AWS Cloud Readiness Assessment

Alexander Robertson

s275931@uos.ac.uk

2024-07-03

About this Report

Thank you for taking the AWS Cloud Readiness Assessment. This tool was produced by AWS.

Services teams using proven frameworks and principles that have helped thousands of customers successfully plan their AWS cloud migrations.

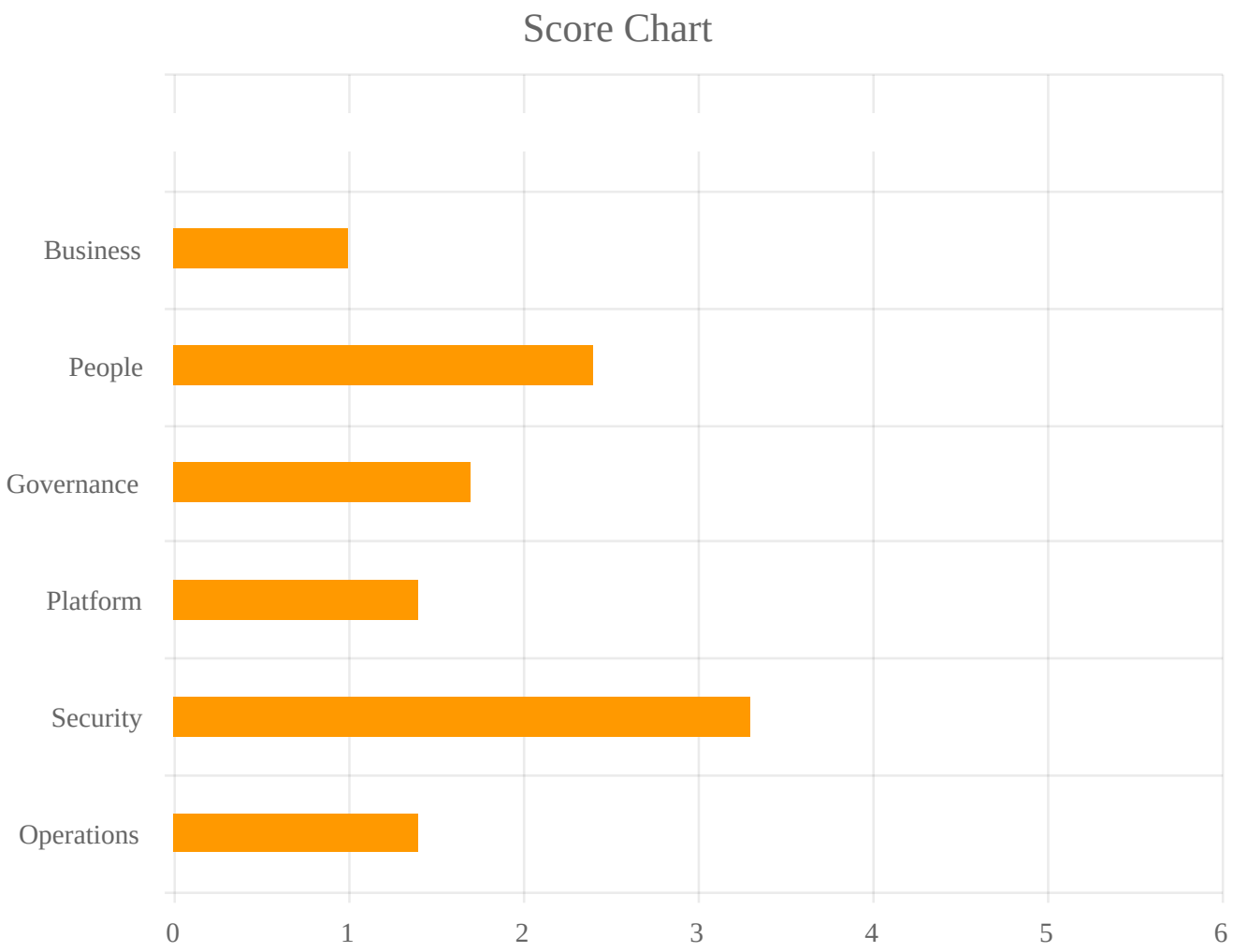
This report helps you understand your cloud readiness scores for each AWS Cloud Adoption Framework (CAF) perspective. It offers additional resources you can use to improve your organization’s readiness. A summary of your cloud adoption readiness scores is shown in a heatmap and radar chart, so you can share your organization’s results with stakeholder.

Summary of Your Cloud Readiness Scores

The chart below shows your organization's cloud readiness scores across the six AWS Cloud Adoption Framework (CAF) perspectives, based on the answers you provided for survey questions. Learn more about CAF.

Green: Questions and Sections that are green indicate a high level of cloud readiness.

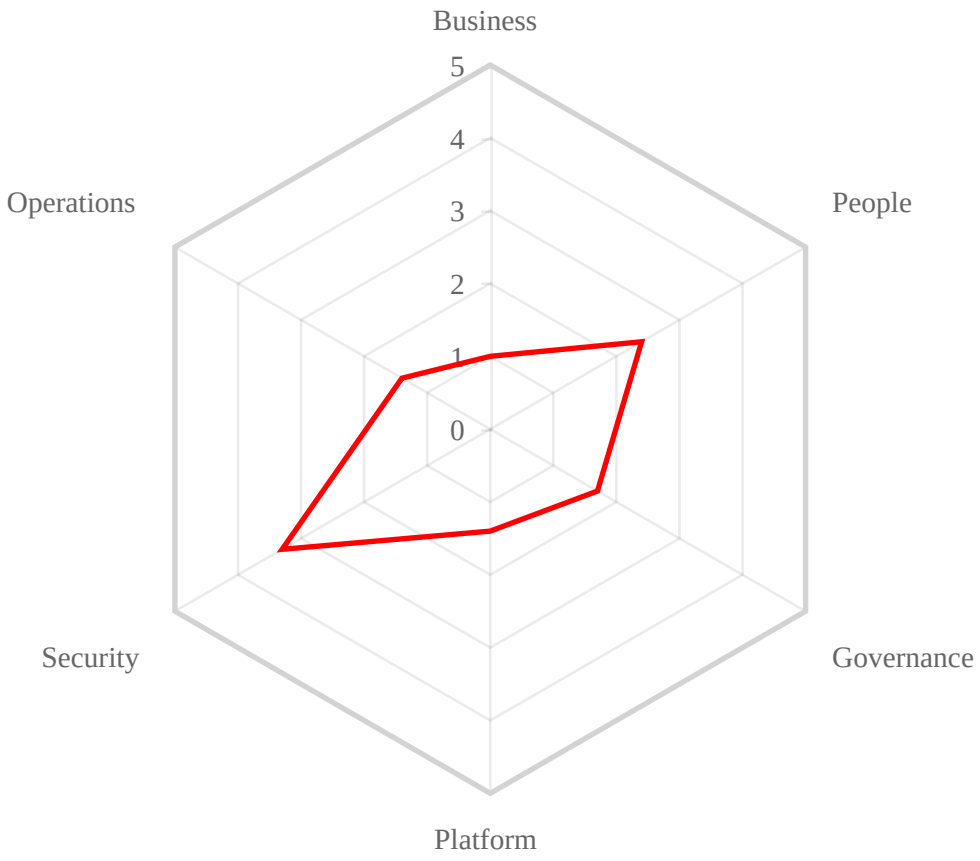
Yellow: Questions and Sections that are yellow indicate that additional prep-work is recommended. Additional resources to help address areas for improvement are provided in this report.



Cloud Readiness Radar Chart

In this section, you will find your assessment scores shown in a radar chart, across the six AWS CAF perspectives. Learn more about CAF.

Visualize your cloud-readiness strengths and weaknesses with the radar chart below, so you can prioritize remediation activities.



Cloud Readiness Heatmap

In this section, you will find your assessment scores shown in a heatmap across the six CAF perspectives. Learn more about CAF.

Green: Questions and Sections that are green indicate a high level of cloud readiness.

Yellow: Questions and Sections that are yellow indicate that additional prep-work is recommended. Additional resources to help address areas for improvement are provided in this report.

Business

- Strategy management
- Portfolio management
- Innovation management
- Product management
- Strategic partnership
- Data monetization
- Business insights
- Data science

People

- Culture evolution
- Transformational leadership
- Cloud fluency
- Workforce transformation
- Change acceleration
- Organization design
- Organizational alignment

Governance

- Program and project management
- Benefits management
- Risk management
- Cloud financial management
- Application portfolio management
- Data governance
- Data curation

Platform

- Platform architecture
- Data architecture
- Platform engineering
- Data engineering
- Provisioning and orchestration
- Modern application development
- Continuous integration and continuous delivery

Security

- Security governance
- Security assurance
- Identity and access management
- Threat detection
- Vulnerability management
- Infrastructure protection
- Data protection
- Application security
- Incident response

Operations

- Observability
- Event management
- Incident and problem management
- Change and release management
- Performance and capacity management
- Configuration management
- Patch management
- Availability and continuity management
- Application management

AWS Cloud Readiness Assessment Summary Report

In this section, you will see your responses across the six AWS CAF perspectives. Learn more about CAF.

Questions and Sections that are green indicate a high level of cloud readiness.

Questions and Sections that are yellow indicate that additional prep-work is recommended. Additional resources to help address areas for improvement are provided in this report.

Business Section

Strategy management

Question: Are you using cloud to enable and shape your long-term business goals?

Response: 1 - No / I don’t know.

Rating: 1

Portfolio management

Question: Are you prioritizing your cloud initiatives in line with your strategic intent, operational efficiency, and your capacity to deliver?

Response: 1 - No / I don’t know.

Rating: 1

Innovation management

Question: Are you leveraging cloud to develop new, and improve existing, processes, products, and experiences?

Response: 1 - No / I don’t know.

Rating: 1

Product management

Question: Do you organize your cross-functional teams around cloud-enabled digital products?

Response: 1 - No / I don’t know.

Rating: 1

Strategic partnership

Question: Are you leveraging your cloud provider to build or grow your business?

Response: 1 - No / I don’t know.

Rating: 1

Data monetization

Question: Have you identified opportunities for leveraging data to improve operations, customer and employee experience, decision-making, or to enable new business models?

Response: 1 - No / I don’t know.

Rating: 1

Business insights

Question: Are you able to gain real-time insights and answer questions about your business?

Response: 1 - No / I don’t know.

Rating: 1

Data science

Question: Do you leverage experimentation, advanced analytics, and machine learning to solve complex

business problems?

Response: 1 - No / I don't know.

Rating: 1

Recommended Actions:

Strategy management

Identify opportunities for retiring technical debt and leverage cloud to optimize your technology and business operations.

Explore new cloud-enabled value propositions and revenue models.

Consider how new or improved cloud-enabled products and services can help you reach new customers or enter new market segments.

Prioritize your strategic objectives and evolve your strategy over time in response to technological developments and changes in your business environment.

Portfolio management

Leverage automated discovery tools and the seven common migration strategies for moving applications to the cloud (known as the 7 Rs) to rationalize your existing application portfolio and build a data-driven business case.

Balance your cloud portfolio by considering short-term and long-term outcomes as well as low-risk (proven) and higher-risk (experimental) opportunities.

Include migration, modernization, and innovation initiatives, and consider financial and non-financial benefits.

Optimize the business value of your portfolio in line with your resource, financial, and schedule constraints.

To reduce your time-to-value, consider increasing the frequency of your planning cycles or adopting a continuous planning strategy.

Innovation management

Develop an innovation strategy that includes a mix of incremental innovation initiatives focused on optimizing your existing products, processes, and experiences, as well as disruptive innovation initiatives focused on enabling new business models.

Create mechanisms for soliciting and selecting ideas in line with your strategic priorities, and develop an end-to-end process for scaling successful innovation pilots.

Product management

Develop a balanced product portfolio that supports your business strategy.

Establish small, enduring, and empowered cross-functional teams that champion the needs of internal and external customers.

Identify product owners, understand customer journeys, define and create product roadmaps, and manage end-to-end product lifecycles and associated value streams.

Leverage your cloud platform and agile methods to rapidly iterate and evolve.

Reduce dependencies between product teams and effectively integrate them into your broader operating model via well-defined interfaces.

Strategic partnership

If you offer cloud-hosted software solutions, cloud-integrated products, or cloud-related professional, consulting, or managed services, strategically partnering with your cloud provider can help you build your cloud expertise, promote your solutions to customers, and drive successful customer engagements.

As you progress along your partnership journey, leverage promotional credits, funding benefits, and co-selling opportunities to help you build or grow your business.

Leverage your cloud provider s marketplace channel to expand reach, and technical resources to help you mature your cloud-based products and services.

Publish joint case studies to highlight success in solving specific business challenges.

Data monetization

To obtain measurable business benefits, develop a comprehensive and long-term data monetization strategy that s aligned with your strategic intent.

Focus on transactional value that helps you understand and complete business transactions, informational value that helps you describe past performance and infer conclusions, and analytical value that helps you automate activities, guide decisions, and predict outcomes.

Monetize data internally within your organization before considering opportunities for external monetization (for example, selling data via a marketplace).

Business insights

Establish cross-functional analytics teams with a good understanding of the business context.

Focus on technical (such as statistics) and non-technical (such as visualization and communication) skills.

Align your analytics efforts with business goals and key performance indicators (KPIs).

Leverage a Data Catalog to locate relevant data products, and visualization tools and techniques to discover trends, patterns, and relationships in the data.

Focus on the big picture first and drill down into the details as required.

Data science

Once you ve identified opportunities for business process transformation, ensure that your Data Catalog contains the data products required to support the building, training, and testing of your machine learning models.

Leverage continuous integration and continuous delivery (CI/CD) practices to improve operational resilience and reproducibility of your machine learning workflows.

Understand how your models make predictions and identify any potential biases.

Deploy suitable models to production and monitor their performance.

To mitigate risk, delegate low confidence predictions for human review.

People Section

Culture evolution

Question: Do you have a plan to evolve your organizational culture in line with your digital transformation aspirations?

Response: 2 - Starting to think about it.

Rating: 2

Transformational leadership

Question: Are your leaders driving transformational change while enabling outcome-focused, cross-functional decision making?

Response: 4 - Yes, but inconsistently implemented across the organization.

Rating: 4

Cloud fluency

Question: Are you building digital acumen to confidently and effectively leverage cloud to accelerate your business outcomes?

Response: 1 - No / I don’t know.

Rating: 1

Workforce transformation

Question: Are you attracting, developing, and retaining a digitally fluent high-performing and adaptable workforce?

Response: 3 - Experimenting with pilot initiatives.

Rating: 3

Change acceleration

Question: Are you accelerating adoption to the new ways of working by applying a programmatic change acceleration framework?

Response: 2 - Starting to think about it.

Rating: 2

Organization design

Question: Are you evolving your organizational structure as you progress through your transformation journey?

Response: 3 - Experimenting with pilot initiatives.

Rating: 3

Organizational alignment

Question: Have you established ongoing partnership between business and technology teams?

Response: 2 - Starting to think about it.

Rating: 2

Recommended Actions:

Culture evolution

To succeed in digital transformation, you ll need to leverage your heritage and core values, while you incorporate new behaviors and mindsets that attract, retain, and empower a workforce that s invested in continuously improving and innovating on behalf of your customers.

Maintain a long-term focus, obsess over customers, and boldly innovate to meet their needs.

Institute an organization-wide approach to recognizing behaviors and goals for all roles that help shape your desired culture.

Consider rapid experimentation, agile methodologies, and cross-functional teams to drive ownership and autonomy, enable rapid decision making, and minimize the need for excessive approvals or bureaucracy.

See AWS Cloud Adoption Framework for additional guidance.

Transformational leadership

Gain active and visible executive sponsorship from both technology and business functions, who will make critical decisions on strategy, vision, scope, and resources, and take actions in communication, coalition building, and holding teams accountable for results.

At both the executive and program levels, ensure that your business and technology leaders co-develop, co-lead, and co-deliver culture change strategies.

Confirm that each layer of management delivers clear and consistent communications to align the organization on cloud value, priorities, and new behaviors.

Consider evolving your cloud leadership function through a transformation office and/or a Cloud Center of Excellence (CCoE) to evangelize and drive your transformation efforts with codified patterns for consistency and scalability.

Incrementally evolve this function to meet your current needs as you progress through your transformation journey.

Cloud fluency

Address your overall training strategy as it relates to timing, tooling, and technology training, and then assess your existing cloud skills to develop a targeted training strategy.

Implement a skills guild to help you generate excitement and build momentum for your transformation journey.

Champion data literacy to advance talent skills and knowledge in data analytics.

Combine virtual, classroom, experiential and just-in-time training, leverage immersion days, and validate skills with formal certifications.

Implement mentoring, coaching, shadowing, and job rotation programs.

Set up communities of practice that own specific domains of interest.

Reward individuals for sharing knowledge, and formalize processes for knowledge elicitation, peer review, and ongoing curation.

Workforce transformation

To succeed in your cloud transformation, take a proactive approach to talent enablement planning beyond traditional HR to include C-suite leadership, and modernize your approaches to leadership, learning, rewards, inclusion, performance management, career mobility, and hiring.

Identify gaps in roles and skills across your entire organization and develop a workforce strategy that will improve your organizational cloud capability.

Leverage talent with digital skills, and those that are eager to learn, and make an example of them.

Strategically consider the use of partners and managed service providers to temporarily or permanently augment your workforce.

To attract new talent, build a strong employer brand by publicly promoting your digital vision and organizational culture, and use it in your recruiting strategy, social networking channels, and external marketing.

Change acceleration

Align and mobilize cross-functional cloud leadership.

Define what success looks like early in the journey.

Envision the future by assessing your organization s readiness for cloud through impact assessments.

Identify key stakeholders, cross-organizational dependencies, key risks, and barriers to transformation.

Develop a change acceleration strategy and roadmap that addresses risks and leverages strengths, comprised of leadership action plans, talent engagement, communications, training, and risk mitigation strategies.

Engage the organization and enable it with new capabilities to increase acceptance to the new ways of working, learn new skills, and accelerate adoption.

Track clearly defined metrics and celebrate early wins.

Establish a change coalition to leverage existing cultural levers that can help you generate momentum.

Make changes stick with continuous feedback mechanisms, and rewards and recognition programs.

Organization design

As you leverage cloud to digitally transform, ensure your organization design supports your core strategies for the business, its people, and operating environment.

Establish a case for change, and assess if your organization design reflects the desired behaviors, roles, and culture that you have determined are key elements to your business success.

Determine if the way your organization is structured and run, in terms of team formations, shift patterns, lines of reporting, decision-making procedures, and communication channels, still supports your desired business outcomes.

Design the new model, and implement it by applying your change acceleration framework.

Consider establishing a centralized team that is built to evolve over time, and which will initially facilitate and enable the transition to a cloud operating model that may be tailored to your vision.

Consider trade-offs between centralized, decentralized, and distributed structures, and align your organization design to support the strategic value of your cloud workloads.

Clarify the relationships between internal and external teams (such as managed service providers).

Organizational alignment

Set measurable targets, joint goals, and mechanisms for cloud adoption, and create expectations for skill development at the role level to generate sustainable change ownership.

Take a top-down approach to developing shared values, processes, systems, working styles, and skills to collectively drive business outcomes and break down functional silos.

Tie innovation efforts to customer experience.

Recognize and reward those who continuously adopt and innovate.

Governance Section

Program and project management

Question: Are you delivering interdependent cloud initiatives in a flexible and coordinated manner?

Response: 1 - No / I don’t know.

Rating: 1

Benefits management

Question: Are you ensuring that the business benefits associated with your cloud investments are realized and sustained?

Response: 1 - No / I don’t know.

Rating: 1

Risk management

Question: Are you leveraging cloud to lower your risk profile?

Response: 1 - No / I don’t know.

Rating: 1

Cloud financial management

Question: Do you plan, measure, and optimize your cloud spend?

Response: 1 - No / I don’t know.

Rating: 1

Application portfolio management

Question: Are you managing and optimizing your application portfolio in support of your business strategy?

Response: 3 - Experimenting with pilot initiatives.

Rating: 3

Data governance

Question: Are you able to exercise authority and control over your data to meet stakeholder expectations?

Response: 4 - Yes, but inconsistently implemented across the organization.

Rating: 4

Data curation

Question: Are you leveraging metadata to organize an inventory of data products in a Data Catalog?

Response: 1 - No / I don't know.

Rating: 1

Recommended Actions:

Program and project management

Manage interdependencies by aligning multiple initiatives for optimized or integrated costs, schedule, effort, and benefits.

Regularly validate your roadmap with your business sponsors and escalate any issues to the senior leadership in a timely fashion to drive accountability and transparency.

Adopt an agile approach to minimize the need to make far-reaching predictions, instead, allowing you to learn from experience and adapt as you progress through your transformation journey.

To help you respond to change, produce well-prioritized backlogs and structure your work in the form of epics and stories.

Benefits management

Identify metrics, quantify desired benefits , and communicate to the relevant stakeholders.

Align the timing and life-span of benefits with your strategic goals.

Incorporate benefits delivery into a benefits realization roadmap.

Regularly measure realized benefits, evaluate progress against the benefits realization roadmap, and adjust the expected benefits as required.

Risk management

Identify and quantify operational risks relating to infrastructure availability, reliability, performance, and security, and business risks relating to reputation, business continuity, and your ability to quickly respond to changing market conditions.

Understand how cloud can help you reduce your risk profile and continue to iteratively identify and manage risk as part of your agile cadence.

Consider leveraging cloud to reduce risks relating to infrastructure operation and failure.

Depending on the needs of your users, mitigate procurement schedule risks by leveraging cloud to instantly provision and deprovision resources.

Cloud financial management

Clarify financial roles and responsibilities as they pertain to cloud, and ensure that key stakeholders across your finance, business and technology organizations have a shared understanding of cloud costs.

Evolve to a more dynamic forecasting and budgeting process, and identify cost variances and anomalies faster.

Align your account structure and tagging strategy with how your organization and products map to the cloud.

Structure your accounts and cost allocations tags to map your cloud resources to specific teams, projects, and business initiatives, and gain a granular view of your consumption patterns.

Define cost categories to organize your cost and usage information using custom rules to simplify showback or chargeback.

Use consolidated billing to help simplify cloud billing and realize volume discounts .

Build guardrails to govern your cloud usage in a scalable manner and with minimal impact to agility.

Leverage demand-based and time-based dynamic provisioning to pay only for the resources you need.

Reduce cloud costs by identifying and eliminating spend associated with idle or underutilized cloud resources.

Centralize the management of on-premises and cloud software licenses to reduce license-related cost overages, reduce non-compliance, and avoid misreporting.

Application portfolio management

An accurate and complete application inventory will help you identify opportunities for rationalization, migration , and modernization.

An effective application portfolio management capability will help you minimize application sprawl, facilitate application lifecycle planning, and ensure ongoing alignment with your cloud transformation strategy.

Start with your most critical applications, define them in terms of the overarching business capabilities, and map them to the underpinning software products and associated resources.

Build a complete picture of each application by sourcing data from related enterprise systems, such as enterprise architecture, IT service management (ITSM), and project and portfolio management.

Identify key technology and business stakeholders (including application owners) and request them to periodically enrich and validate application metadata.

Assess the health of your application portfolio on a regular basis with a view to maximizing the value that your organization derives from its application investments.

Data governance

Define and assign key roles, including data owners, stewards, and custodians.

Consider adopting a federated (data mesh) approach to governance.

Specify standards, including data dictionaries, taxonomies, and business glossaries.

Identify what datasets need to be referenced and model the relationships between reference data entities.

Develop data lifecycle policies, and implement continuous compliance monitoring.

Prioritize your data quality efforts in line with your strategic and operational data needs.

Establish data quality standards: identify key quality attributes, business rules, metrics, and targets.

Monitor data quality at every step of the data value chain.

Identify root causes of data quality problems and improve relevant processes at the source.

Implement data quality dashboards for critical data products.

Data curation

Identify lead curators with responsibility for moderating the Data Catalog.

In line with your data monetization strategy, catalog key data products, including structured and unstructured data.

Identify and capture relevant technical and business metadata, including lineage.

Leverage standard ontologies, business glossaries, and automation (including machine learning) to tag, index, and auto-classify data.

Augment with manual tagging as necessary and appropriately handle any personally identifiable information (PII).

Consider crowdsourcing data enrichment through social curation; consider empowering data consumers to rate, review, and annotate data products.

Platform Section

Platform architecture

Question: Are you establishing and maintaining guidelines, principles, patterns, and guardrails for your cloud environment?

Response: 2 - Starting to think about it.

Rating: 2

Data architecture

Question: Are you designing and evolving a fit-for-purpose data and analytics architecture?

Response: 2 - Starting to think about it.

Rating: 2

Platform engineering

Question: Have you built a compliant multi-account cloud environment with enhanced security features, and packaged, reusable cloud products?

Response: 2 - Starting to think about it.

Rating: 2

Data engineering

Question: Do you automate and orchestrate data flows across your organization?

Response: 1 - No / I don’t know.

Rating: 1

Provisioning and orchestration

Question: Are you creating, managing, and distributing catalogs of approved cloud products to end users?

Response: 1 - No / I don't know.

Rating: 1

Modern application development

Question: Do you build well-architected cloud-native applications?

Response: 1 - No / I don't know.

Rating: 1

Continuous integration and continuous delivery

Question: Are you evolving and improving applications and services at a faster pace than organizations using traditional software development and infrastructure management processes?

Response: 1 - No / I don't know.

Rating: 1

Recommended Actions:

Platform architecture

A well-architected cloud environment will help you accelerate implementation, reduce risk, and drive cloud adoption.

Create consensus within your organization for enterprise standards that will drive cloud adoption.

Define best practice blueprints and guardrails to facilitate authentication, security, networking, and logging and monitoring.

Consider what workloads you may need to retain on-premises due to latency, data processing, or data residency requirements.

Evaluate such hybrid cloud use cases as cloud bursting, backup and disaster recovery to the cloud, distributed data processing, and edge computing.

Data architecture

A well-designed data and analytics architecture can help you reduce complexity, cost, and technical debt while enabling you to gain actionable insights from exponentially growing data volumes.

Adopt a layered and modular architecture that will allow you to use the right tool for the right job as well as iteratively and incrementally evolve your architecture to meet emerging requirements and use cases.

Based on your requirements, select key technologies for each of your architectural layers, including ingestion, storage, catalog, processing, and consumption.

To simplify ongoing management, consider adopting serverless technologies.

Focus on supporting real-time data processing, and consider adopting a modern data architecture to facilitate data movements between data lakes and purpose-built data stores.

Platform engineering

Deploy your best practice blueprints, and detective and preventative guardrails.

Integrate your cloud environment with your existing ecosystem to enable desired hybrid cloud use cases.

Automate the account provisioning workflow and leverage multiple accounts to support your security and governance goals.

Set up connectivity between your on-premises and cloud environments as well as between different cloud accounts.

Implement federation between your existing identity provider (IdP) and your cloud environment so that users can authenticate using their existing login credentials.

Centralize logging, establish cross-account security audits, create inbound and outbound Domain Name System (DNS) resolvers, and get dashboard visibility into your accounts and guardrails.

Evaluate and certify cloud services for consumption in alignment with corporate standards and configuration management.

Package and continuously improve enterprise standards as self-service deployable products and consumable services.

Leverage infrastructure as code (IaC) to define configurations in a declarative way.

Data engineering

Automated data and analytics platforms and pipelines may help you improve productivity and accelerate time

to market.

Form cross-functional data engineering teams comprising infrastructure and operations, software engineering, and data management.

Leverage metadata to automate pipelines that consume raw and produce optimized data.

Implement relevant architectural guardrails and security controls, as well as monitoring, logging, and alerting to help with pipeline failures.

Identify common data integration patterns and build reusable blueprints that abstract away the complexity of pipeline development.

Share blueprints with business analysts and data scientists and enable them to operate using self-service methods.

Provisioning and orchestration

Maintaining consistent infrastructure provisioning in a scalable and repeatable manner becomes more complex as your organization grows.

Streamlined provisioning and orchestration help you achieve consistent governance and meet your compliance requirements, while enabling users to quickly deploy only the approved cloud products.

Design and implement a centrally-managed, self-service portal for publishing, distributing, browsing, and consuming approved cloud products.

Make your cloud products accessible via APIs as well as via personalized portals.

Integrate with your IT service management (ITSM) tools and automate any updates to your configuration management database (CMDB).

Modern application development

Modern application development practices can help you realize the speed and agility that go with innovation.

Using containers and serverless technologies can help you optimize your resource utilization and automatically scale from zero to peak demands.

Consider decoupling your applications by building them as independent microservices leveraging event-driven architectures.

Implement security in all layers and at each stage of the application development lifecycle.

Automate the process of scaling out and scaling in or use serverless technologies.

Modernize your existing applications to reduce costs, gain efficiencies, and make the most of your existing investments.

Consider replatforming (moving your own containers, databases, or message brokers to managed cloud services) and refactoring (rewriting your legacy applications to a cloud native architecture).

Ensure that your architecture takes into account service quotas and physical resources so that they do not negatively impact your workload performance or reliability.

Continuous integration and continuous delivery

Adopting DevOps practices with continuous integration, testing, and deployment will help you to become more agile so that you can innovate faster, adapt to changing markets better, and grow more efficient at driving business results.

Implement continuous integration and continuous delivery (CI/CD) pipelines.

Start with a minimum viable pipeline for continuous integration and then transition to a continuous delivery pipeline with more components and stages.

Encourage developers to create unit tests as early as possible and to run them before pushing the code to the central repository.

Include staging and production steps in your continuous delivery pipeline and consider manual approvals for production deployments.

Consider multiple deployment strategies, including in-place, rolling, immutable, and blue/green deployments.

Security Section

Security governance

Question: Are you developing, maintaining, and effectively communicating security roles, responsibilities, accountabilities, policies, processes, and procedures?

Response: 3 - Experimenting with pilot initiatives.

Rating: 3

Security assurance

Question: Are you continuously monitoring, evaluating, managing, and improving the effectiveness of your security and privacy programs?

Response: 4 - Yes, but inconsistently implemented across the organization.

Rating: 4

Identity and access management

Question: Are you effectively managing identities and permissions at scale?

Response: 4 - Yes, but inconsistently implemented across the organization.

Rating: 4

Threat detection

Question: Do you understand and identify potential security misconfigurations, threats, or unexpected behaviors?

Response: 4 - Yes, but inconsistently implemented across the organization.

Rating: 4

Vulnerability management

Question: Are you continuously identifying, classifying, remediating, and mitigating security vulnerabilities?

Response: 2 - Starting to think about it.

Rating: 2

Infrastructure protection

Question: Are you validating that systems and services within your workload are protected against unintended and unauthorized access and potential vulnerabilities?

Response: 3 - Experimenting with pilot initiatives.

Rating: 3

Data protection

Question: Do you maintain visibility and control over data, and how it is accessed and used in your organization?

Response: 4 - Yes, but inconsistently implemented across the organization.

Rating: 4

Application security

Question: Do you detect and address security vulnerabilities during the software development process?

Response: 3 - Experimenting with pilot initiatives.

Rating: 3

Incident response

Question: Are you reducing potential harm by effectively responding to security incidents?

Response: 3 - Experimenting with pilot initiatives.

Rating: 3

Recommended Actions:

Security governance

Understand your responsibility for security in the cloud .

Inventory, categorize, and prioritize relevant stakeholders, assets, and information exchanges.

Identify laws, rules, regulations, and standards/frameworks that apply to your industry and/or organization.

Perform an annual risk assessment on your organization; risk assessments can assist in determining the likelihood and impact of identified risks and/or vulnerabilities affecting your organization.

Allocate sufficient resources to identified security roles and responsibilities.

Develop security policies, processes, procedures, and controls in line with your compliance requirements and organizational risk tolerance; continuously update based on evolving risks and requirements.

Security assurance

Document controls into a comprehensive control framework , and establish demonstrable security and privacy controls that meet those objectives.

Review the audit reports , compliance certifications, or attestations that your cloud vendor has obtained to help you understand the controls they have in place, how those controls have been validated, and that controls in your extended IT environment are operating effectively.

Continuously monitor and evaluate your environment to verify the operating effectiveness of your controls, and demonstrate compliance with regulations and industry standards.

Review security policies, processes, procedures, controls, and records, and interview key personnel as required.

Identity and access management

Effective identity and access management helps validate that the right people and machines have access to the right resources under the right conditions.

The AWSWell Architected Framework describes relevant concepts, design principles, and architectural best practices to manage identities . These include: relying on a centralized identity provider; leveraging user groups

and attributes for fine-grained access at scale and temporary credentials; and using strong sign-in mechanisms, such as multi-factor authentication (MFA).

To control access by human and machine identities to AWS and your workloads, set permissions to specific service actions on specific resources under specific conditions; use the principle of least privilege, set permissions boundaries, and use service control policies so the right entities can access the right resources as your environment and user base grow; grant permissions based on attributes (ABAC) so your policies can scale; and continuously validate that your policies provide the protection that you need.

Threat detection

Agree on tactical, operational, and strategic intelligence goals and overall methodology.

Mine relevant data sources, process and analyze data, and disseminate and operationalize insights.

Deploy monitoring ubiquitously within the environment to collect essential information and at ad hoc locations to track specific types of transactions.

Correlate monitoring data from multiple event sources , including network traffic, operating systems, applications, databases, and endpoint devices to provide a robust security posture and enhance visibility.

Vulnerability management

Regularly scan for vulnerabilities to help protect against new threats.

Employ vulnerability scanners and endpoint agents to associate systems with known vulnerabilities.

Prioritize remediation actions based on the vulnerability risk.

Apply remediation actions and report to relevant stakeholders.

Leverage red teaming and penetration testing to identify vulnerabilities in your system architecture; seek prior authorization from your cloud provider as required.

Infrastructure protection

Leverage defense in depth to layer a series of defensive mechanisms aimed at protecting your data and systems.

Create network layers and place workloads with no requirements for internet access in private subnets.

Use security groups , network access control lists , and network firewalls to control traffic.

Apply Zero Trust to your systems and data in accordance with their value.

Leverage virtual private cloud (VPC) endpoints for private connection to cloud resources.

Inspect and filter your traffic at each layer; for example, via a web application firewall and/or a network

firewall .

Use hardened operating system images and physically secure any hybrid cloud infrastructure on-premises and at the edge.

Data protection

Protecting your data from unintended and unauthorized access, and potential vulnerabilities, is one of the key objectives of your security program.

In order to help you determine appropriate protection and retention controls, classify your data based on criticality and sensitivity (for example, personally identifiable information).

Define data protection controls and lifecycle management policies.

Encrypt all data at rest and in transit, and store sensitive data in separate accounts.

Leverage machine learning to automatically discover, classify, and protect sensitive data.

Application security

You can save time, effort, and cost when you find and remediate security flaws during the coding phase of an application, and have confidence in your security posture as you launch into production.

Scan and patch for vulnerabilities in your code and dependencies to help protect against new threats.

Minimize the need for human intervention by automating security-related tasks across your development and operations processes and tools.

Use static code analysis tools to identify common security issues.

Incident response

Educate your security operations and incident response teams about cloud technologies and how your organization intends to use them.

Develop runbooks and create a library of incident response mechanisms. Include key stakeholders to better understand the impact of your choices on the broader organization.

Simulate security events and practice your incident response through table-top exercises and game days.

Iterate on the outcome of your simulation to improve the scale of your response posture, reduce time to value, and further reduce risk.

Conduct post-incident analyses to learn from security incidents by leveraging a standardized mechanism to identify and resolve root causes.

Operation Section

Observability

Question: Are you gaining actionable insights from your infrastructure and application data?

Response: 1 - No / I don’t know.

Rating: 1

Event management

Question: Are you effectively detecting events, assessing their potential impact, and determining appropriate control actions?

Response: 3 - Experimenting with pilot initiatives.

Rating: 3

Incident and problem management

Question: Do you quickly restore service operations and minimize adverse business impact?

Response: 1 - No / I don’t know.

Rating: 1

Change and release management

Question: Are you introducing and modifying workloads while minimizing the risk to production environments?

Response: 1 - No / I don’t know.

Rating: 1

Performance and capacity management

Question: Are you monitoring workload performance while ensuring that capacity meets current and future demands?

Response: 1 - No / I don’t know.

Rating: 1

Configuration management

Question: Are you maintaining an accurate and complete record of all your cloud workloads, their relationships, and configuration changes over time?

Response: 1 - No / I don’t know.

Rating: 1

Patch management

Question: Are you systematically distributing and applying software updates?

Response: 2 - Starting to think about it.

Rating: 2

Availability and continuity management

Question: Are you effectively ensuring availability of business-critical information, applications, and services?

Response: 2 - Starting to think about it.

Rating: 2

Application management

Question: Are you investigating and remediating application issues in a single pane of glass?

Response: 1 - No / I don't know.

Rating: 1

Recommended Actions:

Observability

Develop the telemetry (logs, metrics, and traces) necessary to understand the internal state and health of your workloads.

Monitor application endpoints, assess the impact to the end users, and generate alerts when measurements exceed thresholds.

Use synthetic monitoring to create canaries (configurable scripts that run on a schedule) to monitor your endpoints and APIs.

Implement traces to track requests as they travel through the entire application and identify bottlenecks or performance issues.

Gain insights into resources, servers, databases, and networks using metrics and logs.

Set up real-time analysis of time series data to understand causes of performance impacts.

Centralize data in a single dashboard, giving you a unified view of critical information about your workloads and their performance.

Event management

Being able to filter the noise, focus on priority events, predict impending resource exhaustion, automatically generate alerts and incidents, and identify likely causes and remediation actions will help you improve incident detection and response times.

Establish an event store pattern and leverage machine learning (AIOps) to automate event correlation, anomaly detection, and causality determination.

Integrate with cloud services and third-party tools, including with your incident management system and process.

Automate responses to events to reduce errors caused by manual processes and ensure prompt and consistent responses.

Incident and problem management

Practice incident response gamedays and incorporate lessons learned in your runbooks.

Identify incident patterns to determine problems and corrective measures.

Leverage chatbots and collaboration tools to connect your operations teams, tools, and workflows.

Leverage blameless post-incident analyses to identify contributing factors of incidents and develop corresponding action plans.

Change and release management

Establish change processesthat allow for automated approval workflows that align with the agility of the cloud.

Use deployment management systems to track and implement changes.

Use frequent, small, and reversible changes to reduce the scope of a change.

Test changes and validate the results at all lifecycle stages to minimize the risk and impact of failed deployments.

Automate rollback to previous known good state when outcomes are not achieved to minimize recovery time and reduce errors caused by manual processes.

Performance and capacity management

Although the capacity of the cloud is virtually unlimited, service quotas, capacity reservations, and resource constraints restrict the actual capacity of your workloads. Such capacity constraints need to be understood and effectively managed.

Identify key stakeholders and agree on the objectives, scope, goals, and metrics.

Collect and process performance data and regularly review and report performance against targets.

Periodically evaluate new technologies to improve performance and recommend changes to the goals and metrics as appropriate.

Monitor the utilization of your workloads, create baselines for future comparison, and identify thresholds to expand capacity as required.

Analyze demand over time to ensure capacity matches seasonal trends and fluctuating operating conditions.

Configuration management

Define and enforce a tagging schema that overlays your business attributes to your cloud usage, and leverage tags to organize your resources along technical, business, and security dimensions.

Specify mandatory tags and enforce compliance through policy.

Leverage infrastructure as code (IaC) and configuration management tools for resource provisioning and lifecycle management .

Establish configuration baselines and maintain them through version control .

Patch management

A systematic approach to patch management will ensure that you benefit from the latest updates while minimizing risks to production environments.

Apply important updates during your specified maintenance window and critical security updates as soon as possible.

Notify users in advance with the details of the upcoming updates and allow them to defer patches when other mitigating controls are available.

Update your machine images and test patches before rolling out to production.

To ensure continued availability during patching, consider separate maintenance windows for each Availability Zone (AZ) and environment.

Regularly review patching compliance and alert non-compliant teams to apply required updates.

Availability and continuity management

Back up your data and documentation according to a defined schedule.

Develop a disaster recovery plan as a subset of your business continuity plan.

Identify the threat, risk, impact, and cost of different disaster scenarios for each workload and specify Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) accordingly.

Implement your chosen disaster recover strategy leveraging multi-AZ or multi-Region architecture.

Consider leveraging chaos engineering to improve resiliency and performance with controlled experiments.

Review and test you plans regularly and adjust your approach based on lessons learned.

Application management

Aggregating application data into a single management console will simplify operational oversight and accelerate remediation of application issues by reducing the need to switch context between different management tools.

Integrate with other operational and management systems, such as application portfolio management and CMDB,automate the discovery of your application components and resources, and consolidate application data

into a single management console.

Include software components and infrastructure resources, and delineate different environments, such as development, staging, and production.

To remediate operational issues more quickly and consistently, consider automating your runbooks.

How to Use This Report to Advance Your Cloud Readiness

In preparing for an AWS Cloud migration, we recommend that you review the checklist below as your next step:

1. Review the AWS Migration Readiness Guide. This guide walks readers through what it means to be ready to migrate and how to establish a solid foundation to save time and prevent roadblocks. We discuss the impact and importance of driving organizational change, preparing leadership, and establishing foundational readiness for large-scale migrations. We also present our iterative methodology for executing a successful migration.
2. Next, we encourage customers to use our AWS CAF to help address the six perspectives responded to in the Survey. AWS created theCloud Adoption Framework (AWS CAF) whitepaper to help organizations develop efficient and effective plans for their cloud adoption journey. Each CAF perspective is used to create work streams that uncover gaps in your existing skills and processes.
3. Often customers require specialized skills and experience to help supplement their team. AWS offers professional services to help you realize your desired business outcomes. If you would like to request an executive briefing or consultation please contact your sales representative. If you are new to AWS, you may use this link to request support.

Further Reading:

For additional information, tools and customer case studies please consult the following resources:

- AWS Migration
- AWS Migration Acceleration Program (MAP)
- AWS Migration Hub