
NIST Cybersecurity Framework (CSF)

Aligning to the NIST CSF in the AWS Cloud

January 2019



[Secure Cloud Adoption]



© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Notices

This document is provided for informational purposes only. It represents AWS' current product offerings and practices as of the date of issue of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of AWS' products or services, each of which is provided "as is" without warranty of any kind, whether express or implied. This document does not create any warranties, representations, contractual commitments, conditions or assurances from AWS, its affiliates, suppliers or licensors. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.



Contents

| | |
|----------------------------------------------------------------------------------------------------|-----------|
| Abstract..... | ii |
| Intended Audience | 1 |
| Introduction..... | 1 |
| Security Benefits of Adopting the NIST CSF..... | 3 |
| NIST CSF Implementation Use Cases | 4 |
| Health Care | 4 |
| Financial Services | 4 |
| International Adoption..... | 4 |
| AWS Services that Enable Alignment with the NIST CSF..... | 5 |
| CSF Core Function: Identify..... | 6 |
| CSF Core Function: Protect..... | 10 |
| CSF Core Function: Detect..... | 12 |
| CSF Core Function: Respond..... | 14 |
| CSF Core Function: Recover | 15 |
| AWS Services Alignment with the CSF | 17 |
| Conclusion | 18 |
| Appendix A – AWS Services and Customer Responsibility Matrix for Alignment to the CSF | 19 |
| Appendix B – Third Party Assessor Validation | 20 |

Abstract

Governments, industry sectors, and organizations around the world are increasingly recognizing the NIST Cybersecurity Framework (CSF) as a recommended cybersecurity baseline to help improve the cybersecurity risk management and resilience of their systems. This paper evaluates the NIST CSF and the many AWS Cloud offerings public and commercial sector customers can use to align to the NIST CSF to improve your cybersecurity posture. It also provides a third-party validated attestation confirming AWS services' alignment with the NIST CSF risk management practices, allowing you to properly protect your data across AWS.



Intended Audience

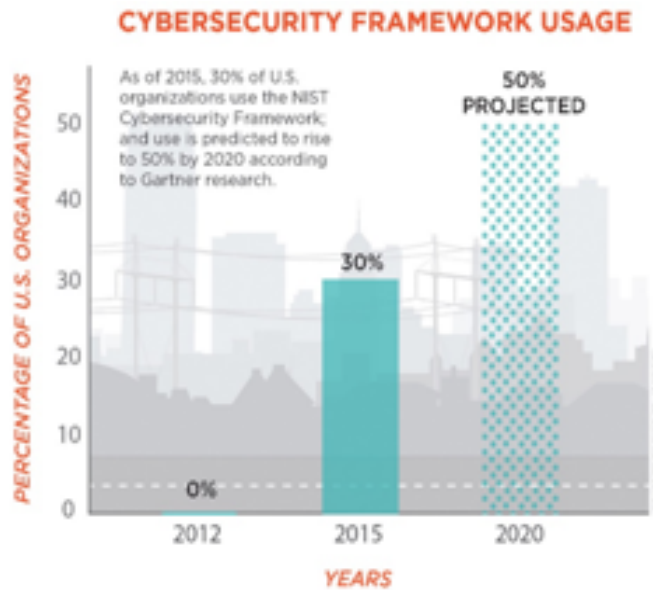
This document is intended for cybersecurity professionals, risk management officers or other organization-wide decision makers considering how to implement a new or improve an existing cybersecurity framework in their organization. For details on how to configure the AWS services identified in this document and in the associated [customer workbook](#) (see Appendix A), contact your [AWS Solutions Architect](#).

Introduction

The NIST Framework for Improving Critical Infrastructure Cybersecurity (NIST Cybersecurity Framework, or CSF) was originally published in February 2014 in response to Presidential Executive Order 13636, “Improving Critical Infrastructure Cybersecurity,” which called for the development of a voluntary framework to help organizations improve the cybersecurity, risk management, and resilience of their systems. NIST conferred with a broad range of partners from government, industry, and academia for over a year to build a consensus-based set of sound guidelines and practices. The Cybersecurity Enhancement Act of 2014 reinforced the legitimacy and authority of the CSF by codifying it and its voluntary adoption into law, until the Presidential Executive Order on “Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure” signed on May 11, 2017, mandated the use of CSF for all U.S. federal entities.

While intended for adoption by the critical infrastructure sector, the foundational set of cybersecurity disciplines comprising the CSF have been supported by government and industry as a recommended baseline for use by any organization, regardless of its sector or size. Industry is increasingly referencing the CSF as a de facto cybersecurity standard.

In Feb 2018, the International Standards Organization released “ISO/IEC 27103:2018 — Information technology— Security techniques -- Cybersecurity and ISO and IEC Standards.” This technical report provides guidance for implementing a cybersecurity framework leveraging existing standards. In fact, ISO 27103 promotes the same concepts and best practices reflected in the NIST CSF; specifically, a framework focused on security outcomes organized around five functions (Identify, Protect, Detect, Respond, Recover) and foundational activities that crosswalk to existing standards, accreditations and frameworks. Adopting this approach can help organizations achieve security outcomes while benefiting from the efficiencies of re-using instead of re-doing.



Credit: Natasha Hanacek/NIST <https://www.nist.gov/industry-impacts/cybersecurity>

According to Gartner, the CSF is used by approximately 30 percent of U.S. private-sector organizations and projected to reach 50 percent by 2020.¹ As of the release of this report, 16 U.S. critical infrastructure sectors use the CSF and over 21 states have implemented it.² In addition to critical infrastructure and other private-sector organizations, other countries, including Italy and Israel, are leveraging the CSF as the foundation for their national cybersecurity guidelines.

Since Fiscal Year 2016, U.S. federal agency Federal Information Security Modernization Act (FISMA) metrics have been organized around the CSF, and now reference it as

a “standard for managing and reducing cybersecurity risks.” According to the FY16 FISMA Report to Congress, the Council of the Inspectors General on Integrity and Efficiency (CIGIE) aligned IG metrics with the five CSF Functions to evaluate agency performance and promote consistent and comparable metrics and criteria between Chief Information Officer (CIO) and Inspector General (IG) assessments.

The most common applications of the CSF have manifested in three distinct scenarios:

1. Evaluation of an organization’s enterprise-wide cybersecurity posture and maturity by conducting an assessment against the CSF model (Current Profile) determine the desired cybersecurity posture (Target Profile), and plan and prioritize resources and efforts to achieve the Target Profile.
2. Evaluation of current and proposed products and services to meet security objectives aligned to CSF categories and subcategories to identify capability gaps and opportunities to reduce overlap/duplicative capabilities for efficiency.
3. A reference for restructuring their security teams, processes, and training.

This paper identifies the key capabilities of AWS service offerings available globally that U.S. federal, state, and local agencies; global critical infrastructure owners and operators; as well as global commercial enterprises can leverage to align to the CSF (i.e., security in the cloud). It also provides support to establish the alignment of AWS cloud services to the CSF as validated by a third-party assessor (i.e. security of the cloud) based on

1 <https://www.nist.gov/industry-impacts/cybersecurity>

2 Ibid.



compliance standards, including FedRAMP Moderate³ and ISO 9001/27001/27017/27018⁴. This means that you can have confidence that AWS services deliver on the security objectives and outcomes identified in the CSF and that you can use AWS solutions to support your own alignment with the CSF and any required compliance standard. For U.S. federal agencies, in particular, leveraging AWS solutions can facilitate your compliance with FISMA reporting metrics. This combination of outcomes should empower you with confidence in the security and resiliency of your data as you migrate critical workloads to the AWS cloud.

Security Benefits of Adopting the NIST CSF

The CSF offers a simple-yet-effective construct consisting of three elements – Core, Tiers, and Profiles. The Core represents a set of cybersecurity practices, outcomes, and technical, operational, and managerial security controls (referred to as Informative References) that support the five risk management functions – Identify, Protect, Detect, Respond, and Recover. The Tiers characterize an organization’s aptitude and maturity for managing the CSF functions and controls, and the Profiles are intended to convey the organization’s “as is” and “to be” cybersecurity postures. Together, these three elements enable organizations to prioritize and address cybersecurity risks consistent with their business and mission needs.

It is important to note that implementation of the Core, Tiers, and Profiles are the responsibility of the organization adopting the CSF (e.g., government agency, financial institution, commercial start-up, etc.). This paper focuses on AWS solutions and capabilities supporting the Core that can enable you to achieve the security outcomes (i.e., Subcategories) in the CSF. It also describes how AWS services that have been accredited under FedRAMP Moderate and ISO 9001/27001/27017/27018 align to the CSF.

The Core references security controls from widely-adopted, internationally-recognized standards such as ISO/IEC 27001, NIST 800-53, Control Objectives for Information and Related Technology (COBIT), Council on Cybersecurity (CCS) Top 20 Critical Security Controls (CSC), and ANSI/ISA-62443 Standards-Security for Industrial Automation and Control Systems. While this list represents some of the most widely reputed standards, the CSF encourages organizations to use any controls catalogue to best meet their organizational needs. The CSF was also designed to be size-, sector- and country-agnostic; therefore, public and private sector organizations should have assurance in the applicability of the CSF regardless of the type of entity or nation-state location.

The CSF encourages organizations to use any controls catalogue to best meet their organizational needs. The CSF was also designed to be size-, sector- and country-agnostic; therefore, public and private sector organizations should have assurance in the applicability of the CSF regardless of the type of entity or nation-state location.

3 Federal Risk and Authorization Management Program (FedRAMP) is the U.S. government’s standardized, federal-wide program for the security authorization of cloud services. FedRAMP’s “do once, use many times” approach was designed to offer significant benefits, such as increasing consistency and reliability in the evaluation of security controls, reducing costs for service providers and agency customers, and streamlining duplicative authorization assessments across agencies acquiring the same service.

4 ISO 27001/27002 is a widely-adopted global security standard that sets out requirements and best practices for a systematic approach to managing company and customer information that’s based on periodic risk assessments appropriate to ever-changing threat scenarios. ISO 27018 is a code of practice that focuses on protection of personal data in the cloud. It is based on ISO information security standard 27002 and provides implementation guidance on ISO 27002 controls applicable to public cloud Personally Identifiable Information (PII). It also provides a set of additional controls and associated guidance intended to address public cloud PII protection requirements not addressed by the existing ISO 27002 control set.



NIST CSF Implementation Use Cases

Health Care

The U.S. Department of Health and Human Services completed a mapping of the Health Insurance Portability and Accountability Act of 1996 (HIPAA)⁵ Security Rule to the NIST CSF. Under HIPAA, covered entities and business associates must comply with the HIPAA Security Rule to ensure the confidentiality, integrity and availability of protected health information.⁶ Since HIPAA does not have a set of controls that can be assessed or a formal accreditation process, covered entities and business associates, like AWS, are HIPAA-eligible based on alignment with NIST 800-53- security controls that can be tested and verified in order to place services on the HIPAA eligibility list. The mapping between the NIST CSF and the HIPAA Security Rule promotes an additional layer of security since assessments performed for certain categories of the NIST CSF may be more specific and detailed than those performed for the corresponding HIPAA Security Rule requirement.

Financial Services

The U.S. Financial Services Sector Coordinating Council⁷ (FS-SCC) comprised of 70 financial services associations, institutions and utilities/exchanges, developed a sector-specific profile- a customized version of the NIST CSF that addresses unique aspects of the sector and its regulatory requirements. The Financial Services Sector Specific Cybersecurity profile, drafted collaboratively with regulatory agencies, is a means to harmonize cybersecurity-related regulatory requirements. For example, the FS-SCC mapped the “Risk Management Strategy” category to nine different regulatory requirements and determined that the language and definitions, while different, largely addressed the same security objective.

International Adoption

Outside of the U.S., many countries have leveraged the NIST CSF for commercial and public sector use. Italy was one of the first international adopters of the NIST CSF and developed a national cybersecurity strategy against the five Functions. In June 2018, the UK aligned its Minimum Cyber Security Standard- mandatory for all government departments- to the five Functions. Additionally, Israel and Japan localized the NIST CSF into their respective languages with Israel creating a cyber defense methodology based on its own adaptation of the NIST CSF. Uruguay performed a mapping of the CSF to ISO standards to strengthen connections to international frameworks. Switzerland, Scotland, Ireland, and Bermuda are also among the list of countries that are using the NIST CSF to improve cybersecurity and resiliency across their public and commercial sector organizations.

5 HIPAA includes provisions to protect the security and privacy of protected health information (PHI). PHI includes a very wide set of personally identifiable health and health-related data, including insurance and billing information, diagnosis data, clinical care data, and lab results such as images and test results. The HIPAA rules apply to covered entities, which include hospitals, medical services providers, employer sponsored health plans, research facilities, and insurance companies that deal directly with patients and patient data. The HIPAA requirement to protect PHI also extends to business associates.

6 PHI includes a very wide set of personally identifiable health and health-related data, including insurance and billing information, diagnosis data, clinical care data, and lab results such as images and test results.

7 <https://www.fsscc.org/About-FSSCC>



AWS Services that Enable Alignment with the NIST CSF

This section provides an overview of AWS capabilities that you can leverage to align with the CSF Core to achieve “security in the cloud.” Appendix A provides a full list of AWS services aligned to functional categories and subcategories. The integration of these tools as part of your enterprise technology portfolio can help you build automated, innovative, and secure solutions to strengthen your cybersecurity posture.

Each CSF Core “Subcategory” was assessed and rendered by an independent third party assessor to meet the following criteria:

- Mapped to the applicable AWS service(s)
- Applicable AWS service(s) accredited under FedRAMP Moderate and/or ISO 9001/27001/27017/27018

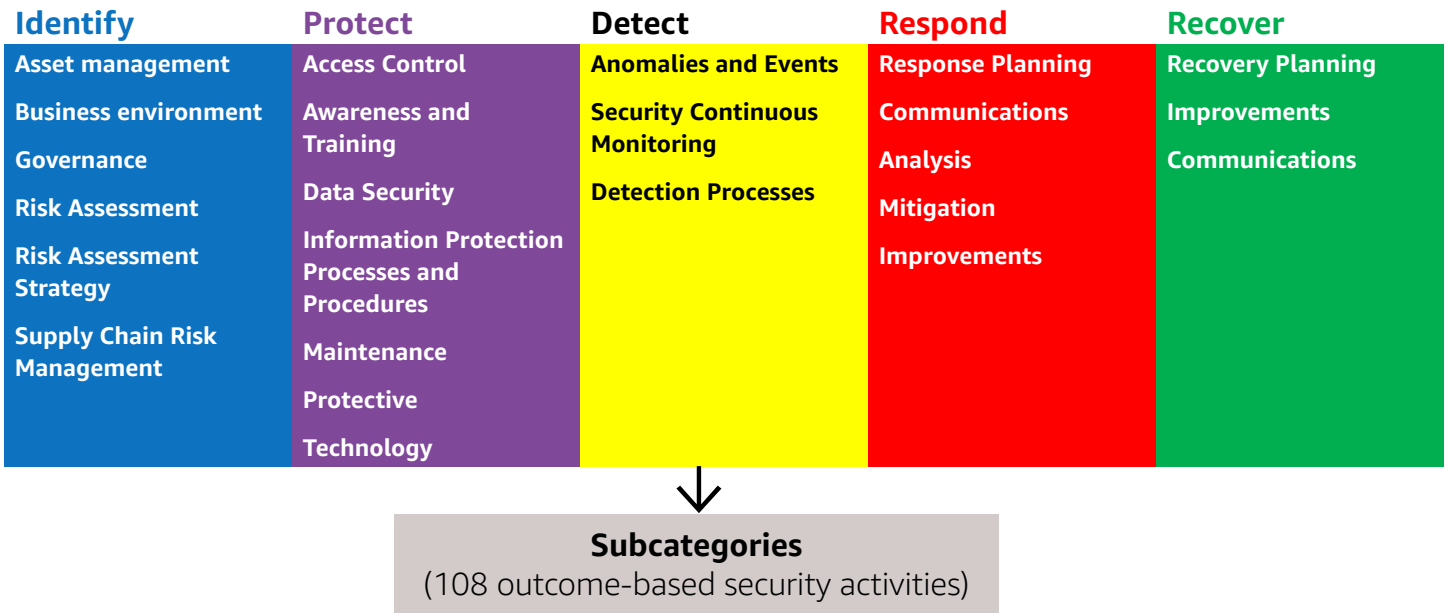
In addition to addressing “security in the cloud,” this section also identifies how AWS services align to the CSF to achieve “security of the cloud.” The third party attestation establishes that AWS services align to the CSF based on meeting compliance standards that have been mapped to the CSF subcategories, specifically, FedRAMP Moderate and ISO 9001/27001/27017/27018. This means that you can have confidence that AWS services deliver on the security objectives in the CSF and that you can use these AWS solutions to also achieve the security and resiliency best practices and outcomes identified in the CSF.

While this paper serves as a resource to provide organizational lifecycle risk management that connects business and mission objectives to cybersecurity activities, AWS also provides other best practices resources for customers moving their organizations to the cloud (AWS Cloud Adoption Framework) and customers designing, building or optimizing solutions on AWS (Well-Architected Framework).⁸ These resources supply complementary tools to support an organization in building and maturing their cybersecurity risk management programs, processes and practices in the cloud. More specifically, this NIST CSF white paper can be used in parallel with either of these best practices guides, serving as the foundation for your security program with Cloud Adoption Framework or Well-Architected Framework as an overlay for operationalizing the CSF security outcomes in the cloud.

For customers migrating to the cloud, the AWS Cloud Adoption Framework (AWS CAF) provides guidance that supports each unit in your organization so that each area understands how to update skills, adapt existing processes, and introduce new processes to take maximum advantage of the services provided by cloud computing. Thousands of organizations around the world have successfully migrated their businesses to the cloud, relying on the AWS CAF to guide their efforts. AWS and our partners provide tools and services that can help you every step of the way to ensure complete understanding and transition.

https://d1.awsstatic.com/whitepapers/aws_cloud_adoption_framework.pdf

⁸ The AWS Well-Architected Framework documents architectural best practices for designing and operating reliable, secure, efficient, and cost-effective systems in the cloud. It provides a set of foundational questions that allow you to understand if a specific architecture aligns well with cloud best practices. https://d1.awsstatic.com/whitepapers/architecture/AWS_Well-Architected_Framework.pdf



CSF Core Function: Identify

This section addresses the six categories that comprise the “Identify” Function: Asset Management, Business Environment, Governance, Risk Assessment, Risk Management Strategy, and Supply Chain Risk Management that “develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities”. A detailed mapping of AWS services to individual “Subcategories” and AWS and Customer Responsibility statements can be found in Appendix A.

CSF Core Subcategories for Identify:

Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.

Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.

Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.

Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.

Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.

Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.



Customer Responsibility

Identifying and managing IT assets is the first step in effective IT governance and security, and yet has been one of the most challenging. The Center for Internet Security (CIS)⁹ recognized the foundational importance of asset inventory and assigned physical and logical asset inventory as controls #1 and #2 of their Top 20. However, an accurate IT inventory, both of physical assets and logical assets, has been difficult to achieve and maintain for organizations of all sizes and resources. Inventory solutions are limited in being able to identify and report on all IT assets across the organization for various reasons, such as network segmentation preventing the solution from “seeing” and reporting from various parts of the enterprise network, endpoint software agents not being fully deployed or functional, and incompatibility across a broad range of disparate technologies. Unfortunately, those assets that are “lost” or unaccounted for pose the greatest risk. If they are not tracked, they are most likely not receiving the most recent patches and updates, are not replaced during lifecycle refreshments, and malware may be allowed to exploit and maintain its hold of the asset.

Migrating to AWS provides two key benefits that can mitigate the challenges with maintaining asset inventories in an on-prem environment. First, AWS assumes sole responsibility for managing physical assets that comprise the AWS cloud infrastructure. This can significantly reduce the burden of physical asset management for customers for those workloads that are hosted in AWS. The customer would still be responsible for maintaining physical asset inventories for the equipment they keep in their environment (e.g., datacenters, offices, deployed IoT, mobile workforce, etc.). The second benefit is the ability to achieve deep visibility and asset inventory for logical assets hosted in a customer’s AWS account. This may sound like a bold claim, but it becomes quickly evident as it does not matter if an EC2 instance (virtual server) is turned on or off, whether the endpoint agent is installed and running, regardless of what network segment the asset is on, or any other factor. Whether using the AWS Console as a visual point-and-click interface, through the command line interface (CLI), or application programmable interface (API), customers can query and obtain visibility of AWS service assets. This reduces the inventory burden on the customer to the software they install on their EC2 instances and what data assets they store in AWS. AWS also has services that can perform this capability, like Amazon Macie,¹⁰ which can identify, classify, label, and apply rules to data stored in Amazon S3.

An organization that understands its mission, stakeholders, and activities can utilize several AWS services to automate processes, assign business risk to IT systems, and manage user roles. For example, Identity and Access Management (IAM) can be used to assign access roles based on business roles for people and services. The use of tags for services and data can be used to prioritize automated tasks and include pre-determined risk decisions, or stop-gates for a person to evaluate the data presented and decide for which direction the system should take.

9 <https://www.cisecurity.org/controls/>

10 https://aws.amazon.com/macie/?sc_channel=PS&sc_campaign=acquisition_US&sc_publisher=google&sc_medium=ACQ-P%7CPS-GO%7CBrand%7CDesktop%7CSU%7CSecurity%7CMacie%7CUS%7CEN%7CText&sc_content=macie_e&sc_detail=aws%20macie&sc_category=Security&sc_segment=293651803573&sc_matchtype=e&sc_country=US&skwid=AL14422!3!293651803573!e!!g!!aws%20macie&ef_id=WMf1pwAAALNCC8Y3:20180918152026:s



Governance is the “unsung hero” of cybersecurity. It lays the foundation and sets the standard for people, processes, and technology. AWS provides several services and capabilities such as AWS IAM, AWS Organizations, AWS Config, AWS Systems Manager, AWS Service Catalog, and others that customers can use to implement, monitor, and enforce governance. Customers can leverage AWS’ compliance with over 50 standard such as FedRAMP, ISO, and PCI DSS¹¹. AWS provides information about its risk and compliance program to enable customers to incorporate AWS controls into their governance framework. This information can assist customers in documenting a complete control and governance framework with AWS included as an important part of that framework. Services such as Amazon Inspector identify technical vulnerabilities that can be fed into a risk posture and management process.¹² The enhanced visibility that the cloud provides increases the accuracy of a customer’s risk posture allowing risk-decisions to be made on more substantial data.

AWS Responsibility

AWS maintains stringent access control management by only providing data center access and information to employees and contractors who have a legitimate business need for such privileges. When an employee no longer has a business need for these privileges, his or her access is immediately revoked, even if they continue to be an employee of Amazon or Amazon Web Services. All physical access to data centers by AWS employees is routinely logged and audited. Controls in place limit access to systems and data and provide that access to systems or data is restricted and monitored. In addition, customer data and server instances are logically isolated from other customers by default. Privileged user access control is reviewed by an independent auditor during the AWS SOC 1, ISO 27001, PCI, and FedRAMP audits.

AWS’ risk management activities include our system development lifecycle (SDLC), which incorporates industry best practices and formal design reviews by the AWS Security Team, threat modeling and completion of a risk assessment. In addition, the AWS control environment is subject to regular internal and external risk assessments. AWS engages with external certifying bodies and independent auditors to review and test the AWS overall control environment.

AWS management has developed a strategic business plan which includes risk identification and the implementation of controls to mitigate or manage risks. AWS management re-evaluates the strategic business plan at least biannually. This process requires management to identify risks within its areas of responsibility and to implement appropriate measures designed to address those risks. In addition, the AWS control environment is subject to various internal and external risk assessments. AWS’ Compliance and Security teams have established an information security framework and policies based on the Control Objectives for Information and related Technology (COBIT) framework and have effectively integrated the ISO 27001 certifiable framework based

11 The Payment Card Industry Data Security Standard (also known as PCI DSS) is a proprietary information security standard administered by the PCI Security Standards Council (<https://www.pcisecuritystandards.org/>), which was founded by American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. PCI DSS applies to all entities that store, process or transmit cardholder data (CHD) and/or sensitive authentication data (SAD) including merchants, processors, acquirers, issuers, and service providers.

12 https://aws.amazon.com/inspector/?sc_channel=PS&sc_campaign=acquisition_US&sc_publisher=google&sc_medium=ACQ-P%7CPS-GO%7CBrand%7CDesktop%7CSU%7CSecurity%7CInspector%7CUS%7CEN%7CText&sc_content=aws_inspector_e&sc_detail=aws%20inspector&sc_category=Security&sc_segment=293647559947&sc_matchtype=e&sc_country=US&skwid=AL!4422!3!293647559947!e!!g!!aws%20inspector&ef_id=Wmf1pwAAALNCC8Y3:20180918153103:s



on ISO 27002 controls, American Institute of Certified Public Accountants (AICPA) Trust Services Principles, the PCI DSS v3.2, and the National Institute of Standards and Technology (NIST) Publication 800-53 Rev 4 (Recommended Security Controls for Federal Information Systems). AWS maintains the security policy, provides security training to employees, and performs application security reviews. These reviews assess the confidentiality, integrity, and availability of data, as well as alignment with the information security policy. AWS Security regularly scans all Internet facing service endpoint IP addresses for vulnerabilities (these scans do not include customer instances). AWS Security notifies the appropriate parties to remediate any identified vulnerabilities. In addition, external vulnerability threat assessments are performed regularly by independent security firms. Findings and recommendations resulting from these assessments are categorized and delivered to AWS leadership. These scans are done in a manner for the health and viability of the underlying AWS infrastructure and are not meant to replace the customer's own vulnerability scans required to meet their specific compliance requirements.

AWS maintains formal agreements with key third party suppliers and implements appropriate relationship management mechanisms in line with their relationship to the business. AWS' third party management processes are reviewed by independent auditors as part of AWS ongoing compliance with SOC and ISO 27001. In alignment with ISO 27001 standards, AWS hardware assets are assigned an owner, tracked and monitored by the AWS personnel with AWS proprietary inventory management tools. AWS procurement and supply chain team maintain relationships with all AWS suppliers. Refer to ISO 27001 standards; Annex A, domain 8 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.



CSF Core Function: Protect

This section addresses the six categories that comprise the “Protect” Function: Access Control, Awareness and Training, Data Security, Information Protection Processes and Procedures, Maintenance, and Protective Technology. The section also highlights AWS solutions that you can leverage to align to this Function. A detailed mapping of AWS services to individual “Subcategories” and AWS and Customer Responsibility statements can be found in Appendix A.

CSF Core Subcategory for Protect:

Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.

Awareness and Training (PR.AT): The organization’s personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.

Data Security (PR.DS): Information and records (data) are managed consistent with the organization’s risk strategy to protect the confidentiality, integrity, and availability of information.

Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.

Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.

Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.

Customer Responsibility

When looking at meeting the three security objectives of Confidentiality, Integrity, and Availability, the third can be very difficult to achieve in an on-prem environment with only one or two datacenters. This is one of the greatest benefits of hyperscale cloud service providers, and AWS in particular, due to our unique infrastructure architecture. You can distribute your application across multiple Availability Zones (AZ), which are logical fault isolation zones within a region. If architected properly with enhanced capacity management and autoscaling capabilities, your application and data would not be impacted by a single datacenter outage. If you take advantage of all the AZs in a region (where there are three or more), the loss of two datacenters may still not have any impact to your application. Likewise, services such as Amazon Simple Storage Service (S3) automatically replicates your data to at least three AZs in the region for a guaranteed availability of 99.99% and data durability of 99.999999999%.

Confidentiality can be achieved through encryption at rest and encryption in transit using AWS encryption services such as Elastic Block Store (EBS) Encryption, S3 encryption, Transparent Database Encryption for RDS



SQL Server and RDS Oracle, and VPN Gateway, or encryption using your existing encryption solution. AWS supports TLS/SSL encryption for all of its API endpoints and the ability to create VPN tunnels to protect data in transit. AWS also provides a Key Management Service and dedicated Hardware Security Module appliances to encrypt data at rest. You can choose to secure your data using the AWS provided capabilities, or use your own security tools.

Integrity can be facilitated in a variety of means. Amazon CloudWatch and Amazon CloudTrail have integrity checks, customers can use digital signatures for API calls and logs, MD5 checksums can be employed in Amazon S3, and then there are numerous third-party solutions from our partners. Amazon Config even provides integrity of the customer's AWS environment by monitoring for changes.

Within the customer AWS environment, AWS services such as AWS IAM, AWS Cognito, AWS Single Sign-On (SSO), AWS Cloud Directory, AWS Directory Service and features such as Multi-Factor Authentication allows you to implement, manage, secure, monitor, and report on user identities, authentication standards, and access rights.

You are responsible for training your staff and end users on the policies and procedures for managing your environment. For technical training, AWS and our training partners provide comprehensive training for various roles such as Solutions Architects, SysOps staff, Developers, and Security teams.¹³

AWS Responsibility

AWS employs the concept of least privilege, whereby employee access is granted based on business need and job responsibilities, providing temporary role-based access to only those resources and data required at that moment in time.

AWS provides physical data center access only to approved employees. All employees who need data center access must first apply for access and provide a valid business justification. These requests are granted based on the principle of least privilege, where requests must specify to which layer of the data center the individual needs access, and are time-bound. Requests are reviewed and approved by authorized personnel, and access is revoked after the requested time expires. Once granted admittance, individuals are restricted to areas specified in their permissions.

Third-party access is requested by approved AWS employees, who must apply for third-party access and provide a valid business justification. These requests are granted based on the principle of least privilege, where requests must specify to which layer of the data center the individual needs access, and are time-bound. These requests are approved by authorized personnel, and access is revoked after request time expires. Once granted admittance, individuals are restricted to areas specified in their permissions. Anyone granted visitor badge access must present identification when arriving on site and are signed in and escorted by authorized staff.

AWS has implemented formal, documented security awareness and training policies and procedures for our

¹³ Available online and classroom training can be found at: <https://aws.amazon.com/training>. There are also several books covering many aspects of AWS, which can be found at <https://www.amazon.com> by searching for "AWS". AWS white papers can be found at: <https://aws.amazon.com/whitepapers>



employees and contractors that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

AWS' FedRAMP and ISO 27001 certifications document in detail the policies and procedures by which AWS operates, maintains, controls, approves, deploys, reports, and monitors all changes to its environment and infrastructure, as well as how AWS provides redundancy and emergency responses for its physical infrastructure. Additionally, the certifications document in detail the manner in which all remote maintenance for AWS services is approved, performed, logged and reviewed so as to prevent unauthorized access. They also address the manner in which AWS sanitizes media and destroys data. AWS uses products and procedures that align with NIST Special Publication 800-88 Guidelines for Media Sanitization. You are also responsible for preparing the policies, processes, and procedures for data protection.

To support billing and maintenance requirements, AWS assets are assigned an owner, tracked, and monitored with AWS proprietary inventory management tools. AWS asset owner maintenance procedures are carried out by utilizing a proprietary tool with specified checks that must be completed according to the documented maintenance schedule. Third party auditors test AWS asset management controls by validating that the asset owner is documented and that the condition of the assets are visually inspected according to the documented asset management policy.

AWS services can also greatly improve managing and performing systems maintenance for our customers. First, based on AWS infrastructure discussed above with Availability Zones (AZ), an application that was architected for high availability across multiple AZs can allow you to segregate maintenance activities. You can take assets within on AZ offline for maintenance without affecting the performance of the overall application as the duplicate assets in the other AZs scale out and pick up the load. Maintenance can be accomplished one AZ at a time, and can be automated with stop-gates and reporting as required. In addition, entire architectures can be shifted over from a DevTest (Blue) environment to an operations (Green) environment, and vice versa, where that method is desired.

CSF Core Function: Detect

This section addresses the three categories that comprise the "Detect" Function: Anomalies and Events, Security Continuous Monitoring, and Detection Processes. We summarize the key AWS solutions that you can leverage to align to this Function. A detailed mapping of AWS services to individual "Subcategories" and AWS and Customer Responsibility statements can be found in Appendix A.

CSF Core Subcategory for Detect:

Anomalies and Events (DE.AE): Anomalous activity is detected in a timely manner and the potential impact of events is understood.

Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.

Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.



Customer Responsibility

The ability to gather, synthesize, and alert on security-relevant events is fundamental to any cybersecurity risk management program. The API-driven nature of cloud technology provides a new level of visibility and automation not previously possible. With every action taken resulting in one or more audit records, AWS provides a wealth of activity information available to customers within their account structure. However, the volume of data can present its own challenges. Finding the proverbial “needle in the haystack” is a real problem, but the capacity and capabilities the cloud provides are well-suited to resolve these challenges. With the appropriate log processing infrastructure, automation, and data analysis, it is possible to achieve near-real-time detection and response for critical events while filtering out false-positives and low/accepted risks.

AWS has several services that can be utilized as part of a comprehensive Security Operations strategy for continuous monitoring and threat detection. At the fundamental level, there are services such as AWS CloudTrail¹⁴ for logging all API calls, where the logs can be digitally signed and encrypted, and then stored in a secure Amazon S3 bucket. Virtual Private Cloud (VPC) Flow Logs¹⁵ monitor all network activity going in and out of your VPC. There is also Amazon CloudWatch¹⁶, which monitors your AWS environment and generates alerts similar to a Security Information Event Management (SIEM) system, and can be ingested into a customer’s on-prem SIEM.

There are also other advanced services such as Amazon GuardDuty¹⁷ that correlates activity within your AWS environment with threat intelligence from multiple sources that provides additional risk context and anomaly detection. Amazon Macie is another advanced service that can identify sensitive data, classify and label it, and track its location and access. Some customers may even choose to take advantage of AWS artificial intelligence (AI) and machine learning (ML) services to model and analyze log data.

AWS Responsibility

AWS provides near real-time alerts when the AWS monitoring tools show indications of compromise or potential compromise, based upon threshold alarming mechanisms determined by AWS service and Security teams. AWS correlates information gained from logical and physical monitoring systems to enhance security on an as-needed basis. Upon assessment and discovery of risk, Amazon disables accounts that display atypical usage matching the characteristics of bad actors.

AWS employees are trained on how to recognize suspected security incidents and where to report them. When appropriate, incidents are reported to relevant authorities. AWS maintains the AWS security bulletin webpage¹⁸ to notify customers of security and privacy events affecting AWS services. Customers can subscribe to the

14 <https://aws.amazon.com/cloudtrail/>

15 <https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs.html>

16 https://aws.amazon.com/cloudwatch/?sc_channel=PS&sc_campaign=acquisition_US&sc_publisher=google&sc_medium=ACQ-P%7CPS-GO%7CBrand%7CDesktop%7CSU%7CManagement%20Tools%7CCloudWatch%7CUS%7CEN%7CText&sc_content=cloudwatch_e&sc_detail=aws%20cloudwatch&sc_category=Management%20Tools&sc_segment=293615620998&sc_matchtype=e&sc_country=US&s_kwcid=AL!4422!3!293615620998!e!g!aws%20cloudwatch&ef_id=WMf1pwAAALNCC8Y3:20180918153820:s

17 <https://aws.amazon.com/guardduty/>

18 <https://aws.amazon.com/security/security-bulletins>



Security Bulletin RSS Feed to keep abreast of security announcements on the Security Bulletin webpage. The customer support team maintains a Service Health Dashboard webpage¹⁹ to alert customers to any broadly impacting availability issues.

CSF Core Function: Respond

This section addresses the five categories that comprise the “Respond” Function: Response Planning, Communications, Analysis, Mitigations, and Improvements. We also summarize the key AWS solutions that you can leverage to align to this Function. A detailed mapping of AWS services to individual “Subcategories” and AWS and Customer Responsibility statements can be found in Appendix A.

CSF Core Subcategory for Respond:

Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.

Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.

Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.

Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities.

Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.

Customer Responsibility

The time between detection and response is critical. Well-executed, repeatable response plans minimize exposure and speed recovery. Automation enabled by the cloud allows for the implementation of sophisticated playbooks as code with much quicker response times.

By simply tagging an Amazon EC2 instance, for example, automation can isolate the instance, take a forensic snapshot, install analysis tools, connect the suspect instance to a forensic workstation, and cut a ticket to a cybersecurity analyst. The capabilities listed below facilitate the creation of automated processes to add speed and consistency to your incident response processes. Moreover, these tools allow you to maintain a history of the communications for use in a post-event review.

While the cloud does offer capabilities to streamline and expedite the collection and dissemination of information, there is always a human element involved in response coordination. Cybersecurity analysis requires investigative action, forensics, and understanding of the incident. These necessarily require some level of human interaction. Though AWS services do not provide direct incident analytics, they do provide services to assist with executing a formalized process and assessing the breadth of impact.

¹⁹ <http://status.aws.amazon.com/>



AWS Responsibility

AWS has implemented a formal, documented incident response policy and program. The policy addresses purpose, scope, roles, responsibilities, and management commitment.

AWS utilizes a three-phased approach to manage incidents:

1. Activation and Notification Phase
2. Recovery Phase
3. Reconstitution Phase

To ensure the effectiveness of the AWS Incident Management plan, AWS conducts incident response testing. This testing provides excellent coverage for the discovery of previously unknown defects and failure modes. In addition, it allows the Amazon Security and Service teams to test the systems for potential customer impact and further prepare staff to handle incidents such as detection and analysis, containment, eradication, and recovery, and post-incident activities.

The Incident Response Test Plan is executed annually, in conjunction with the Incident Response plan. AWS Incident Management planning, testing and test results are reviewed by third party auditors.

CSF Core Function: Recover

This section addresses the three categories that comprise the “Recover” Function: Recovery Planning, Improvements, and Communications. We also summarize the key AWS solutions that you can leverage to align to this Function. A detailed mapping of AWS services to individual “Subcategories” and AWS and Customer Responsibility statements can be found in Appendix A.

CSF Core Subcategory for Recover:

Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.

Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.

Communications (RC.CO): Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.

Customer Responsibility

Customers are responsible for planning, testing, and performing recovery operations for their applications and data to maintain their business continuity. The cause of an outage may come from many different sources. AWS services provide many advanced capabilities for self-healing and automated recovery. For example, the use of auto-scaling groups across multiple Availability Zones allows for the infrastructure to monitor the health of EC2



instances and rapidly replace a failed instance with a new Amazon Machine Image (AMI). Additionally, the use of Amazon CloudWatch, AWS Lambda, and other services/service capabilities can automate recovery actions to include everything from deploying an entire AWS environment and application, to failing over to a different AWS region, restoring data from backups, and more.

Lastly, actions involving public relations, reputation management, and communicating recovery activities are respective to how the organization handles the event that impacted their environment, which, in this case, is the customer.

AWS Responsibility

AWS' resilient infrastructure, reliable automation, disciplined processes, and exceptional people are able to recover from events very quickly and with minimal (if any) disruption to our customers.

The AWS business continuity plan details the three-phased approach that AWS has developed to recover and reconstitute the AWS infrastructure:

- Activation and Notification Phase
- Recovery Phase
- Reconstitution Phase

This approach ensures that AWS performs system recovery and reconstitution efforts in a methodical sequence, maximizing the effectiveness of the recovery and reconstitution efforts and minimizing system outage time due to errors and omissions.

AWS maintains a ubiquitous security control environment across all regions. Each data center is built to physical, environmental, and security standards in an active-active configuration, employing an n+1 redundancy model to ensure system availability in the event of component failure. Components (N) have at least one independent backup component (+1), so the backup component is active in the operation even if all other components are fully functional. In order to eliminate single points of failure, this model is applied throughout AWS, including network and data center implementation. All data centers are online and serving traffic; no data center is "cold." In case of failure, there is sufficient capacity to enable traffic to be load-balanced to the remaining sites.



AWS Services Alignment with the CSF

AWS assessed the alignment of our cloud services to the CSF to demonstrate “security of the cloud.” In an increasingly interconnected world, applying strong cybersecurity risk management practices for each interconnected system to protect the confidentiality, integrity and availability of data is a necessity. Our public and private sector customers fully expect that we employ best-in-class security to safeguard our cloud services, and the data processed and stored in those systems. In order to effectively protect data and systems at hyperscale, security cannot be an afterthought, but rather an integral part of our systems lifecycle management. This means that security starts at Phase 0 (i.e., systems inception) and is continuously delivered as an inherent part of our service delivery model.

As validated by our third party assessor, AWS solutions available today for our public and commercial sector customers alignment with the NIST CSF. Each of these services maintains a current accreditation under FedRAMP Moderate and/or ISO 27001. When deploying AWS solutions, organizations can have the assurance that AWS services uphold risk management best practices defined in the CSF and can leverage these solutions for their own alignment to the CSF.

AWS exercises a rigorous, risk-based approach to the security of our services and the safeguarding of customer data. We enforce our own internal security assurance process for our services, which evaluates the effectiveness of the managerial, technical, and operational controls necessary for protecting against current and emerging security threats impacting the resiliency of our services. Hyper-scale commercial cloud service providers, such as AWS, are already subject to robust security requirements in the form of sector-specific, national, and international security certifications (e.g. FedRAMP, ISO 27001, PCI DSS, SOC, etc.) that sufficiently address the risk concerns identified by public and private sector customers worldwide.

AWS adopts the security high bar across all of our services based on our “high watermark” approach for all of our customers. This means that we take the highest classification level of data traversing and stored in our cloud services and apply those same levels of protection to all of our services and for all of our customers. These services are then queued for certification against the highest compliance bar, which translates to customers benefiting from elevated levels of protection for customer data processed and stored in our cloud. As validated by our third party assessor, AWS solutions available today for our public and commercial sector customers align with the CSF Core. Each of these services maintains a current accreditation under FedRAMP Moderate and/or ISO 27001. When deploying AWS solutions, organizations can have the assurance that AWS services uphold risk management best practices defined in the CSF and can leverage these solutions for their own alignment to the CSF. Refer to Appendix B for the third party attestation letter.



Conclusion

Public and private sector entities acknowledge the security value in adopting the NIST CSF into their environments. U.S. federal agencies, in particular, are directed to align their cybersecurity risk management and reporting practices to the CSF. As U.S. State and Local governments, non-U.S. governments, critical infrastructure operators, and commercial organizations assess their own alignment with the CSF, they need the right tools and solutions to achieve a secure and compliant system and organizational risk posture.

You can strengthen your cybersecurity posture by leveraging AWS as part of your enterprise technology to build automated, innovative, and secure solutions to achieve the security outcomes in the CSF. You reap an additional layer of security with the assurance that AWS services also employ sound risk management practices identified in the CSF, which have been validated by a third party assessor.



Appendix A – AWS Services and Customer Responsibility Matrix for Alignment to the CSF

The [AWS Services and Customer Responsibility Matrix for Alignment to the CSF](#) spreadsheet assists customers with mapping their alignment to the NIST CSF. This spreadsheet is located under the Workbooks tab within the Resources section of the AWS Compliance website.



Appendix B – Third Party Assessor Validation

September 19, 2018
Amazon Web Services
Attn: Jennifer Gray
Security - Growth Strategy | Senior
Manager, Service Design



Kratos SecureInfo
14130 Sullyfield Circle,
Suite H
Chantilly, VA 20151
Tel: 1-888-677-9351
www.kratossecureinfo.com

Dear Mrs. Gray,

Per your request, I assumed the task to review the requirements set forth in the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), version 1.1, dated April 16, 2018 and analyzed the requirements outlined in the Function and Regulation Text of the NIST CSF as they relate to AWS and the associated cloud computing reference architectures. These requirements were overlaid with the security control requirements established by NIST, documented in NIST Special Publication (SP) 800-53.

For my review, I validated the NIST CSF Citations mapping to NIST SP 800-53 security control requirements. Additionally, I reviewed the AWS services that have undergone the FedRAMP Moderate and ISO 9001 / 27001 / 27017 / 27018 accreditations that meet the citation or control requirement available for customers to deploy. During the service validation, I identified additional citations that may have available scoped services that meet the requirement. All services recommended for inclusion were validated as in scope to the AWS FedRAMP Moderate and ISO attestations.

The results of the analysis revealed that while not required by a particular compliance framework at this time, AWS has satisfied the intent of these citations through AWS services in scope for FedRAMP and ISO.

Based on my analysis of the AWS developed CSF Core Mapping Workbook and our understanding of the AWS environment, it is Kratos SecureInfo's opinion that AWS has adequately demonstrated the alignment of its adherence to the NIST CSF via the implementation of the corresponding FedRAMP and ISO security controls.

If you have any questions about the design review I performed, please contact me directly at (571)-308-3397 or by email at Emily.Cummins@KratosSecureInfo.com

Sincerely,
Emily Cummins
Principal Security Consultant
Kratos SecureInfo