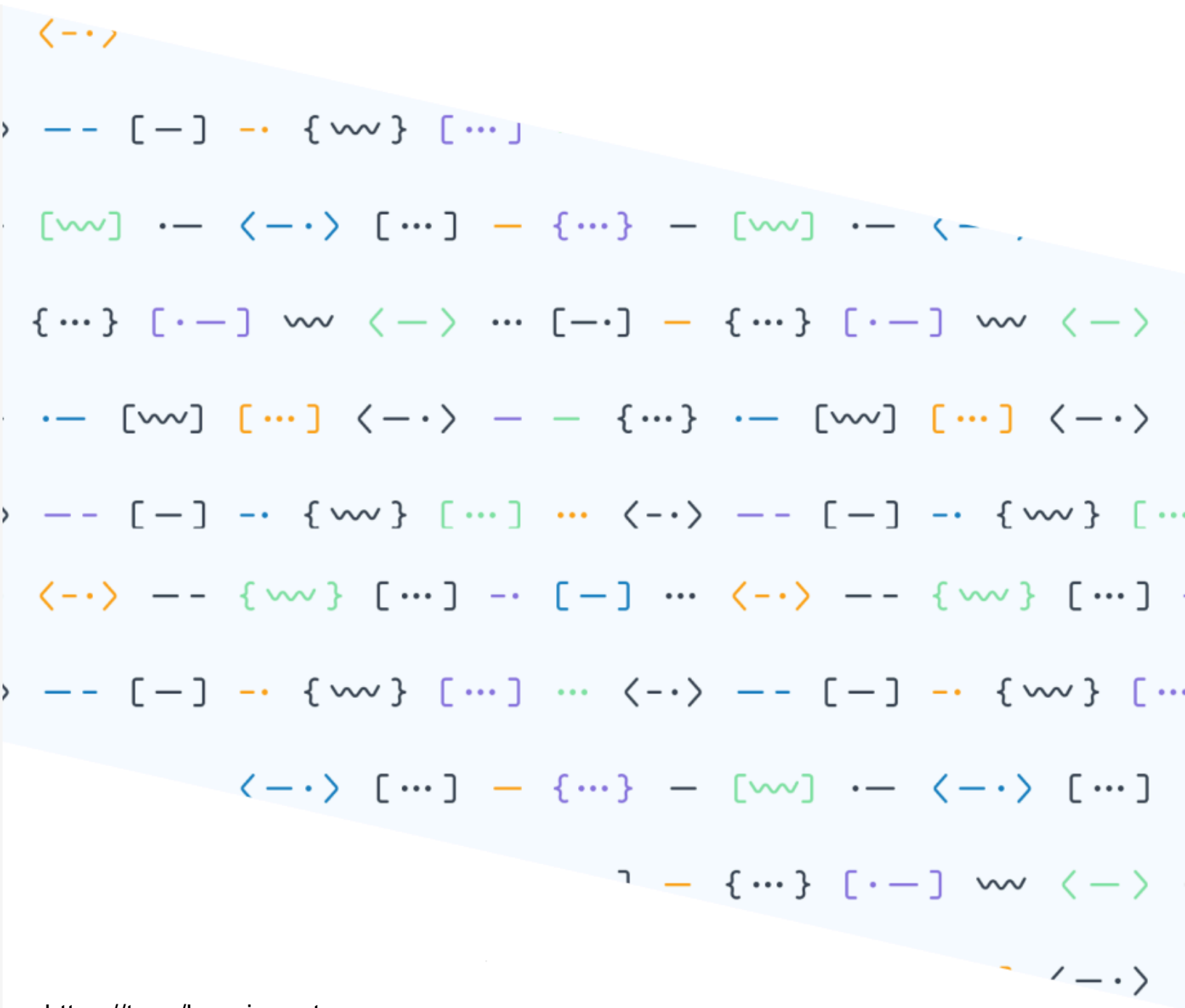
aws

Crawl, walk, run: Accelerating security maturity in the AWS Cloud

AWS Prescriptive Guidance



AWS Prescriptive Guidance: Crawl, walk, run: Accelerating security maturity in the AWS Cloud

Table of Contents

Crawl, walk, run: Accelerating security maturity in the AWS Cloud

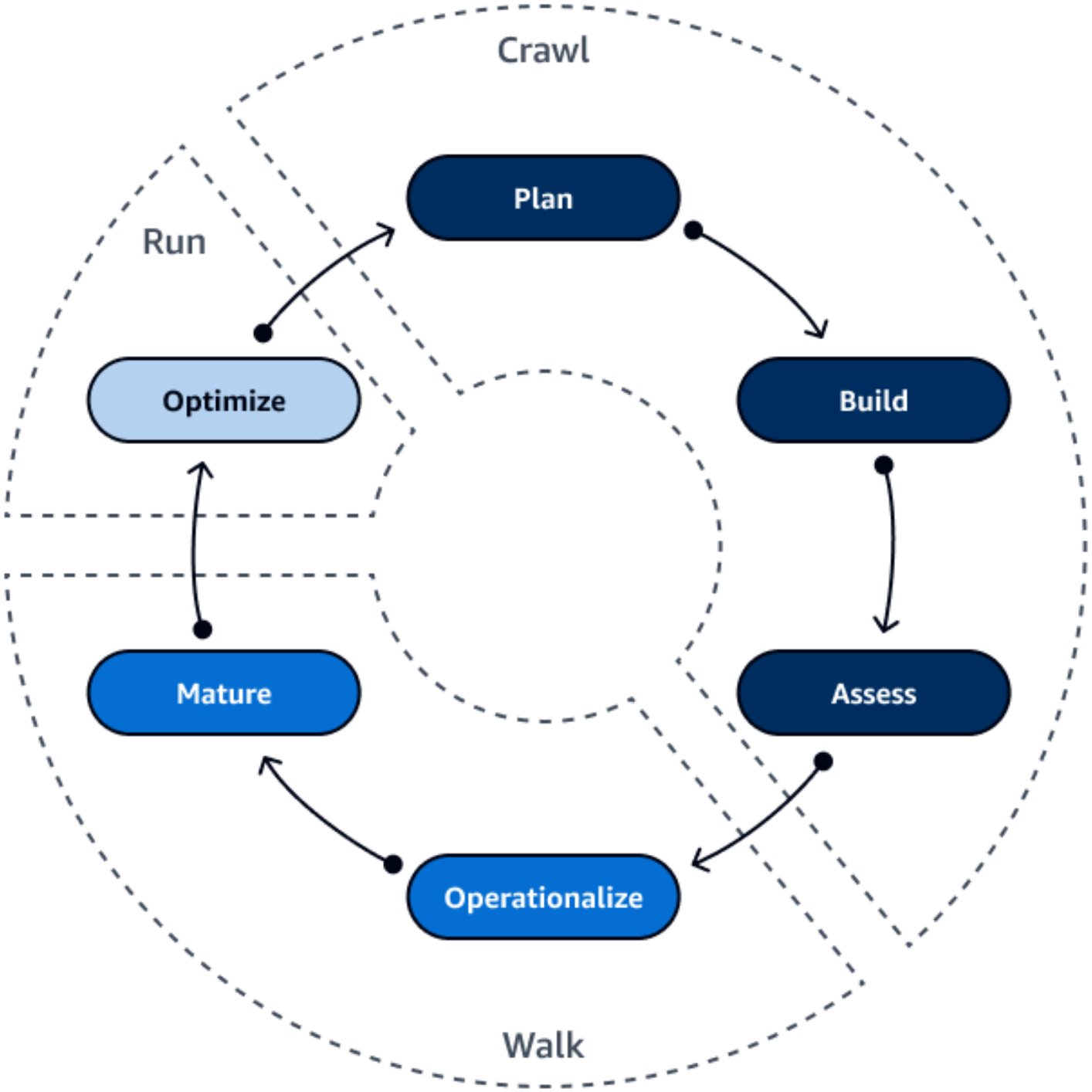
Amazon Web Services (AWS)

December 2023 (document history)

For many organizations, security is the number one priority and consideration when migrating to the cloud. Implementing cloud security capabilities and controls is not a one-time activity—it's an iterative model. You gradually increase your security posture and maturity as you increase cloud operations. For example, you might start with AWS managed policies and then, when your organization is ready, you can implement custom policies that follow the principle of least privilege.

This guide provides a roadmap for using a *crawl, walk, run* methodology to accelerate your organization's maturity in cloud security. It defines a step-by-step approach to automate security capabilities. It also pragmatically explains how to get the most functionality out of AWS services and features. This guide helps you understand the challenges and opportunities in the cloud and how to quickly move forward and achieve success with AWS.

A cloud journey requires building frameworks, managing and maturing operations, and optimizing processes. The following image shows the phases in each stage of the crawl, walk, run methodology: plan, build, assess, operationalize, mature, and optimize.



The crawl stage consists of planning, building the foundation, and assessing your current security posture. In the walk stage, you operationalize your people, processes, and technology, and then you mature your operations through tuning and measurement. The run stage consists of optimizing through assessment and automation.

Crawl stage: Planning, building, and assessing

The crawl stage starts with planning. Planning involves determining the security scope and choosing the model that best fits your organization. After you establish the plan, you can start building a foundation. This is followed by assessing your current security posture and setting up a discipline as soon as you build the security infrastructure. The crawl stage is iterative. Iteration in the cloud is faster than iteration in an on-premises environment. As you mature your cloud capabilities, the process for iteration accelerates.

The following are the phases in the crawl stage:

- Plan – How do you figure out your scope and select a model?
- Build – How are you going to establish the framework?
- Assess – What is your current security posture?

Plan: Establishing your security scope and model

Planning is an iterative process as you mature your security model. Key steps in the planning process include:

- Understanding the security scope – Security scope varies and depends on how the cloud is used.
- Choosing a security model – Identify the best-fitting security model for your security use case.
- Creating a business objective model – Define clear goals and mechanisms to measure success.

As you develop your plan, consider the following:

- Be willing to iterate. Iteration is constant in the cloud. Iteration helps you identify gaps in the plan.
- Do not start with services. Start with your plan instead of picking out what services you need. This helps drive your organization to its intended outcomes.

Understanding the security scope

The AWS shared responsibility model defines how you share responsibility with AWS for security and compliance in the cloud. AWS secures the infrastructure that runs all of the services offered in the AWS Cloud, and you are responsible for securing your use of those services, such as your data and applications.

This shared model can help relieve your compliance and operational burden because AWS operates, manages, and controls many components, from the host operating system and virtualization layer down to the physical security of the facilities in which the service operates. Managed services help you reduce your security and compliance obligations by allowing AWS to manage some security tasks, such as patching and vulnerability management. Using managed services is a best practice in the AWS Well-Architected Framework. In general, as infrastructure is modernized, more responsibility is shifted onto the service provider.

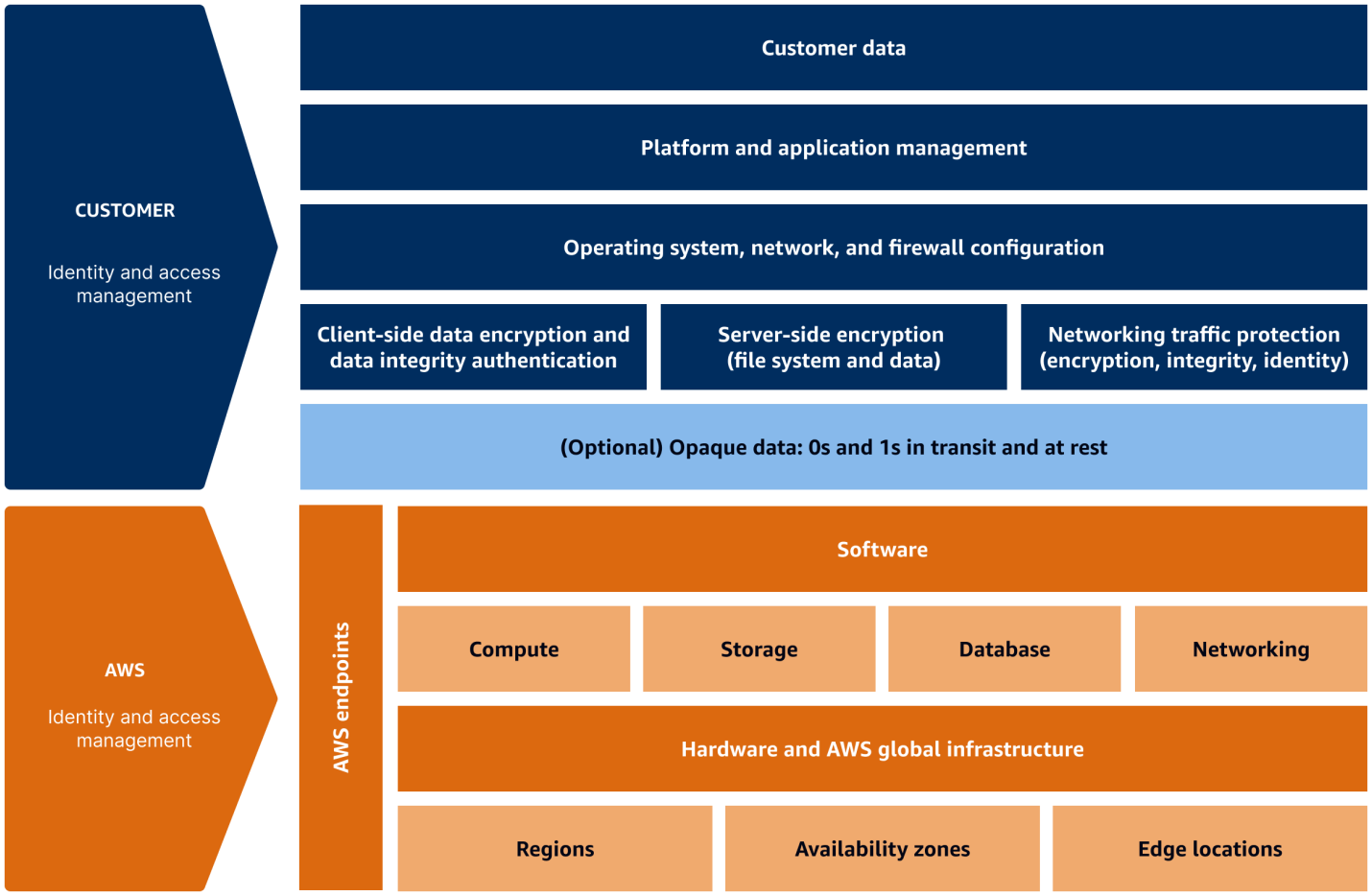
The following are three different service examples to help you understand how your security scope changes based on which services you choose:

- Infrastructure services
- Container services
- Serverless services

Your responsibility for security is not static, and it changes with the type of architecture that you select. Your time, effort, and costs are affected by the cloud architecture you choose.

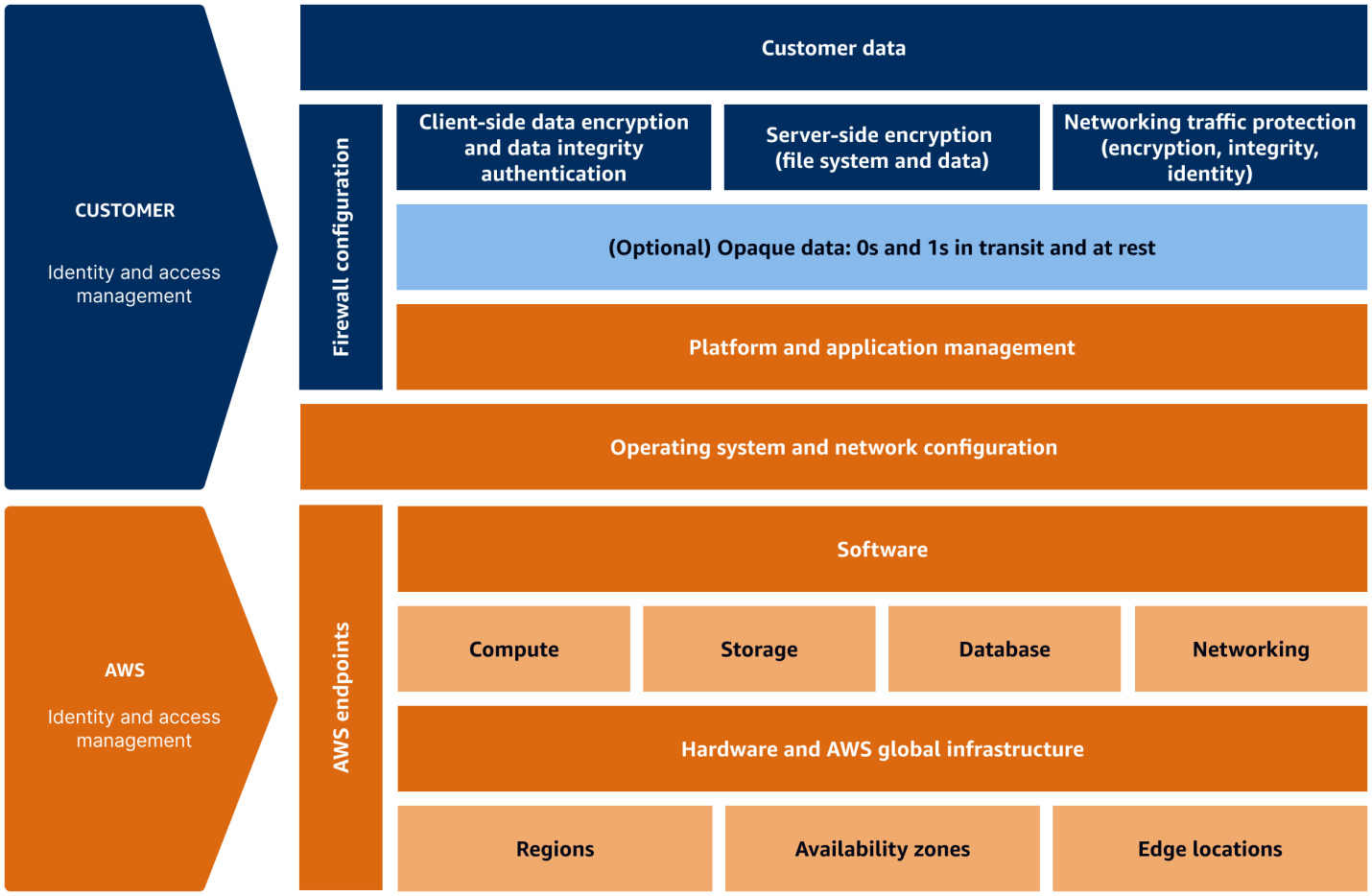
Infrastructure services

For infrastructure services, AWS focuses on securing the underlying infrastructure. Within infrastructure services, the scope is larger for the customer because they need to address platform security, OS patching, and application management, as compared to the other models. Amazon Elastic Compute Cloud (Amazon EC2) is an example of a common infrastructure service.



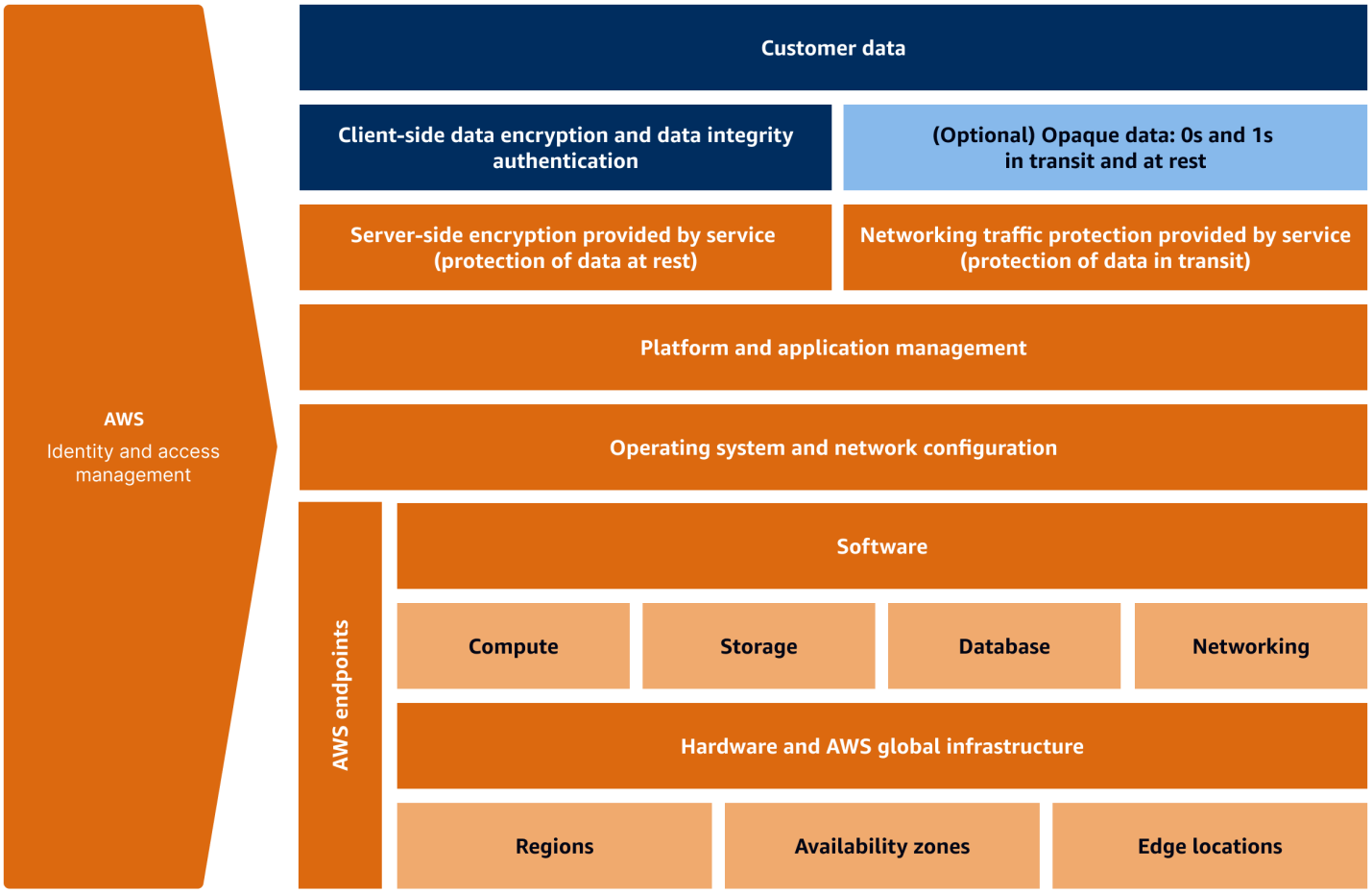
Container services

As the infrastructure becomes more abstracted and modernized, the footprint becomes smaller. Your scope shrinks because responsibility for some security elements shifts to AWS. Container services is an example which some of the backend responsibilities shift back to AWS. For example, AWS becomes responsible for the operating system (OS) configuration, network configuration, platform management, and application management. Examples of common container services include Amazon Elastic Kubernetes Service (Amazon EKS), Amazon Elastic Container Registry (Amazon ECR), Amazon Elastic Container Service (Amazon ECS), and AWS Fargate.



Serverless services

When using serverless services, nearly all of the responsibility for security belongs to AWS. The scope of your responsibility is minimal. For example, a managed serverless database (DB) eliminates the need for you to secure the network, hardware, and operating system. All OS and DB patching is covered by AWS. Your only concern is securing access to the data through encryption and authentication.



Choosing a security model

You can choose from various security models or approaches for AWS. The choice of approach and the best-fitting model depends on your audience, the target business outcomes, and the overall business process. It is possible to use a blend of multiple models.

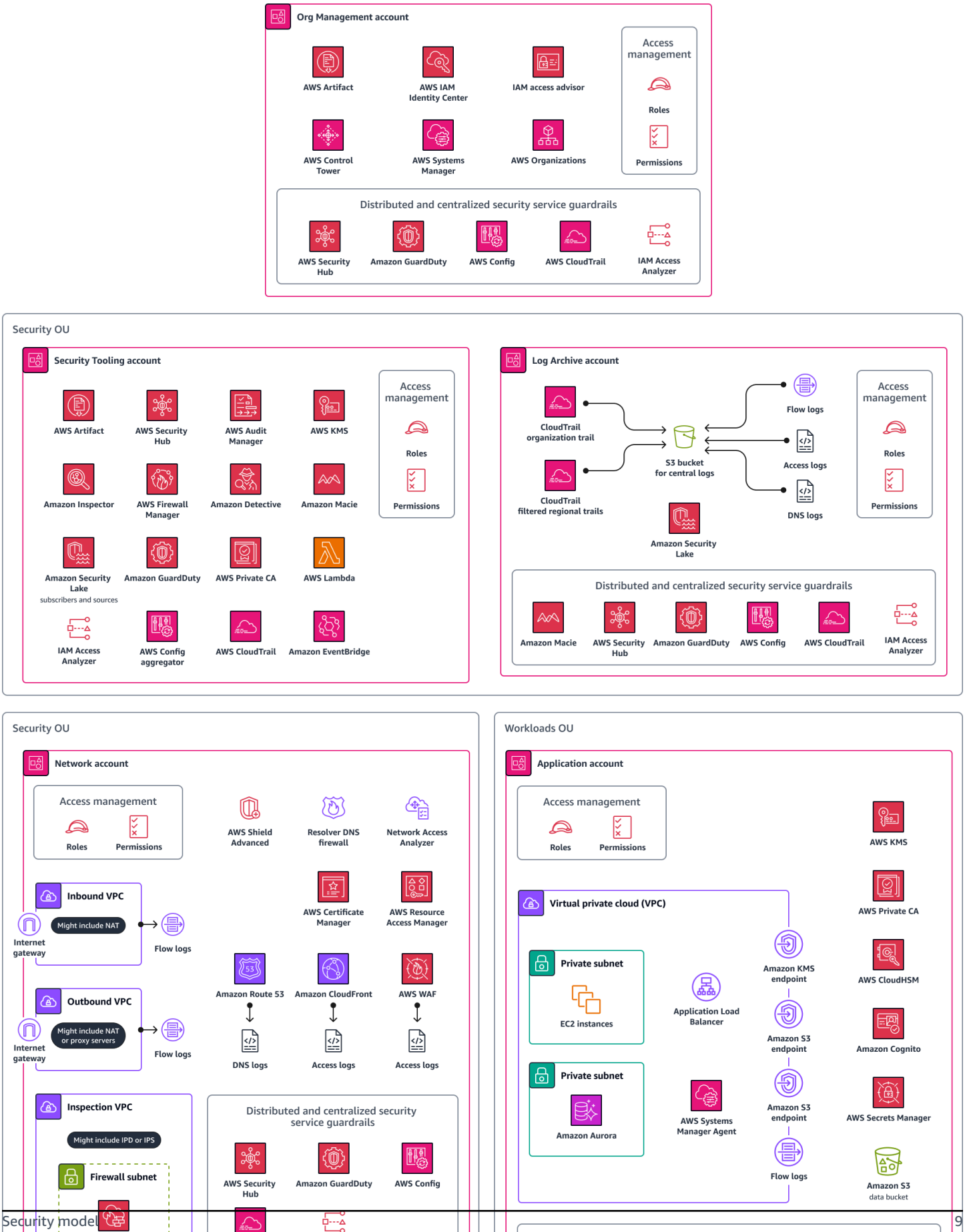
The following are a few common models:

- Architectural model
- Maturity model
- Governance model

Each model has its own set of benefits and drawbacks. It is important to consider which approach is best suited for your organization. Involve security professionals early in the process of modernizing your infrastructure and adopting cloud strategies. The model you choose has a significant impact on the roles and responsibilities within your organization.

Architectural model

The following image shows the AWS Security Reference Architecture. This architectural approach provides a blueprint for a security model. This approach is best suited when you are engaging with technical teams within your organization. It helps set an ideal future-state goal. It also aligns with many compliance and AWS frameworks.



Advantages of the architectural model:

- Aligns with Health Insurance Portability and Accountability Act (HIPAA) and Health Information Trust Alliance Common Security Framework (HITRUST CSF) requirements
- Provides an architectural perspective
- Aligns to cloud strategies and guidance for large enterprises
- Aligns with the AWS Cloud Adoption Framework (AWS CAF)
- Aligns with the AWS Well-Architected Framework

Disadvantage of the architectural model:

- Is technology-focused rather than business-focused

Maturity model

The AWS Security Maturity Model approach focuses on managing and reducing risk by prioritizing the implementation of security measures. This approach is well-suited for security directors and CISOs, but it's not business-focused.

Advantages of the maturity model:

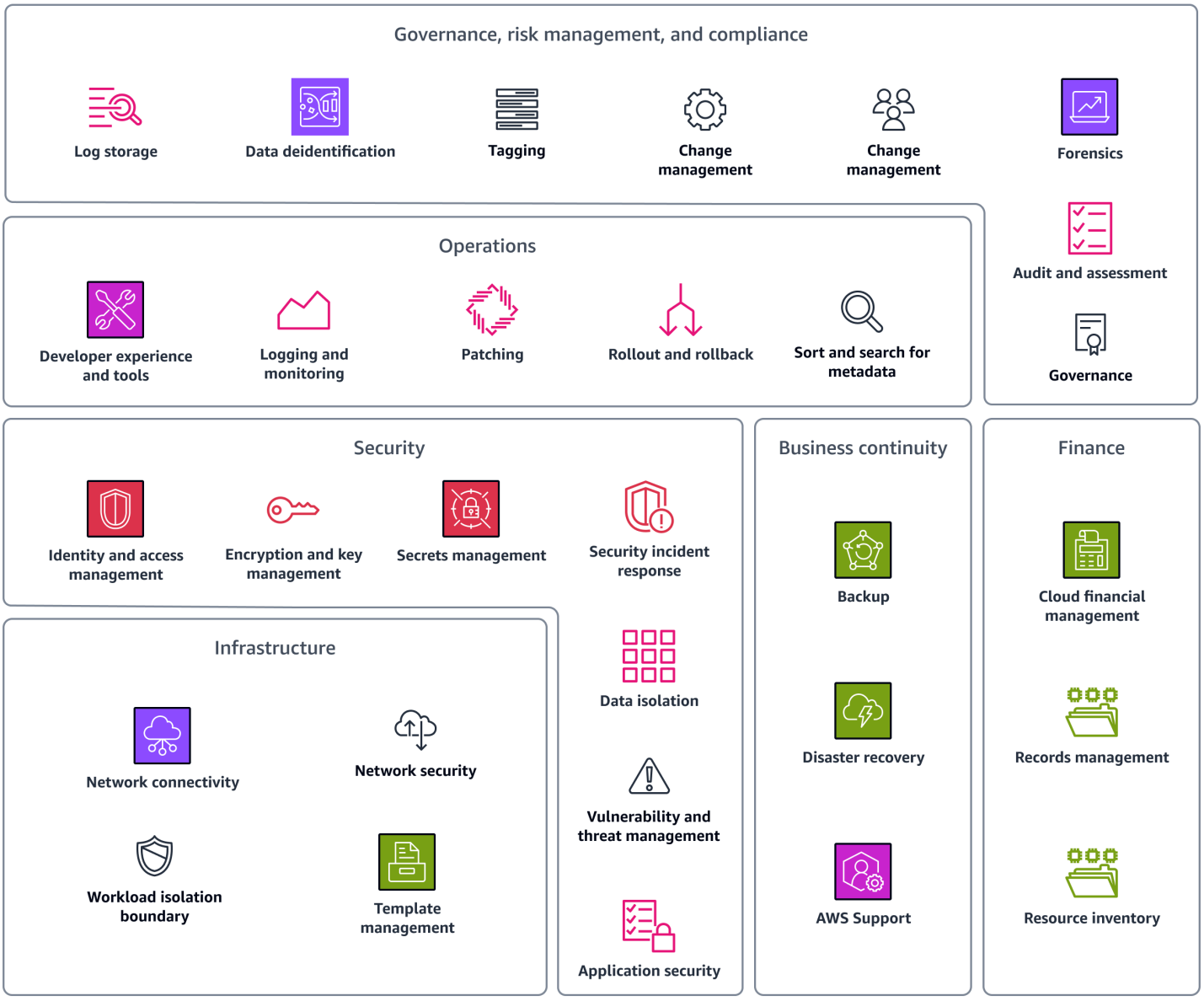
- Is security focused
- Is a model that focuses on using an agile-based implementation approach
- Helps you quickly reduce risk
- Aligns with the AWS Cloud Adoption Framework (AWS CAF)

Disadvantages of the maturity model:

- Is technology-focused rather than business-focused

Governance model

The Cloud Foundation on AWS model uses a governance, risk management, and compliance (GRC) approach to help organizations meet security and compliance requirements. It defines the overall policies your cloud environment should follow. The capabilities within this model help you define action items, define your risk appetite, and align internal policies.



The Cloud Foundation model is a capability and governance guide that helps you build and evolve your AWS Cloud environment. It is based on a set of definitions, scenarios, guidance, and automations. The guide includes the people, process, and technology aspects of establishing an AWS Cloud environment. It covers six categories of capabilities that are essential for a cloud foundation:

- Governance, risk management, and compliance
- Operations
- Security
- Business continuity

- Finance
- Infrastructure

The guide also provides examples, timelines, and further reading for each capability.

Advantages of the governance model:

- Has a broad technology focus
- Is designed for reliability
- Uses an operational approach

Disadvantage of the governance model:

- Is technology-focused rather than business-focused

Creating a business objective model

The business objective model involves defining business outcomes. It is similar to the AWS Cloud Adoption Framework and the AWS Well-Architected Framework. This approach focuses on what the business is interested in by interpreting the target business outcomes. The value of this approach is that it is easy to tie business objectives to security objectives. An example of a business objective is "Enable secure external connections and accelerated provisioning of new users and environments, by automating visibility and measuring against best practices to continuously drive down risk." You establish technology objectives that help you meet corresponding business outcomes. The business objective model ties back to security objectives, such as maintaining visibility. You then implement a technical objective, such as AWS Identity and Access Management (IAM) security best practices, in order to reduce security risk.

Advantages of business objective approach:

- Includes cost justification
- Provides a clear, business-aligned security direction
- Defines measures of success through achieving target business outcomes

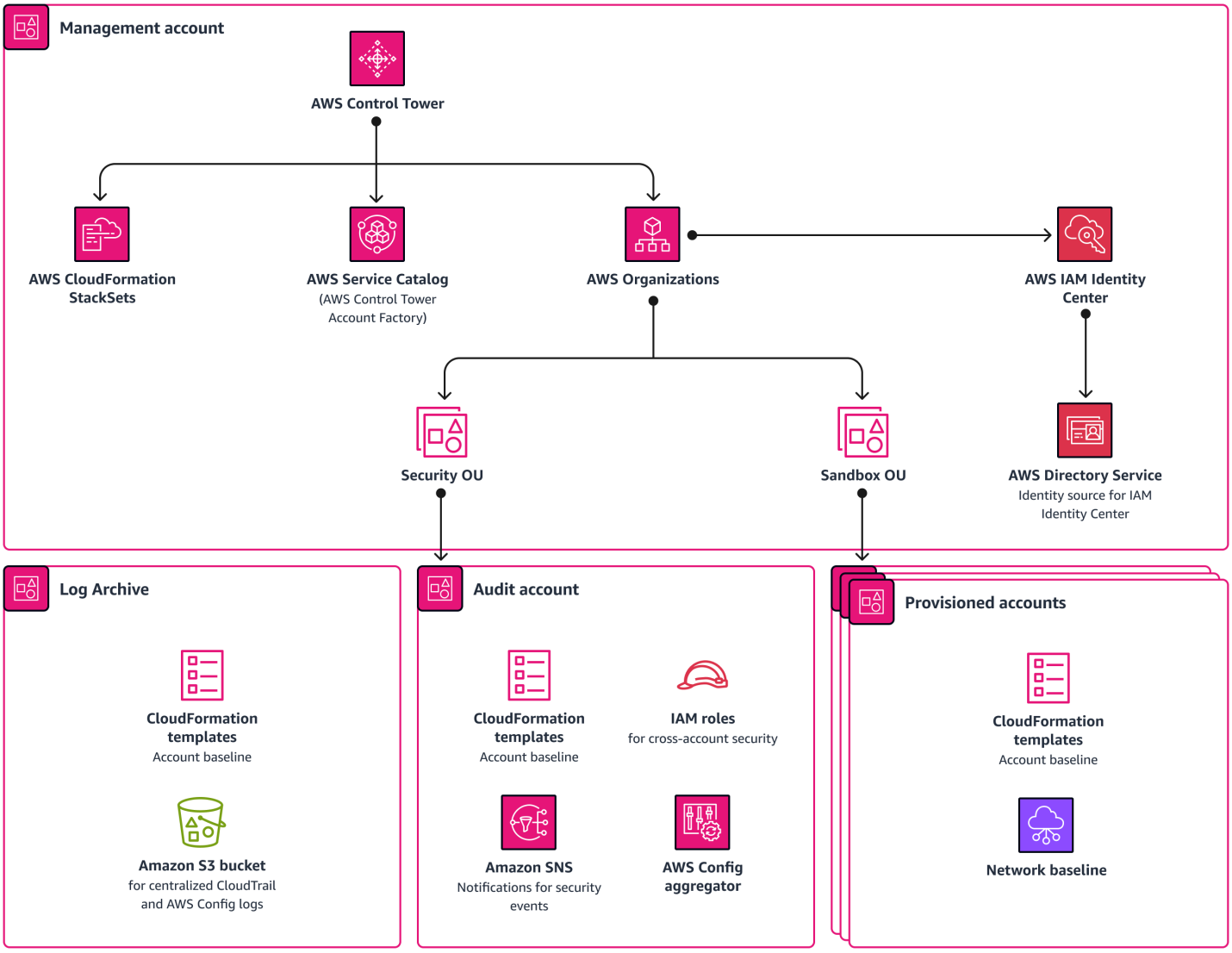
Disadvantages of business objective approach:

- Can be time consuming because you have to figure out what the business wants

- Is business-focused rather than technology-focused

Build: Laying the groundwork for a strong cloud security foundation

Now that you have a plan, the next step is laying the groundwork. This step demonstrates how to build an initial cloud foundation on AWS that is secure, resilient, scalable, and automated across multiple accounts. Laying the groundwork can be specifically designed and customized according to your business goals. You can adapt controls to a new landing zone, or you can include them in an existing landing zone. The automations in AWS Control Tower can help you lay the security groundwork in the AWS Cloud. The following image shows a landing zone that is set up through AWS Control Tower.



AWS Control Tower orchestrates multiple AWS services on your behalf, such as AWS Organizations, AWS Service Catalog, and AWS IAM Identity Center. You can set up a new landing zone within an hour, and that landing zone is designed to meet your security and compliance requirements. AWS Control Tower sets up your landing zone according to prescriptive security best practices. AWS Control Tower helps you manage cloud provisioning by enhancing visibility and control over accounts and end users. It helps administrators efficiently allocate and oversee compute resources, implement role-based access control, monitor performance through logging and monitoring tools, effectively manage costs, automate deployment processes, enforce security measures, and ensure compliance to industry standards.

AWS Control Tower is the fastest way to set up and govern a secure, compliant, multi-account AWS environment based on best practices. For more information about the working with AWS Control

Tower and the best practices outlined in the AWS multi-account strategy, see AWS multi-account strategy: Best practices guidance.

Although AWS Control Tower is the fastest approach, it's not the only one. The important part is that you set up a landing zone that, at a minimum, provides the following:

- Multi-account management
- Identity and federated access management
- A centralized archive for logs
- Cross-account audit access
- End-user account provisioning
- Centralized monitoring and notifications

Assess: Evaluating your current cloud security posture

Before you deploy anything to the landing zone, assess your landing zone to make sure it meets your requirements and to establish a baseline. This practice is called a *cloud posture assessment*. It helps you identify and remediate risks across your cloud infrastructure. Assessing your cloud security posture provides visibility of the relevant security controls in the cloud environment.

The following are the benefits of a cloud posture assessment:

- It helps you understand your current security posture and get recommendations to reduce your risk profile, remediate existing vulnerabilities, or correct misconfigurations.
- It helps you identify security best practices so that you can avoid missteps and reduce business risks.
- It provides metrics that help you track improvement and measure success.

This section reviews services and tools, AWS Security Hub and Prowler, that you can use to perform a cloud posture assessment in your environment.

Prowler

Prowler is an open source command-line tool that helps you assess, audit, and monitor your accounts for adherence to AWS security best practices and other security frameworks and standards. It inspects your configuration and identifies security issues. You can use Prowler in

multi-account environments, and third-party vendors can also use it to assess the security of your AWS environment.

The following are the benefits of Prowler:

- It is free and open source.
- It has flexible deployment options and is scalable.
- It runs compliance checks, such as for Center for Internet Security (CIS) Benchmark for AWS, General Data Protection Regulation (GDPR), and HIPAA.
- It helps you create snapshots and baselines.

Prowler Pro is also an option for continuous assessment. Prowler Pro runs over 250 checks, and it provides faster scanning and dashboards that help you visualize scan results.

AWS Security Hub

AWS Security Hub provides a comprehensive view of your security state in AWS. It also helps you check your environment against security industry standards and best practices. It is integrated with AWS Control Tower so that you can configure Security Hub detective controls through the AWS Control Tower service. The objective of accelerating security maturity is to mature the assessment process from a one-time snapshot to a continuous process for monitoring progress.

The following are the benefits of Security Hub:

- It provides a unified dashboard that shows current status of the environment and helps you identify and remediate issues.
- It performs continuous assessments with automated checks.

Walk stage: Operationalizing and maturing

The walk stage focuses on operationalization. During this stage, your organization needs to evaluate its current operating model, determine how it should be adapted for the cloud, implement those changes, and then measure progress. This includes addressing skills, operating processes, and technology. Tuning the cloud deployment and measuring progress is vital throughout the walk stage to validate success.

The following are the phases in the walk stage:

- Operationalize – How do you prepare your people, technology, and processes for the cloud?
- Mature – How do you measure progress and success?

Operationalize: Preparing your organization for a mature cloud security posture

In order to move forward with the process of deploying operational loads into the cloud, it is important to focus on the alignment of people, process, and technology. This is particularly crucial in the cloud environment because processes and skills likely differ from on-premises operations. In this section, you use a framework to align your people, processes, and technology, and then you confirm that the framework has helped you achieve your expected outcomes.

AWS Cloud Adoption Framework

The AWS Cloud Adoption Framework (AWS CAF) helps you accelerate your business outcomes through innovative use of AWS services and features. AWS CAF identifies six specific organizational perspectives that underpin successful cloud transformations: Business, People, Governance, Platform, Security, and Operations. Each perspective contains capabilities that can improve your cloud readiness and help you accelerate your cloud transformation journey.

The following image shows the six perspectives in the AWS CAF and the capabilities in each perspective. For more information, see Foundational capabilities in *An Overview of the AWS Cloud Adoption Framework*.

Expected outcomes

When you use the AWS CAF to align your people, processes, and technology, you can expect to achieve the following outcomes:

- **DevSecOps pipeline and process** – Implementing a DevOps pipeline with integrated security tools can help you more securely deploy infrastructure as a code (IaC). You can implement code-

scanning and security checks in the pipeline process, such as cfn_nag (GitHub), which is an open source static code analyzer.

- **Tagging and asset management** – Tags can help you more efficiently and consistently manage resources in the cloud. For more information, see Tagging your AWS resources. It's important to develop a dynamic asset management strategy that can adapt to the constantly changing nature of the cloud. AWS Systems Manager Inventory helps you assign tags so that you can quickly search, manage, and identify your resources.
- **Monitoring and detective integration** – It is crucial to establish a method for sending alerts from the cloud to on-premises security operations centers (SOCs) and security information and event management (SIEM) systems. Amazon GuardDuty is a continuous security monitoring service that analyzes and processes logs to identify unexpected and potentially unauthorized activity in your AWS environment. It also integrates with many third-party tools.
- **Cloud incident response plan and program** – It is important to make sure that the personnel responsible for handling the cloud alerts are familiar with the process of ingesting those alerts and know how to respond to cloud alerts, as compared to on-premises alerts. To improve incident response capabilities, train personnel to use Amazon Detective for log analysis. Amazon Detective helps you analyze, investigate, and identify the root cause of security findings or suspicious activities. Amazon Detective should be part of an incident response plan.
- **Cloud vulnerability management** – The process of managing vulnerabilities in the cloud differs from on-premises environments. In addition to traditional vulnerability management, you also must assess the infrastructure code layer. Amazon Inspector is an automated vulnerability management service that continually evaluates your resources for vulnerabilities and unintended network exposure.
- **Cloud posture management** – Cloud posture management, as described in the Assess section, is an important aspect of cloud security. You can use AWS Security Hub to automate security best practice checks and evaluate your overall cloud posture across all of your AWS accounts.
- **Cloud security training** – It is essential to provide appropriate training to employees so they become proficient in cloud security. This includes providing access to resources and allocating time for employees to acquire the necessary knowledge and skills. AWS provides many training resources to upskill and educate, such as AWS Skill Builder.

Mature: Tuning and measuring processes, tools, and risk

In the mature phase of the cloud security model, the focus is on aligning security teams with the AWS Cloud Adoption Framework (AWS CAF) security capabilities and on instituting agile

processes. This alignment helps specialized teams accelerate innovation in short sprints while also incorporating roadmaps and long-range planning. The mature phase emphasizes collaboration with IT operations and scaling up deep, specialized cloud skills. Each security capability implements key tools and processes to enhance efficiency and impact, accompanied by the development of metrics and reporting mechanisms to measure incremental changes and overall impact.

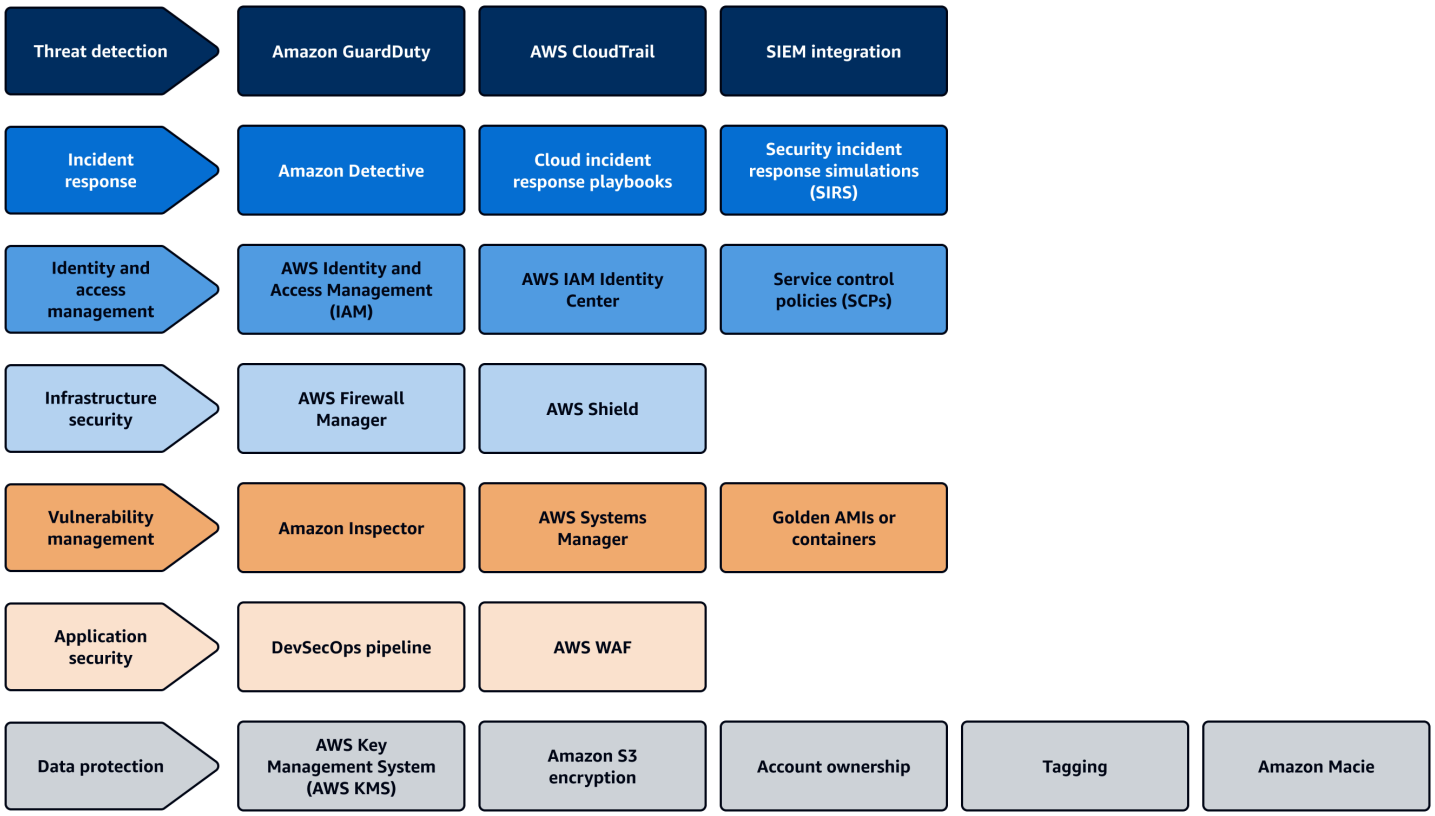
In this phase, you:

- Tune and measure processes
- Tune and measure tools
- Tune and measure risk
- Review examples of use cases in the mature phase

Tune and measure processes

The agile approach provides more flexibility and innovation, and it can help you quickly test and implement new ideas. Divide your security teams into specialized roles, such as incident responders and vulnerability managers. The roles should align with the categories in the following image, which correspond to the capabilities in the AWS Cloud Adoption Framework (AWS CAF). The agile approach encourages teams to think big, invent, simplify, and identify potential gaps in security. This results in the creation of a backlog of user stories or roadmaps for future improvements.

An agile process allows for more dynamic and adaptive solutions, instead of relying solely on the capabilities of a specific tool. *Fail fast* is a philosophy that uses frequent and incremental testing to reduce the development lifecycle, and it is a critical part of an agile approach. Make a change, test it out, and then decide whether to continue with the current approach or switch to an alternate one. If the teams work in this cycle, it helps your organization stay current with the fast-paced nature of the cloud. Focused training is also crucial, and you should provide training that is specific to a particular domain of cloud security.



> **Note**
>
> This image doesn't contain the security assurance and security governance capabilities in the AWS CAF. This guide focuses on security operations, and security assurance and governance are outside the scope of this guide. For more information about security assurance, see AWS re:Inforce 2023 - Scaling compliance with AWS Control Tower on YouTube.

In your organization, use an agile approach that helps your organization keep up with rapid development and change in the cloud. The following are some ways to start experimenting and iterating in your cloud environment:

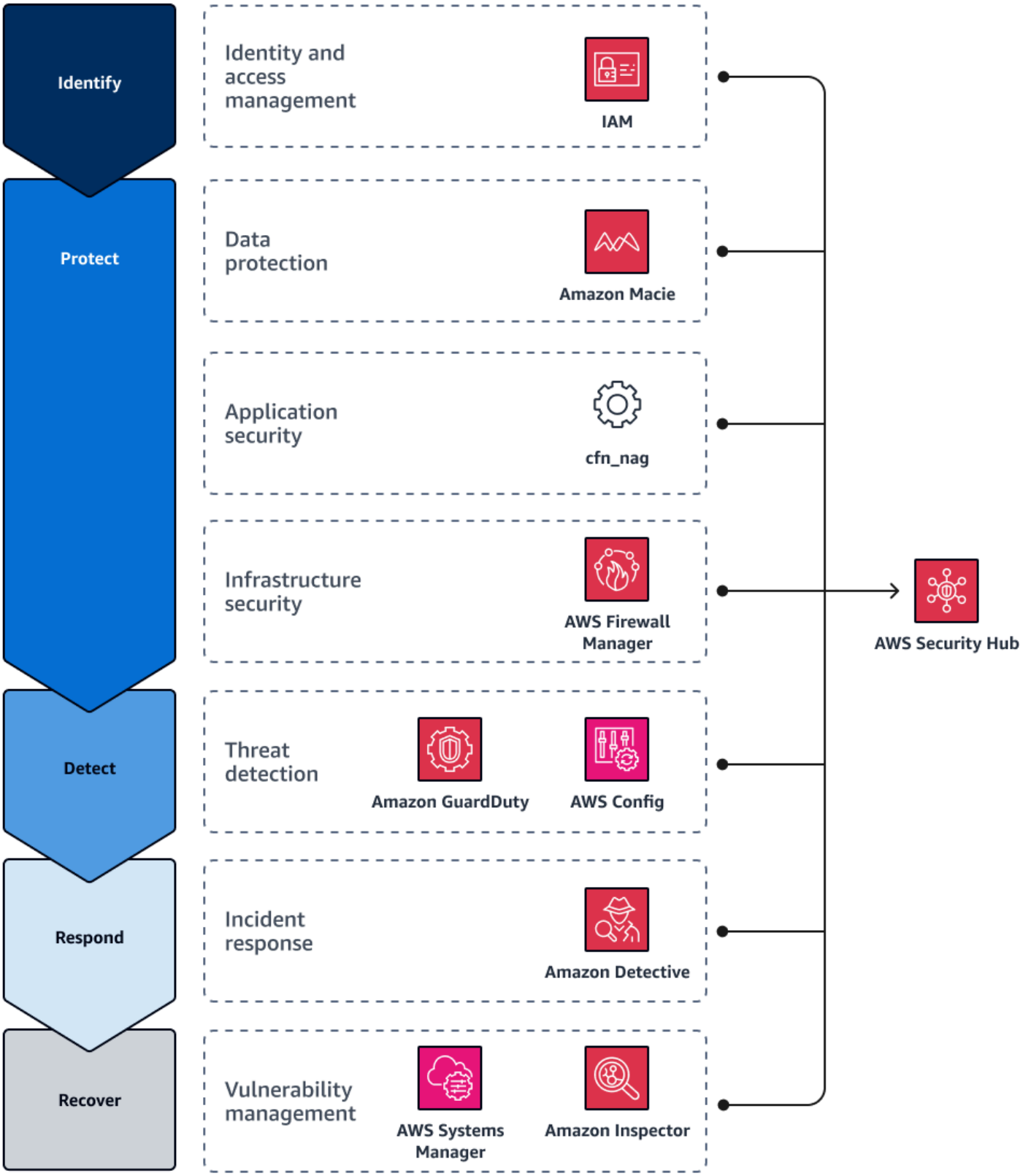
- Specialize on the categories defined in AWS CAF, as shown in the previous image.
- To be more dynamic, focus on innovating instead of operations.
- Move quickly in sprints by allowing people to test, fail fast, and implement quickly and continue with this cycle to keep up with the business.

- To support continuous operations, where possible, align processes for cloud-based and on-premises environments.
- To help individuals drill down and focus on one area, provide focused training instead of broad training.
- Encourage people to think big, investigate "what ifs," and create backlogs (such as roadmaps or gaps).

Tune and measure tools

After you establish specialized teams for different security domains, align the teams with each other. AWS Security Hub can help you achieve this. Security Hub provides a centralized, unified dashboard to monitor progress against frameworks. It also integrates with AWS security services any many third-party tools.

The National Institute of Standards and Technology (NIST) Cybersecurity Framework on the NIST website is comprised of five functions: identify, protect, detect, respond, and recover. The following image shows how you can use different AWS services during each function and then configure those services to send their findings to Security Hub for consolidated reporting. If you choose to use other tools, you can use the Security Hub API, AWS Command Line Interface (AWS CLI), and AWS Security Finding Format (ASFF) to create custom integrations. For more information about Security Hub integrations with other services, see Product integrations in AWS Security Hub in the Security Hub documentation.



Security Hub integrates with all of these services and tools and provides the following:

- Provides a unified dashboard that shows updates and helps teams to iterate in place
- Automatically integrates with AWS security services, such as Amazon Macie, Amazon GuardDuty , and Amazon Detective
- Supports integration with third-party tools, such as Prowler and cfn_nag
- Supports custom integrations with tools, such as Security Hub API, AWS CLI, and the AWS Security Finding Format (ASFF)

Tune and measure risk

During the mature phase of the walk stage, you can use AWS Security Hub to continually tune and measure security risk. Security Hub continually assesses an organization's security posture and takes actions to remediate identified issues. Security Hub centralizes and prioritizes security findings from across AWS accounts, services, and supported third-party partners. This helps you analyze security trends and identify the high priority security issues.

Security Hub performs hundreds of security checks and classifies them based on risk to your AWS environment. You can view your score against security controls in a unified dashboard in the Security Hub console. For more information, see Determining security scores in the Security Hub documentation. Through this dashboard, the DevSecOps function can quickly identify any checks that have failed, the severity of the security issue, and which AWS Region and resource is affected. Once identified, the DevSecOps team can prioritize and remediate the issue. As issues are remediated, Security Hub automatically updates the state.

Review examples of use cases in the mature phase

The following are examples of the mature phase. These examples dive deeper into the models, tools, and processes for different business objectives, at a practical level.

Mature: Threat detection example

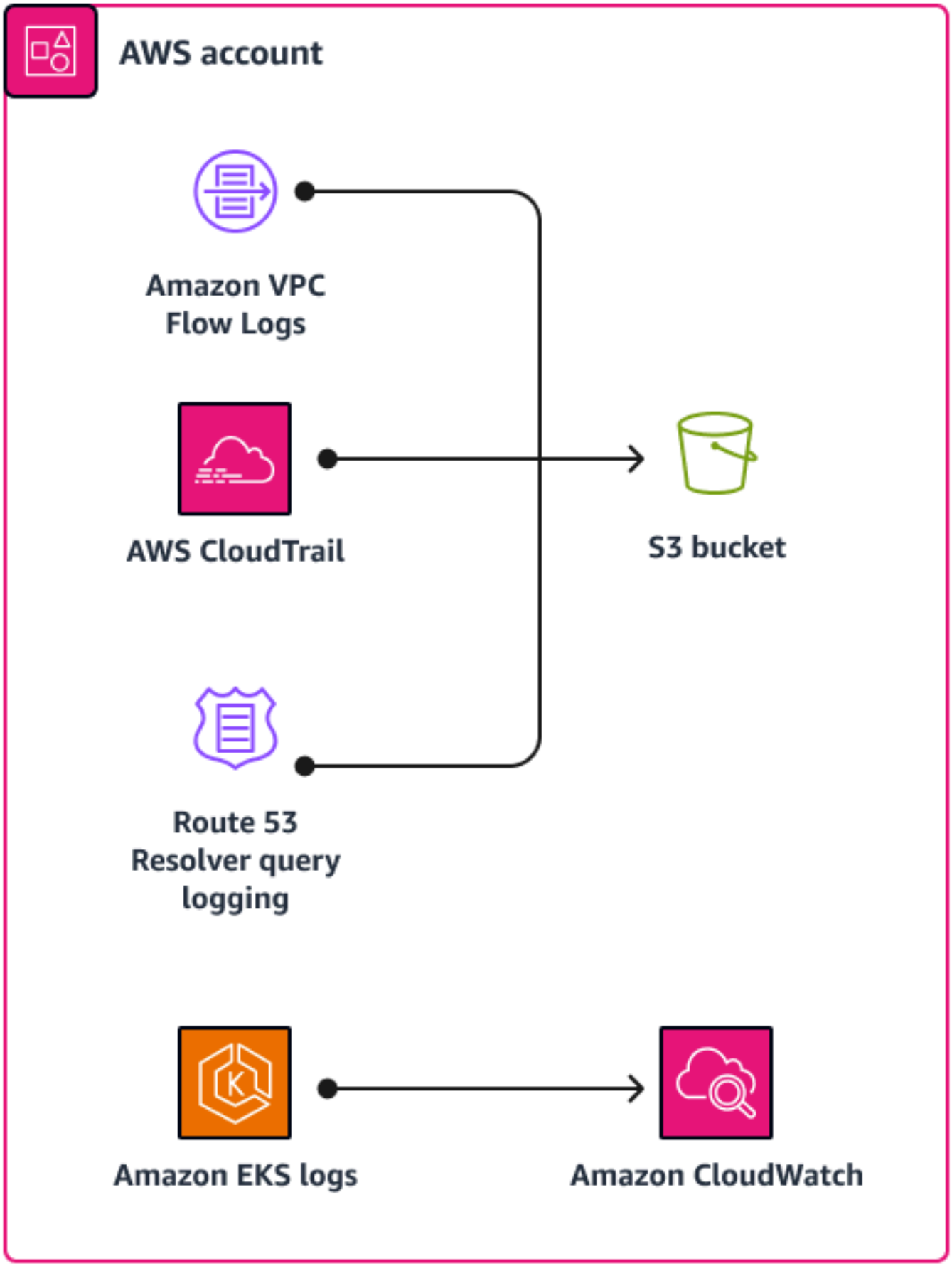
Business outcome for detective controls: Increase visibility and speed of detection of cloud incidents in order to lower risk and enable accelerated use and development of cloud resources.

Tool: Assisted Log Enabler for AWS (GitHub) is an open source tool that helps you turn on logging in the middle of a security incident. It can quickly increase your visibility into an incident.

Sample use case: Consider the single account use case depicted in the following diagram. There are events that require further investigation. You are unsure whether logging is enabled. In this

case, the best course of action is to perform a dry run with the Assisted Log Enabler to see which services are enabled or disabled. Assisted Log Enabler checks for AWS CloudTrail trails, DNS query logs, VPC flow logs, and other logs. If they are not enabled, Assisted Log Enabler enables them. Assisted Log Enabler can check for and turn on logging across all AWS Regions.

You can also throttle Assisted Log Enabler up or down. After you complete your dry run, close the event, and resolve the issue, you realize that you no longer need this level of logging. You can quickly clean up the deployment to stop logging. This feature allows you to use Assisted Log Enabler as a triage tool.



The following are the key features of Assisted Log Enabler for AWS:

- You can run it in a single-account or multi-account environment.
- You can use it to establish a baseline for logging into your environment.
- You can use the dry run feature to check the current state and determine which services have logging enabled.
- You can select which services you want to enable logging for.
- You can throttle Assisted Log Enabler up or down, for your use case.

Mature: IAM example

IAM business outcome: Automate visibility and measure against best practices to continuously reduce risk, to enable secure, external connections, and to quickly provision new users and environments

Tool: AWS Identity and Access Management Access Analyzer (IAM Access Analyzer) helps you identify resources that are shared with an external entity, validates IAM policies against policy grammar and best practices, and generates IAM policies based on historical access activity. We highly recommend that you enable IAM Access Analyzer at both the account and organization levels.

Service benefits: IAM Access Analyzer provides a wealth of insightful findings. It can identify your organization's resources and accounts that are shared with an external entity. It can detect resources such as a public S3 bucket, an AWS KMS key shared with another account, or a role shared with an external account, giving you excellent visibility into identifying resources that are not under your organization's control. It not only validates IAM policies but can also generate them for you.

Run stage: Optimizing your cloud security operations

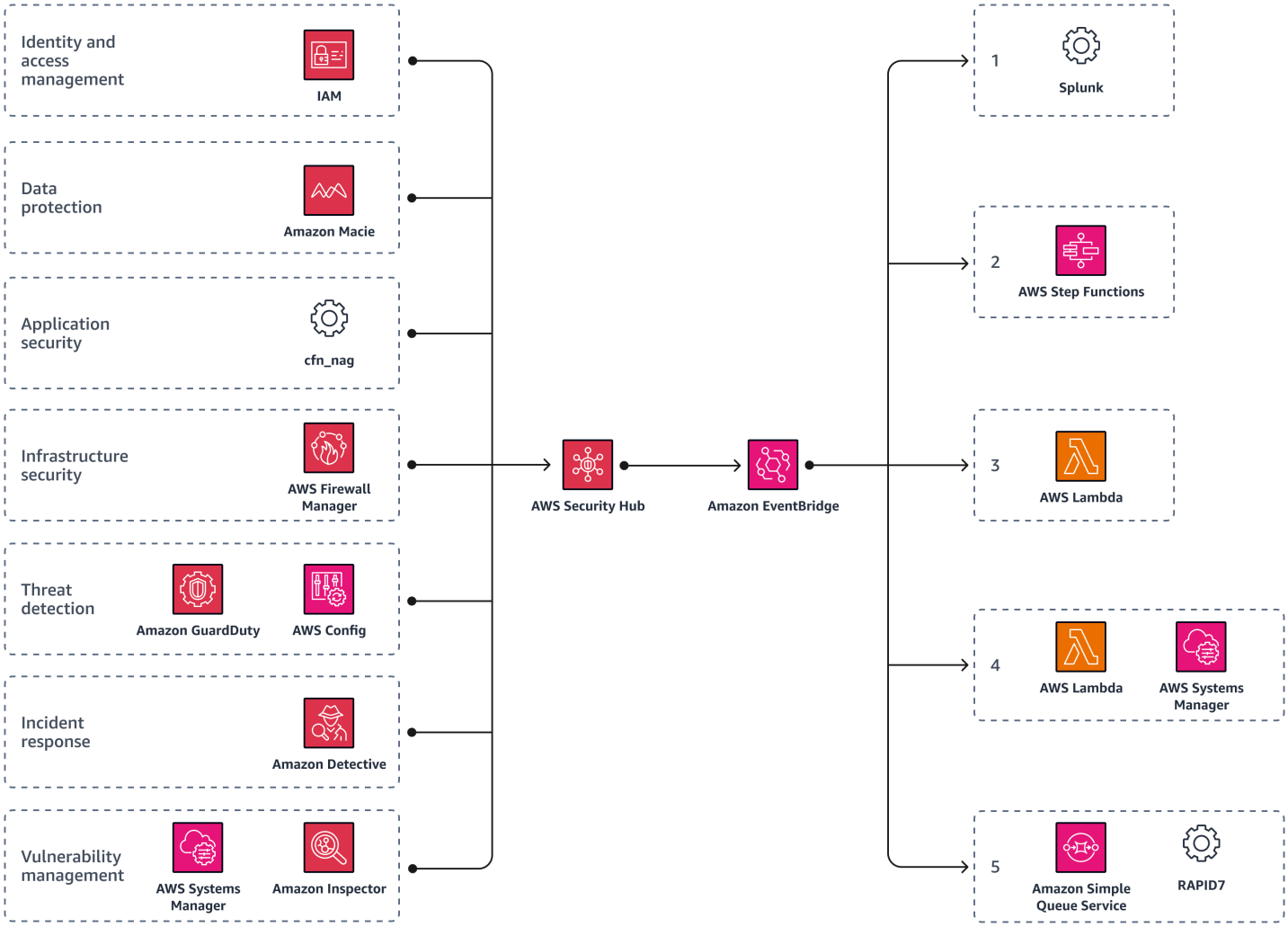
After you implement a baseline in the walk stage, your organization progresses to the run stage. This stage is focused on demonstrating the cybersecurity capabilities that are available in the cloud, many of which are not possible or are very difficult to implement with on-premises solutions. This stage brings together different security components and automates processes. Automations free up your resources so that they can focus on high-value work.

The following is the only phase in the run stage:

- Optimize – How do I improve this process and add automation?

Optimize: Automate and iterate your cloud security operations

In the optimize phase, you automate your security operations. Like the crawl and walk stages, you can use AWS Security Hub during the run stage to achieve automation and iteration. The following image shows how Security Hub can trigger a custom Amazon EventBridge rule that defines automatic actions to take against specific findings and insights. For more information, see Automations in the Security Hub documentation.



By using Security Hub as a central automation hub, you can also forward activities to Splunk. Splunk can then detect the ones that are anomalous and trigger corresponding actions in EventBridge. This helps you automate repetitive tasks and provides more time for skilled team members to focus on higher-value activities. You can also use AWS Step Functions to collect logs, take forensic snapshots, quarantine compromised servers, and replace them with a golden image. Additionally, you can use an AWS Lambda function that uses AWS Systems Manager to remediate vulnerabilities across the environment and uses an Amazon Simple Queue Service (Amazon SQS) function to validate the security of the systems. By taking this approach, it's possible to quickly contain and remediate security incidents with minimal impact to normal business operations.

The following is an example of repeated automated actions, as shown in the previous image:

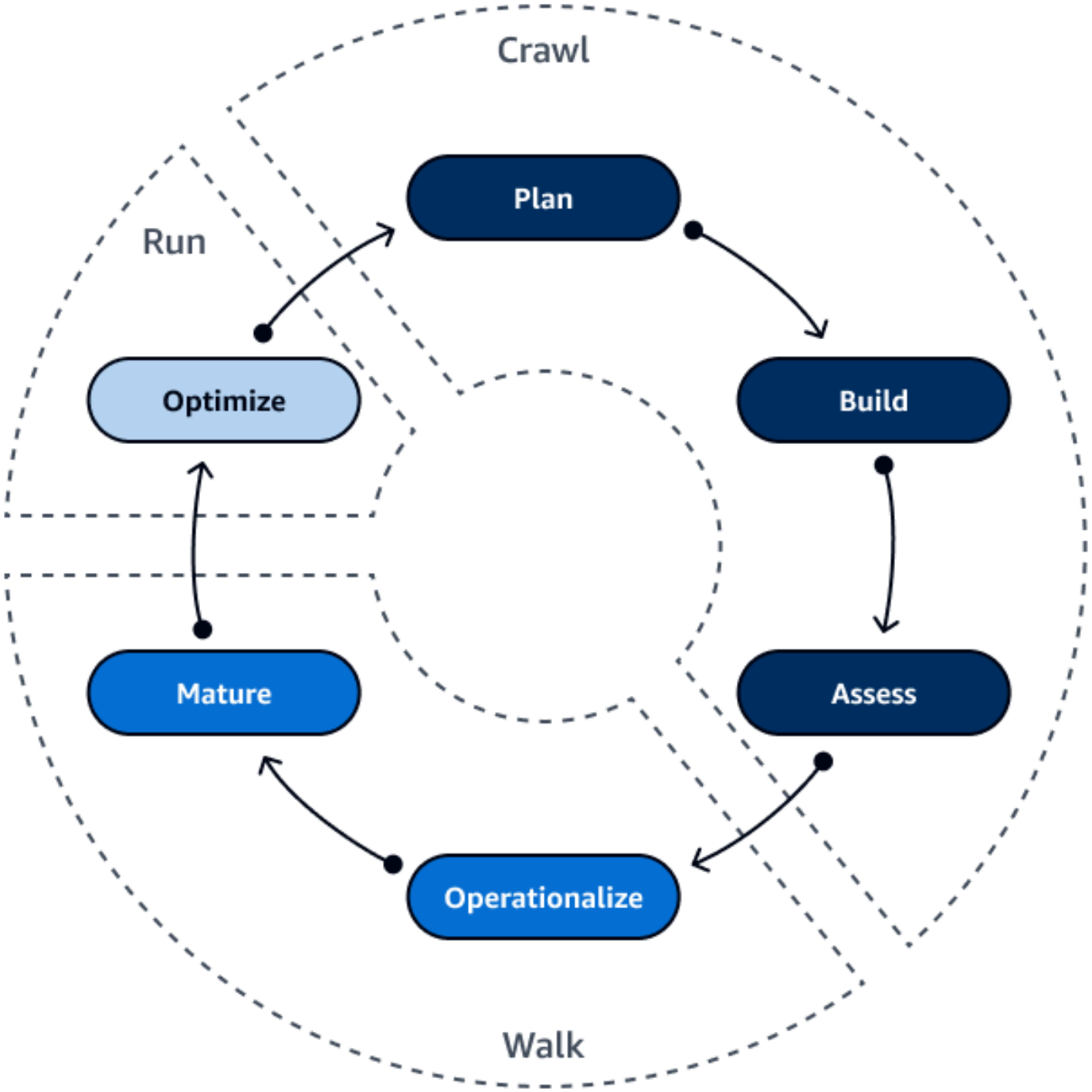
1. Use Splunk to detect questionable activity.
2. Use Step Functions to collect logs, revoke access, quarantine, and take forensic snapshots.

3. Use an EventBridge rule to start a Lambda function that quarantines, takes forensic snapshots, and replaces compromised servers with a golden image.
4. Start a Lambda function that uses Systems Manager to remediate and apply patches throughout the rest of the environment.
5. Start an Amazon SQS message that uses the Rapid7 scanner to scan and validate whether the AWS resource is secure.

For more information, see How to automate incident response in the AWS Cloud for EC2 instances in the AWS Security Blog.

Conclusion: Crawl, walk, run, then fly!

In summary, the *crawl, walk, run* model is a framework that helps you gradually improve your security posture and adopt best practices for securing AWS infrastructure. This process continues to evolve as new technologies and business needs arise. By following this framework and using the resources provided by AWS, you can establish a solid foundation for cloud security, effectively manage security risks, accelerate security maturity, and drive innovation.

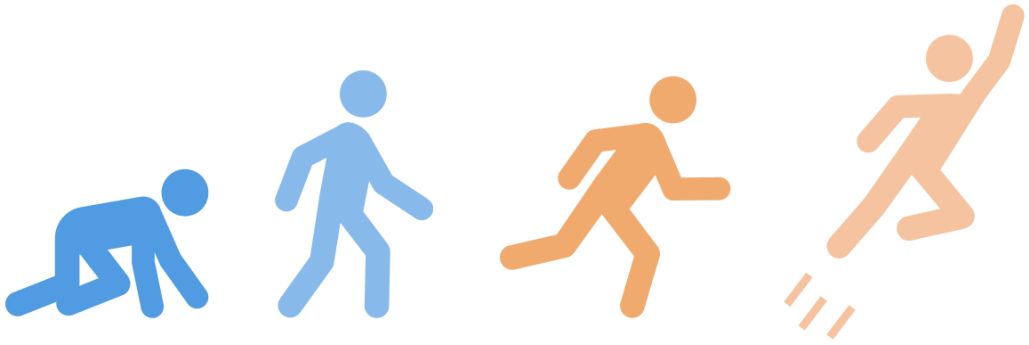


In the crawl stage, you set the foundation. You define what your security plan is, use a defined security best practice architecture, and drive a continuous assessment toward your organization's business objectives.

In the walk stage, you take the first steps. You look at policies, build out playbooks, train people, and align strategies. This stage helps you understand how to take advantage of innovation to keep up with the technologies in the cloud.

In the run stage, you think big. You use automation and strategically place your skilled people in the right place. You implement automation to drive continuous assessment toward your organization's business objectives.

Now, it is time for you fly. Use the recommendations in this guide to accelerate your security maturity in the AWS Cloud.



Resources

Frameworks and models

- AWS Cloud Adoption Framework (AWS CAF)
- AWS Well-Architected Framework
- AWS Security Reference Architecture (AWS SRA)
- AWS Security Maturity Model
- HIPAA Reference Architecture
- HITRUST Reference Architecture

AWS services

- AWS Control Tower
- AWS Identity and Access Management Access Analyzer
- AWS Security Hub

Other AWS resources

- Automated Security Response on AWS in the AWS Solutions Library
- Automate Your IT Operations Using AWS Step Functions and Amazon CloudWatch Events in the AWS Compute Blog
- How to automate incident response in the AWS Cloud for EC2 instances in the AWS Security Blog
- How to perform automated incident response in a multi-account environment in the AWS Security Blog
- AWS re:Inforce 2022 - Crawl, walk, run: Accelerating security maturity video on YouTube
- AWS re:Inforce 2022 - Crawl, walk, run: Accelerating security maturity PowerPoint presentation (Attachment)

Contributors

The following individuals contributed to this guide.

Authoring

- Chad Lorenc, Security Practice Manager, AWS
- Ivy Gin, Security Assurance Consultant, AWS
- Sayali Paseband, Security Consultant, AWS

Reviewing

- Deeps Baisya, Senior Security Architect, AWS
- Mike LaRue, Senior Security Consultant, AWS
- Raul Radu, Senior Security Engineer, AWS

Technical writing

- Lilly AbouHarb, Senior Technical Writer, AWS

Document history

The following table describes significant changes to this guide. If you want to be notified about future updates, you can subscribe to an RSS feed.

Change	Description	Date
Initial publication	—	December 20, 2023

AWS Prescriptive Guidance glossary

The following are commonly used terms in strategies, guides, and patterns provided by AWS Prescriptive Guidance. To suggest entries, please use the **Provide feedback** link at the end of the glossary.

Management and governance terms

Cloud Center of Excellence (CCoE)

: A multi-disciplinary team that drives cloud adoption efforts across an organization, including developing cloud best practices, mobilizing resources, establishing migration timelines, and leading the organization through large-scale transformations. For more information, see the CCoE posts on the AWS Cloud Enterprise Strategy Blog.

cloud operating model

: In an IT organization, the operating model that is used to build, mature, and optimize one or more cloud environments. For more information, see Building your Cloud Operating Model.

development value stream mapping (DVSM)

: A process used to identify and prioritize constraints that adversely affect speed and quality in a software development lifecycle. DVSM extends the value stream mapping process originally designed for lean manufacturing practices. It focuses on the steps and teams required to create and move value through the software development process.

RACI matrix

: A matrix that defines the roles and responsibilities for all parties involved in migration activities and cloud operations. The matrix name is derived from the responsibility types defined in the matrix: responsible (R), accountable (A), consulted (C), and informed (I). The support (S) type is optional. If you include support, the matrix is called a *RASCI matrix*, and if you exclude it, it's called a *RACI matrix*.

RASCI matrix

: See RACI matrix.

tags

Key-value pairs that act as metadata for organizing your AWS resources. Tags can help you manage, identify, organize, search for, and filter resources. For more information, see Tagging your AWS resources.

undifferentiated tasks

Also known as *heavy lifting*, work that is necessary to create and operate an application but that doesn't provide direct value to the end user or provide competitive advantage. Examples of undifferentiated tasks include procurement, maintenance, and capacity planning.

Security terms

anonymization

The process of permanently deleting personal information in a dataset. Anonymization can help protect personal privacy. Anonymized data is no longer considered to be personal data.

anti-pattern

A frequently used solution for a recurring issue where the solution is counter-productive, ineffective, or less effective than an alternative.

attribute-based access control (ABAC)

The practice of creating fine-grained permissions based on user attributes, such as department, job role, and team name. For more information, see ABAC for AWS in the AWS Identity and Access Management (IAM) documentation.

asymmetric encryption

An encryption algorithm that uses a pair of keys, a public key for encryption and a private key for decryption. You can share the public key because it isn't used for decryption, but access to the private key should be highly restricted.

behavior graph

A unified, interactive view of resource behavior and interactions over time. You can use a behavior graph with Amazon Detective to examine failed logon attempts, suspicious API calls, and similar actions. For more information, see Data in a behavior graph in the Detective documentation.

client-side encryption

Encryption of data locally, before the target AWS service receives it.

conformance pack

A collection of AWS Config rules and remediation actions that you can assemble to customize your compliance and security checks. You can deploy a conformance pack as a single entity in an AWS account and Region, or across an organization, by using a YAML template. For more information, see Conformance packs in the AWS Config documentation.

data at rest

Data that is stationary in your network, such as data that is in storage.

data classification

A process for identifying and categorizing the data in your network based on its criticality and sensitivity. It is a critical component of any cybersecurity risk management strategy because it helps you determine the appropriate protection and retention controls for the data. Data classification is a component of the security pillar in the AWS Well-Architected Framework. For more information, see Data classification.

data in transit

Data that is actively moving through your network, such as between network resources.

data minimization

The principle of collecting and processing only the data that is strictly necessary. Practicing data minimization in the AWS Cloud can reduce privacy risks, costs, and your analytics carbon footprint.

data provenance

The process of tracking the origin and history of data throughout its lifecycle, such as how the data was generated, transmitted, and stored.

data subject

An individual whose data is being collected and processed.

defense-in-depth

An information security approach in which a series of security mechanisms and controls are thoughtfully layered throughout a computer network to protect the confidentiality, integrity, and availability of the network and the data within. When you adopt this strategy on AWS,

you add multiple controls at different layers of the AWS Organizations structure to help secure resources. For example, a defense-in-depth approach might combine multi-factor authentication, network segmentation, and encryption.

delegated administrator

In AWS Organizations, a compatible service can register an AWS member account to administer the organization's accounts and manage permissions for that service. This account is called the *delegated administrator* for that service. For more information and a list of compatible services, see Services that work with AWS Organizations in the AWS Organizations documentation.

detective control

A security control that is designed to detect, log, and alert after an event has occurred. These controls are a second line of defense, alerting you to security events that bypassed the preventative controls in place. For more information, see Detective controls in *Implementing security controls on AWS*.

encryption key

A cryptographic string of randomized bits that is generated by an encryption algorithm. Keys can vary in length, and each key is designed to be unpredictable and unique.

endpoint service

A service that you can host in a virtual private cloud (VPC) to share with other users. You can create an endpoint service with AWS PrivateLink and grant permissions to other AWS accounts or to IAM principals. These accounts or principals can connect to your endpoint service privately by creating interface VPC endpoints. For more information, see Create an endpoint service in the Amazon VPC documentation.

envelope encryption

The process of encrypting an encryption key with another encryption key. For more information, see Envelope encryption in the AWS Key Management Service (AWS KMS) documentation.

fine-grained access control (FGAC)

The use of multiple conditions to allow or deny an access request.

geographic restrictions (geo blocking)

In Amazon CloudFront, an option to prevent users in specific countries from accessing content distributions. You can use an allow list or block list to specify approved and banned countries.

For more information, see Restricting the geographic distribution of your content in the CloudFront documentation.

guardrail

A high-level rule that helps govern resources, policies, and compliance across organizational units (OUs). *Preventive guardrails* enforce policies to ensure alignment to compliance standards. They are implemented by using service control policies and IAM permissions boundaries. *Detective guardrails* detect policy violations and compliance issues, and generate alerts for remediation. They are implemented by using AWS Config, AWS Security Hub, Amazon GuardDuty, AWS Trusted Advisor, Amazon Inspector, and custom AWS Lambda checks.

identity-based policy

A policy attached to one or more IAM principals that defines their permissions within the AWS Cloud environment.

inbound (ingress) VPC

In an AWS multi-account architecture, a VPC that accepts, inspects, and routes network connections from outside an application. The AWS Security Reference Architecture recommends setting up your Network account with inbound, outbound, and inspection VPCs to protect the two-way interface between your application and the broader internet.

inspection VPC

In an AWS multi-account architecture, a centralized VPC that manages inspections of network traffic between VPCs (in the same or different AWS Regions), the internet, and on-premises networks. The AWS Security Reference Architecture recommends setting up your Network account with inbound, outbound, and inspection VPCs to protect the two-way interface between your application and the broader internet.

least privilege

The security best practice of granting the minimum permissions required to perform a task. For more information, see Apply least-privilege permissions in the IAM documentation.

member account

All AWS accounts other than the management account that are part of an organization in AWS Organizations. An account can be a member of only one organization at a time.

organization trail

A trail that's created by AWS CloudTrail that logs all events for all AWS accounts in an organization in AWS Organizations. This trail is created in each AWS account that's part of the organization and tracks the activity in each account. For more information, see Creating a trail for an organization in the CloudTrail documentation.

outbound (egress) VPC

In an AWS multi-account architecture, a VPC that handles network connections that are initiated from within an application. The AWS Security Reference Architecture recommends setting up your Network account with inbound, outbound, and inspection VPCs to protect the two-way interface between your application and the broader internet.

origin access control (OAC)

In CloudFront, an enhanced option for restricting access to secure your Amazon Simple Storage Service (Amazon S3) content. OAC supports all S3 buckets in all AWS Regions, server-side encryption with AWS KMS (SSE-KMS), and dynamic PUT and DELETE requests to the S3 bucket.

origin access identity (OAI)

In CloudFront, an option for restricting access to secure your Amazon S3 content. When you use OAI, CloudFront creates a principal that Amazon S3 can authenticate with. Authenticated principals can access content in an S3 bucket only through a specific CloudFront distribution. See also OAC, which provides more granular and enhanced access control.

permissions boundary

An IAM management policy that is attached to IAM principals to set the maximum permissions that the user or role can have. For more information, see Permissions boundaries in the IAM documentation.

personally identifiable information (PII)

Information that, when viewed directly or paired with other related data, can be used to reasonably infer the identity of an individual. Examples of PII include names, addresses, and contact information.

policy

An object that can define permissions (see identity-based policy), specify access conditions (see resource-based policy), or define the maximum permissions for all accounts in an organization in AWS Organizations (see service control policy).

preventative control

A security control that is designed to prevent an event from occurring. These controls are a first line of defense to help prevent unauthorized access or unwanted changes to your network. For more information, see Preventative controls in *Implementing security controls on AWS*.

principal

An entity in AWS that can perform actions and access resources. This entity is typically a root user for an AWS account, an IAM role, or a user. For more information, see *Principal* in Roles terms and concepts in the IAM documentation.

Privacy by Design

An approach in system engineering that takes privacy into account throughout the whole engineering process.

pseudonymization

The process of replacing personal identifiers in a dataset with placeholder values. Pseudonymization can help protect personal privacy. Pseudonymized data is still considered to be personal data.

ransomware

A malicious software that is designed to block access to a computer system or data until a payment is made.

resource-based policy

A policy attached to a resource, such as an Amazon S3 bucket, an endpoint, or an encryption key. This type of policy specifies which principals are allowed access, supported actions, and any other conditions that must be met.

responsive control

A security control that is designed to drive remediation of adverse events or deviations from your security baseline. For more information, see Responsive controls in *Implementing security controls on AWS*.

SAML 2.0

An open standard that many identity providers (IdPs) use. This feature enables federated single sign-on (SSO), so users can log into the AWS Management Console or call the AWS API

operations without you having to create user in IAM for everyone in your organization. For more information about SAML 2.0-based federation, see About SAML 2.0-based federation in the IAM documentation.

security control

A technical or administrative guardrail that prevents, detects, or reduces the ability of a threat actor to exploit a security vulnerability. There are three primary types of security controls: preventative, detective, and responsive.

security hardening

The process of reducing the attack surface to make it more resistant to attacks. This can include actions such as removing resources that are no longer needed, implementing the security best practice of granting least privilege, or deactivating unnecessary features in configuration files.

security information and event management (SIEM) system

Tools and services that combine security information management (SIM) and security event management (SEM) systems. A SIEM system collects, monitors, and analyzes data from servers, networks, devices, and other sources to detect threats and security breaches, and to generate alerts.

server-side encryption

Encryption of data at its destination, by the AWS service that receives it.

service control policy (SCP)

A policy that provides centralized control over permissions for all accounts in an organization in AWS Organizations. SCPs define guardrails or set limits on actions that an administrator can delegate to users or roles. You can use SCPs as allow lists or deny lists, to specify which services or actions are permitted or prohibited. For more information, see Service control policies in the AWS Organizations documentation.

shared responsibility model

A model describing the responsibility you share with AWS for cloud security and compliance. AWS is responsible for security *of* the cloud, whereas you are responsible for security *in* the cloud. For more information, see Shared responsibility model.

symmetric encryption

An encryption algorithm that uses the same key to encrypt and decrypt the data.

trusted access

Granting permissions to a service that you specify to perform tasks in your organization in AWS Organizations and in its accounts on your behalf. The trusted service creates a service-linked role in each account, when that role is needed, to perform management tasks for you. For more information, see Using AWS Organizations with other AWS services in the AWS Organizations documentation.

vulnerability

A software or hardware flaw that compromises the security of the system.

workload

A collection of resources and code that delivers business value, such as a customer-facing application or backend process.

zero-day exploit

An attack, typically malware, that takes advantage of a zero-day vulnerability.

zero-day vulnerability

An unmitigated flaw or vulnerability in a production system. Threat actors can use this type of vulnerability to attack the system. Developers frequently become aware of the vulnerability as a result of the attack.