NIST Cybersecurity Framework (CSF)

Aligning to the NIST CSF in the AWS Cloud

May 2017

Notices

This document is provided for informational purposes only. It represents AWS's 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's 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

Governments, 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' conformance to the NIST CSF risk management practices, allowing you to properly protect your data across AWS.

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.

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. According to Gartner, the CSF is used by approximately 30 percent of U.S. organizations and projected to reach 50 percent by 2020. In addition to critical infrastructure and other private-sector organizations, foreign governments, such as Italy, are leveraging the CSF as the foundation for their national cybersecurity guidelines.

Since Fiscal Year 2016, 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 risk posture (e.g., How does organization X align to the CSF as an enterprise?)

2. Evaluation of products and services that organizations can leverage for their own conformance to the CSF (e.g., How can organization X use a particular technology product or service to conform to the CSF?)
3. CSF Core Overlay on existing standards and requirements to evaluate the risk management practices of technology products and services (e.g., How do specific cloud services used by organization X align to the CSF Core Overlay?)

This paper identifies the key capabilities of AWS service offerings available in the AWS GovCloud (US) and AWS US East/West regions that federal, state, and local agencies; critical infrastructure owners and operators; as well as 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-managed cloud services to the CSF as validated by a third party assessor (i.e. security *of* the cloud). 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 conformance to the CSF. For 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

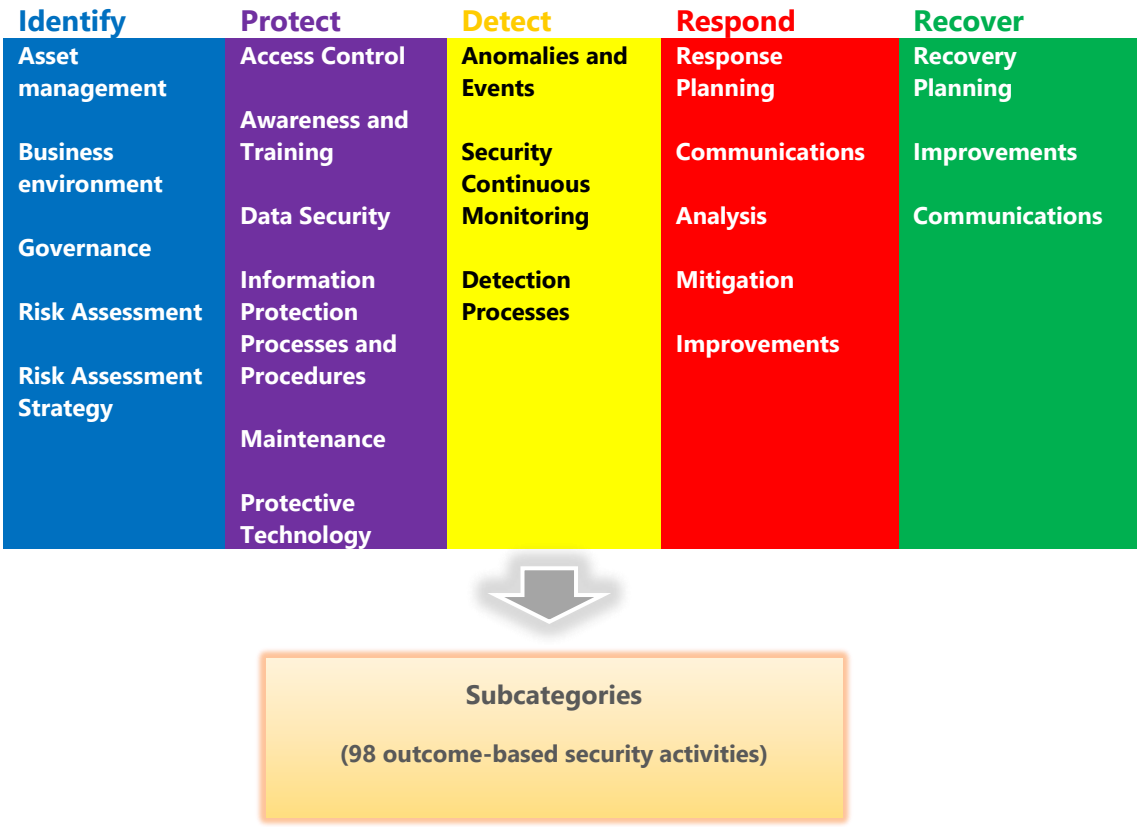
The CSF offers a simple-yet-effective construct consisting of three elements – Core, Tiers, and Profiles. The Core represents a set of cybersecurity practices, outcomes, and technical, operational, and managerial security controls (referred to as Informative References) that support the five risk management functions – Identify, Protect, Detect, Respond, and Recover. The Tiers characterize an organization's aptitude for managing cybersecurity risk and the Profiles are intended to convey the organization's "as is" and "to be" risk posture. 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., federal 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 practices and outcomes (i.e., Subcategories) in the CSF.

As shown in Figure 1, 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. ISO 27001 and NIST 800-53 (including the FedRAMP Overlay), in particular, are among the most highly demanded accreditations by public sector and enterprise customers worldwide. The AWS services described below have been accredited against FedRAMP Moderate, FedRAMP High, and/or ISO 27001 and their alignment with the CSF was validated by a third party auditor. 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 conformance to the CSF.

Figure 1: CSF Core Structure



AWS Services that Enable Conformance to the NIST CSF

This section provides an overview of the AWS services that you can leverage to fully align with the CSF Core and achieve "security *in* the cloud." The integration of these tools as part of your enterprise technology can help you build automated, innovative, and secure solutions to strengthen your cybersecurity posture. The AWS services described in this document have been accredited against FedRAMP Moderate, FedRAMP High, and/or ISO 27001 and their alignment with the CSF was validated by a third party auditor (Refer to Appendix B).

Each CSF Core "Subcategory" was assessed and rendered to meet one or more of the following criteria:

- Mapped to the applicable AWS service(s)
- Identified as a customer responsibility
- Designated as satisfied through a third party certification

A comprehensive and detailed mapping of AWS services to each of the CSF Core's "Subcategories" is included in Appendix A.

CSF Core Function: Identify

This section addresses the five categories that comprise the "Identify" Function: Asset Management, Business Environment, Governance, Risk Assessment, and Risk Management Strategy. The section also summarizes the key AWS solutions that you can leverage to align to this Function. A detailed mapping to individual "Subcategories" can be found in Appendix A.

CSF Core Category

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.

Identifying and managing IT assets is the first step in effective IT governance. IT assets can range from the high-end routers, switches, servers, hosts, and firewalls, to the applications, services, operating systems, and other software assets deployed in your network. An updated inventory of hardware and software assets is vital for decisions on upgrades and purchases, tracking warranty status, or for troubleshooting and security reasons. It is becoming a business imperative to have an accurate asset inventory listing to provide on-demand views and comprehensive reports. Moreover, comprehensive asset inventories are specifically required for certain compliance regulations. However, the nature of pieced-together, on-premises resources can make maintaining this listing arduous at best, and impossible at worst. Often organizations have to employ third-party solutions to enable automation of the asset inventory listing and, even then, it is not always possible to see a detailed inventory of every type of asset on a single console.

You can use multiple AWS features to easily and accurately understand and control your IT resources and the costs associated with them, and you can also quickly obtain an accurate inventory of these resources.

AWS Features	Alignment to the NIST Cybersecurity Framework
Account Activity page	Provides a summarized listing of IT resources by detailing usage of each service by region.
Amazon Glacier vault inventory	You can leverage Glacier data inventory to show all IT resources in Glacier.
AWS CloudHSM	Virtual and physical control over encryption keys by providing dedicated Hardware Security Modules (HSMs) for key storage.
AWS Management Console	Real-time inventory of assets and data by showing all IT resources running in AWS, by service. One-stop-shop view for cost drivers by showing all IT resources running in AWS by service including actual costs and run rate.
AWS Config	Discover existing and deleted AWS resources, determine your overall compliance against rules, and dive into configuration details of a resource at any point in time. These capabilities enable compliance auditing, security analysis, resource change tracking, and troubleshooting.
AWS Storage Gateway Application Programming Interfaces (APIs)	Inventory assets and data by programming interfaces, tools, and scripts to manage resources.
Account Activity page	Anytime view of spending on IT resources by showing resources used by service.
Amazon EC2 resource tagging	Conveys association between resource expenditures and business units by applying custom searchable labels to compute resources.

CSF Core Category

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.

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.

AWS Features	Alignment to the NIST Cybersecurity Framework

AWS SOC 1, PCI DSS, ISO 27001, FedRAMP physical access controls	Transparency into the controls in place that prevent unauthorized access to data centers relevant to the Service Organization Controls 1 audit, Payment Card Industry Data Security Standard, ISO 27001 security best practice standard and NIST 800-53 under FedRAMP- which provide an in-depth audit of both the design and operating effectiveness of AWS's defined control objectives and control activities (which include control objectives and control activities over the part of the infrastructure AWS manages). Controls are properly designed, tested, and audited by an independent audit firm.
AWS Trusted Advisor	Automated security management assessment by identifying and escalating possible security and permission issues.

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 summarizes the key AWS solutions that you can leverage to align to this Function. A detailed mapping to individual "Subcategories" can be found in Appendix A.

CSF Core Category

Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.

AWS user access privileges are restricted based on business need and job responsibilities. AWS employs the concept of least privilege, allowing only necessary access for users to accomplish their job function.

Physical access to all AWS datacenters housing IT infrastructure components is restricted to authorized data center employees, vendors, and contractors who require access to execute their job functions. Facility admission is only permitted at controlled access points that require multi-factor authentication, which are designed to prevent tailgating and ensure that only authorized individuals enter an AWS datacenter. On a quarterly basis, access lists and authorization credentials of personnel with access to data centers housing systems and devices within the system boundary are reviewed by the respective data center Area Access Managers (AAM). All entrances to AWS data centers, including the main entrance, the loading dock, and any roof doors/hatches, are secured with intrusion detection devices that sound alarms if the door is forced

open or held open. Trained security guards are stationed at the building entrance 24/7.

Amazon Virtual Private Cloud (Amazon VPC) lets you provision a logically isolated section of the AWS cloud where you can launch AWS resources in a virtual network that you define and control. You have complete control over your virtual networking environment, including selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways. You also have complete control over access to the compute, storage, databases and other AWS services you deploy or access in your VPC.

AWS Feature	Alignment to Cybersecurity Framework
Amazon Virtual Private Cloud	Facilitates network isolation using Security Groups and Network Access Controls.
Amazon EC2 Tags	Allows users and automation to annotate instances with key/value pairs (for example, to indicate a specific security access domain).
Amazon CloudWatch Logs	Provides a facility for log aggregation. Alert thresholds emit alarms.
Amazon S3 Access Control Lists (ACLs)	Centralize permissions and conditions by adding specific conditions to control how a user can use AWS, such as time of day, their originating IP address, whether they are using SSL, or whether they have authenticated with a Multi-Factor Authentication device.
Amazon S3 Bucket Policies	Create conditional rules for managing access to your buckets and objects by allowing you to restrict access based on account as well as request-based attributes, such as HTTP referrer and IP address.
AWS Identity and Access Management (IAM)	Allows you to securely control access to AWS services and resources for your users. IAM manages AWS users, groups, and roles, using permissions to allow and deny their access to AWS resources.
AWS IAM Multi-Factor Authentication (MFA)	Enforcement of MFA across all resources by requiring a token to sign in and access resources.
AWS IAM Permissions	Easily manage permissions by letting you specify who has access to AWS resources, and what actions they can perform on those resources.
AWS IAM Policies	Achieve detailed, least-privilege access management by allowing you to create multiple users within your AWS account, assign them security credentials, and manage their permissions.
AWS IAM Roles	Temporarily delegate access for users or services that normally don't have access to your AWS resources by defining a set of permissions to access the resources that a user or service needs.

AWS has implemented formal, documented security awareness and training policies and procedures that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. The security awareness and training policy and procedures are reviewed and updated at least annually; sooner, if required due to information system changes. The policy is disseminated through the internal Amazon communication portal to all employees, vendors, and contractors prior to receiving authorized access to the information system or performing assigned duties.

You are responsible for training your staff and end users on the policies and procedures for managing your environment.

CSF Core Category

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.

AWS treats all customer content and associated assets as critical information. AWS services are content agnostic, in that they offer the same high level of security to all customers, regardless of the type of content being stored. We are vigilant about our customers' security and have implemented sophisticated technical and physical measures against unauthorized access. AWS has no insight as to what type of content the customer chooses to use with AWS, and you retain complete control of how to classify, store, use, archive, and protect your content – including the use of AWS-provided or third party encryption applications (generally referred to as the shared responsibility model).

To support asset management inventory 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 maintains a capacity planning model that constantly assesses infrastructure usage and demands. The AWS capacity planning model supports planning for future demands based upon current resources and forecasted requirements.

You have full control of your assets within the AWS environment. You can provision and de-provision your own assets as needed through the AWS Console, Command Line Interface, or SDKs. Consistent with the shared responsibility model, you are responsible for implementing mechanisms to protect your environments from data leakage.

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.

AWS Feature	Alignment to Cybersecurity Framework
AWS KMS	Allows users to automate encryption and key management.
AWS CloudHSM	Allows users to encrypt assets with dedicated Hardware Security Module (HSM) appliances.
Amazon Virtual Private Cloud	Facilitates network isolation using Security Groups and Network Access Controls.
Access Logs (Amazon S3, Amazon Elastic Load Balancing)	Provide audit records for activities within the system.
AWS Identity and Access Management	Provides mechanisms for controlling access to the AWS application programming interface.
Amazon Simple Storage Solution (S3)	Provides secure, encrypted storage for data objects. Additionally, Server-Side Encryption (SSE) can be enabled to encrypt a customer's S3 data-at-rest.
Amazon Elastic Block Store (EBS)	Provides secure, encrypted file system storage.
Amazon Relational Database Service (RDS)	Provides secure managed relational database as a service.
Amazon DynamoDB	Provides secure NOSQL database as a service.
Amazon Redshift	Provides secure Data Warehouse as a service.

CSF Core Category

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.

AWS's 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 conform to NIST Special Publication 800-88 Guidelines for Media Sanitization.

AWS also maintains policy documents that describe our incident response and recovery plans as well as business continuity plans that we manage. Our Personnel Security policy documents our process for background investigations and how we apply the principle of least privilege to control access to systems and assets for AWS services. These practices are augmented with our Audit and Accountability policy documents which specify the manner in which all audit logs and records for AWS services are implemented and reviewed.

You are responsible for ensuring your policy documents detail the manner in which risk and vulnerabilities are assessed, managed, remediated, and reported within the AWS services you deploy. You are also responsible for preparing the Contingency Planning policy, Incident Response, and Business Continuity documents that detail the manner in which your contingency, incident response & recovery, and business continuity plans are managed for all AWS resources you deploy within your AWS account. In addition, you are responsible for creating your own Personnel Security policy documents to show how security is implemented for all of your personnel.

AWS Feature	Alignment to Cybersecurity Framework
Amazon EC2 Tags	Allows users and automation to annotate instances with key/value pairs (for example, to indicate a specific security access domain).
Amazon CloudWatch, Amazon CloudWatch Logs, AWS CloudTrail, Amazon VPC Flow Logs	The combination of these services provide a facility for log aggregation.
AWS Config, AWS Config Rules	Detects change events, such as sentinel tag values, and triggers initiation of a playbook.
Amazon Virtual Private Cloud	Facilitates network isolation using Security Groups and Network Access Controls.

AWS CloudFormation	Uses structured JSON or YAML to create and manage a collection of AWS resources, provisioning and updating them in a predictable fashion. Hydrates a consistently secure environment, for example.
AWS Identity and Access Management	Provides mechanisms for controlling access to the AWS application programming interface.
AWS Glacier	Online file storage web service that provides storage for data archiving and long-term backup.
Amazon S3	Provides secure, encrypted storage for data objects.
https://aws.amazon.com/documentation/	For guidance on how to develop customer policies and procedures leveraging AWS services.
https://aws.amazon.com/compliance/services-in-scope/	To identify the services that are within scope for FedRAMP Moderate, FedRAMP High, and ISO 27001.

CSF Core Category

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

AWS's FedRAMP and ISO 27001 accreditations document the manner in which remote maintenance policies for AWS services are approved, performed, logged, and reviewed so as to assure timeliness and use of only approved and authorized tools. They also document the manner in which both the communications and control networks for AWS services are isolated and protected, consistent with the principle of least privilege for controlling access to systems and assets for AWS services.

You are responsible for documenting your remote maintenance policies for the AWS services you deploy, in order to ensure maintenance is approved, performed, logged, and reviewed so as to assure timeliness and use of only approved and authorized tools.

AWS provides you with a number of services and tools for the AWS Virtual Private Cloud, which includes: AWS Identity Access Management, Security Groups, ACLs, Routing Tables, Amazon VPC Flowlogs, AWS CloudTrail, AWS CloudTrail Logs, and others to aid you in protecting your communications and control network planes. These services also permit all remote maintenance of your AWS services to be approved, performed, logged, and reviewed so as to prevent unauthorized access. In addition, you are free to implement third party services or your own custom tools to meet individual needs.

AWS Feature	Alignment to Cybersecurity Framework
AWS SOC 1, PCI DSS, ISO 27001, FedRAMP physical access controls	Transparency into the controls in place that prevent unauthorized access to data centers relevant to the Service Organization Controls 1 audit, Payment Card Industry Data Security Standard, ISO 27001 security best practice standard and NIST 800-53 under FedRAMP- which provide an in-depth audit of both the design and operating effectiveness of AWS's defined control objectives and control activities (which include control objectives and control activities over the part of the infrastructure AWS manages). Controls are properly designed, tested, and audited by an independent audit firm.
Amazon EC2 Tags	Allows users and automation to annotate instances with key/value pairs (for example, to indicate a specific security access domain).
Amazon CloudWatch, Amazon CloudWatch Logs, AWS CloudTrail, Amazon VPC Flow Logs	Provides a facility for log aggregation. Alert thresholds emit alarms.
AWS Config, AWS ConfigRules	Detects change events, such as sentinel tag values, and triggers initiation of a playbook.
Amazon Virtual Private Cloud	Facilitates network isolation using Security Groups and Network Access Controls.
AWS CloudFormation	Uses structured JSON or YAML to create and manage a collection of AWS resources, provisioning and updating them in a predictable fashion. Hydrates a consistently secure environment, for example.
AWS Identity and Access Management	Provides mechanisms for controlling access to the AWS application programming interface.

CSF Core Category

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.

AWS's FedRAMP and ISO 27001 accreditations document the manner in which all assets, networks, and controls for AWS services are used and protected. No customer is permitted direct access to any physical media within the AWS infrastructure. Should you choose to load data or configurations from AWS onto removable media in your own infrastructure, it is your responsibility to protect and control access to this removable media.

AWS Feature	Alignment to Cybersecurity Framework
Amazon EC2 Dedicated Instances	Private, isolated virtual network; Amazon EC2 compute instances are isolated at the hardware level by launching these instances into a Dedicated Tenancy.

Amazon EC2 Tags	Allows users and automation to annotate instances with key/value pairs (for example, to indicate a specific security access domain).
Amazon CloudWatch, Amazon CloudWatch Logs, AWS CloudTrail, Amazon VPC Flow Logs	Provides a facility for log aggregation. Alert thresholds emit alarms.
AWS Config, AWS ConfigRules	Detects change events, such as sentinel tag values, and triggers initiation of a playbook.
Amazon Virtual Private Cloud	Facilitates network isolation using Security Groups and Network Access Controls.
AWS CloudFormation	Uses structured JSON or YAML to create and manage a collection of AWS resources, provisioning and updating them in a predictable fashion. Hydrates a consistently secure environment, for example.
AWS Identity and Access Management	Provides mechanisms for controlling access to the AWS application programming interface.

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 also summarize the key AWS solutions that you can leverage to align to this Function. A detailed mapping to individual "Subcategories" can be found in Appendix A.

CSF Core Category

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.

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 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 and data analysis, it is possible to achieve near-real-time detection.

AWS Feature	Alignment to Cybersecurity Framework
AWS CloudTrail	Provides a history of AWS API calls, including API calls made through the AWS Management Console, AWS SDKs, command line tools, and other AWS services. Optionally provides encrypted logs and file integrity validation.
Amazon VPC Flow Logs	Provides non-sampled capture information about the IP traffic going to and from network interfaces in your VPC.
Amazon Elastic MapReduce (EMR)	Provides big data analytics tools for synthesizing multiple data sources and formats.
Amazon Glacier Vault Lock	Provides Write Once, Read Many (WORM) operations for archiving unaltered log data.
Amazon Redshift	Provides petabyte scale data warehouse capabilities for executing sophisticated searches on structured log data.
Amazon Simple Notification Service	Provides a mechanism for emitting alert information.
Amazon CloudWatch Logs	Provides a facility for log aggregation. Alert thresholds emit alarms.
Amazon CloudFront access logs	Log files with information about end user access to your objects. Logs can be distributed directly to a specific Amazon S3 bucket.
Amazon RDS database logs	Monitor a number of log files generated by Amazon RDS DB Instances. Used to diagnose, trouble shoot and fix database configuration or performance issues.
Amazon S3 server access logs	Logs of access requests with details about the request such as the request type, the resource with which the request was made, and the time and date that the request was processed.
AWS Config	Detects change events and analyzes for deviations from expected baselines.
Access Logs (Amazon S3, AWS ELB)	Provide audit records for activities within the system.
AWS Lambda	Provides event-driven processing of audit data.

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 to individual "Subcategories" can be found in Appendix A.

CSF Core Category

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.

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. 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.

AWS Feature	Alignment to Cybersecurity Framework
Amazon EC2 Tags	Allows users and automation to annotate instances with key/value pairs to indicate, for example, a compromised instance.
Amazon S3	Provides storage for forensic data, such as snapshots and instance memory dumps; houses AWS CloudFormation templates.
Amazon Elastic Block Store (EBS)	Provides block-level snapshots for forensic analysis. Restored snapshots allow for data analysis without modifying the original system volume images.
Amazon Glacier Vault Lock	Provides Write Once, Read Many (WORM) operations for archiving unaltered data files.
Amazon Simple Workflow Service	Executes the steps/tasks in your response playbook. Redundantly stores the tasks, reliably dispatches them to application components, tracks their progress, and keeps their latest state.
Amazon Simple Notification Service	Provides a mechanism for emitting alert information, such as generating a ticket to an analyst.
Amazon CloudWatch Logs	Provides a facility for log aggregation. Alert thresholds emit alarms.

AWS Config	Detects change events, such as sentinel tag values, and triggers initiation of a playbook.
Amazon Virtual Private Cloud	Facilitates network isolation using Security Groups and Network Access Controls.
AWS CloudFormation	Uses structured JSON or YAML to create and manage a collection of AWS resources, provisioning and updating them in a predictable fashion. Hydrates the forensic environment, for example.
AWS Identity and Access Management	Provides mechanisms for automating the revocation of temporary and long-lived credentials as part of a run book.
AWS Lambda	Provides event-driven serverless compute operations, such as triggering the installation of forensic tools.

CSF Core Category

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

There is always a human element involved in response coordination. The cloud does, however, offer capabilities to streamline and expedite the collection and dissemination of information. Moreover, these tools allow you to maintain a history of the communications for use in a post-event review.

AWS Feature	Alignment to Cybersecurity Framework
Amazon API Gateway	Provides an API endpoint for ingestion of system-generated event data.
Amazon Simple Email Service	Provides outbound email distribution. Receives, filters, and processes inbound email through S3, Lambda, or SNS.
Amazon S3	Provides backend persistence for communication data.
AWS Lambda	Provides event-driven code execution for parsing and routing communication data.
Amazon Simple Notification Service	Provides a mechanism for emitting communication information via email, HTTP endpoints, Simple Queue Services, or SMS.
Amazon Glacier Vault Lock	Provides Write Once, Read Many (WORM) operations for archiving unaltered communication data.
Amazon Simple Queue Services	Provides message queueing for asynchronous delivery of communications data.

CSF Core Category

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

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.

AWS Feature	Alignment to Cybersecurity Framework
Amazon Simple Workflow Service	Executes the steps/tasks in your response playbook. Redundantly stores the tasks, reliably dispatches them to application components, tracks their progress, and keeps their latest state.
AWS CloudTrail	Provides a history of AWS API calls, including API calls made through the AWS Management Console, AWS SDKs, command line tools, and other AWS services.
AWS Config	Maintains a configuration history.
Amazon S3	Persistence store for analytic data.
Amazon Glacier Vault Lock	Provides Write Once, Read Many (WORM) operations for archiving unaltered communication data.
Amazon CloudWatch Logs	Provides aggregated logs for analysis.
Amazon VPC Flow Logs	Provides non-sampled capture information about the IP traffic going to and from network interfaces in your VPC.

CSF Core Category

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

With the high level of automation offered by the cloud, you can incorporate your lessons learned from an incident back into your code.

AWS Feature	Alignment to Cybersecurity Framework
Amazon EC2	Deliver new baseline OS security configurations.
Amazon Simple Notification Services	Update the subscribers to an alert or notification topic.

Amazon Simple Workflow Service	Update your playbooks to add new or updated automation.
Amazon VPC	Update instance isolation approach.
AWS CloudFormation	Update your baselines configurations.
Amazon CloudWatch Logs	Identify new log sources to aggregate.
AWS Identity and Access Management	Update identity and credential management practices.
AWS Lambda	Create and update event-driven compute to reflect lessons learned.
AWS Key Management System	Apply cryptography as appropriate to secure data.

CSF Core Function: Recover

You are individually responsible for fulfilling the requirements that comprise the "Recover" Function: Recovery Planning, Improvements, and Communications. While AWS manages security *of* the cloud, security *in* the cloud is your responsibility. You retain control of what security you choose to implement to protect your own content, platform, applications, systems and networks no differently than you would for applications in an on-site datacenter.

Developing and implementing recovery plans and strategies are required for federal agencies under the Federal Information Security Modernization Act (FISMA), which states that each agency should develop, document, and implement an agency-wide information security program that includes "procedures for detecting, reporting, and responding to security incidents." Further, DHS's Continuous Diagnostics and Mitigation (CDM) Program Phase 3: Boundary Protection and Event Management for Managing the Security Lifecycle also includes capabilities such as event response and planning that agencies are required to implement. Lastly, actions involving public relations,

CSF Core Category

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.

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 agency customer.

AWS Services' Conformance to the CSF

In addition to enabling an organization's alignment to the CSF (i.e., security *in* the cloud), 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 design) and is continuously delivered as an inherent part of our service delivery model.

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, 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 "highest factor" 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 conform to the CSF Core. Each of these services maintains a current accreditation under FedRAMP Moderate, FedRAMP High, 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.

Conclusion

Public and private sector entities acknowledge the security value in adopting the NIST CSF into their environments. Federal agencies, in particular, are increasingly directed to align their cybersecurity risk management and reporting practices to the CSF. As public sector, critical infrastructure, and commercial organizations assess their own conformance to 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.

AWS continues to actively participate in the revisions to the CSF (Version 1.1). Once the draft version is finalized later this year, AWS intends to update the assessment of our services against the revised baseline.

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 – 3rd Party Attestation

COALFIRE

Coalfire
8229 Boone Blvd, Suite 750
Vienna, VA 22182
Tel 1-703-760-9168
Fax 1-703-760-9164
www.Coalfire.com

April 13, 2017
Amazon Web Services
Attn: Jenn Gray
AWS US Public Sector Compliance Program Manager

Dear Mrs. Gray,

Per your request, Coalfire engaged an Amazon Web Services (AWS)-certified solutions architect, who is a member of the AWS FedRAMP assessment team, to review the AWS Cyber Security Framework (CSF) control mapping created by the AWS Security Assurance Team. The activity is part of an ongoing effort to demonstrate the alignment between the AWS FedRAMP and ISO-certified services and the National Institute of Standards and Technology (NIST) CSF and its associated categories and subcategories. As part of this review, this team member analyzed the AWS developed CSF Core Mapping Workbook, the identified AWS and customer responsibilities, and the associated control requirements for both the FedRAMP and ISO security control frameworks.

In performing our review, we noted that each of the categories and subcategories identified in the NIST CSF, v1.0, dated February 12, 2014 were accounted for and that each subcategory was aligned with a corresponding FedRAMP and/or ISO security control requirement. Each of these alignments contained the applicable information detailing AWS's responsibility as well the associated customer responsibility with regards to the implementation of the identified security control. In addition, AWS has documented the AWS services which have been assessed against the FedRAMP or ISO security control frameworks and were determined to meet or exceed the control requirements outlined by at least one of these security control frameworks by a third-party assessment organization (3PAO).

Based on our analysis of the AWS developed CSF Core Mapping Workbook and our understanding of the AWS environment, it is Coalfire'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 our team performed, please contact me directly at (571) 722-1729 or by email at Michael.Caruso@Coalfire.com.

Sincerely,

Michael Caruso
Managing Principal, FedRAMP Assessment Services – Coalfire

Contributors

The following individuals contributed to this document:

- Michael Cotton, Senior Solutions Architect
- David Cruley, Senior Solutions Architect
- Jennifer Gray, Security Assurance Manager
- Alan Halachmi, Senior Solutions Architect
- Min Hyun, Cloud Security Strategist
- Jim Jennis, Senior Solutions Architect
- Dennis O'Neill, Technical Assessment Specialist
- Camil Samaha, Senior Solutions Architect

Document Revisions

Date	Description
May 2017	First publication