AWS Academy Cloud Foundations

Module 9: Cloud Architecture

Module overview

Topics

- AWS Well-Architected Framework
- Reliability and high availability
- AWS Trusted Advisor

Activities

- AWS Well-Architected Framework Design Principles
- Interpret AWS Trusted Advisor Recommendations

Knowledge check

Module objectives

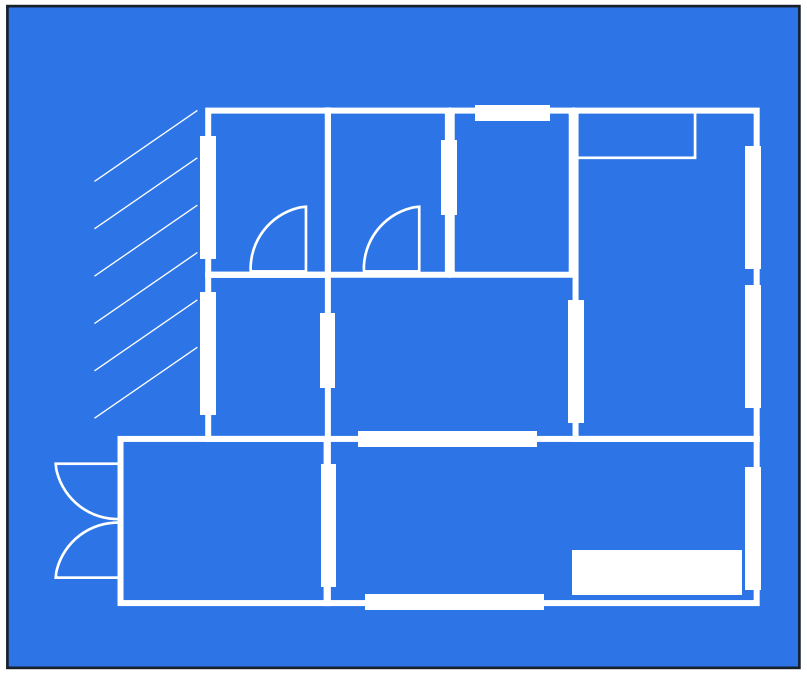
After completing this module, you should be able to:

- Describe the AWS Well-Architected Framework, including the five pillars
- Identify the design principles of the AWS Well-Architected Framework
- Explain the importance of reliability and high availability
- Identify how AWS Trusted Advisor helps customers
- Interpret AWS Trusted Advisor recommendations

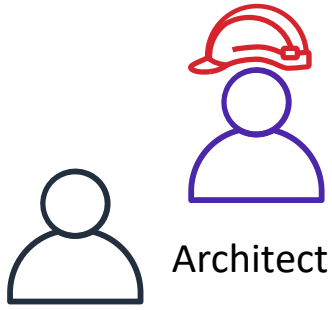
Module 9: Cloud Architecture

Section 1: AWS Well-Architected Framework

Architecture: designing and building

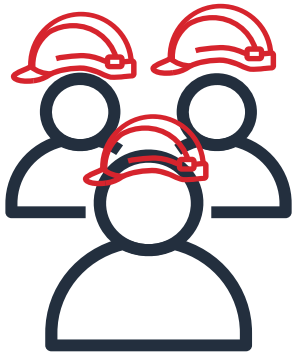


Structure design

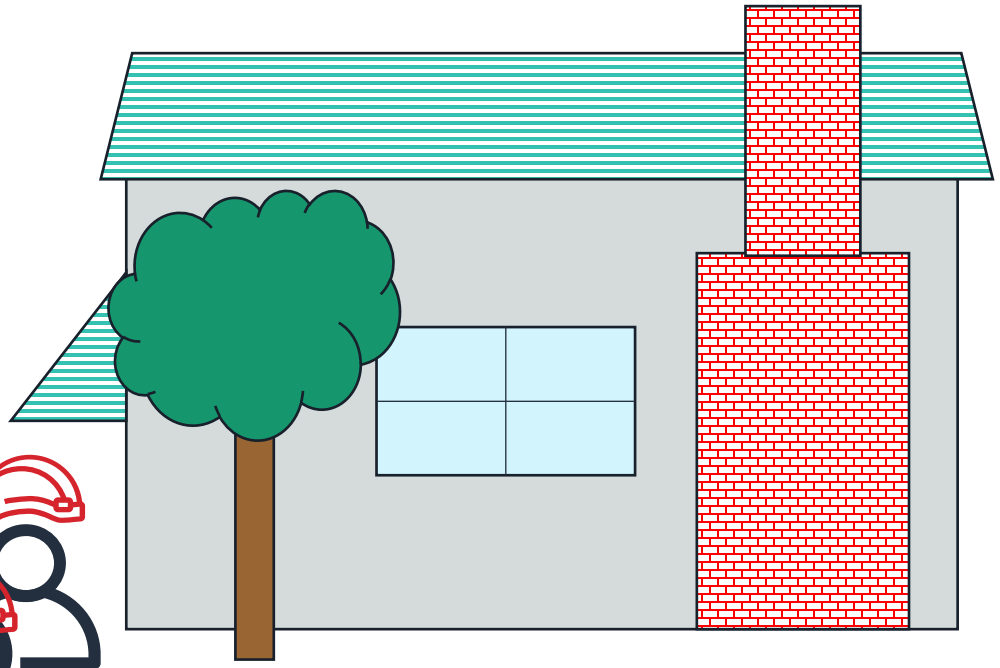


Customer
(Decision maker)

Architect



Building crew
(Delivery team)

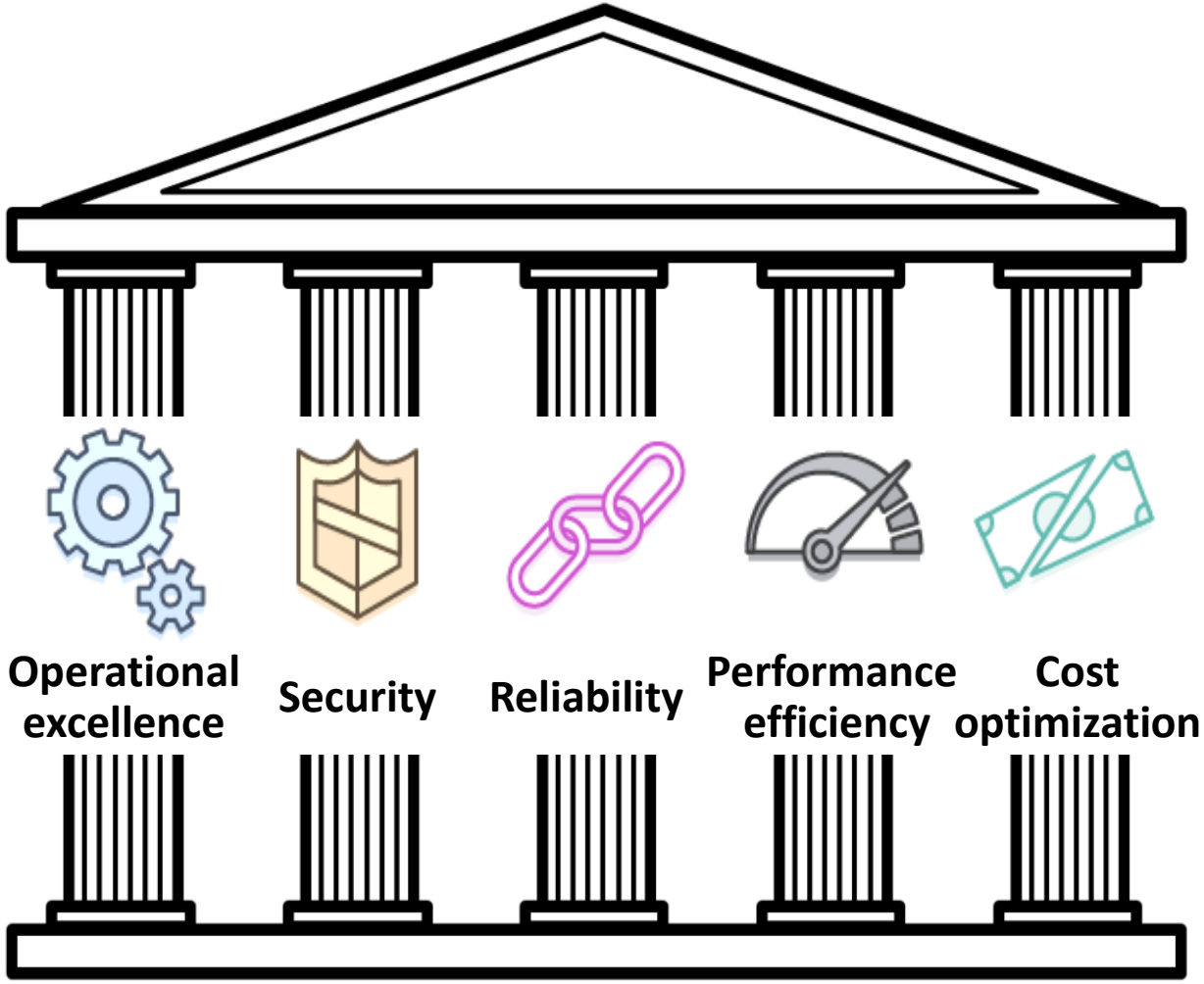


Completed structure

What is the AWS Well-Architected Framework?

- A guide for designing infrastructures that are:
  - ✓Secure
  - ✓High-performing
  - ✓Resilient
  - ✓Efficient
- A consistent approach to evaluating and implementing cloud architectures
- A way to provide best practices that were developed through lessons learned by reviewing customer architectures

Pillars of the AWS Well-Architected Framework



Pillar organization

Best practice area — **Identity and Access Management**

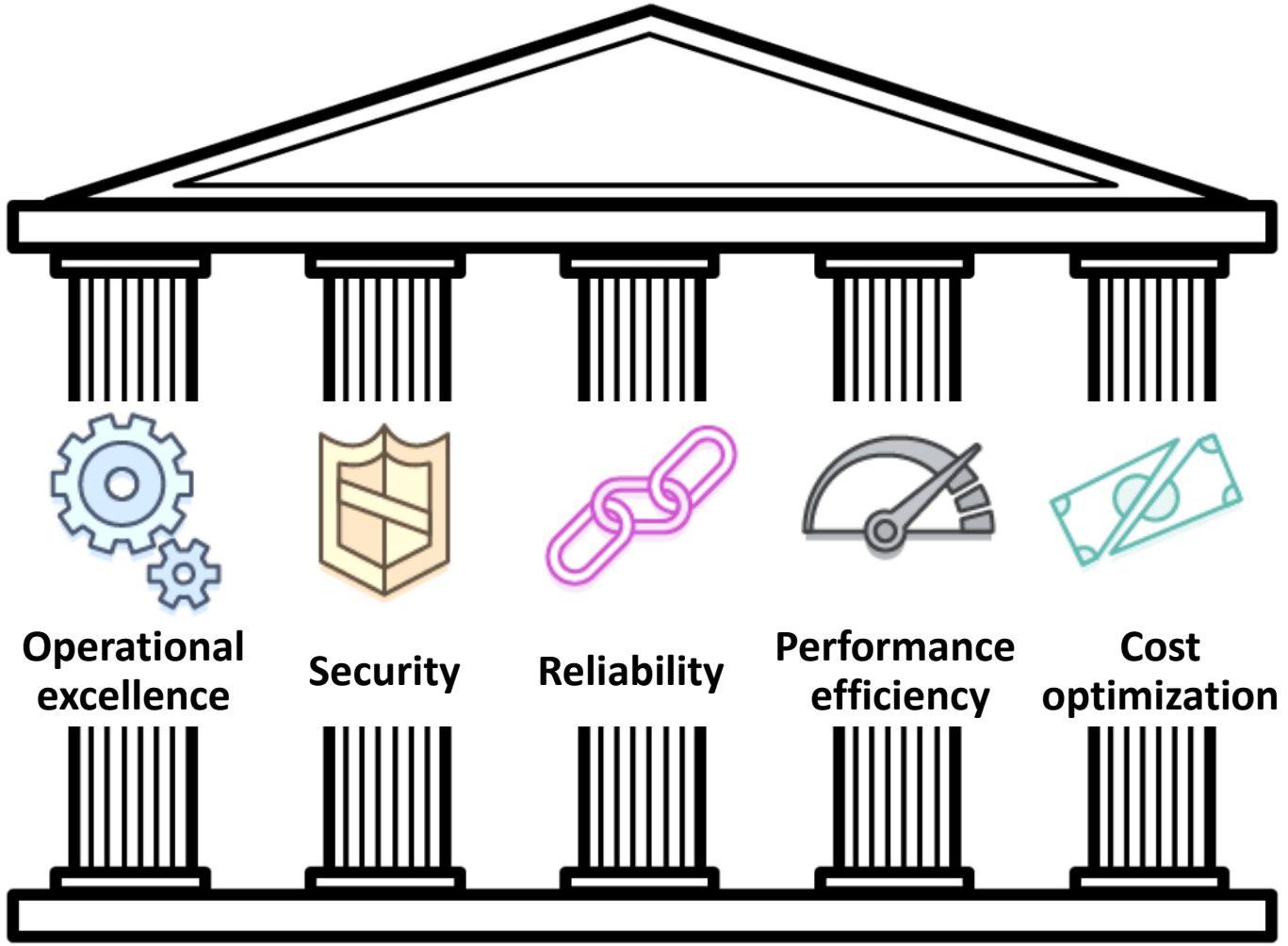
Question text — **SEC 1: How do you manage credentials and authentication?**

Question context — Credential and authentication mechanisms include passwords, tokens, and keys that grant access directly or indirectly in your workload. Protect credentials with appropriate mechanisms to help reduce the risk of accidental or malicious use.

Best practices — Best practices:

- Define requirements for identity and access management
- Secure AWS account root user
- Enforce use of multi-factor authentication
- Automate enforcement of access controls
- Integrate with centralized federation provider
- Enforce password requirements
- Rotate credentials regularly
- Audit credentials periodically

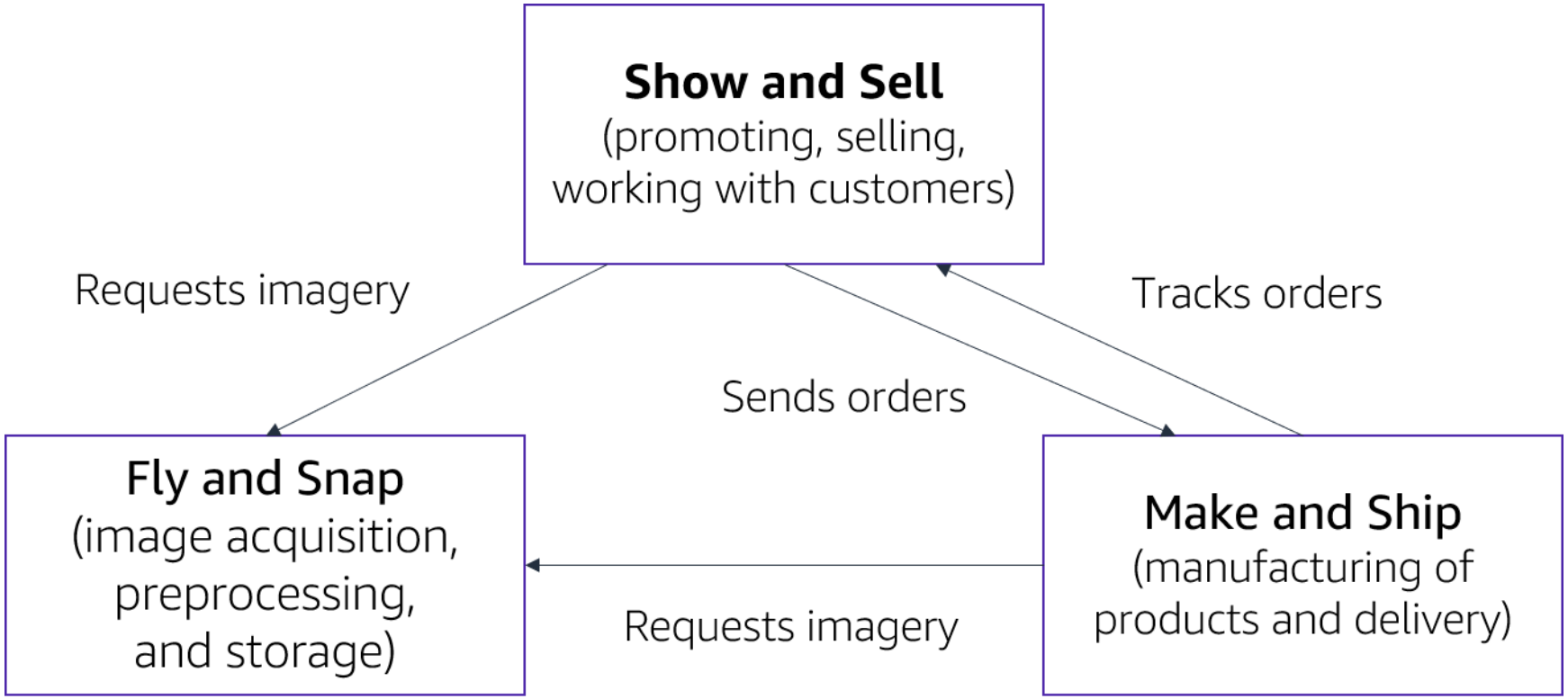
Introduction to the AWS Well-Architected Framework Design Principles Activity



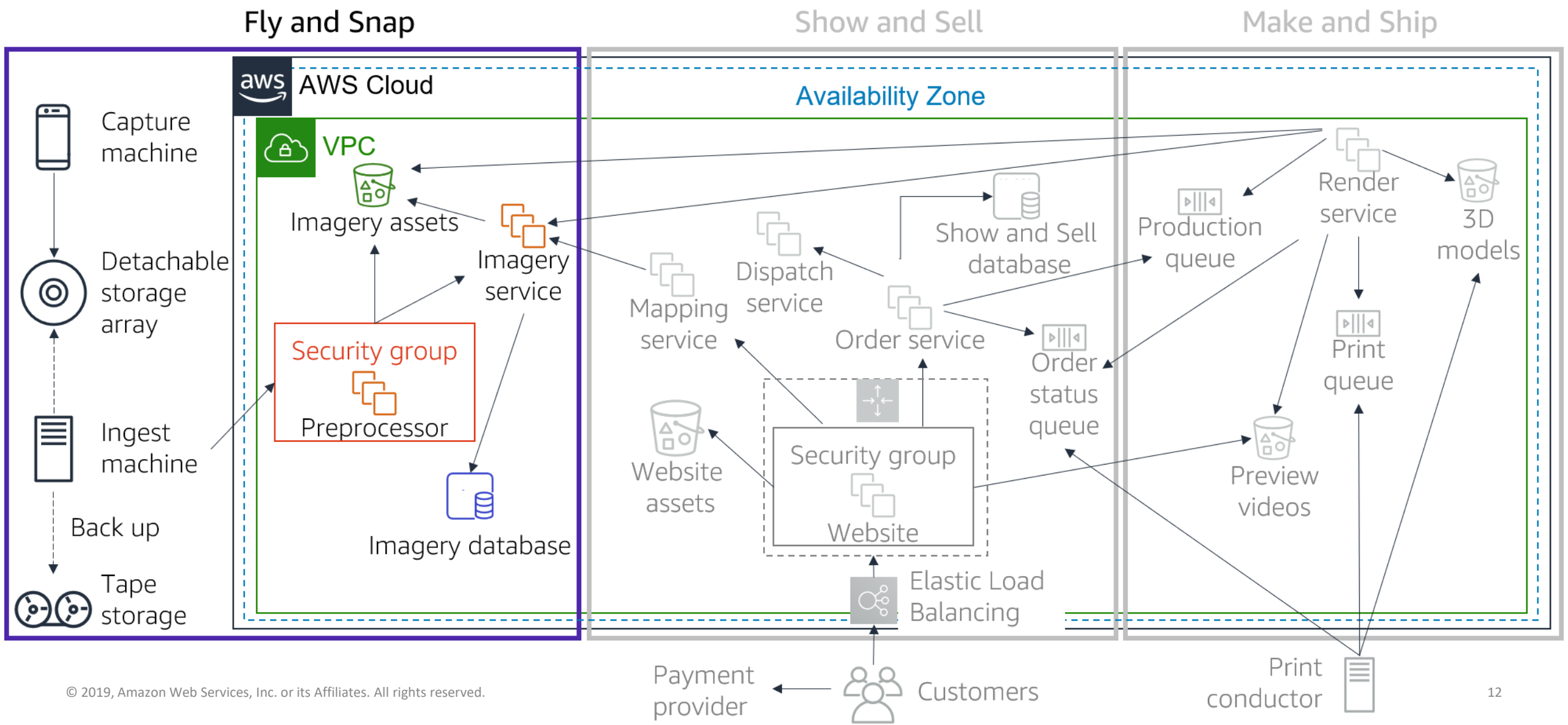
AnyCompany background

- AnyCompany Corporation: "*Cityscapes you can stand over*"
- Founded in 2008 by John Doe
- Sells 3D-printed cityscapes
- About to apply for investment
- Has asked **you** to perform a review of their platform as part of their due diligence
- Cloud native

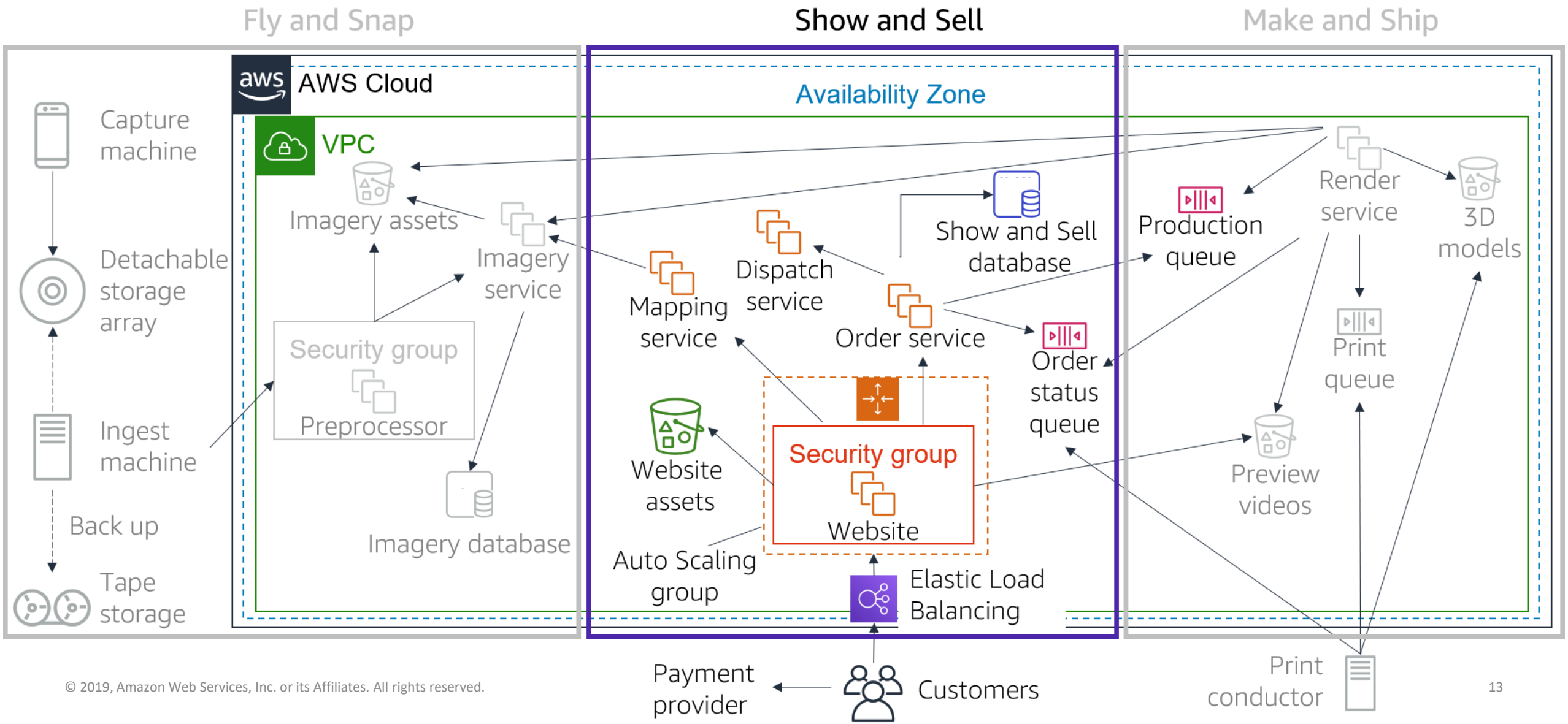
AnyCompany background (continued)



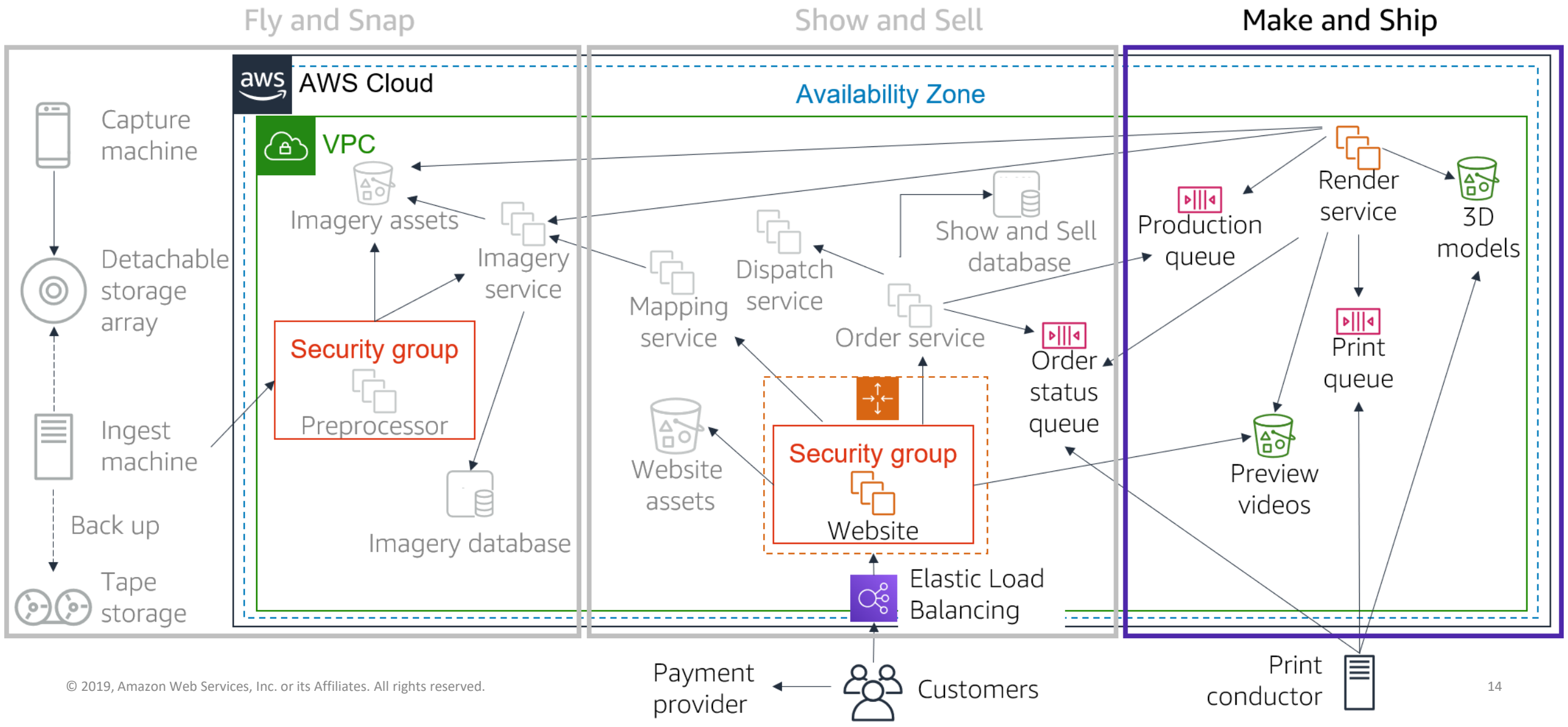
AnyCompany architecture: Fly and Snap



AnyCompany architecture: Show and Sell



AnyCompany architecture: Make and Ship



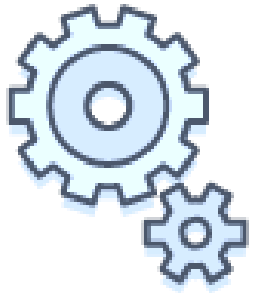
Activity overview

- Break into small groups.
- You will learn about each of the pillars. At the end of each pillar, there is a set of questions from the AWS Well-Architected Framework for you to work through with your group. Use these Framework questions to guide your review of the AnyCompany architecture.
- For each Well-Architected Framework question, answer the following questions about the AnyCompany architecture:
  - What is the CURRENT STATE (what is AnyCompany doing now)?
  - What is the FUTURE STATE (what do you think AnyCompany should be doing?)
- Agree on the top improvement that AnyCompany should make to its architecture for each set of Well-Architected Framework questions.
- Hint: There are no right or wrong answers.

Operational Excellence pillar

Operational Excellence pillar

Operational Excellence pillar

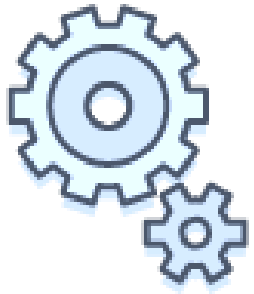


Deliver business value

- Focus
  - Run and monitor systems to deliver business value, and to continually improve supporting processes and procedures.
- Key topics
  - Automating changes
  - Responding to events
  - Defining standards to manage daily operations

Operational excellence design principles

Operational Excellence pillar



Deliver business value

- Perform operations as code
- Make frequent, small, reversible changes
- Refine operations procedures frequently
- Anticipate failure
- Learn from all operational events and failures

Operational excellence questions

Organization

- How do you determine what your priorities are?
- How do you structure your organization to support your business outcomes?
- How does your organizational culture support your business outcomes?

Prepare

- How do you design your workload so that you can understand its state?
- How do you reduce defects, ease remediation, and improve flow into production?
- How do you mitigate deployment risks?
- How do you know that you are ready to support a workload?

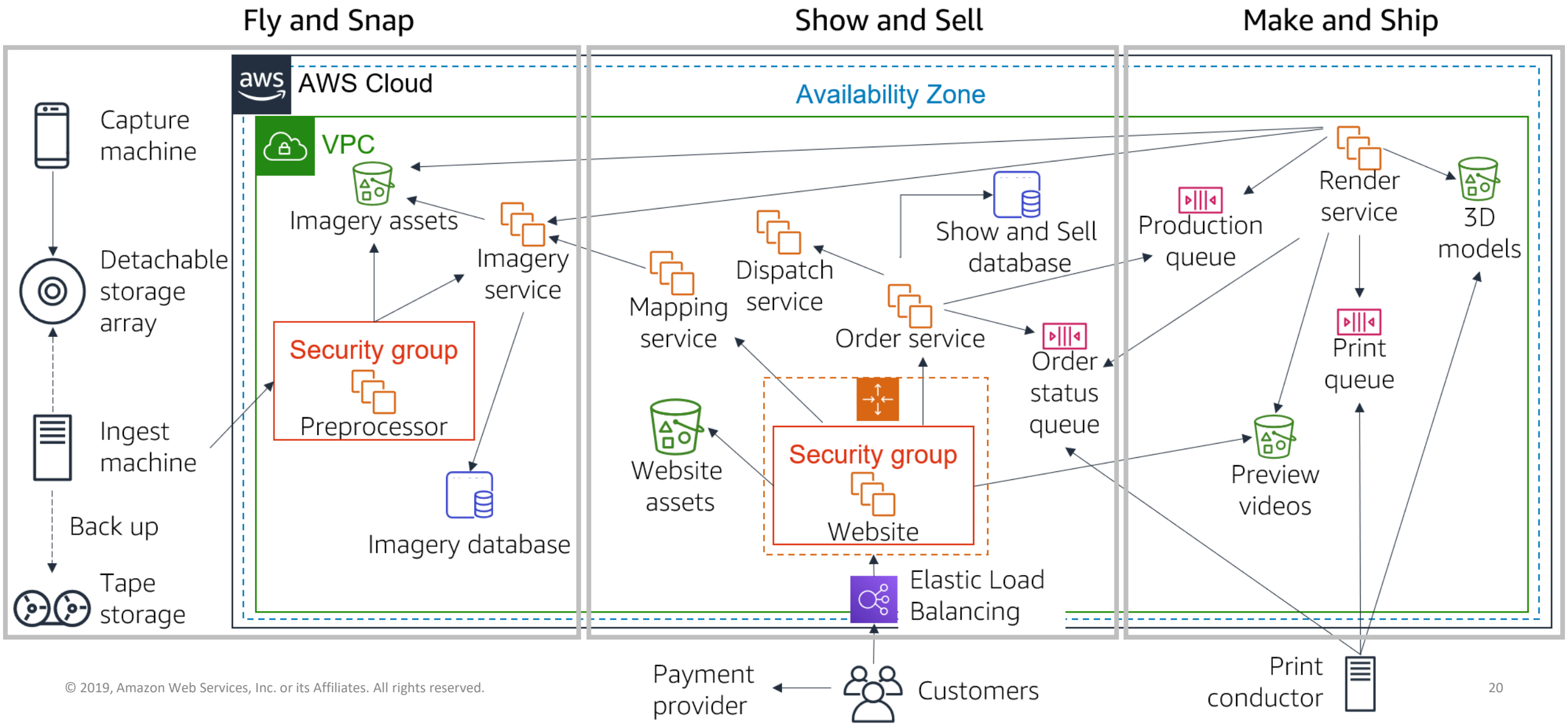
Operate

- How do you understand the health of your workload?
- How do you understand the health of your operations?
- How do you manage workload and operations events?

Evolve

- How do you evolve operations?

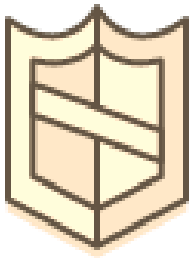
Activity breakout



Security pillar

Security pillar

Security pillar

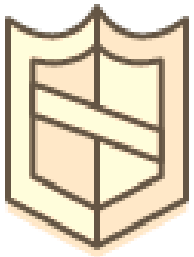


Protect and monitor systems

- Focus
  - Protect information, systems, and assets while delivering business value through risk assessments and mitigation strategies.
- Key topics
  - Protecting confidentiality and integrity of data
  - Identifying and managing who can do what
  - Protecting systems
  - Establishing controls to detect security events

Security design principles

Security pillar



Protect and monitor systems

- Implement a strong identity foundation
- Enable traceability
- Apply security at all layers
- Automate security best practices
- Protect data in transit and at rest
- Keep people away from data
- Prepare for security events

Security questions

Security

- How do you securely operate your workload?

Identity and access management

- How do you manage identities for people and machines?
- How do you manage permissions for people and machines?

Detection

- How do you detect and investigate security events?

Infrastructure protection

- How do you protect your network resources?
- How do you protect your compute resources?

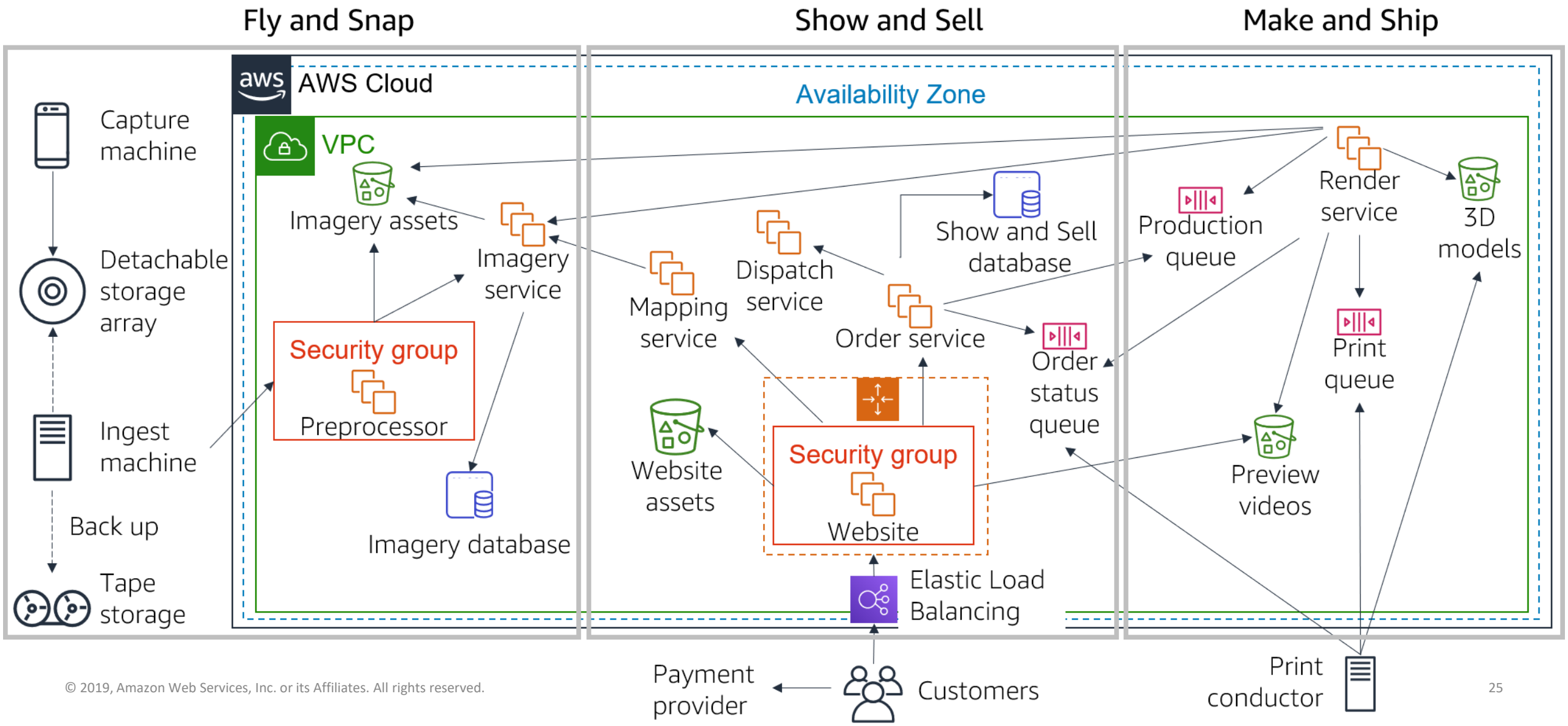
Data protection

- How do you classify your data?
- How do you protect your data at rest?
- How do you protect your data in transit?

Incident response

- How do you anticipate, respond to, and recover from incidents?

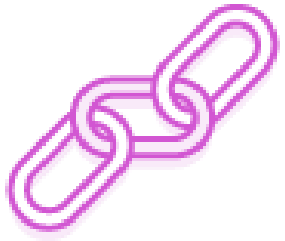
Activity breakout



Reliability pillar

Reliability pillar

Reliability pillar

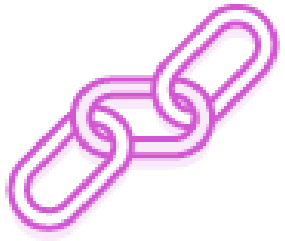


Recover from failure and mitigate disruption.

- Focus
  - Ensure a workload performs its intended function correctly and consistently when it’s expected to.
- Key topics
  - Designing distributed systems
  - Recovery planning
  - Handling change

Reliability design principles

Reliability pillar



Recover from failure and mitigate disruption.

- Automatically recover from failure
- Test recovery procedures
- Scale horizontally to increase aggregate workload availability
- Stop guessing capacity
- Manage change in automation

Reliability questions

Foundations

- How do you manage service quotas and constraints?
- How do you plan your network topology?

Workload architecture

- How do you design your workload service architecture?
- How do you design interactions in a distributed system to prevent failure?
- How do you design interactions in a distributed system to mitigate or withstand failures?

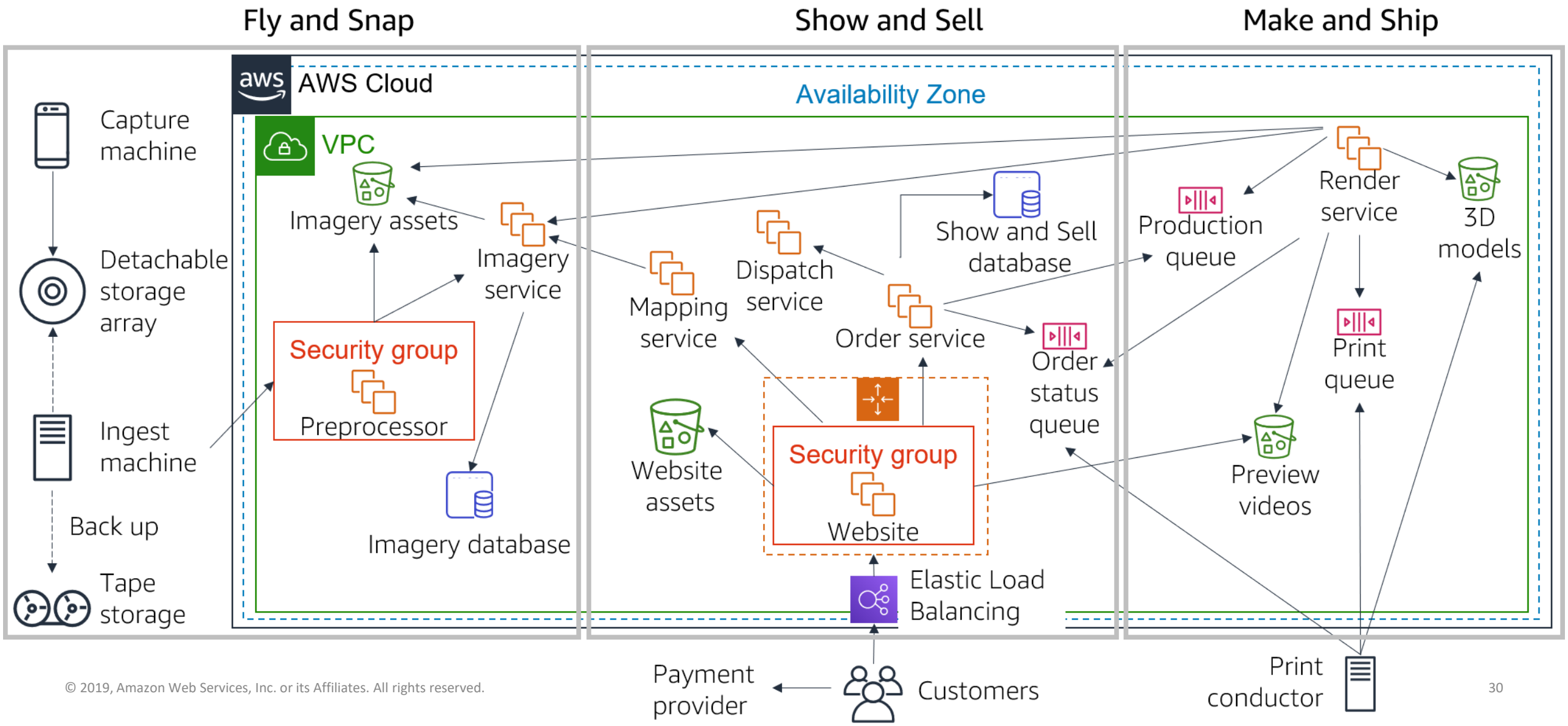
Change management

- How do you monitor workload resources?
- How do you design your workload to adapt to changes in demand?
- How do you implement change?

Failure management

- How do you back up data?
- How do you use fault isolation to protect your workload?
- How do you design your workload to withstand component failures?
- How do you test reliability?
- How do you plan for disaster recovery?

Activity breakout



Performance Efficiency pillar

Performance Efficiency pillar

Performance Efficiency pillar

Use resources sparingly.

- Focus
  - Use IT and computing resources efficiently to meet system requirements and to maintain that efficiency as demand changes and technologies evolve.
- Key topics
  - Selecting the right resource types and sizes based on workload requirements
  - Monitoring performance
  - Making informed decisions to maintain efficiency as business needs evolve

Performance efficiency design principles

Performance Efficiency pillar

Use resources sparingly.

- Democratize advanced technologies
- Go global in minutes
- Use serverless architectures
- Experiment more often
- Consider mechanical sympathy

Performance efficiency questions

Selection

- How do you select the best performing architecture?
- How do you select your compute solution?
- How do you select your storage solution?
- How do you select your database solution?
- How do you configure your networking solution?

Review

- How do you evolve your workload to take advantage of new releases?

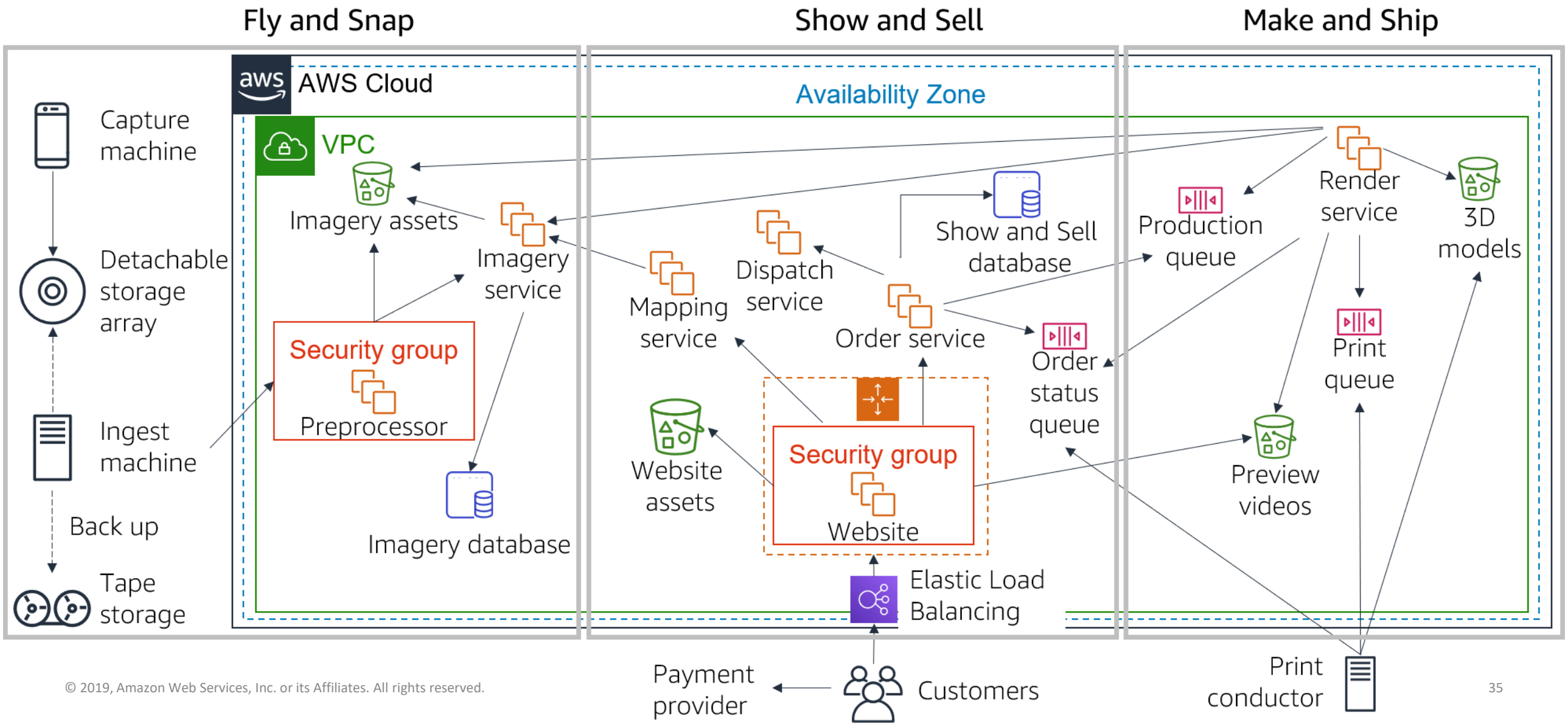
Monitoring

- How do you monitor your resources to ensure they are performing?

Tradeoffs

- How do you use tradeoffs to improve performance?

Activity breakout



Cost Optimization pillar

Cost Optimization pillar

Cost Optimization pillar

Eliminate unneeded expense.

- Focus
  - Avoid unnecessary costs.
- Key topics
  - Understanding and controlling where money is being spent
  - Selecting the most appropriate and right number of resource types
  - Analyzing spend over time
  - Scaling to meeting business needs without overspending

Cost optimization design principles

Cost Optimization pillar

Eliminate unneeded expense.

- Implement Cloud Financial Management
- Adopt a consumption model
- Measure overall efficiency
- Stop spending money on undifferentiated heavy lifting
- Analyze and attribute expenditure

Cost optimization questions

Practice cloud financial management

- How do you implement cloud financial management?

Expenditure and usage awareness

- How do you govern usage?
- How do you monitor usage and cost?
- How do you decommission resources?

Cost-effective resources

- How do you evaluate cost when you select services?
- How do you meet cost targets when you select resource type, size, and number?
- How do you use pricing models to reduce cost?
- How do you plan for data transfer changes?

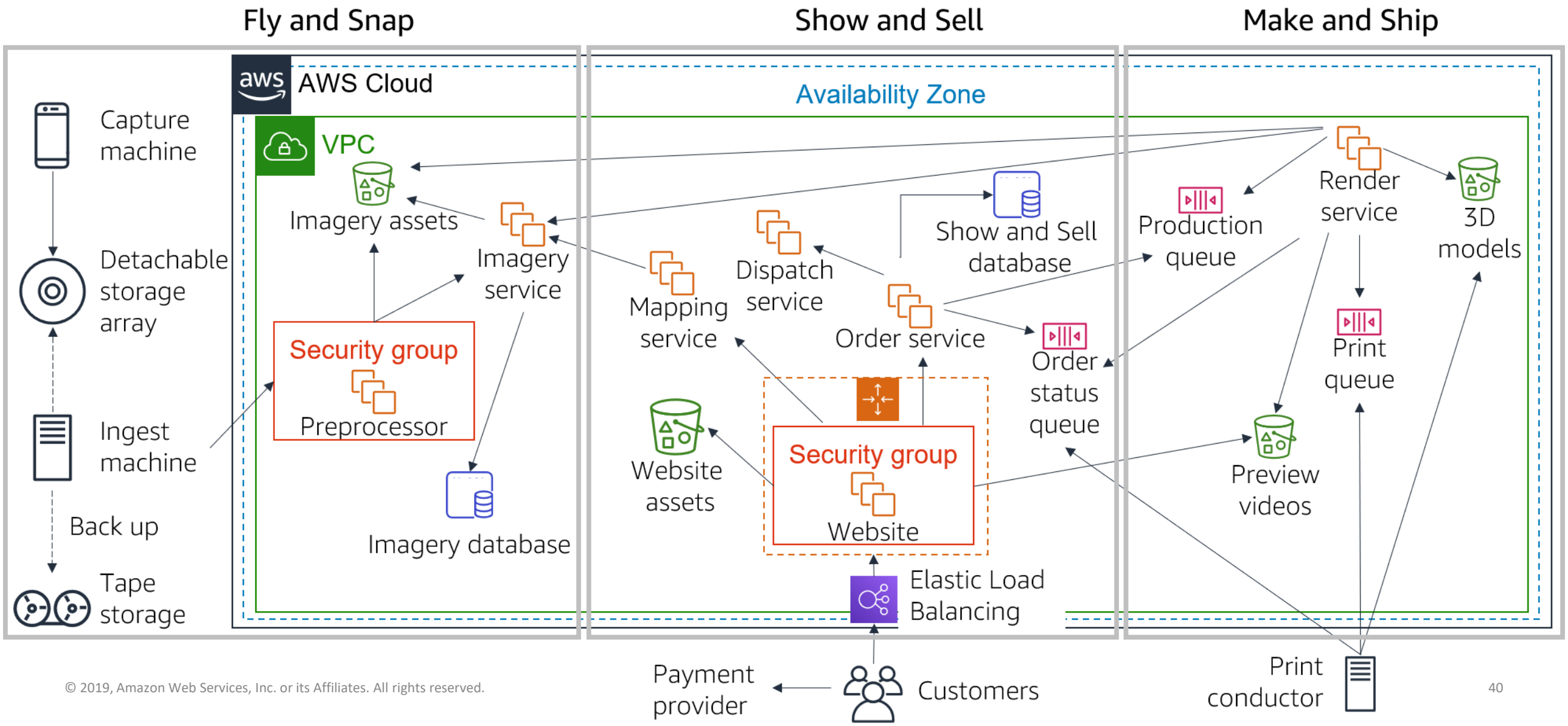
Manage demand and supply resources

- How do you manage demand and supply resources?

Optimize over time

- How do you evaluate new services?

Activity breakout



Sustainability Pillar

Sustainability pillar

- Focus
  - addresses the long-term environmental, economic, and societal impact of your business activities
- Key topics
  - Understand your impact
  - Establish sustainability goals
  - Maximize utilization
  - Anticipate and adopt new, more efficient hardware and software offerings
  - Use managed services
  - Reduce the downstream impact of your cloud workloads:

Sustainability Best Practices

Sustainability pillar

- Optimize geographic placement of workloads for user locations
- Optimize areas of code that consume the most time or resources
- Optimize impact on customer devices and equipment
- Implement a data classification policy
- Use lifecycle policies to delete unnecessary data
- Minimize data movement across networks
- Optimize your use of GPUs
- Adopt development and testing methods that allow rapid introduction of potential sustainability improvements
- Increase the utilization of your build environments

The AWS Well-Architected Tool

- Helps you review the state of your workloads and compares them to the latest AWS architectural best practices
- Gives you access to knowledge and best practices used by AWS architects, whenever you need it
- Delivers an action plan with step-by-step guidance on how to build better workloads for the cloud
- Provides a consistent process for you to review and measure your cloud architectures

Section 1 key takeaways

- The AWS Well-Architected Framework provides a consistent approach to evaluate cloud architectures and guidance to help implement designs.
- The AWS Well-Architected Framework documents a set of foundational questions that enable you to understand if a specific architecture aligns well with cloud best practices.
- The AWS Well-Architected Framework is organized into five pillars.
- Each pillar includes a set of design principles and best practices.

Module 9: Cloud Architecture

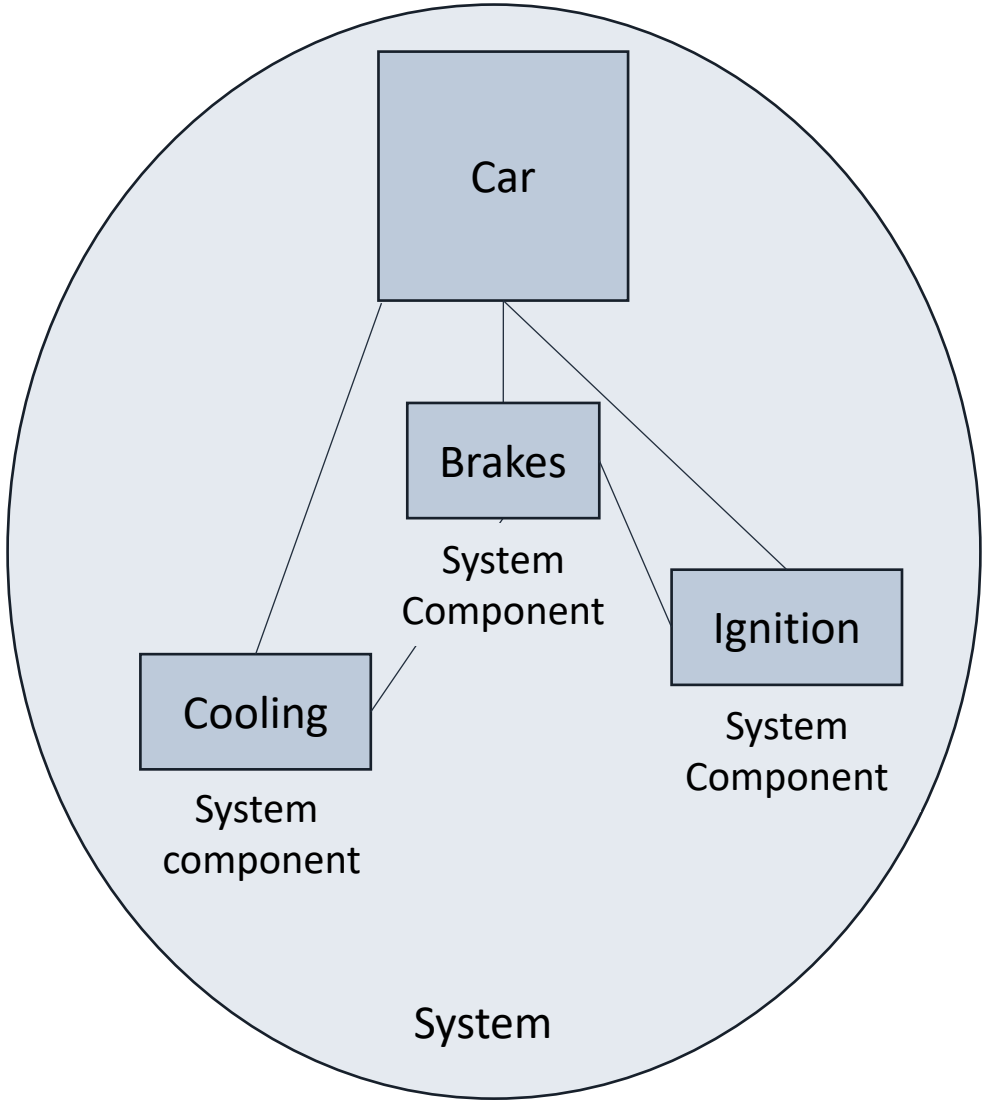
Section 2: Reliability and availability

“Everything fails, all the time.”

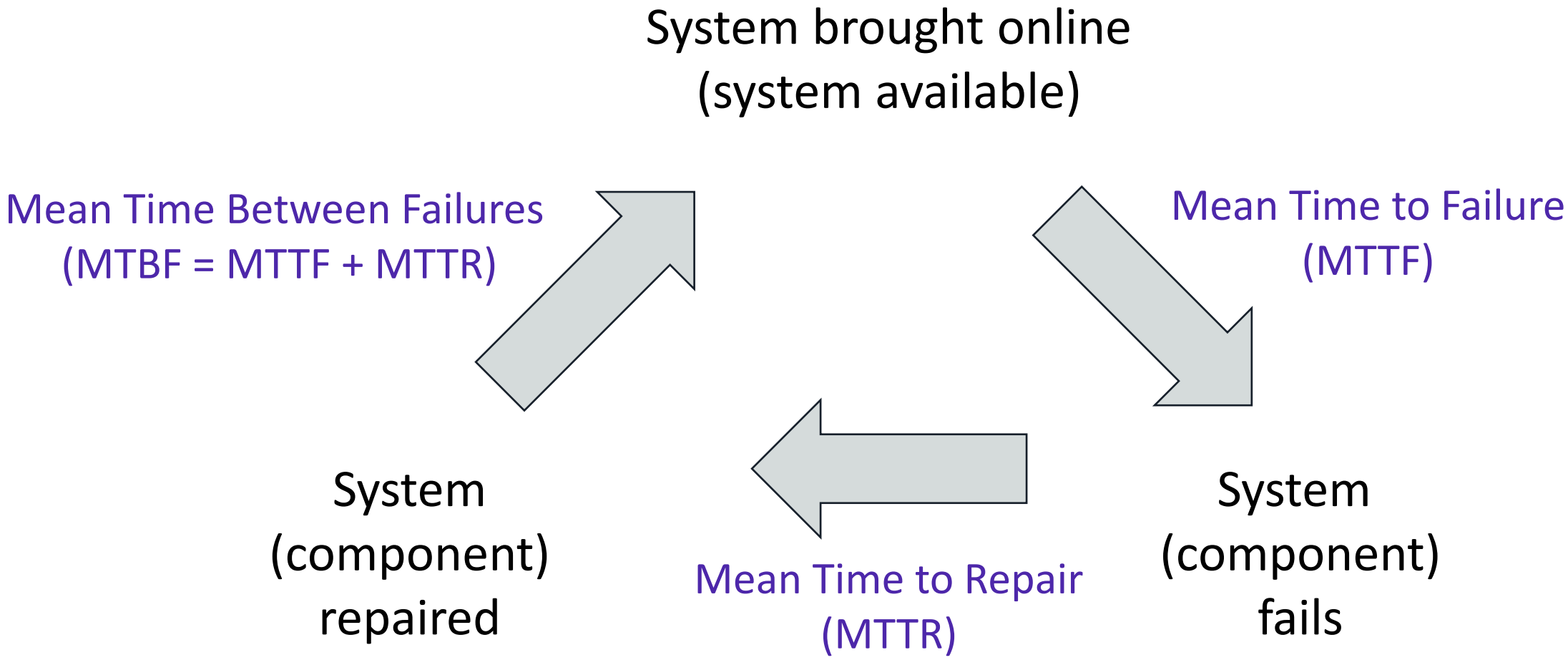
Werner Vogels, CTO, Amazon.com

Reliability

- A measure of your system's ability to provide functionality when desired by the user.
- System includes all system components: hardware, firmware, and software.
- Probability that your entire system will function as intended for a specified period.
- Mean time between failures (MTBF) = total time in service/number of failures



Understanding reliability metrics



Availability

- Normal operation time / total time
- A percentage of uptime (for example, 99.9 percent) over time (for example, 1 year)
- Number of 9s – Five 9s means 99.999 percent availability

High availability

- System can withstand some measure of degradation while still remaining available.
- Downtime is minimized.
- Minimal human intervention is required.

Availability tiers

Availability	Max Disruption (per year)	Application Category
99%	3 days 15 hours	Batch processing, data extraction, transfer, and load jobs
99.9%	8 hours 45 minutes	Internal tools like knowledge management, project tracking
99.95%	4 hours 22 minutes	Online commerce, point of sale
99.99%	52 minutes	Video delivery, broadcast systems
99.999%	5 minutes	ATM transactions, telecommunications systems

Factors that influence availability

Fault tolerance

- The built-in redundancy of an application's components and its ability to remain operational.

Scalability

- The ability of an application to accommodate increases in capacity needs without changing design.

Recoverability

- The process, policies, and procedures that are related to restoring service after a catastrophic event.

Section 2 key takeaways

- Reliability is a measure of your system's ability to provide functionality when desired by the user, and it can be measured in terms of MTBF.
- Availability is the percentage of time that a system is operating normally or correctly performing the operations expected of it (or normal operation time over total time).
- Three factors that influence the availability of your applications are fault tolerance, scalability, and recoverability.
- You can design your workloads and applications to be highly available, but there is a cost tradeoff to consider.

Module 9: Cloud Architecture

Section 3: AWS Trusted Advisor

AWS Trusted Advisor

AWS Trusted Advisor

- Online tool that provides real-time guidance to help you provision your resources following AWS best practices.
- Looks at your entire AWS environment and gives you real-time recommendations in five categories.

Cost Optimization

0 9 0

$7,516.85

Potential monthly savings

Performance

3 7 0

Security

2 4 11

Fault Tolerance

0 15 5

Service Limits

37 0 1

Activity: Interpret AWS Trusted Advisor recommendations

Activity: Recommendation #1

MFA on Root Account

Description: Checks the root account and warns if multi-factor authentication (MFA) is not enabled. For increased security, we recommend that you protect your account by using MFA, which requires a user to enter a unique authentication code from their MFA hardware or virtual device when interacting with the AWS console and associated websites.

Alert Criteria: MFA is not enabled on the root account.

Recommended Action: Log in to your root account and activate an MFA device.

Activity: Recommendation #2

IAM Password Policy

Description: Checks the password policy for your account and warns when a password policy is not enabled, or if password content requirements have not been enabled. Password content requirements increase the overall security of your AWS environment by enforcing the creation of strong user passwords. When you create or change a password policy, the change is enforced immediately for new users but does not require existing users to change their passwords.

Alert Criteria: A password policy is enabled, but at least one content requirement is not enabled.

Recommended Action: If some content requirements are not enabled, consider enabling them. If no password policy is enabled, create and configure one. See Setting an Account Password Policy for IAM Users.

Activity: Recommendation #3

Security Groups – Unrestricted Access

Description: Checks security groups for rules that allow unrestricted access to a resource. Unrestricted access increases opportunities for malicious activity (hacking, denial-of-service attacks, loss of data).

Alert Criteria: A security group rule has a source IP address with a /0 suffix for ports other than 25, 80, or 443.)

Recommended Action: Restrict access to only those IP addresses that require it. To restrict access to a specific IP address, set the suffix to /32 (for example, 192.0.2.10/32). Be sure to delete overly permissive rules after creating rules that are more restrictive.

Region	Security Group Name	Security Group ID	Protocol	Port	Status	IP Range
us-east-1	WebServerSG	sg-xxxxxxx1 (vpc-xxxxxxx1)	tcp	22	Red	0.0.0.0/0
us-west-2	DatabaseServerSG	sg-xxxxxxx2 (vpc-xxxxxxx2)	tcp	8080	Red	0.0.0.0/0

Activity: Recommendation #4

Amazon EBS Snapshots

Description: Checks the age of the snapshots for your Amazon Elastic Block Store (Amazon EBS) volumes (available or in-use). Even though Amazon EBS volumes are replicated, failures can occur. Snapshots are persisted to Amazon Simple Storage Service (Amazon S3) for durable storage and point-in-time recovery.

Alert Criteria:
Yellow: The most recent volume snapshot is between 7 and 30 days old.
Red: The most recent volume snapshot is more than 30 days old.
Red: The volume does not have a snapshot.

Recommended Action: Create weekly or monthly snapshots of your volumes

Region	Volume ID	Volume Name	Snapshot ID	Snapshot Name	Snapshot Age	Volume Attachment	Status	Reason
us-east-1	vol-xxxxxxxx	My-EBS-Volume				/dev/…	Red	No snapshot

Activity: Recommendation #5

Amazon S3 Bucket Logging

Description: Checks the logging configuration of Amazon Simple Storage Service (Amazon S3) buckets. When server access logging is enabled, detailed access logs are delivered hourly to a bucket that you choose. An access log record contains details about each request, such as the request type, the resources specified in the request, and the time and date the request was processed. By default, bucket logging is not enabled; you should enable logging if you want to perform security audits or learn more about users and usage patterns.

Alert Criteria:

Yellow: The bucket does not have server access logging enabled.

Yellow: The target bucket permissions do not include the owner account. Trusted Advisor cannot check it.

Recommended Action:

Enable bucket logging for most buckets.

If the target bucket permissions do not include the owner account and you want Trusted Advisor to check the logging status, add the owner account as a grantee.

Region	Bucket Name	Target Name	Target Exists	Same Owner	Write Enabled	Reason
us-east-2	my-hello-world-bucket		No	No	No	Logging not enabled

Section 3 key takeaways

- AWS Trusted Advisor is an online tool that provides real-time guidance to help you provision your resources by following AWS best practices.
- AWS Trusted Advisor looks at your entire AWS environment and gives you real-time recommendations in five categories.
- You can use AWS Trusted Advisor to help you optimize your AWS environment as soon as you start implementing your architecture designs.

Module 9: Cloud Architecture

Module wrap-up

Module summary

In summary, in this module you learned how to:

- Describe the AWS Well-Architected Framework, including the five pillars
- Identify the design principles of the AWS Well-Architected Framework
- Explain the importance of reliability and high availability
- Identify how AWS Trusted Advisor helps customers
- Interpret AWS Trusted Advisor recommendations

Complete the knowledge check

Sample exam question

A SysOps engineer working at a company wants to protect their data in transit and at rest. What services could they use to protect their data?

A. Elastic Load Balancing
B. Amazon Elastic Block Store (Amazon EBS)
C. Amazon Simple Storage Service (Amazon S3)
D. All of the above

Additional resources

- AWS Well-Architected website
- AWS Well-Architected Framework whitepaper
- AWS Well-Architected Labs
- AWS Trusted Advisor Best Practice Checks

Thank You

aws academy