An Overview of the AWS Cloud Adoption Framework

AWS Whitepaper

An Overview of the AWS Cloud Adoption Framework: AWS Whitepaper

Table of Contents

An Overview of the AWS Cloud Adoption Framework

Publication date: **November 22, 2021** (*Document revisions* (p. 30))

Abstract

As the proliferation of digital technologies continues to disrupt market segments and industries, adopting Amazon Web Services (AWS) can help you transform your organization to meet the changing business conditions and evolving customer needs. As the world's most comprehensive and broadly adopted cloud platform, AWS can help you lower costs, reduce business risks, improve operational efficiency, become more agile, innovate faster, create new revenue streams, and reinvent customer and employee experience.

The AWS Cloud Adoption Framework (AWS CAF) leverages AWS experience and best practices to help you digitally transform and accelerate your business outcomes through innovative use of AWS. Use the AWS CAF to identify and prioritize transformation opportunities, evaluate and improve your cloud readiness, and iteratively evolve your transformation roadmap.

Introduction

Rapid proliferation of digital technologies has accelerated change and increased competition across a range of market segments and industries. Because sustaining any particular competitive advantage has become increasingly difficult, enterprises are being forced to reinvent themselves at increasingly shorter time intervals. For example, 50% of companies on the S&P 500 are projected to be replaced in the next decade.

Similarly, citizens' evolving expectations and behaviors are putting pressure on public sector organizations to improve digital service delivery. Organizations across the globe are digitally transforming; they are leveraging digital technologies to drive organizational change that allows them to adapt to changing market conditions, delight their customers, and accelerate their business outcomes.

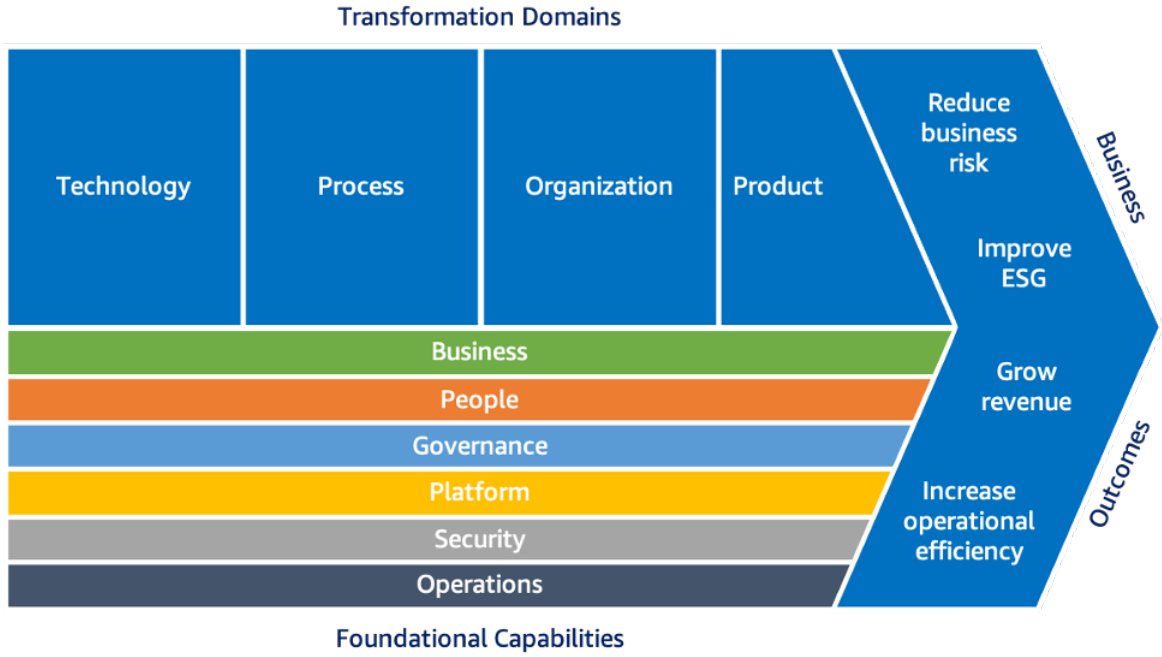
Millions of AWS customers, including the fastest-growing startups, largest enterprises, and leading government organizations, are leveraging AWS to migrate and modernize legacy workloads, become data-driven, digitize and optimize business processes, and reinvent operating and business models. Through cloud powered digital transformation (cloud transformation), they are able to improve their business outcomes, including lower costs, reduce business risks, improve operational efficiency, become more agile, innovate faster, create new revenue streams, and improve customer and employee experience.

Your ability to effectively leverage cloud to digitally transform (your cloud readiness) is underpinned by a set of foundational organizational capabilities. The AWS CAF identifies these capabilities and provides prescriptive guidance that thousands of organizations around the world have successfully used to accelerate their cloud transformation journeys.

AWS and the AWS Partner Network provide tools and services that can help you along each step of the way. AWS Professional Services is a global team of experts that provides assistance through a collection of AWS CAF aligned offerings that can help you achieve specific outcomes related to your cloud transformation.

Accelerating business outcomes with cloud powered digital transformation

The cloud transformation value chain in the following figure shows that business outcomes are accelerated through cloud powered organizational change (transformation) that is enabled by a set of foundational capabilities. The transformation domains represent a value chain where technological transformation enables process transformation which enables organizational transformation that enables product transformation. Key business outcomes include reduced business risk, improved environmental, social and governance (ESG) performance, as well as increased revenue and operational efficiency.



Cloud transformation value chain

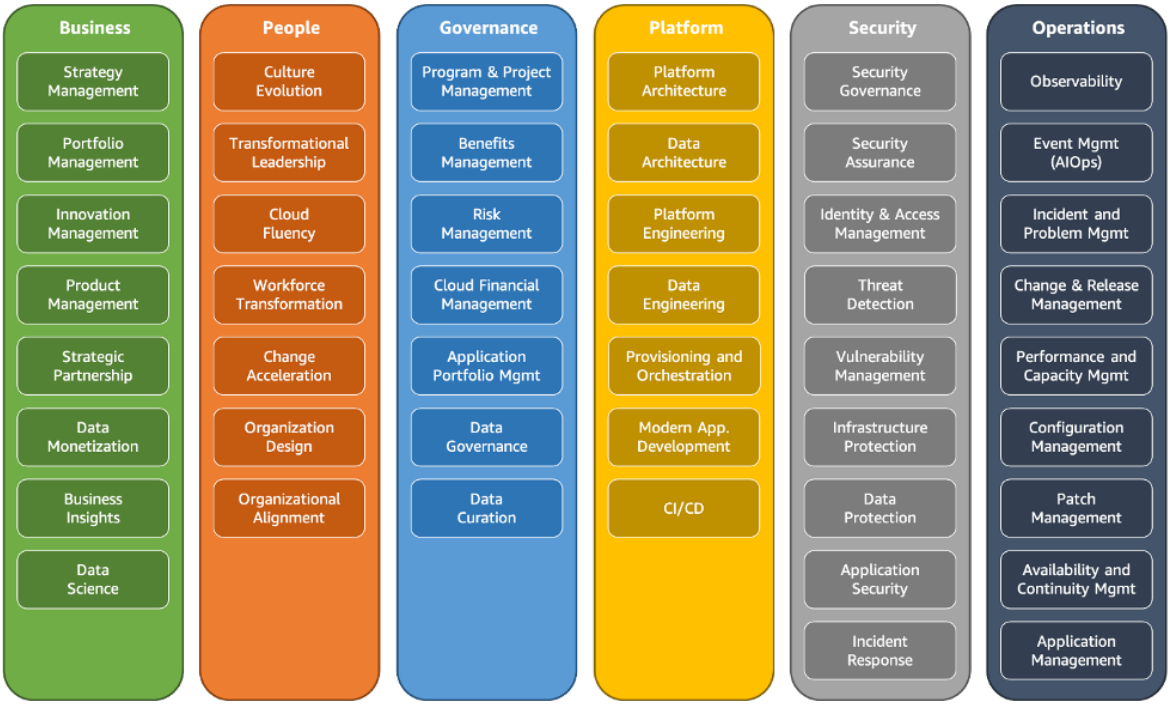
- **Technological transformation** focuses on using cloud to migrate and modernize legacy infrastructure, applications, and data and analytics platforms. Cloud Value Benchmarking shows that migrating from on-premises to AWS leads to a 27% reduction in cost per user, a 58% increase in VMs managed per admin, a 57% decrease in downtime, and a 34% decrease in security events.
- **Process transformation** focuses on digitizing, automating, and optimizing your business operations. This may include leveraging new data and analytics platforms to create actionable insights or using machine learning (ML) to improve your customer service experience, employee productivity and decision-making, business forecasting, fraud detection and prevention, industrial operations, and so on. Doing so may help you improve operational efficiency while lowering operating costs and improving employee and customer experience.
- **Organizational transformation** focuses on reimagining your operating model; how your business and technology teams orchestrate their efforts to create customer value and meet your strategic intent.

Organizing your teams around products and value streams while leveraging agile methods to rapidly iterate and evolve will help you become more responsive and customer centric.

- **Product transformation** focuses on reimagining your business model by creating new value propositions (products, services) and revenue models. Doing so may help you reach new customers and enter new market segments. Cloud Value Benchmarking shows that adopting AWS leads to a 37% reduction in time-to-market for new features and applications, a 342% increase in code deployment frequency, and a 38% reduction in the time to deploy new code.

Foundational capabilities

Each of the transformation domains described in the preceding section is enabled by a set of foundational capabilities shown in the following figure. A capability is an organizational ability to leverage processes to deploy resources (people, technology, and any other tangible or intangible assets) to achieve a particular outcome. AWS CAF capabilities provide best practice guidance that helps you improve your cloud readiness (your ability to effectively leverage cloud to digitally transform). AWS CAF groups its capabilities in six perspectives: Business, People, Governance, Platform, Security, and Operations. Each perspective comprises a set of capabilities that functionally related stakeholders own or manage in your cloud transformation journey.



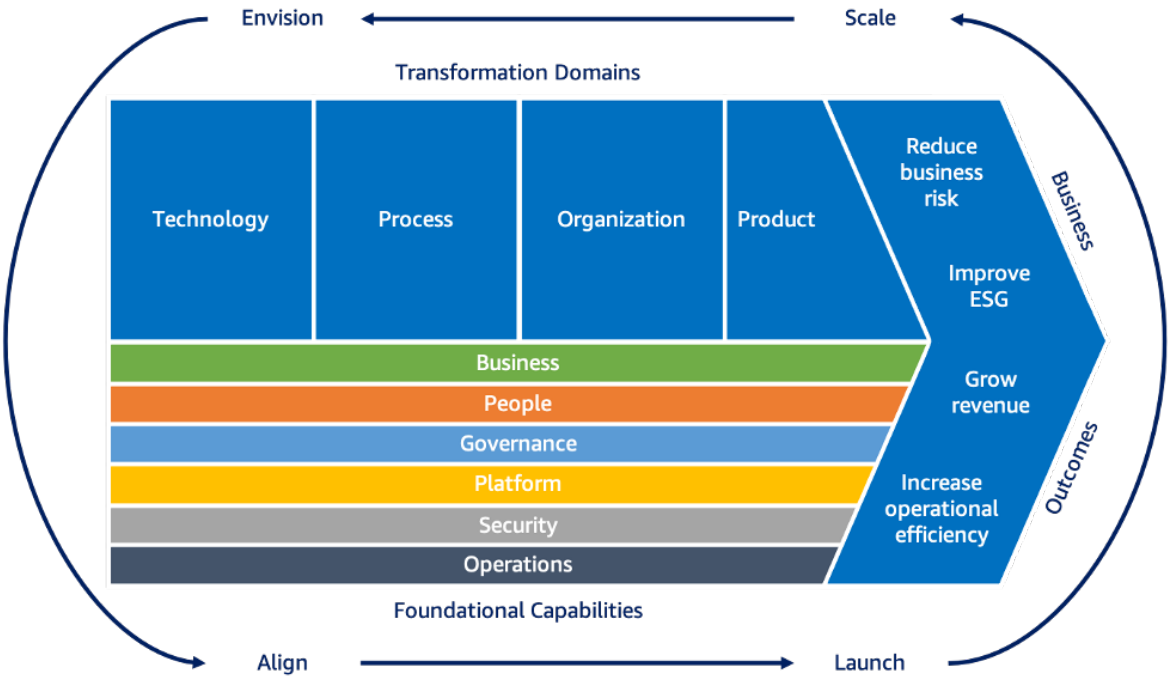
AWS CAF perspectives and foundational capabilities

- **Business perspective** helps ensure that your cloud investments accelerate your digital transformation ambitions and business outcomes. Common stakeholders include chief executive officer (CEO), chief financial officer (CFO), chief operations officer (COO), chief information officer (CIO), and chief technology officer (CTO).
- **People perspective** serves as a bridge between technology and business, accelerating the cloud journey to help organizations more rapidly evolve to a culture of continuous growth, learning, and where change becomes business-as-normal, with focus on culture, organizational structure, leadership, and workforce. Common stakeholders include CIO, COO, CTO, cloud director, and cross-functional and enterprise-wide leaders.
- **Governance perspective** helps you orchestrate your cloud initiatives while maximizing organizational benefits and minimizing transformation-related risks. Common stakeholders include chief transformation officer, CIO, CTO, CFO, chief data officer (CDO), and chief risk officer (CRO).
- **Platform perspective** helps you build an enterprise-grade, scalable, hybrid cloud platform, modernize existing workloads, and implement new cloud-native solutions. Common stakeholders include CTO, technology leaders, architects, and engineers.

- **Security perspective** helps you achieve the confidentiality, integrity, and availability of your data and cloud workloads. Common stakeholders include chief information security officer (CISO), chief compliance officer (CCO), internal audit leaders, and security architects and engineers.
- **Operations perspective** helps ensure that your cloud services are delivered at a level that meets the needs of your business. Common stakeholders include infrastructure and operations leaders, site reliability engineers, and information technology service managers.

Your cloud transformation journey

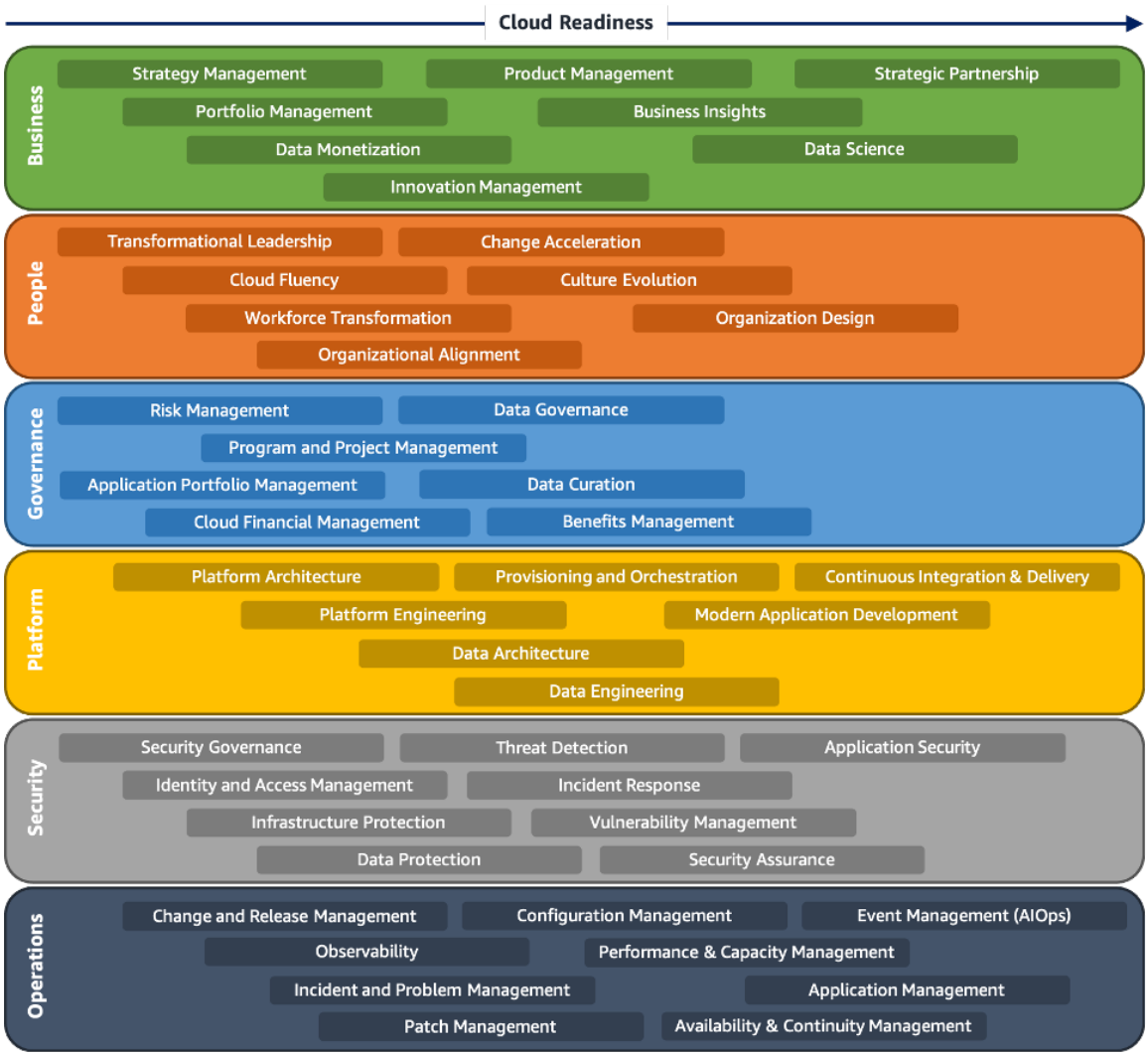
Each organization's cloud journey is unique. To succeed in your transformation, you'll need to envision your desired target state, understand your cloud readiness, and adopt an agile approach to closing the gaps. Transforming incrementally will allow you to demonstrate value quickly while minimizing the need to make far-reaching predictions. Adopting an iterative approach will help you maintain momentum and evolve your roadmap as you learn from experience. The AWS CAF recommends four iterative and incremental cloud transformation phases shown in the following figure.



Cloud transformation journey

- **Envision phase** focuses on demonstrating how cloud will help accelerate your business outcomes. It does so by identifying and prioritizing transformation opportunities across each of the four transformation domains in line with your strategic business objectives. Associating your transformation initiatives with key stakeholders (senior individuals capable of influencing and driving change) and measurable business outcomes will help you demonstrate value as you progress through your transformation journey.
- **Align phase** focuses on identifying capability gaps across the six AWS CAF perspectives, identifying cross-organizational dependencies, and surfacing stakeholder concerns and challenges. Doing so will help you create strategies for improving your cloud readiness, ensure stakeholder alignment, and facilitate relevant organizational change management activities.
- **Launch phase** focuses on delivering pilot initiatives in production and on demonstrating incremental business value. Pilots should be highly impactful and if/when successful they will help influence future direction. Learning from pilots will help you adjust your approach before scaling to full production.
- **Scale phase** focuses on expanding production pilots and business value to desired scale and ensuring that the business benefits associated with your cloud investments are realized and sustained.

You may not need to tackle all the foundational capabilities at once. Evolve the foundational capabilities and improve your cloud readiness as you progress through your cloud transformation journey. Consider tailoring the suggested sequence shown in the following figure to your particular needs.



Evolution of AWS CAF perspectives and foundational capabilities

The next sections describe each of the six AWS CAF perspectives and the underpinning capabilities in more detail.

Business perspective: strategy and outcomes

The *business* perspective focuses on ensuring that your cloud investments accelerate your digital transformation ambitions and business outcomes. It comprises eight capabilities shown in the following figure. Common stakeholders include the CEO, CFO, COO, CIO, and CTO.

AWS CAF Business perspective capabilities

- **Strategy management** – Leverage cloud to accelerate your business outcomes. Consider how cloud can support and shape your long-term business goals. Identify opportunities for retiring technical debt and leveraging 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** – Prioritize cloud products and initiatives in line with strategic intent, operational efficiency, and your capacity to deliver. Delivering the right cloud products and initiatives at the right time will help you operationalize your strategy and accelerate your business outcomes. 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 (lower costs and/or increased revenue) and non-financial (for example, improved customer and employee experience) 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** – Leverage cloud to develop new, and improve existing, processes, products, and experiences. By enabling you to instantly provision and shut down resources, cloud can help you reduce your time-to-value and innovation-related cost and risk. To fully take advantage of the potential for increased business agility that comes with cloud adoption, 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** – Manage data- and cloud-enabled offerings that deliver repeatable value to internal and external customers as products through their lifecycles. Organizing your teams around data- and cloud-enabled products will help you become more agile and customer-centric:
  - 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** – Build or grow your business through a strategic partnership with your cloud provider. 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** – Leverage data to obtain measurable business benefit. Cloud facilitates the collection, storage, and analysis vast amounts of data. To obtain measurable business benefits, develop a comprehensive and long-term data monetization strategy that's aligned with your strategic intent. Identify opportunities for leveraging data and analytics to improve operations, customer and employee experience, and decision-making, as well as to enable new business models.

  For example, consider leveraging customer behavior insights to drive hyper-personalization and localization, micro-segmentation, subscriber retention, loyalty and rewards programs, and the like. 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. First monetize data internally within your organization before considering opportunities for external monetization (for example, selling data via a marketplace).
- **Business insights** – Gain real-time insights and answer questions about your business. Near real-time descriptive insights can help you complete your data monetization strategy by enabling you to track business performance, improve decision-making, and optimize operations. 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 the 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** – Leverage experimentation, advanced analytics, and machine learning to solve complex business problems. Predictive and prescriptive analytics can help you complete your data monetization strategy by enabling you to improve operational effectiveness and decision-making as well as customer and employee experience.

  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 perspective: culture and change

The *people* perspective serves as a bridge between technology and business, accelerating the cloud journey to help organizations more rapidly evolve to a culture of continuous growth, learning, and where change becomes business-as-normal, with focus on culture, organizational structure, leadership, and workforce. This perspective comprises seven capabilities shown in the following figure. Common stakeholders include CIO, COO, CTO, cloud director, and cross-functional and enterprise-wide leaders.

AWS CAF People perspective capabilities

- **Culture evolution** – Evaluate, incrementally evolve, and codify organizational culture with digital transformation aspirations, and best practices for agility, autonomy, clarity, and scalability. 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.
- **Transformational leadership** – Strengthen your leadership capability and mobilize leaders to drive transformational change and enable outcome-focused, cross-functional decision making. To succeed with cloud transformation, your leaders must put as much focus on the people side of change as they do on technology, as without an effective blend of technical and business leadership, your transformation may slow down or stall. 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** – Build digital acumen to confidently and effectively leverage cloud to accelerate business outcomes. The requirement for an exceptional workforce goes beyond adapting to a digital environment, and the greatest challenge is not the technology itself, but, rather, the ability to hire, develop, retain and motivate a talented, knowledgeable, proficient, and high-performing workforce.

  Given the rapid pace of technological innovation, address your overall training strategy as it relates to timing, tooling, and technology training, and then assess your existing cloud skills to develop a targetedtraining 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** – Enable talent and modernize roles to attract, develop, and retain a digitally fluent high-performing and adaptable workforce that can autonomously drive key capabilities. 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.

  You will need a diverse and inclusive workforce with the appropriate mix of technical and non-technical skills. 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** – Accelerate adoption to the new ways of working by applying a programmatic change acceleration framework that identifies and minimizes impacts to people, culture, roles, and organization structure when moving from current to future state. Cloud transformation creates widespread changes across business and technology functions, and organizations that apply a programmatic end-to-end change process that is structured, integrated, and transparent achieve higher rates of success with value realization and adoption to the new ways of working.

  Customize and apply a change acceleration framework from project onset to enable organizational alignment, create a one shared enterprise reality, and reduce waste from the process. 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** – Assess organization design for alignment with the new cloud ways of working, and evolve as you progress through your transformation journey. 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 (using managed service providers).

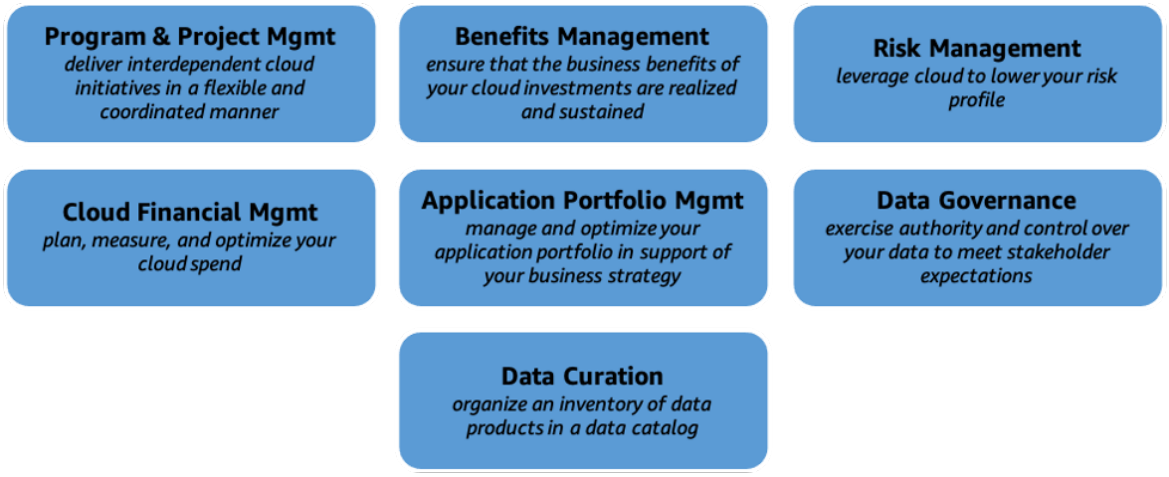
- **Organizational alignment** – Establish ongoing partnership between organizational structures, business operations, processes, talent, and culture to enable enterprise rapid adaptation to market conditions, and the ability to capitalize on new opportunities. To augment cloud value realization, organizational alignment serves as a bridge between technology and business strategy so that technology changes are embraced by the business units who produce business outcomes.

  Prioritize business outcomes like operational resiliency, business agility, and product/service innovation. Enable talent to work autonomously, focus on key objectives, make better decisions, and improve productivity. Get leadership commitment on the early application of a change acceleration framework so that people capabilities in leadership agility, workforce transformation, talent enablement, culture, and organization structure are integrated from the start.

  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 develop 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 perspective: control and oversight

The *governance* perspective focuses on orchestrating your cloud initiatives while maximizing organizational benefits and minimizing transformation-related risks. It comprises seven capabilities shown in the following figure. Common stakeholders include chief transformation officer, CIO, CTO, CFO, CDO, and CRO.



AWS CAF Governance perspective capabilities

- **Program and project management** – Deliver interdependent cloud initiatives in a flexible and coordinated manner. Complex cross-functional cloud transformation initiatives require careful coordination, especially in more traditionally structured organizations. Program management is especially critical since many of these interdependencies only become obvious during delivery. 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** – Ensure that the business benefits associated with your cloud investments are realized and sustained. The success of your transformation is determined by the resulting business benefits. Clear identification of the desired benefits upfront will allow you to prioritize your cloud investments and track transformation progress over time. 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** – Leverage cloud to lower your risk profile. 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. Reduce the need for large upfront infrastructure expenditures and reduce the risk of purchasing assets that may be no longer needed. Depending on the needs of your users, mitigate procurement schedule risks by leveraging cloud to instantly provision and deprovision resources.

- **Cloud financial management** – Plan, measure, and optimize your cloud spend. Combine the ease of resource provisioning and agility benefits provided by cloud with financial accountability for your teams' cloud spend. This helps ensure your teams continuously optimize their cloud workloads and use the best pricing models. 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.

  To avoid incurring technical debt, ensure your workloads are Well-Architected, and operated in the most cost-effective manner. 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. Differentiate between licenses that are included with cloud resources and licenses that you own. Leverage rule-based controls on the consumption of licenses to set hard or soft limits on new and existing cloud deployments. Use dashboards to create visibility into license usage and accelerate vendor audits. Implement real-time alerts for non-compliance.

- **Application portfolio management** – Manage and optimize your application portfolio in support of your business strategy. Applications underpin your business capabilities and link them to the associated resources. 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** – Exercise authority and control over your data to meet stakeholder expectations. Your business processes and analytics capabilities depend on accurate, complete, timely, and relevant data. 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

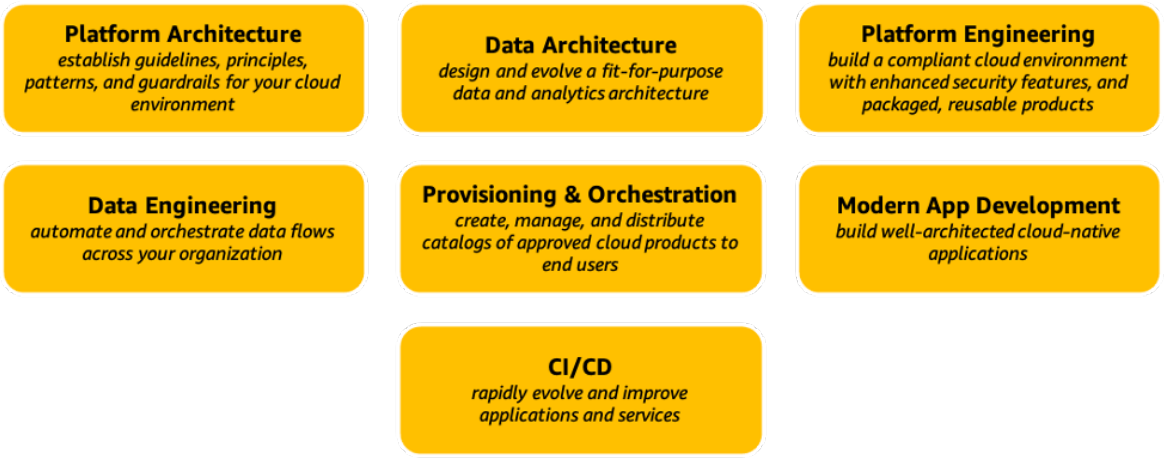
of the data value chain. Identify root causes of data quality problems and improve relevant processes at the source. Implement data quality dashboards for critical data products.

- **Data curation** – Collect, organize, access, and enrich metadata and use it to organize an inventory of data products in a Data Catalog. A Data Catalog can help facilitate data monetization and self-service analytics by helping data consumers quickly locate relevant data products as well as understand their context, such as provenance and quality.

  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. In other words, consider empowering data consumers to rate, review, and annotate data products.

Platform perspective: infrastructure and applications

The *platform* perspective focuses on accelerating the delivery of your cloud workloads via an enterprise-grade, scalable, hybrid cloud environment. It comprises seven capabilities shown in the following figure. Common stakeholders include CTO, technology leaders, architects, and engineers.



AWS CAF Platform perspective capabilities

- **Platform architecture** – Establish and maintain guidelines, principles, patterns, and guardrails for your cloud environment. A well-architectedcloud 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** – Design and evolve a fit-for-purpose data and analytics 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 Lake House architecture to facilitate data movements between data lakes and purpose-built data stores.
- **Platform engineering** – Build a compliant multi-account cloud environment with enhanced security features, and packaged, reusable cloud products. An effective cloud environment will allow your teams to easily provision new accounts, while ensuring that those accounts conform to organizational policies. A curated set of cloud products will enable you to codify best practices, helping you with governance while increasing the speed and consistency of your cloud deployments. 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** – Automate and orchestrate data flows across your organization. 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** – Create, manage, and distribute catalogs of approved cloud products to end users. 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** – Build well-architected cloud-native applications. 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** – Evolve and improve applications and services at a faster pace than organizations using traditional software development and infrastructure management processes. 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 perspective: compliance and assurance

The *security* perspective helps you achieve the confidentiality, integrity, and availability of your data and cloud workloads. It comprises nine capabilities shown in the following figure. Common stakeholders include CISO, CCO, internal audit leaders, and security architects and engineers.

AWS CAF Security perspective capabilities

- **Security governance** – Develop, maintain, and effectively communicate security roles, responsibilities, accountabilities, policies, processes, and procedures. Ensuring clear lines of accountability is critical to the effectiveness of your security program. Understanding your assets, security risks, and compliance requirements that apply to your industry and/or organization will help you prioritize your security efforts. Providing ongoing direction and advice will help accelerate your transformation by allowing your teams to move faster.

  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** – Continuously monitor, evaluate, manage, and improve the effectiveness of your security and privacy programs. Your organization, and the customers you serve, need trust and confidence that the controls that you have implemented will enable you to meet regulatory requirements, and effectively and efficiently manage security and privacy risks in line with your business objectives and risk tolerance.

  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 permissions management** – Manage identities and permissions at scale. You can create identities in AWS or connect your identity source, and then grant users the necessary permissions, so they can sign-in, access, provision, or orchestrate AWS resources and integrated applications. Effective identity and access management helps validate that the right people and machines have access to the right resources under the right conditions.

  The AWS Well 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** – Understand and identify potential security misconfigurations, threats, or unexpected behaviors. A better understanding of security threats will enable you to prioritize protective controls. Effective threat detection will allow you to respond to threats faster and learn from security events. 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. Consider leveraging deception technology (for example, honeypots) to gain understanding of unauthorized user behavior patterns.
- **Vulnerability management** – Continuously identify, classify, remediate, and mitigate security vulnerabilities. Vulnerabilities may also be introduced with changes to existing systems or with addition of new systems. 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** – Validate that systems and services within your workload are protected against unintended and unauthorized access and potential vulnerabilities. Protecting your infrastructure from unintended and unauthorized access and potential vulnerabilities will help you elevate your security posture in the cloud. 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** – Maintain visibility and control over data, and how it is accessed and used in your organization. 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** – Detect and address security vulnerabilities during the software development process. 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** – Reduce potential harm by effectively responding to security incidents. Quick, effective, and consistent responses to security incidents will help you reduce potential harm. 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.

Operations perspective: health and availability

The *operations* perspective focuses on ensuring that cloud services are delivered at a level that is agreed upon with your business stakeholders. Automating and optimizing operations will allow you to effectively scale while improving the reliability of your workloads. This perspective comprises nine capabilities shown in the following figure. Common stakeholders include infrastructure and operations leaders, site reliability engineers, and information technology service managers.

AWS CAF Operations perspective capabilities

- **Observability** – Gain actionable insights from your infrastructure and application data. When you are operating at cloud speed and scale, you need to be able to spot problems as they arise, ideally before they disrupt the customer experience. 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 (AIOps)** – Detect events, assess their potential impact, and determine the appropriate control action. 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** – Quickly restore service operations and minimize adverse business impact. With cloud adoption, processes for response to service issues and application health issues can be highly automated, resulting in greater service uptime. As you move to a more distributed

operating model, streamlining interactions between relevant teams, tools, and processes will help you accelerate the resolution of critical and/or complex incidents. Define escalation paths in your runbooks, including what triggers escalation, and procedures for escalation.

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** – Introduce and modify workloads while minimizing the risk to production environments. Traditional release management is a complex process that is slow to deploy and difficult to roll back. Cloud adoption provides the opportunity to leverage CI/CD techniques to rapidly manage releases and rollbacks. Establish change processes that 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** – Monitor workload performance and ensure that capacity meets current and future demands. 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** – Maintain an accurate and complete record of all your cloud workloads, their relationships, and configuration changes over time. Unless effectively managed, the dynamic and virtual nature of cloud resource provisioning can lead to a configuration drift. 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** – Systematically distribute and apply software updates. Software updates address emerging security vulnerabilities, fix bugs, and introduce new features. 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** – Ensure availability of business-critical information, applications, and services. Building cloud-enabled backup solutions requires careful consideration of existing technology investments, recovery objectives, and available resources. Timely restoration after disasters and security events will help you maintain system availability and business continuity. 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.

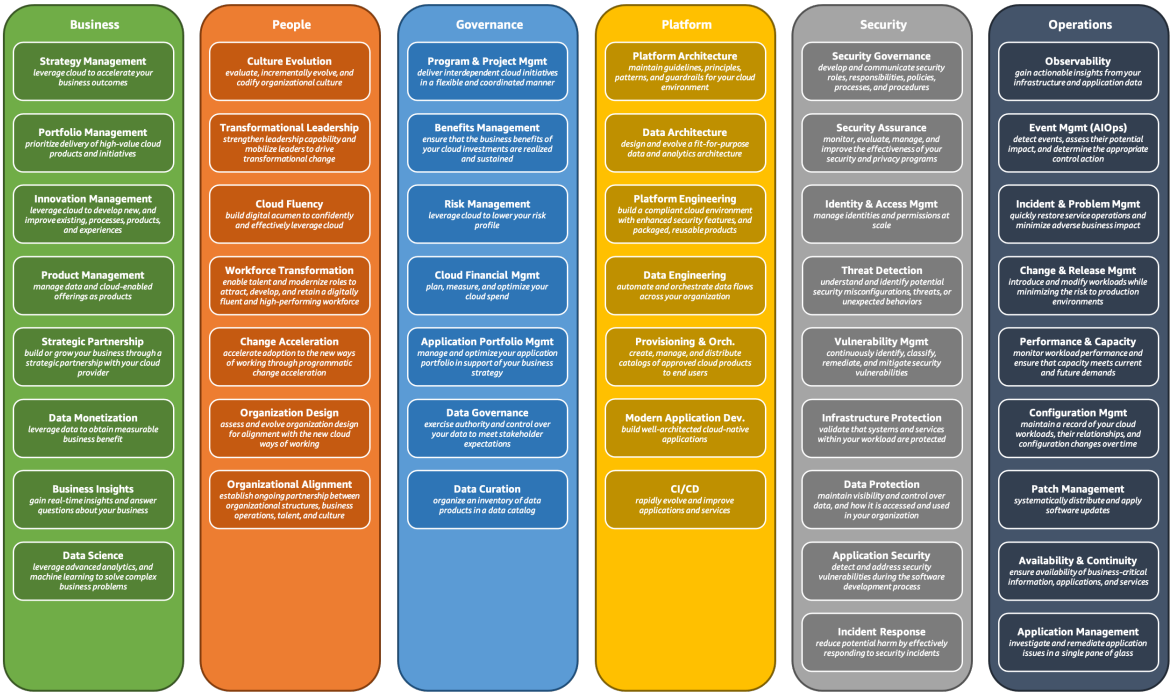
- **Application management** – investigate and remediate application issues in a single pane of glass. Aggregating application data into a single management console will simplify operational oversight and accelerate remediation of application issues by reducing the need to switch context between different 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.

Conclusion

As technological innovation continues to accelerate, the need for continuous digital transformation will become even more pressing. The AWS CAF leverages AWS experience and best practices to help you accelerate your business outcomes through innovative use of AWS. Use the AWS CAF to identify and prioritize transformation opportunities, evaluate and improve your cloud readiness, and iteratively evolve your transformation roadmap.

Appendix: AWS CAF capabilities poster



AWS CAF foundational capabilities

Contributors

- Authored by Dr. Saša Baškarada, World Wide Lead, AWS CAF, with input from numerous AWS subject matter experts.

Further reading

For additional information, refer to:

- AWS Architecture Center
- AWS case studies
- AWS General Reference
- AWS glossary
- AWS Knowledge Center
- AWS Prescriptive Guidance
- AWS Quick Starts
- AWS Security Documentation
- AWS Solutions Library
- AWS Training and Certification
- AWS Well-Architected
- AWS Whitepapers & Guides
- Getting Started with AWS
- Overview of Amazon Web Services

Document revisions

To be notified about updates to this whitepaper, subscribe to the RSS feed.

update-history-change	update-history-description	update-history-date
Third publication (p. 30)	Updated and expanded capabilities. Added transformation domains and journey phases.	November 22, 2021
Second publication (p. 30)	Structural changes to perspectives and capabilities.	February 1, 2017
Initial publication (p. 30)	Whitepaper first published.	February 1, 2015

Notices

Customers are responsible for making their own independent assessment of the information in this document. This document: (a) is for informational purposes only, (b) represents current AWS product offerings and practices, which are subject to change without notice, and (c) does not create any commitments or assurances from AWS and its affiliates, suppliers or licensors. AWS products or services are provided “as is” without warranties, representations, or conditions of any kind, whether express or implied. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.