.g., [Independent Audit Function (GV.AU)]. Further, each configuration outcome aligns to an area of the NIST Cybersecurity Framework[4]. Those areas are specified in the configuration title.

Terminology

Platform: the control plane or fundamental setup of the cloud environment

Services: assets within the cloud environment that FIs consume, such as IaaS, PaaS, SaaS, and related products (such as frameworks akin to Kubernetes)

Security Posture Management (NIST Cybersecurity Framework Area: Govern)

The Workstream proposes the following outcome related to security.

- **Outcome**
  CSPs make the latest regulatory control attestation for the consumed services to the FIs, without the need for third parties.

> **CRI Cloud Profile section:**
> Independent Audit Function: (GV.AU)

Vulnerability Management

The Workstream proposes the following outcome related to security.

- **Outcome**
  CSPs enable FIs to perform their own pen tests as appropriate.

> **CRI Cloud Profile section:**
> Supply Chain Risk Management: (GV.SC)]

Evidence for Regulators

The Workstream proposes that CSPs provide the following outcomes (and associated examples) related to security.

- **Outcome**
  FIs can produce evidence for regulators that the required security controls are in place. (The easier or more templated the process, the better it is for all FIs.)

  > Example: Templates, which could include standardized documentation, configuration settings, or compliance reports that show regulators the specific security controls and protocols in use.

  CRI Cloud Profile section:
  Oversight: (GV.OV)

- **Outcome**
  FIs have CSP support in data collection to comply with regulations.

  > Example: FIs are able to generate detailed reports to meet FFIEC, ICCR, and other regulatory consumers requiring attestation and documentation (through a CSP risk manager or equivalent function).

  CRI Cloud Profile section:
  Oversight: (GV.OV)

Identity (NIST Cybersecurity Framework Area: Protect)

The Workstream proposes that CSPs enable the following outcomes (and associated example) related to security:

- **Outcome**
  Eliminate the management overhead of securing and maintaining an additional Identity Provider, reducing the risk of an identity breach, and enabling FIs to focus their efforts on ensuring continual analysis and addressing the principle of least privilege.

  CRI Cloud Profile section:
  Identity Management, Authentication, and Access Control (PR.AA)

  > Example: Enabling federation and Bring Your Own Identity (BYOI).

  CRI Cloud Profile section:
  Identity Management, Authentication, and Access Control (PR.AA)

- **Outcome**
  FIs can, by default, close CSP services that are commonly made "open" or "public" access.

Data Protection

FIs need to be confident that their data is managed using least privileged access in locations expected and controlled by the FI, and that FIs can access and/or retrieve the data even in worst case scenarios. The Workstream proposes that CSPs enable the following outcomes (and associated examples) related to security.

- **Outcome**
  FIs can limit access to their data as much as possible and take steps to limit impact should any third party have a breach (including CSPs).

  > Example: FIs request all third parties, including CSPs, to:
  - Implement least privileged models.
  - Reduce access from staff, services, and ecosystem partners, as well as the control plane itself, to FI data.

  CRI Cloud Profile section:
  Identity Management, Authentication, and Access Control (PR.AA)

Outcome
In the case of a catastrophic disaster, FIs can retrieve data from cold backup to maintain operations.

> Example: CSPs enable FIs to implement the Sheltered Harbor standard (recommended for all FIs).

CRI Cloud Profile section:
Data Security (PR.DS)

Encryption and Key Management

FIs need to be confident their data is secure within the CSP, and that it is using industry best practices and following the zero-trust model. The Workstream proposes that CSPs enable the following outcomes (and associated examples) related to security.

Outcome
FIs can use secure and commonly accepted levels of ciphers.

> Example: Use ciphers that meet NIST guidelines for strength in FI specific workloads.

CRI Cloud Profile section:
Data Security (PR.DS)

Outcome
CSPs help minimize key access to safeguard sensitive information and minimize the risk of unauthorized access, data breaches, and potential misuse.

> Example: CSPs provide documentation on when their staff, services, and ecosystem partners access FI keys.

CRI Cloud Profile section:
Data Security (PR.DS)

Outcome
CSPs help FIs reduce risk of contagion of attacks, specifically through limiting proliferation of master keys.

> Example: CSPs have unique master keys per FI.

CRI Cloud Profile section:
Data Security (PR.DS)

There are situations, such as those relevant to ISO standards, when CSPs need access to FI-owned data, or overall data management of sensitive data. Those are bigger contractual topics between the CSP and the FI for overall operations and are not applicable to this document.

Vulnerability Management

CSPs need to attest to adhering to the FI's regulatory requirements regarding vulnerability management processes and standards. Accordingly, the Workstream proposes that CSPs enable these outcomes (and associated examples) related to security.

Outcome
The FI and the CSP actively contribute to identifying and mitigating the potential risks of exposed attack vectors/open web surfaces. They also align with the shared security responsibility model where both parties play a role in maintaining secure ecosystems.

> Example: CSPs facilitate FIs "Bringing Their Own Vulnerability Scanners."

CRI Cloud Profile section:
Risk Assessment (ID.RA)

Outcome
CSPs help FIs easily secure their environment, such as through frequent posture assessments of their responsibility in securing the workload.

> Example: Monitoring or reporting changes to binary security controls.

CRI Cloud Profile section:
Platform Security (PR.PS)

Network/Firewall/Segmentation

The Workstream proposes that CSPs help enable these outcomes (and associated examples) related to security.

- **Outcome**
  FIs use secure communications, with CSP services requiring external access.
  - > Example: Use of dedicated VPN tunnel, PIPs, etc.
  - > Example: CSPs have encryption and protect data-in-motion for intra-CSP data movement between services.

> **CRI Cloud Profile section:**
> Technology Infrastructure Resilience (PR.IR)

- **Outcome**
  FIs operate in a known secure state that requires explicit enabling of external services. This helps reduce the internet-facing attack surface by limiting internet access to services by default. This includes both the management/control and data plane access.
  - > Example: All CSP services' internet access disabled by default.

> **CRI Cloud Profile section:**
> Technology Infrastructure Resilience (PR.IR)

- **Outcome**
  Only authorized code is executed within the computing environment and/or unauthorized code is prohibited.

> **CRI Cloud Profile section:**
> Platform Security (PR.PS)

Service Resilience (NIST Cybersecurity Framework Area: Recover)

The Workstream proposes that CSPs help enable this outcome related to security.

- **Outcome**
  FIs map their service usage by application to maintain accurate service mappings.

> **CRI Cloud Profile section:**
> Incident Management (RS.MA)

Default Platform Configuration Options

In determining default configuration options, it's important to consider what the CSP presents to users who are selecting an FI-specific workload and the flexibility and configuration options available to them.

Identity (NIST Cybersecurity Framework Area: Protect)

Some workloads use different IDPs, and this step of the wizard will determine the integration for this workload. The Workstream proposes that CSPs allow the FIs the following outcomes (and associated examples) related to security.

- **Outcome**
  FIs are allowed to use common password, identity, and login strategies.
  - > Example: CSPs facilitate password rotation, password complexity, MFA, etc.
  - > Example: CSPs support FIs to use federated and other managing/operating/supporting logins for CSP services.

> **CRI Cloud Profile section:**
> Identity Management, Authentication, and Access Control (PR.AA)

Alerting (NIST Cybersecurity Framework Area: Detect)

FIs need alerts on many aspects of FI workloads, beyond the direct services, for their overall fiduciary duty to safeguard their workloads and ensure the consistency and security of the operations. The Workstream proposes that CSPs allow the FIs the following outcomes (and associated example) related to security.

- **Outcome**
  FIs view and meet compliance with stated SLAs.
  - > Example: CSPs provide options for the FI to consider at instantiation.

> **CRI Cloud Profile section:**
> Continuous Monitoring (DE.CM)

- **Outcome for future consideration:**
  Automated configuration monitoring from CSPs to alert and inform FIs when CSPs or FIs make configuration changes that could reduce the target security.

> **CRI Cloud Profile section:**
> Continuous Monitoring (DE.CM)

The Workstream recommends that FIs decide their necessary setups or requirements in alignment with their non-negotiable needs and overall design considerations before they put any FI-specific workloads into a CSP.

SLAs (NIST Cybersecurity Framework Area: Respond)

Financial services workloads require various SLAs to comply with FI and/or regulatory requirements. The Workstream proposes that CSPs allow the FIs the following outcome.

- **Outcome**
  FIs meet regulatory timelines to respond to a cybersecurity incident.

> **CRI Cloud Profile section:**
> Incident Management (RS.MA)

Service Resilience (NIST Cybersecurity Framework Area: Recover)

The Workstream proposes that CSPs allow the FIs the following outcome (and associated example) related to security.

- **Outcome**
  FIs are able to easily select configurations or options that reduce/eliminate single points of failure.
  - > Example: CSP UI encourages the user to take the options to reduce/eliminate single points of failure.

> **CRI Cloud Profile section:**
> Incident Recovery Plan Execution (RC.RP)

Resources

1 Review of the Summer 2023 Microsoft Exchange Online Intrusion (cisa.gov)

2 Lambda is a service from AWS providing "Serverless" infrastructure for a customer's operations, typically siting in front of other infrastructure.

3 Cyber Risk Institute CRI Profile V2.0

4 NIST Cybersecurity Framework

Contact

fsisac.com
media@fsisac.com