2019	2020
Operational Excelence	
How do you determine what your priorities are?	
OPS 1	OPS 1
	Evaluate governance requirements
How do you structure your organization to support your business outcomes?	
	OPS 2
	Resources have identified owners
	Processes and procedures have identified owners
	Operations activities have identified owners responsible for their performance
	Team members know what they are responsible for
	Mechanisms exist to identify responsibility and ownership
	Mechanisms exist to request additions, changes, and exceptions
	Responsibilities between teams are predefined or negotiated
How does your organizational culture support your business outcomes?	
	OPS 3
	Executive Sponsorship
	Team members are empowered to take action when outcomes are at risk
	Escalation is encouraged
	Communications are timely, clear, and actionable
	Experimentation is encouraged
	Team members are enabled and encouraged to maintain and grow their skillsets
	Resource teams appropriately
	Diverse opinions are encouraged and sought within and across teams
How do you design your workload so that you can understand its state?	
OPS 2	OPS 4
How do you reduce defects, ease remediation, and improve flow into production?	
OPS 3	OPS 5
How do you mitigate deployment risks?	
OPS 4	OPS 6
How do you know that you are ready to support a workload?	
OPS 5	OPS 7
Use playbooks to identify issues	Use playbooks to investigate issues
How do you understand the health of your workload?	
OPS 6	OPS 8
How do you understand the health of your operations?	
OPS 7	OPS 9
How do you manage workload and operations events?	
OPS 8	OPS 10
Use a process for root cause analysis	
How do you evolve operations?	
OPS 9	OPS 11
	Perform post-incident analysis
	Perform Knowledge Management

2019	2020
Security	
How do you manage credentials and authentication?	
SEC 1	
Define identity and access management requirements	
Secure AWS 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	
How do you control human access?	
SEC 2	
Define human access requirements	
Grant least privileges	
Allocate unique credentials for each individual	
Manage credentials based on user lifecycles	
Automate credential management	
Grant access through roles or federation	
How do you control programmatic access?	
SEC 3	
Define programmatic access requirements	
Grant least privileges	
Automate credential management	
Allocate unique credentials for each component	
Grant access through roles or federation	
Implement dynamic authentication	
How do you securely operate your workload?	
	SEC 1
	Separate workloads using accounts
	Secure AWS account
	Identify and validate control objectives
	Keep up to date with security threats
	Keep up to date with security recommendations
	Automate testing and validation of security controls in pipelines
	Identify and prioritize risks using a threat model
	Evaluate and implement new security services and features regularly
How do you manage identities for people and machines?	
	SEC 2
	Use strong sign-in mechanisms
	Use temporary credentials
	Store and use secrets securely
	Rely on a centralized identity provider
	Audit and rotate credentials periodically
	Leverage user groups and attributes
How do you manage permissions for people and machines?	
	SEC 3
	Define access requirements
	Grant least privilege access
	Establish emergency access process
	Reduce permissions continuously
	Define permission guardrails for your organization
	Manage access based on life cycle
	Analyze public and cross account access
	Share resources securely
How do you detect and investigate security events?	
SEC 4	SEC 4
Define requirements for logs	
Define requirements for metrics	
Define requirements for alerts	
Analyze logs centrally	Analyze logs, findings, and metrics centrally
Automate alerting on key indicators	
Develop investigation processes	
	Automate response to events
	Implement actionable security events
How do you defend against emerging security threats?	
SEC 5	
Keep up to date with organizational, legal, and compliance requirements	
Keep up to date with security best practices	
Keep up to date with security threats	
Evaluate new security services and features regularly	
Define and prioritize risks using a threat model	
Implement new security services and features	

How do you protect your networks? How do you protect your network resources?	
SEC 6	SEC 5
	Create network layers
Define network protection requirements	
Limit exposure	
Automate configuration management	
How do you protect your compute resources?	
SEC 7	SEC 6
Define compute protection requirements	
Scan for and patch vulnerabilities	Perform vulnerability management
Automate configuration management	Enable people to perform actions at a distance
	Validate software integrity
How do you classify your data?	
SEC 8	SEC 7
Define data classification requirements	
Implement data identification	Identify the data within your workload
Identify the types of data	
	Define data lifecycle management
How do you protect your data at rest?	
SEC 9	SEC 8
Define data management and protection at rest requirements	
Provide mechanisms to keep people away from data	Use mechanisms to keep people away from data
How do you protect your data in transit?	
SEC 10	SEC 9
Define data protection in transit requirements	
Automate detection of data leak	Automate detection of unintended data access
How do you respond to an incident? How do you anticipate, respond to, and recover from incidents?	
SEC 11	SEC 10
Identify tooling	
Develop incident response plans	Develop incident management plans
Identify forensic capabilities	Prepare forensic capabilities

2019	2020
Reliability	
How do you manage service limits? How do you manage service quotas and constraints?	
REL 1	REL 1
Aware of limits but not tracking them	Aware of service quotas and constraints
Monitor and manage limits	Monitor and manage quotas
Use automated monitoring and management of limits	Automate quota management
Accommodate fixed service limits through architecture	Accommodate fixed service quotas and constraints through architecture
Ensure a sufficient gap between the current service limit and the maximum usage to accommodate failover	Ensure that a sufficient gap exists between the current quotas and the maximum usage to accommodate failover
Manage service limits across all relevant accounts and regions	Manage service quotas across accounts and regions
How do you manage your network topology? How do you plan your network topology?	
REL 2	REL 2
Use highly available connectivity between private addresses in public cloud and on-premises environments	Provision redundant connectivity between private networks in the cloud and on-premises environments
Use highly available network connectivity for the users of the workload	Use highly available network connectivity for your workload public endpoints
Enforce non-overlapping private IP address ranges in multiple private address spaces where they are connected	Enforce non-overlapping private IP address ranges in all private address spaces where they are connected
	Prefer hub-and-spoke topologies over many-to-many mesh
How do you design your workload service architecture?	
	REL 3
	Choose how to segment your workload
	Build services focused on specific business domains and functionality
	Provide service contracts per API
How do you design interactions in a distributed system to prevent failures?	
	REL 4
	Identify which kind of distributed system is required
	Implement loosely coupled dependencies
	Make all responses idempotent
	Do constant work
How do you design interactions in a distributed system to mitigate or withstand failures?	
	REL 5
	Implement graceful degradation to transform applicable hard dependencies into soft dependencies
	Throttle requests
	Control and limit retry calls
	Fail fast and limit queues
	Set client timeouts
	Make services stateless where possible
	Implement emergency levers
How does your system adapt to changes in demand? How do you design your workload to adapt to changes in demand?	
REL 3	REL 7
Procure resources automatically when scaling a workload up or down	Use automation when obtaining or scaling resources
Procure resources upon detection of lack of service within a workload	Obtain resources upon detection of impairment to a workload
Procure resources manually upon detection that more resources may be needed soon for a workload	Obtain resources upon detection that more resources are needed for a workload
Load test the workload	Load test your workload
How do you monitor your resources? How do you monitor workload resources?	
REL 4	REL 6
Monitor the workload in all tiers	Monitor all components for the workload (Generation)
	Define and calculate metrics (Aggregation)
Send notifications based on the monitoring	Send notifications (Real-time processing and alarming)
Perform automated responses on events	Automate responses (Real-time processing and alarming)
	Storage and Analytics
	Monitor end-to-end tracing of requests through your system
How do you implement change?	
REL 5	REL 8
Deploy changes in a planned manner	Use runbooks for standard activities such as deployment
	Integrate functional testing as part of your deployment
	Integrate resiliency testing as part of your deployment
	Deploy using immutable infrastructure
	Deploy changes with automation
How do you back up data?	
REL 6	REL 9
dentify all data that needs to be backed up and perform backups or reproduce the data from sources	Identify and back up all data that needs to be backed up, or reproduce the data from sources
Perform data backup automatically or reproduce the data from sources automatically	Perform data backup automatically
Secure and encrypt backups or ensure the data isa vailable from a secure source for reproduction	Secure and encrypt backups

How do you use fault isolation to protect your workload?	
	REL 10
	Deploy the workload to multiple locations
	Automate recovery for components constrained to a single location
	Use bulkhead architectures
How does your system withstand component failures? How do you design your workload to withstand component failures?	
REL 7	REL 11
Monitor all layers of the workload to detect failures	Monitor all components of the workload to detect failures
Implement loosely coupled dependencies	
Implement graceful degradation to transform applicable hard dependencies into soft dependencies	
Automating complete recovery because technology constraints exist in parts or all of the workload requiring a single location	
Deploy the workload to multiple locations	Fail over to healthy resources
	Use static stability to prevent bimodal behavior
Send notifications upon availability impacting events	Send notifications when events impact availability
How do you test resilience? How do you test reliability?	
REL 9	REL 12
Use playbooks for unanticipated failures	Use playbooks to investigate failures
Conduct root cause analysis (RCA) and share results	Perform post-incident analysis
	Test functional requirements
	Test scaling and performance requirements
Inject failures to test resiliency	Test resiliency using chaos engineering
How do you plan for disaster recovery? How do you plan for disaster recovery (DR)?	
Manage configuration drift on all changes	Manage configuration drift at the DR site or region

2019	2020
Performance Efficiency	
How do you select the best performing architecture?	
PERF 1	PERF 1
Factor cost or budget into decisions	Factor cost requirements into decisions
Use guidance from AWS or an APN Partner	Use guidance from your cloud provider or an appropriate partner
How do you select your compute solution?	
PERF 2	PERF 2
How do you select your storage solution?	
PERF 3	PERF 3
How do you select your database solution?	
PERF 4	PERF 4
How do you configure your networking solution?	
PERF 5	PERF 5
Understand available product options	
Use minimal network ACLs	
	Choose appropriately sized dedicated connectivity or VPN for hybrid workloads
Leverage encryption offloading and load-balancing	Leverage load-balancing and encryption offloading
Choose location based on network requirements	Choose your workload's location based on network requirements
How do you evolve your workload to take advantage of new releases?	
PERF 6	PERF 6
Keep up-to-date on new resources and services	Stay up-to-date on new resources and services
How do you monitor your resources to ensure they are performing as expected? How do you monitor your resources to ensure they are performing?	
PERF 7	PERF 7
Establish KPIs to measure workload performance	Establish Key Performance Indicators (KPIs) to measure workload performance
How do you use tradeoffs to improve performance?	
PERF 8	PERF 8

2019	2020
Cost Optimization	
How do you implement cloud financial management?	
	COST 1
	Establish a cost optimization function
	Establish a partnership between finance and technology
	Establish cloud budgets and forecasts
	Implement cost awareness in your organizational processes
	Report and notify on cost optimization
	Monitor cost proactively
	Keep up to date with new service releases
How do you govern usage?	
	COST 2
	Implement goals and targets
How do you monitor usage and cost?	
COST 2	COST 3
Configure AWS Cost and Usage Report	Configure detailed information sources
Define and implement tagging	Add organization information to cost and usage
Report and notify on cost optimization	
Monitor cost proactively	
How do you decommission resources?	
COST 3	COST 4
Decommission resources in an unplanned manner	Decommission resources
How do you evaluate cost when you select services?	
COST 4	COST 5
	Select software with cost effective licensing
How do you meet cost targets when you select resource type and size? **How do you meet cost targets when you select resource type, size and number?**	
COST 5	COST 6
Select resource type and size based on estimates	
Select resource type and size based on metrics	Select resource type and size based on data
	Select resource type and size automatically based on metrics
How do you use pricing models to reduce cost?	
COST 6	COST 7
Implement different pricing models, with low coverage	
	Select third party agreements with cost efficient terms
	Perform pricing model analysis at the master account level
How do you plan for data transfer charges?	
COST 7	COST 8
How do you match supply of resources with demand?	
COST 8	COST 9
Provision resources reactively or unplanned	
	Implement a buffer or throttle to manage demand
Provision resources dynamically	Supply resources dynamically
How do you evaluate new services?	
COST 9	COST 10
Establish a cost optimization function	
Review and implement services in an unplanned way	
Keep up to date with new service releases	