AWS Cloud Adoption Framework

Security Perspective

June 2016

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

The Amazon Web Services (AWS) Cloud Adoption Framework[1] (CAF) provides guidance for coordinating the different parts of organizations migrating to cloud computing. The CAF guidance is broken into a number of areas of focus relevant to implementing cloud-based IT systems. These focus areas are called *perspectives*, and each perspective is further separated into *components*. There is a whitepaper for each of the seven CAF perspectives.

This whitepaper covers the Security Perspective, which focuses on incorporating guidance and process for your existing security controls specific to AWS usage in your environment.

Introduction

Security at AWS is job zero. All AWS customers benefit from a data center and network architecture built to satisfy the requirements of the most security-sensitive organizations. AWS and its partners offer hundreds of tools and features to help you meet your security objectives around visibility, auditability, controllability, and agility. This means that you can have the security you need, but without the capital outlay, and with much lower operational overhead

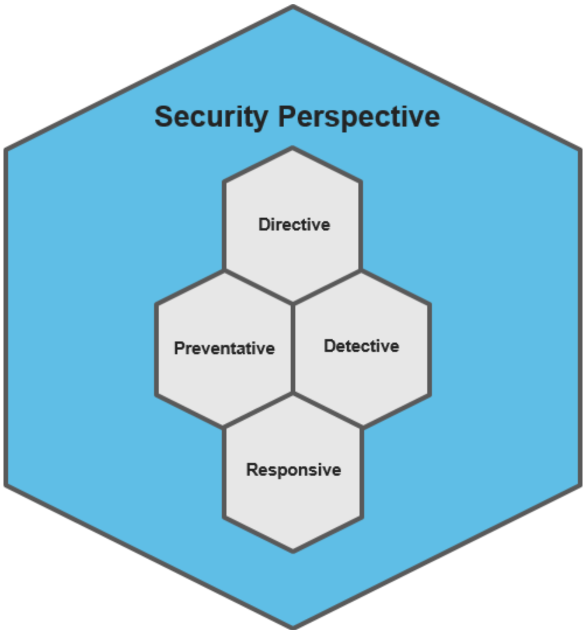


Figure 1: AWS CAF Security Perspective

than in an on-premises environment.

The Security Perspective goal is to help you structure your selection and implementation of controls that are right for your organization. As Figure 1 illustrates, the components of the Security Perspective organize the principles that will help drive the transformation of your organization's security culture. For each component, this whitepaper discusses specific actions you can take, and the means of measuring progress:

- **Directive** controls establish the governance, risk, and compliance models the environment will operate within.
- **Preventive** controls protect your workloads and mitigate threats and vulnerabilities.
- **Detective** controls provide full visibility and transparency over the operation of your deployments in AWS.
- **Responsive** controls drive remediation of potential deviations from your security baselines.

Security in the cloud is familiar. The increase in agility and the ability to perform actions faster, at a larger scale and at a lower cost, does not invalidate well-established principles of information security.

After covering the four Security Perspective components, this whitepaper shows you the steps you can take to on your journey to the cloud to ensure that your environment maintains a strong security footing:

- Define a **strategy for security** in the cloud. When you start your journey, look at your organizational business objectives, approach to risk management, and the level of opportunity presented by the cloud.
- Deliver a **security program** for development and implementation of security, privacy, compliance, and risk management capabilities. The scope can initially appear vast, so it is important to create a structure that allows your organization to holistically address security in the cloud. The implementation should allow for iterative development so that capabilities mature as programs develop. This allows the security component to be a catalyst to the rest of the organization's cloud adoption efforts.

- Develop robust **security operations** capabilities that continuously mature and improve. The security journey continues over time. We recommend that you intertwine operational rigor with the building of new capabilities, so the constant iteration can bring continuous improvement.

Security Benefits of AWS

Cloud security at AWS is the highest priority. As an AWS customer, you will benefit from a data center and network architecture built to meet the requirements of the most security-sensitive organizations.

An advantage of the AWS cloud is that it allows customers to scale and innovate, while maintaining a secure environment. Customers pay only for the services they use, meaning that you can have the security you need, but without the upfront expenses, and at a lower cost than in an on-premises environment.

This section discusses some of the security benefits of the AWS platform.

Designed for Security

The AWS Cloud infrastructure is operated in AWS data centers and is designed to satisfy the requirements of our most security-sensitive customers. The AWS infrastructure has been designed to provide high availability, while putting strong safeguards in place for customer privacy. All data is stored in highly secure AWS data centers. Network firewalls built into Amazon VPC, and web application firewall capabilities in AWS WAF let you create private networks, and control access to your instances and applications

When you deploy systems in the AWS Cloud, AWS helps by sharing the security responsibilities with you. AWS engineers the underlying infrastructure using secure design principles, and customers can implement their own security architecture for workloads deployed in AWS.

Highly Automated

At AWS we purpose-build security tools, and we tailor them for our unique environment, size, and global requirements. Building security tools from the ground up allows AWS to automate many of the routine tasks security experts normally spend time on. This means AWS security experts can spend more time focusing on measures to increase the security of your AWS Cloud environment. Customers also automate security engineering and operations functions using a comprehensive set of APIs and tools. Identity management, network security and data protection, and monitoring capabilities can be fully automated and delivered using popular software development methods you already have in place. Customers take an automated approach to responding to security issues. When you automate using the AWS services, rather than having people monitoring your security position and reacting to an event, your system can monitor, review, and initiate a response.

Highly Available

AWS builds its data centers in multiple geographic Regions. Within the Regions, multiple Availability Zones exist to provide resiliency. AWS designs data centers with excess bandwidth, so that if a major disruption occurs there is sufficient capacity to load-balance traffic and route it to the remaining sites, minimizing the impact on our customers. Customers also leverage this Multi-Region, Multi-AZ strategy to build highly resilient applications at a disruptively low cost, to easily replicate and back up data, and to deploy global security controls consistently across their business.

Highly Accredited

AWS environments are continuously audited, with certifications from accreditation bodies across the globe. This means that segments of your compliance have already been completed. For more information about the security regulations and standards with which AWS complies, see the AWS Cloud Compliance[2] web page. To help you meet specific government, industry, and company security standards and regulations, AWS provides certification reports that describe how the AWS Cloud infrastructure meets the requirements of an extensive list of global security standards. You can obtain available compliance reports by contacting your AWS account representative. Customers inherit many controls operated by AWS into their own compliance and certification programs, lowering the cost to maintain and run security assurance efforts in addition to actually maintaining the controls themselves. With a strong foundation in place, you are free to optimize the security of your workloads for agility, resilience, and scale.

The rest of this whitepaper introduces each of the components of the Security Perspective. You can use these components to explore the security goals you need to be successful on your journey to the cloud.

Directive Component

The Directive component of the AWS Security Perspective provides guidance on planning your security approach as you migrate to AWS. The key to effective planning is to define the guidance you will provide to the people implementing and operating your security environment. The information needs to provide enough direction to determine the controls needed and how they should be operated. Initial areas to consider include:

- **Account Governance**— Direct the organization to create a process and procedures for managing AWS accounts. Areas to define include how account inventories will be collected and maintained, which agreements and amendments are in place, and what criteria to use for when to create an AWS account. Develop a process to create accounts in a consistent manner, ensuring that all initial settings are appropriate and that clear ownership is established.
- **Account Ownership and contact information**—Establish an appropriate governance model of AWS accounts used across your organization, and plan how contact information is maintained for each account. Consider creating AWS accounts tied to email distribution lists rather than to an individual's email address. This allows a group of people to monitor and respond to information from AWS about your account activity. Additionally, this provides resilience when internal personnel change, and it provides a means of assigning security accountability. List your security team as a security point of contact to speed time-sensitive communications.
- **Control framework**—Establish or apply an industry standard control framework and determine if you need modifications or additions in order to incorporate AWS services at expected security levels. Perform a compliance mapping exercise to determine how compliance requirements and security controls will reflect AWS service usage.
- **Control ownership**—Review the AWS Shared Responsibility Model[3] information on the AWS website to determine if control ownership

modifications should be made. Review and update your responsibility assignment matrix (RACI chart) to include ownership of controls operating in the AWS environment.

- **Data classification**—Review current data classifications and determine how those classifications will be managed in the AWS environment and what controls will be appropriate.
- **Change and asset management**—Determine how change management asset management are to be performed in AWS. Create a means to determine what assets exist, what the systems are used for, and how the systems will be managed securely. This can be integrated with an existing configuration management database (CMDB). Consider creating a practice for naming and tagging that allows identification and management to occur to the security level required. You can use this approach to define and track the metadata that enables identification and control.
- **Data locality**—Review criteria for where your data can reside to determine what controls will be needed to manage the configuration and usage of AWS services across Regions. AWS customers choose the AWS Region(s) where their content will be hosted. This allows customers with specific geographic requirements to establish environments in locations they choose. Customers can replicate and back up content in more than one Region, but AWS does not move customer content outside of the customer's chosen Region(s).
- **Least privilege access**— Establish an organizational security culture built on the principle of least privilege and strong authentication. Implement protocols to protect access to sensitive credential and key material associated with every AWS account. Set expectations on how authority will be delegated down through software engineers, operations staff, and other job functions involved in cloud adoption.
- **Security operations playbook and runbooks**—Define your security patterns to create durable guardrails the organization can reference over time. Implement the plays through automation as runbooks; document human-in-the-loop interventions as appropriate.

Considerations

- **Do** create a tailored AWS shared responsibility model for your ecosystem.
- **Do** use strong authentication as part of a protection scheme for all actors in your account.
- **Do** promote a culture of security ownership for application teams.
- **Do** extend your data classification model to include services in AWS.
- **Do** integrate developer, operations, and security team objectives and job functions.
- **Do** consider creating a strategy for naming and tracking accounts used to manage services in AWS.
- **Do** centralize phone and email distribution lists so that teams can be monitored.

Preventive Component

The Preventive component of the AWS Security Perspective provides guidance for implementing security infrastructure with AWS and within your organization. The key to implementing the right set of controls is enabling your security teams to gain the confidence and capability they need to build the automation and deployment skills necessary to protect the enterprise in the agile, scalable environment that is AWS.

Use the Directive component to determine the controls and guidance that you will need and then use the Preventive component to determine how you will operate the controls effectively. AWS regularly provides guidance on best practices for AWS service utilization and workload deployment patterns which can be used as control implementation references. Visit the AWS Security Center, blog, and most recent AWS Summit and re:Invent conference Security Track videos.

Consider the following areas to determining what changes (if any) you need to make to your current security architectures and practices. This will help you with a smooth and planned AWS adoption strategy.

- **Identity and access**—Integrate the use of AWS into the workforce lifecycle of the organization, as well as into the sources of authentication and authorization. Create fine-grained policies and roles associated with appropriate users and groups. Create guardrails that permit important changes through automation only, and prevent unwanted changes or roll them back automatically. These steps will reduce human access to production systems and data.
- **Infrastructure protection**—Implement a security baseline including trust boundaries, system security configuration and maintenance (e.g., harden and patch), and other appropriate policy enforcement points (e.g., security groups, AWS WAF, Amazon API Gateway) to meet the needs that you identified using the Directive component.
- **Data protection**—Utilize appropriate safeguards to protect data in transit and at rest. Safeguards include fine-grained access controls to objects, creating and controlling the encryption keys used to encrypt your data,

selecting appropriate encryption or tokenization methods, integrity validation, and appropriate retention of data.

Considerations

- **Do** treat security as code, allowing you to deploy and validate security infrastructure in a manner that allows you the scale and agility to protect the organization.
- **Do** create guardrails, sensible defaults, and offer templates and best practices as code.
- **Do** build security services that the organization can leverage for highly repetitive or particularly sensitive security functions.
- **Do** define actors and then storyboard their experience interacting with AWS services.
- **Do** use the AWS Trusted Advisor tool to continually assess your AWS security posture, and consider an AWS Well Architected review.
- **Do** establish a minimal viable security baseline, and continually iterate to raise the bar for the workloads you’re protecting.

Detective Component

The Detective component of the AWS CAF Security Perspective provides guidance for gaining visibility into your organization's security posture. A wealth of data and information can be gathered by using services like AWS CloudTrail, service-specific logs, and API/CLI return values. Ingesting these information sources into a scalable platform for managing and monitoring logs, event management, testing, and inventory/audit will give you the transparency and operational agility you need to feel confident in the security of your operations.

- **Logging and monitoring**—AWS provides native logging as well as services that you can leverage to provide greater visibility near to real time for occurrences in the AWS environment. You can use these tools to integrate into your existing logging and monitoring solutions. Integrate the output of logging and monitoring sources deeply into the workflow of the IT organization for end-to-end resolution of security-related activity.
- **Security testing**—Test the AWS environment to ensure that defined security standards are met. By testing to determine if your systems will respond as expected when certain events occur you will be better prepared for actual events. Examples of security testing include vulnerability scanning, penetration testing, and error injection to prove standards are being met. The goal is to determine if your control will respond as expected.
- **Asset inventory**—Knowing what workloads you have deployed and operational will allow you to monitor and ensure that the environment is operating at the security governance levels expected and demanded by the security standards.
- **Change detection**—Relying on a secure baseline of preventive controls also requires knowing when these controls change. Implement measures to determine drift between secure configuration and current state.

Considerations

- **Do** determine what logging information for your AWS environment you want to capture, monitor, and analyze.
- **Do** determine how your existing security operations center (SOC) business capability will integrate AWS security monitoring and management into existing practices.
- **Do** continually conduct vulnerability scans and penetration tests in accordance with AWS procedures for doing so.

Responsive Component

The Responsive component of the AWS CAF Security Perspective provides guidance for the responsive portion of your organization's security posture. By incorporating your AWS environment into your existing security posture, and then preparing and simulating actions that require response, you will be better prepared to respond to incidents as they occur.

With automated incident response and recovery, and the ability to mitigate portions of disaster recovery, it is possible to shift the primary focus of the security team from response to performing forensics and root cause analysis. Some things to consider as part of adapting your security posture include the following:

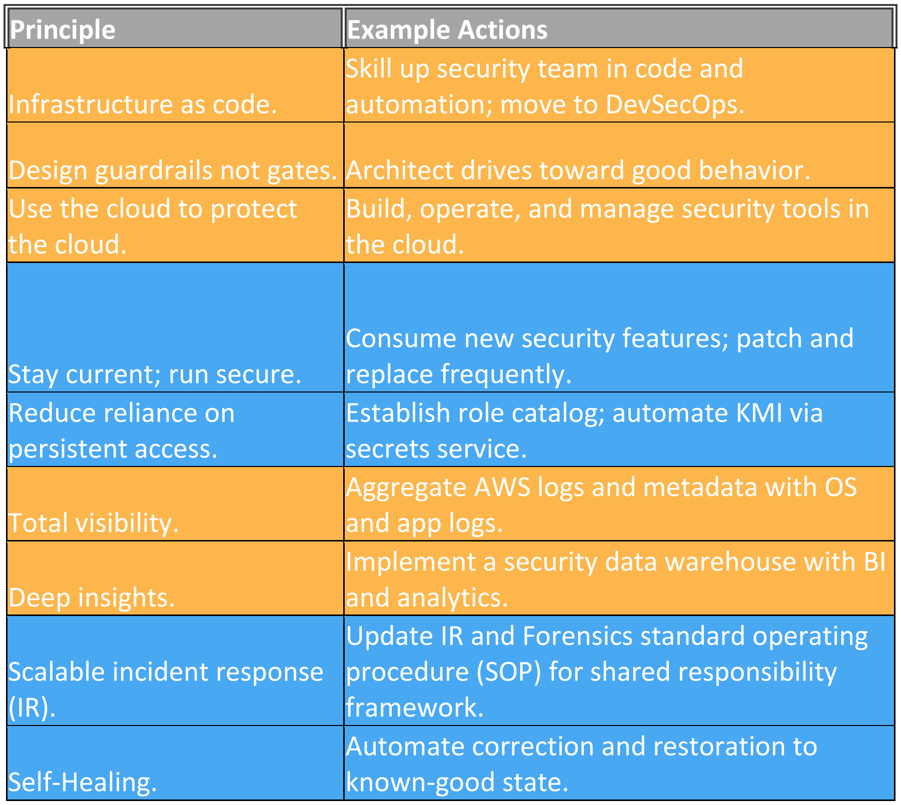
- **Incident response**—During an incident, containing the event and returning to a known good state are important elements of a response plan. For instance, automating aspects of those functions using AWS Config rules and AWS Lambda responder scripts gives you the ability to scale your response at Internet speeds. Review current incident response processes and determine if and how automated response and recovery will become operational and managed for AWS assets. The security operations center's functions should be tightly integrated with the AWS APIs to be as responsive as possible. This provides the security monitoring and management function for AWS Cloud adoption.
- **Security incident response simulations**—By simulating events you can validate that the controls and processes you have put in place react as expected. Using this approach you can determine if you are effectively able to recover and respond to incidents when they occur.
- **Forensics**—In most cases, your existing forensics tools will work in the AWS environment. Forensic teams will benefit from the automated deployment of tools across regions and the ability to collect large volumes of data quickly, with low friction using the same robust, scalable services their business-critical applications are built on, such as Amazon Simple Storage Service (S3), Amazon Elastic Block Store (EBS), Amazon Kinesis, Amazon DynamoDB, Amazon Relational Database Service (RDS), Amazon RedShift, and Amazon Elastic Compute Cloud (EC2).

Considerations

- **Do** update your incident response processes to recognize the AWS environment.
- **Do** leverage services in AWS to forensically ready your deployments through automation and feature selection.
- **Do** automate response for robustness and scale.
- **Do** use services in AWS for data collection and analysis in support of an investigation.
- **Do** validate your incident response capability through simulations of security incident responses.

Taking the Journey – Defining a Strategy

Review your current security strategy to determine if portions of the strategy would benefit from change as part of a cloud adoption initiative. Map your AWS cloud adoption strategy against the level of risk your business is willing to accept, your approach to meeting regulatory and compliance objectives, as well as your definitions for what needs to be protected and how it will be protected. Table 1 provides an example of a security strategy that articulates a set of principles which are then mapped to specific initiatives and work streams.



Principle	Example Actions
Infrastructure as code.	Skill up security team in code and automation; move to DevSecOps.
Design guardrails not gates.	Architect drives toward good behavior.
Use the cloud to protect the cloud.	Build, operate, and manage security tools in the cloud.
Stay current; run secure.	Consume new security features; patch and replace frequently.
Reduce reliance on persistent access.	Establish role catalog; automate KMI via secrets service.
Total visibility.	Aggregate AWS logs and metadata with OS and app logs.
Deep insights.	Implement a security data warehouse with BI and analytics.
Scalable incident response (IR).	Update IR and Forensics standard operating procedure (SOP) for shared responsibility framework.
Self-Healing.	Automate correction and restoration to known-good state.

Table 1: Example Security Strategy

As your strategy evolves you will want to begin iterating on your third-party assurance frameworks and organizational security requirements, and incorporating into a risk management framework that will guide your journey to AWS. It is often an effective practice to evolve your compliance mapping as you gain a better understanding of the needs of your workloads in the cloud and the security capabilities provided by AWS.

Another key element of your strategy is mapping out the shared responsibility model specific to your ecosystem. In addition to the macro relationship you share with AWS, you'll want to explore internal organizational shared responsibilities as well as those you impart upon your partners. Companies can break their shared responsibility model into three major areas: a control framework; a responsible, accountable, consulted, informed model (RACI); and a risk register. The control framework describes how the security aspects of the business are expected to work and what controls will be put in place to manage risk. You can use the RACI to identify and assign a person with responsibility for controls in the framework. Finally, use a risk register to capture controls without proper ownership. Prioritize residual risks that have been identified, aligning their treatment with new work streams and initiatives put in place to resolve them.

As you map these shared responsibilities you can expect to find new opportunities to automate operations and improve workflow between critical actors in your security, compliance, and risk management community. Figure 2 shows an example extended shared responsibility model.

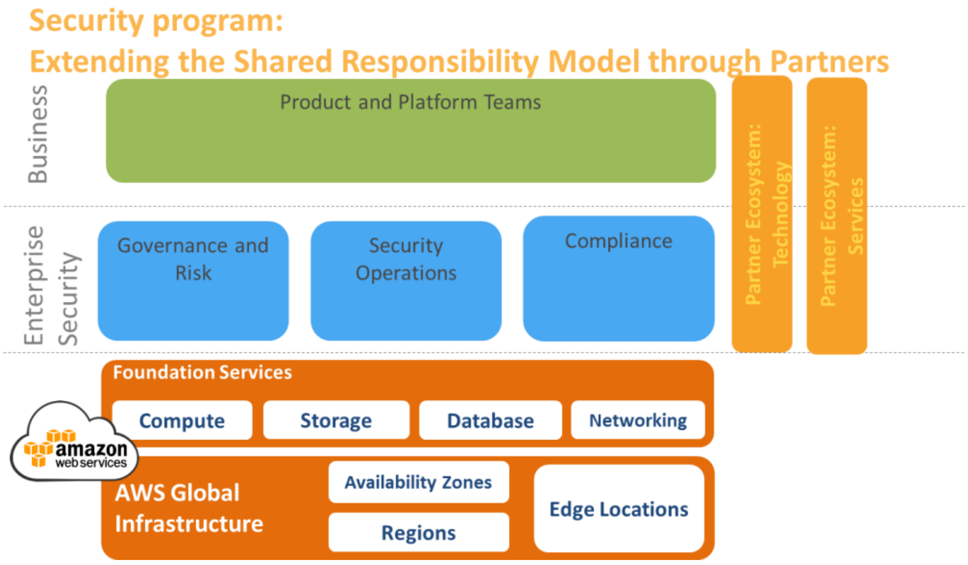


Figure 2: Example Shared Responsibility Model

Considerations

- **Do** create a tailored strategy that addresses your organizational approach to implementing security in the cloud.
- **Do** promote automation as an underlying theme for all your strategy.
- **Do** clearly articulate your approach to cloud first.
- **Do** promote agility and flexibility by defining guardrails.
- **Do** take strategy as a short exercise that defines your organization’s approach to information security in the cloud.
- **Do** iterate quickly while laying down what the strategy is. Your aim is to have a set of guiding principles that will drive the core of the effort forward – strategy is not the end in itself. Move quickly and be willing to adapt and evolve.
- **Do define** strategic principles which will impart the culture you want in security and which inform the design decisions you’ll make, rather than a strategy which implies specific solutions.

Taking the Journey – Delivering a Program

With a strategy in place, it is now time to put it into practice and initiate the implementation that will transform your security organization and secure the cloud journey. While you have a wide choice of options and features, your implementation should not be not a protracted effort. This process of designing and implementing how different capabilities will work together represents an opportunity to quickly gain familiarity and learn how to iterate your designs to best meet your requirements. Learn from actual implementation early, then adapt and evolve using small changes as you learn.

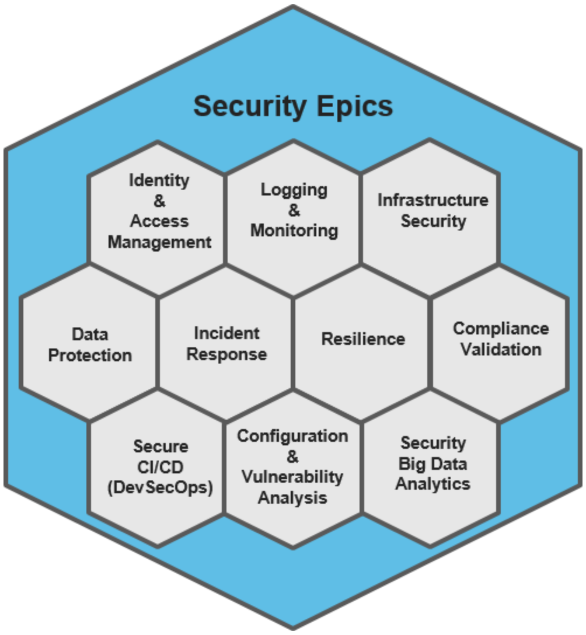


Figure 3: AWS CAF Security Epics

To help you with your implementation, you can use the CAF Security Epics. (See Figure 3.) The Security Epics consist of groups of user stories (use cases and abuse cases) that you can work on during sprints. Each of these epics has multiple iterations addressing increasingly complex requirements and layering in robustness. Although we advise the use of agile, the epics can also be treated as general work streams or topics that help in prioritizing and structuring delivery using any other framework. A proposed structure consists of the following 10 security epics (Figure 4) to guide your implementation.

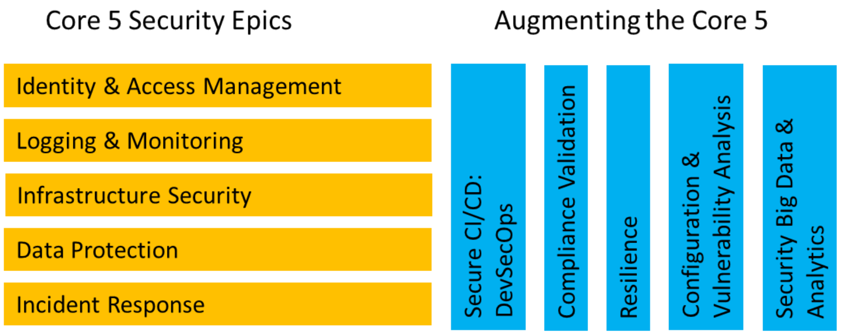


Figure 4: AWS Ten Security Epics

The Core Five

The following five epics are the core control and capability categories that you should consider early on because they are fundamental to getting your journey started.

- **IAM**—AWS Identity and Access Management (IAM) forms the backbone of your AWS deployment. In the cloud you must establish an account and be granted privileges before you can provision or orchestrate resources. Typical automation stories may include entitlement mapping/grants/audit, secret material management, enforcing separation of duties and least privilege access, just-in-time privilege management, and reducing reliance on long term credentials.
- **Logging and monitoring**—AWS services provide a wealth of logging data to help you monitor your interactions with the platform. The performance of AWS services based upon your configuration choices, and the ability to ingest OS and application logs to create a common frame of reference. Typical automation stories may include log aggregation, thresholds/alarming/alerting, enrichment, search platform, visualization, stakeholder access, and workflow and ticketing to initiate closed-loop organizational response.
- **Infrastructure security**—When you treat infrastructure as code, security infrastructure becomes a first tier workload that must also be deployed as code. This approach will afford you the opportunity to programmatically configure AWS services and deploy security infrastructure from AWS

Marketplace partners, or solutions of your own design. Typical automation stories may include creating custom templates to configure AWS services to meet your requirements, implementing security architecture patterns and security operations plays as code, crafting custom security solutions from AWS services, using patch management strategies like blue/green deployments, reducing exposed attack surface, and validating the efficacy of deployments.

- **Data protection**—Safeguarding important data is a critical piece of building and operating information systems, and AWS provides services and features giving you robust options to protect your data throughout its lifecycle. Typical automation stories may include making workload placement decisions, implementing a tagging schema, constructing mechanisms to protect data in motion such as VPN and TLS/SSL connections (including AWS Certificate Manager), constructing mechanisms to protect data at rest through encryption at appropriate tiers in your infrastructure, using AWS Key Management Service (AWS KMS) implementation/integration, deploying AWS CloudHSM, creating tokenization schemes, and implementing and operating of AWS Marketplace Partner solutions.
- **Incident response**—Automating aspects of your incident management process improves reliability and increases the speed of your response and often creates and environment easier to assess in after-action reviews. Typical automation stories may include using AWS Lambda function “responders” that react to specific changes in the environment, orchestrating auto scaling events, isolating suspect system components, deploying just-in-time investigative tools, and creating workflow and ticketing to terminate and learn from a closed loop organizational response.

Augmenting the Core

These five epics represent the themes that will drive continued operational excellence through availability, automation, and audit. You’ll want to judiciously integrate these epics into each sprint. When additional focus is required, you may consider treating them as their own epics.

- **Resilience**—High availability, continuity of operations, robustness and resilience, and disaster recovery are often reasons for cloud deployments with AWS. Typical automation stories may include using Multi-AZ and Multi-Region deployments, changing the available attack surface, scaling and shifting allocation of resources to absorb attacks, safeguarding exposed resources, and deliberately inducing resource failure to validate continuity of system operations.

- **Compliance validation**—Incorporating compliance end-to-end into your security program prevents compliance from being reduced to a checkbox exercise or an overlay that occurs post deployment. This epic provides the platform that consolidates and rationalizes the compliance artifacts generated through the other epics. Typical automation stories may include creating security unit tests mapped to compliance requirements, designing services and workloads to support compliance evidence collection, creating compliance notification and visualization pipelines from evidentiary features, monitoring continuously, and creating compliance-tooling-oriented DevSecOps teams.
- **Secure CI/CD (DevSecOps)** —Having confidence in your software supply chain through the use of trusted and validated continuous integration and continuous deployment tool chains is a targeted way to mature security operations practices as you migrate to the cloud. Typical automation stories may include hardening and patching the tool chain, least privilege access to the tool chain, logging and monitoring of the production process, security integration/deployment visualization, and code integrity checking.
- **Configuration and vulnerability analysis**—Configuration and vulnerability analysis gain big benefit from the scale, agility, and automation afforded by AWS. Typical automation stories may include enabling AWS Config and creating customer AWS Config Rules, using Amazon CloudWatch Events and AWS Lambda to react to change detection, implementing Amazon Inspector, selecting and deploying continuous monitoring solutions from the AWS Marketplace, deploying triggered scans, and embedding assessment tools into the CI/CD tool chains.
- **Security big data and predictive analytics**—Security operations benefit from big data services and solutions just like any other aspect of the business. Leveraging big data gives you deeper insights in a more timely fashion, thus enhancing your agility and ability to iterate on your security posture at scale. Typical automation stories may include creating security data lakes, developing analytics pipelines, creating visualization to drive security decision making, and establishing feedback mechanisms for autonomic response.

After this structure is defined, an implementation plan can be crafted. Capabilities change over time and opportunities for improvement will be continually identified. As a reminder, the themes or capability categories above can be treated as epics in an agile methodology, which contain a range of user stories including both use cases and abuse cases. Multiple sprints will lead to increased maturity while retaining flexibility to adapt to business pace and demand.

Example Sprint Series

Consider organizing a sample set of six two-week sprints (a group of epics driven over a twelve-week calendar quarter), including a short prep period, in the following way. Your approach will depend on resource availability, priority, and level of maturity desired in each capability as you move towards your minimally viable production capability (MVP).

- **Sprint 0**—Security cartography: compliance mapping, policy mapping, initial threat model review, establish risk registry; Build a backlog of use and abuse cases; plan the security epics
- **Sprint 1**—IAM; logging and monitoring
- **Sprint 2**—IAM; logging and monitoring; infrastructure protection
- **Sprint 3**—IAM; logging and monitoring; infrastructure protection
- **Sprint 4**—IAM; logging and monitoring; infrastructure protection; data protection
- **Spring 5**—Data protection, automating security operations, incident response planning/tooling; resilience
- **Sprint 6**—Automating security operations, incident response; resilience

A key element of compliance validation is incorporating the validation into each sprint through security and compliance unit test cases, and then undergoing the promotion to production process. When explicit compliance validation capability is required, sprints can be established to focus specifically on those user stories. Over time, iteration can be leveraged to achieve continuous validation and implementation of auto-correction of deviation where appropriate.

The overall approach aims to clearly define what an MVP or baseline is, which will then map to first sprint in each area. In the initial stages the end goal can be less defined, but a clear roadmap of initial sprints is created. Timing, experience, and iteration will allow refining and adjusting the end state to be just right for your organization. In reality, the final state may continuously shift, but ultimately the process does lead to continuous improvement at a faster pace. This approach can be more effective and have greater cost efficiency than a big bang approach based on long timelines and high capital outlays.

Diving a little deeper, the first sprint for IAM can consist of defining the account structure and implementing the core set of best practices. A second sprint can implement federation. A third sprint can expand account management to cater for multiple accounts, and so on. IAM user stories that may span one or more of these initial sprints could include stories such as the following:

“As an access administrator, I want to create an initial set of users for managing privileged access and federation identity provider trust relationships.”

“As an access administrator, I want to map users in my existing corporate directory to functional roles, or sets of access entitlements, on the AWS platform.”

“As an access administrator, I want to enforce multi-factor authentication on all interaction with the AWS console by interactive users.”

In this example, the following logging and monitoring user stories may span one or more initial sprints:

“As a security operations analyst, I want to receive platform-level logging for all AWS Regions and AWS Accounts.”

“As a security operations analyst, I want all platform-level logs delivered to one shared location from all AWS Regions and accounts.”

“As a security operations analyst, I want to receive alerts for any operation that attaches IAM policies to users, groups or roles.”

You can build capability in parallel or serial fashion and maintain flexibility by including security capability user stories in the overall product backlog. You can also split the user stories out into a security-focused DevOps team. These are decisions you can periodically revisit, allowing you to tailor your delivery to the needs of the organization over time.

Considerations

- **Do** review your existing control framework to determine how AWS services will be operated to meet your required security standards.
- **Do** define actors and then storyboard their experience interacting with AWS services.
- **Do** define what the first sprint is and what the initial high-level longer term goal will be.
- **Do** establish a minimally viable security baseline, and continually iterate to raise the bar for the workloads and data you’re protecting.

Taking the Journey – Develop Robust Security Operations

In an environment where infrastructure is code, security must also be treated as code. The Security Operations component provides a means to communicate and operationalize the fundamental tenets of security as code:

- Use the cloud to protect the cloud.
- Security infrastructure should be cloud-aware.
- Expose security features as services using the API.
- Automate everything, so that your security and compliance can scale.

To make this governance model practical, lines of business often organize as DevOps teams to build and deploy infrastructure and business software. You can extend the core tenets of the governance model by integrating security into your DevOps culture or practice; which is sometimes called DevSecOps. Build a team around the following principles:

- The security team embraces DevOps cultures and behaviors.
- Developers contribute openly to code used to automate security operations.
- The security operations team is empowered to participate in testing and automation of application code.
- The team takes pride in how fast and frequently they deploy. Deploying more frequently, with smaller changes, reduces operational risk and shows rapid progress against the security strategy.

Integrated development, security, and operations teams have three shared, key missions.

- Harden the continuous integration/ continuous deployment tool chain.
- Enable and promote the development of resilient software as it traverses the tool chain.
- Deploy all security infrastructure and software through the tool chain.

Determining the changes (if any) to current security practices will help you plan a smooth AWS adoption strategy.

Conclusion

As you embark on your AWS adoption journey, you will want to update your security posture to include the AWS portion of your environment. This Security Perspective whitepaper prescriptively guides you on an approach for taking advantage of the benefits that operating on AWS has for your security posture. Much more security information is available on the AWS website, where security features are described in detail and more detailed prescriptive guidance is provided for common implementations. There is also a comprehensive list of security-focused content[4] that should be reviewed by various members of your security team as you prepare for AWS adoption initiatives.

Appendix A: Tracking Progress Across the AWS CAF Security Perspective

You can use the key security enablers and the security epics progress model discussed in this appendix to measure the progress and the maturity of your implementation of the AWS CAF Security Perspective. The enablers and the progress model can be used for project planning purposes, to evaluate the robustness of implementations, or simply as a means to drive conversation about the road ahead.

Key Security Enablers

Key security enablers are milestones that help you stay on track. We use a scoring model that consists of three values: Unaddressed, Engaged, and Completed.

- Cloud Security Strategy [Unaddressed, Engaged, Completed]
- Stakeholder Communication Plan [Unaddressed, Engaged, Completed]
- Security Cartography [Unaddressed, Engaged, Completed]
- Document Shared Responsibility Model [Unaddressed, Engaged, Completed]
- Security Operations Playbook & Runbooks [Unaddressed, Engaged, Completed]
- Security Epics Plan [Unaddressed, Engaged, Completed]
- Security Incident Response Simulation [Unaddressed, Engaged, Completed]

Security Epics Progress Model

The security epics progress model helps you evaluate your progress in implementing the 10 Security Epics described in this paper. We use a scoring model of 0 (zero) through 3 to measure robustness. We provided examples for the Identity and Access Management and the Logging and Monitoring epics, so you could see how this progression works.

Core 5 Security Epics

0- Not addressed

1- Addressed in architecture and plans

2- Minimal viable implementation

3- Enterprise ready production implementation

Security Epic	**0**	**1**	**2**	**3**
Identity and Access Management	Example: No relationship between on-premises and AWS identities.	Example: An approach is defined for workforce lifecycle identity management. IAM architecture is documented. Job functions are mapped to IAM policy needs.	Example: Implemented IAM as defined in architecture. IAM policies implemented that map to some job functions. IAM implementation validated.	Example: Automation of IAM lifecycle workflows.
Logging and Monitoring	Example: No utilization of AWS provided logging and monitoring solutions.	Example: An approach is defined for log aggregation, monitoring, and integration into security event management processes.	Example: Platform-level and service-level logging is enabled and centralized.	Example: Events with security implications are deeply integrated into security workflow and incident management processes and systems.
Infrastructure Security				
Data Protection				
Incident Management				

Augmenting the Core 5

0- Not addressed

1- Addressed in architecture and plans

2- Minimal viable implementation

3- Enterprise ready production implementation

Security Epic	0	1	2	3
Resilience				
DevSecOps				
Compliance Validation				
Configuration & Vulnerability Management				
Security Big Data				

CAF Taxonomy and Terms

The Cloud Adoption Framework (CAF) is the framework AWS created to capture guidance and best practices from previous customer engagements. An AWS CAF *perspective* represents an area of focus relevant to implementing cloud-based IT systems in organizations. For example, the Security Perspective provides guidance and process for evaluating and enhancing your existing security controls as you move to the AWS environment.

Each CAF Perspective is made up of components and activities. A *component* is a sub-area of a perspective that represents a specific aspect that needs attention. This whitepaper explores the components of the Security perspective. An *activity* provides more prescriptive guidance for creating actionable plans that the organization can use to move to the cloud and to operate cloud-based solutions on an ongoing basis.

For example, *Directive* is one component of the Security Perspective and tailoring an AWS shared responsibility model for your ecosystem may be an activity within that component.

When combined, the Cloud Adoption Framework (CAF) and the Cloud Adoption Methodology (CAM) can be used as guidance during your journey to the AWS cloud.

Notes

[1] https://d0.awsstatic.com/whitepapers/aws_cloud_adoption_framework.pdf

[2] https://aws.amazon.com/compliance/

[3] https://aws.amazon.com/compliance/shared-responsibility-model/

[4] https://aws.amazon.com/security/security-resources/