Cloud Forward

A Framework for Embracing the Cloud in Oregon

Version 1.0

ENTERPRISE
information services

Cloud Forward

A Framework for Embracing the Cloud in Oregon – version I. 0

Vision.

Oregon will strive to conduct 75% of its business via cloud-based services and infrastructure by 2025–leveraging these platforms to modernize state IT systems and make Oregon a place where everyone has an opportunity to thrive.

Cloud Forward – Guiding Principles

Cloud-First. Cloud will be the first and preferred option for all new IT investments. It should not be conflated with the idea of "cloud everything."

Agility Counts. Cloud migration decisions will be driven by considerations of business agility and overall cloud value, in addition to considerations of cost, time, effort and risk.

Saas, please. Software-as-a-Service (SaaS) will be the preferred cloud tier and be evaluated before other cloud tiers (i.e., PaaS or laaS) or migration models.

Lift-and-Shift Last. As a migration strategy, re-hosting or "lifting and shifting" provides little (if any) cloud value or cost savings. Re-hosting should only be considered as last resort.

Multicloud. Embracing multicloud positions the state to leverage the unique value propositions and capabilities offered by leading cloud service providers.

Upskilling. As a state we are committed to upskilling our existing IT workforce and preparing them for a cloud-defined future.

Business Enablement. Embracing the cloud frees up IT organizations from having to manage traditional IT infrastructure and operations tasks and provides opportunities to enable their business and program units through strategic use of data, business intelligence, integrations, and agile development.

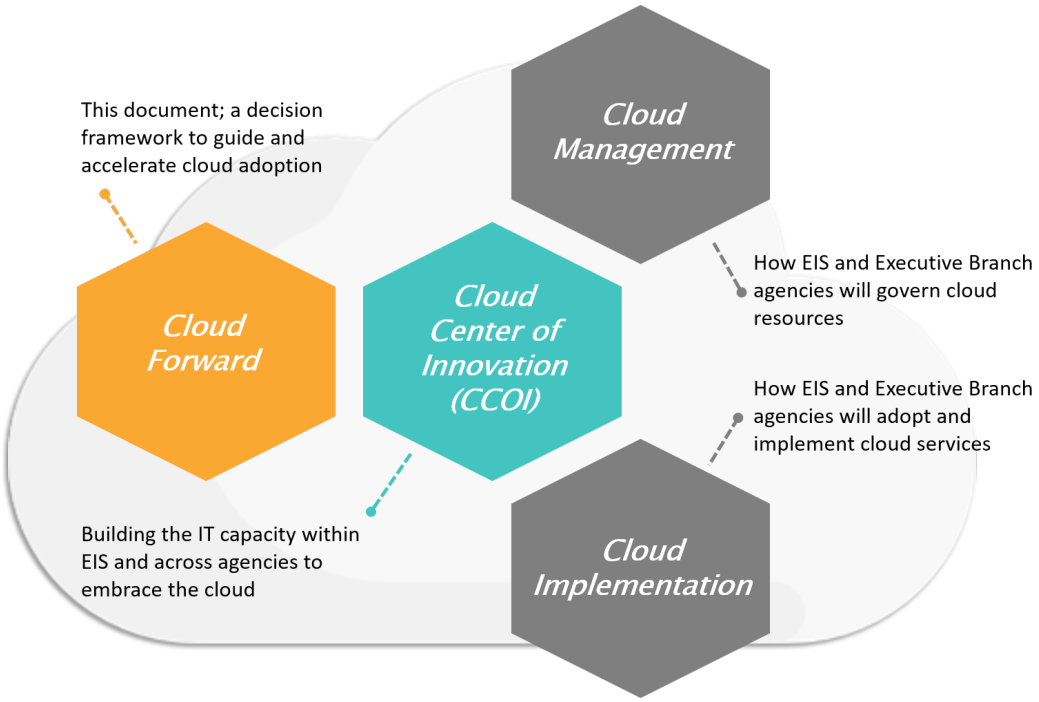
ENTERPRISE information services

Table of Contents

EXECUTIVE SUMMARY

The purpose of *Cloud Forward—A Framework for Embracing the Cloud in Oregon* is to define and communicate the Enterprise Information Services (EIS) cloud vision and to enable state agencies to accelerate cloud adoption across the Enterprise. Consequently, the scope of this document is limited to guiding principles, critical decision points, and cloud migration approaches and methodologies. The framework will be further elaborated through the establishment of cloud governance, detailed implementation planning, development of agency cloud adoption toolkits, and realignment of existing EIS policies and oversight processes.

Figure 1. Cloud Forward in Context



Since the advent of cloud computing in 2006 when Amazon Web Services (AWS) first offered Elastic Cloud Compute and nearly a decade since the publication of the 2011 Federal Cloud Computing Strategy ("Cloud First"), innumerable local, state, and federal agencies, as well as countless private-sector companies, have embarked on their cloud adoption journeys.[1] Since then, the cloud market has matured, become increasingly competitive and best practices in cloud migration and management have emerged. The 2019 revised Federal Cloud Computing Strategy (*aka* "Cloud Smart"), is a case in point, as it provides valuable insights on the importance of security, procurement, and workforce in accelerating cloud adoption; albeit within the context of the federal government.[2] Given these developments, the State of Oregon is uniquely positioned to embrace best practice and apply lessons learned, while tailoring them to the needs of Oregonians in working to realize our *Cloud Forward* vision.

---

[1] Vivek Kundra, "Federal Cloud Computing Strategy" (Office of Management and Budget, February 8, 2011).
[2] Suzette Kent, "Federal Cloud Computing Strategy" (Office of Management and Budget, June 24, 2019), https://cloud.cio.gov/strategy/.

Cloud Forward – Vision and Alignment

Now more than ever, people rely on the State of Oregon to provide essential services that keep them healthy and safe and enable them to live fulfilling lives. Whether enrolling for healthcare or unemployment benefits, tracking student's progress in school, or effectively managing a public health crisis, effective service delivery increasingly demands modern, user-friendly, reliable, and secure state information technology (IT) systems.[3]

To realize this vision, Enterprise Information Services (EIS) is adopting *Cloud Forward—A Framework for Embracing the Cloud in Oregon*, wherein the state will strive to conduct 75% of its business via cloud-based services and infrastructure by 2025—leveraging these highly-scalable, resilient, and elastic infrastructure and technology platforms to modernize state IT systems and make Oregon a place where everyone has an opportunity to thrive. This vision aligns with strategies outlined in the Governor's Action Plan for IT, *User Friendly, Reliable, and Secure: Modernizing State Information Technology Systems and Oversight* and the *EIS Strategic Framework 2020-2023, Version 1.0.*[4]

While the state has and will continue to realize value from its long-term investment in Data Center Services (DCS) as a provider of managed compute services and future co-location offerings (*i.e.*, private-cloud), the State of Oregon's current physical IT infrastructure alone lacks the agility, scalability, resilience and cloud-native capabilities necessary to meet the emergent and future needs of Oregonians. Beyond the inherent advantages of the cloud, *Cloud Forward* provides opportunities to limit the need for long-term capital expenditures (*e.g.*, lifecycle replacement), reduce technical debt, lay the foundation for the modernization of state IT systems, and establish IT as a broker of cloud and IT services.

Key objectives of Oregon's *Cloud Forward* framework include:

- A cloud-first approach for all new IT investments;
- Improve operational and business agility by enabling the State of Oregon to react to federal, state, and business changes more quickly and deploy cloud-native capabilities;
- Improve workforce productivity through access to cloud services and mitigating the delay to acquire timely environment access;
- Reduce operational costs for new and re-factored applications through cloud infrastructure efficiencies that enable supply and demand for environments and employ elastic cost base and transparency;

As part of Oregon's *Cloud Forward* strategy and implementation, EIS will establish a Cloud Center of Innovation (CCOI) and Cloud Services Advisory Council (CSAC), deploy enterprise services in the cloud (e.g., Microsoft 365), invest in cloud enablement capabilities at DCS, and ensure that Executive Branch agencies adhere to the guiding principles and decision framework that follows.

---

[3] Kate Brown, Nik Blosser, and Terrence Woods, "User-Friendly, Reliable and Secure: Modernizing State Information Technology Systems and Oversight" (State of Oregon, September 24, 2018).
[4] Brown, Blosser, and Woods; Terrence Woods, "EIS Strategic Framework 2020-2023, Version 1.0" (State of Oregon: Enterprise Information Services (EIS), n.d.).

Cloud Forward – Guiding Principles

Cloud Forward—A Framework for Embracing the Cloud in Oregon is built around the following principles.

Cloud-First. Cloud will be the first and preferred option for all new IT investments. It should not be conflated with the idea of "cloud everything."

Agility Counts. Cloud migration decisions will be driven by considerations of business agility and overall cloud value, in addition to typical considerations of cost, time, effort and risk.

SaaS, please. Software-as-a-Service (SaaS) will be targeted as the preferred cloud tier and should be evaluated before other cloud tiers (i.e., PaaS or IaaS) or migration models.

Lift-and-Shift Last. As a migration strategy, re-hosting or "lifting and shifting" provides little (if any) cloud value or cost savings. Re-hosting should only be considered when there are no other feasible alternatives or there are compelling reasons to do so; e.g., urgent need to migrate and a lack of data center capacity.

Multicloud. Embracing multicloud acknowledges both the current reality and the unique value propositions and capabilities offered by leading cloud service providers.

Upskilling. As a state we are committed to upskilling our existing IT workforce and preparing them for a cloud-defined future.

Business Enablement. Embracing the cloud frees up IT organizations from having to manage traditional IT infrastructure and operations tasks (i.e., "keeping the lights on"), and provides them with an opportunity to enable their business and program units through strategic use of data, business intelligence, integrations, and agile development.

Cloud Forward – Business and Technical Benefits

As part of the *Cloud Forward* framework, EIS and state Executive Branch agencies have adopted and committed to the principle of cloud-first. Cloud will be the first and preferred option for all new IT investments. Where compelling reasons exist to not use cloud computing, Executive Branch agencies will be strongly encouraged to use DCS private- and hybrid-cloud managed and co-location services. The accelerated adoption of cloud services will generate many business- and technical-related benefits to Executive Branch agencies, both in terms of service delivery and IT capacity:

Business Benefits

- **Agility.** Empower agencies with greater agility in dealing with legislative mandates and unanticipated or novel service demands—enabling them to rapidly innovate, develop, test, and adapt new applications and service models within no-code or low-code, cloud-based development environments with lower initial costs;

- **Resilience.** Employ redundant, modular, durable, and secure cloud architectures to improve the availability and resiliency of critical services when people need them most;
- **Scalability.** Scale new or existing services in real-time in response to sudden increases or shifts in demand;
- **Security.** Leverage world-class information security capabilities of cloud service providers (CSPs) and automated, policy-based cloud backup services that ensure data availability and protection against ransomware and other cyber threats;
- **Innovation.** Deploy current and emergent cloud-native services such as big-data analytics machine learning, artificial intelligence (AI), internet of things (IoT) and high-performance computing (HPC) to enhance existing services and innovate new ones;
- **IT Value.** Embrace cloud cost transparency, asset accountability, and elastic cost models (i.e., *"paying for what you use"*), eliminate wasteful overprovisioning as a form of capacity management and achieve cost savings by deploying cloud-native applications, reducing the state's overall IT infrastructure footprint, limiting future capital investments and avoiding technical debt.

IT Benefits

- **IT Management.** Enable self-service provisioning, leverage cloud management capabilities, orchestration, and cloud automation to handle repetitive, error-prone administration tasks and effectively manage dynamic workloads, and eliminate physical supply chain constraints and technical debt associated with the management of IT physical infrastructure;
- **IT Staffing.** Increased productivity from existing IT personnel by shifting them towards higher-value tasks versus managing physical hardware. Embracing the cloud will free up IT organizations from having to manage traditional IT infrastructure and operations tasks (i.e., "keeping the lights on"), and provides them with an opportunity to enable their business and program units through the strategic use of data, business intelligence, integrations, and agile development within no-code and low-code dev-ops environments.

Cloud Forward – Assumptions

Embracing the cloud in Oregon and working to realize the vision of *Cloud Forward* is an ambitious agenda for both agency and IT leadership alike—it is an opportunity to reimagine the way that we define and deliver services to the people of Oregon. As we embark on building a cloud-defined future in Oregon, the importance of sustained leadership and commitment to agency modernization cannot be understated. At the same time, however, it is important to acknowledge that this vision will require sustained capacity, sufficient resourcing, commitment to *Cloud Forward's* guiding principles, and the ability to navigate organizational change.

CLOUD FORWARD – ORGANIZATIONAL IMPACT

Oregon's *Cloud Forward* framework has the potential to transform how state agencies manage IT and enable the delivery of services to the people of Oregon, with far-reaching organizational implications for both IT and agency leadership in terms of people, processes, and technologies. Given the nature and breadth of service offerings and capabilities available via cloud service providers, innumerable configuration options, and opportunities for self-service provisioning, successful implementation of Cloud-First will require the creation of new governance and organizational structures, the development and maturation of new skillsets, roles and capabilities within EIS and agency IT divisions, and a shift towards IT as a broker of cloud services. Throughout this transformation, EIS will provide change leadership and commit to embracing new ways of doing things. EIS plans to:

- **Establish a Cloud Center of Innovation (CCoI)**. Lead by a Cloud Architect and supported by a team of dedicated Cloud Engineers with ready access to domain-specific expertise throughout EIS, the CCoI will become the state's primary repository for cloud expertise, knowledge, and cloud management tools. Cloud Engineers will have experience across multiple IT silos, gain deep knowledge of the service offerings and configurations available from different CSPs, be able to design successful cloud solutions, and facilitate the migration of existing workloads. The CCoI will also work to ensure that the necessary operational processes and tools are in place to manage and monitor operations across hybrid- and multi-cloud environments (i.e., cost management, template repository, utilization, and performance, workload orchestration, and self-service portals).
- **Establish a Cloud Services Advisory Council (CSAC).** The CSAC will be established as a subcommittee of the Enterprise IT Governance Committee (EITG). It will be co-chaired by a current member of EITG and the State's Chief Technology Officer. Its voting membership will include agency business and IT representation from the six policy area verticals. Additionally, it will have advisory representation from the DAS Chief Financial Office, DAS Procurement, and the Chief Human Resources Office. The Council will be responsible for providing the CCoI with strategic direction in implementing this strategy, serving as an escalation point for decisions with cross-agency or significant impact, and making recommendations to EITG on all policies related to cloud computing.
- **Establish DCS as a broker of cloud services.** The role of DCS as a services broker is to enable agency IT divisions, developers, and end-users to quickly access and deploy cloud environments with minimal friction and IT overhead while maintaining effective guardrails in terms of centralized policies and procedures that leverage pre-built templates. This represents a fundamental shift from the traditional approaches to providing centralized IT infrastructure, and it requires a close partnership with the CCoI in vetting, implementing, adopting, and making new cloud solutions available. As the brokering function matures, end-users will be increasingly able to leverage self-service portals.

Cloud Forward – Workforce

As Oregon moves towards a cloud-defined future where the traditional aspects of IT infrastructure management, networking, computing, and service delivery are abstracted from physical hardware and defined in code, it will require both new skills and new ways of thinking about the IT profession. New roles will need to be established and existing IT roles will need to be enlarged to encompass the unique skills required to manage cloud-based services.

To this end, EIS will partner with the DAS Chief Human Resources Office and Executive Branch agencies to develop a roadmap for building and retaining a cloud-ready workforce—leveraging vendor-specific cloud certification programs and training to "skill up" up our existing IT workforce and hiring for critical skills gaps when necessary. These single- and multi-day certification programs, training courses, and certification exams will be critical to our transformation and will require the requisite investment of staff time and resources.

Given that the development of a cloud-ready workforce will take time, EIS and Executive Branch agencies will also leverage outside consulting and staffing resources as necessary during the initial implementation of this strategy.

In working to develop a cloud-ready workforce, EIS envisions the establishment of the following roles, including cloud architects, cloud engineers, cloud account and relationship managers, and cloud application developers.

Cloud Architects with an enterprise focus will:

- Configure guardrails, blueprints, and policy to assure security, consistency, and compliance
- Assure business alignment with cloud capabilities
- Foster a shared services culture
- Provide workload placement assessments
- Design for resiliency, business continuity, and auditability

Cloud Engineers, Security, and Operations Analysts will:

- Plan, build and run virtual networks
- Plan, build and run resilient, durable cloud compute and storage
- Monitor cloud health, performance, and capacity
- Integrate on-premises and cloud services
- Assure secure configurations and monitor compliance
- Provide backup and recovery services

Cloud Account and Relationship Managers will:

- Perform cloud billing and cost management
- Assist customers with consumption-based billing estimates
- Partner with members of the *Basecamp IT Supply Chain Management* initiative on procurement and contracting, enterprise licensing, vendor relationship management, and vendor performance management

Cloud Application Developers will:

- Develop new applications leveraging functions, containers, and event hubs
- Migrate existing applications to database and runtime services

- Automate build and run tasks
- Develop capabilities based on cloud-native technologies such as machine learning and artificial intelligence

At the same time, our IT workforce must remain cognizant of what constitutes an enterprise-grade service as we integrate cloud capabilities into our existing service offerings—ensuring that the same resiliency, security, compliance, and engineering rigor we apply to our on-premise infrastructure translates to our cloud service offerings.

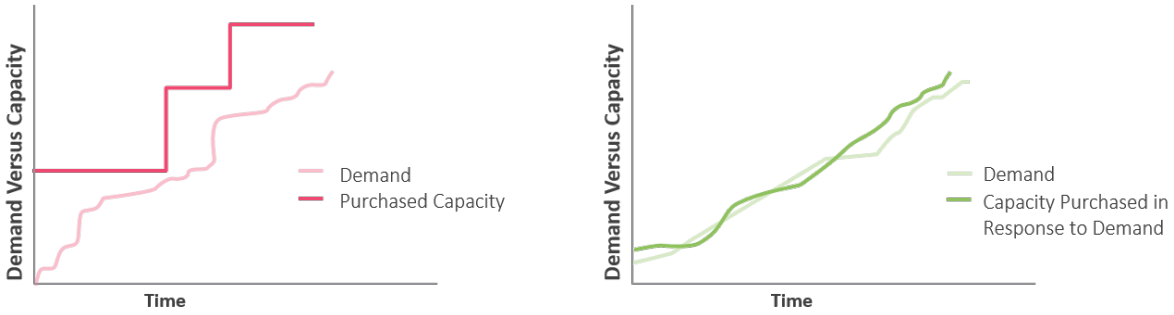
Business Processes

Given the inherent nature of cloud computing, it will also be necessary for EIS to adapt current business processes in terms of IT procurement, operations, infrastructure provisioning, and IT budgeting and cost recovery.

- **IT Procurement and Vendor Management.** Self-service and on-demand provisioning are inherent characteristics of cloud computing environments. Dynamic provisioning within a hybrid- or multi-cloud environment coupled with an ever-growing list of cloud-based services and capabilities, requires a modern procurement approach and effective vendor and relationship management. As part of the Cloud-First strategy, EIS will continue to partner with DAS Procurement Services through its engagement as a member of the CSAC and the *Basecamp IT Supply Chain Management* initiative—working to establish the portfolio of contracts necessary for a cloud-defined future and to mitigate against the risks of vendor lock-in with any single cloud services provider.
- **DCS Operations.** Current DCS infrastructure services are designed to provision and maintain services within the state-owned data center. In adapting to a cloud computing model, DCS will invest in cloud enablement capabilities and establish processes, frameworks, and tools for dynamically managing on-premise, co-location, and cloud computing resources. Initially, DCS will prioritize the use of native tooling for each cloud service provider within workload-based silos. As DCS cloud enablement capabilities mature, it will work to develop dynamic cross-platform cloud management capabilities and tools to enable composite and redundant cloud architectures.
- **Infrastructure Resource Provisioning.** Historically, when hardware resources were provisioned for customers at the state data center, DCS sized them for future growth and anticipated peak loads (as has long been common practice within the industry). Consequently, on any given day (i.e., non-peak), these resources may be substantially over-provisioned, and additional expenses are incurred to maintain idle capacity. In moving to the cloud and through application modernization, there will be opportunities to right-size these workloads enabling them to scale up or down based on demand and reduce the costs associated with over-provisioning.
- **IT Budgeting and Forecasting.** Cloud-First has significant financial implications for IT budgeting and cost recovery. Current IT budgeting and rate development are developed as part of the biennial budget development process—in effect, requiring agencies to forecast demand for particular service lines up to 3 years in advance with limited visibility into the operational service costs at a granular level. At the same time, current DCS rate and assessment models are

premised on predictable capital expenditures (CapEx) for the lifecycle replacement of hardware every 3-5 years. In transitioning to cloud computing, relatively-fixed long-term CapEx will be increasingly replaced by dynamic operational expenditures (OpEx) that may fluctuate substantially from one month, day, or even second to the next.

Figure 2. Comparing Fixed Capacity Planning (CapEx) versus On-Demand (OpEx)[5]



Demand Alignment	Tendency to overprovision	→	Ability to buy just the amount needed
Cost	Heavy CapEx, with a focus on budgeting and balance sheet	→	Negligible CapEx, with a focus on billing
Upgrade Cycle	Upgrades tied to asset depreciation cycle (slow)	→	Upgrades tied to vendor service improvement cycles (fast)

Beyond the shift from CapEx to OpEx, cloud services will require new approaches to rate development, assessment, and billing practices. Current cost recovery practices may have the unintended consequence of discouraging agency cloud adoption among DCS customers if savings realized from migrating workloads to the cloud are offset by increased rates and assessments to cover fixed costs associated with the data center. Accelerating agency cloud adoption requires new models of IT cost recovery, realignment of the state's budgetary and accounting systems to accurately differentiate cloud expenditures (i.e., ORBITS and SFMS) from other IT cost centers, increased utilization of pass-through expenditure limitation, the adoption of dynamic price lists and service offerings and enhanced maturity within the domains of IT Service Management (ITSM) and Technology Business Management (TBM). However, these changes will require the commitment of Enterprise Leadership and legislative action. Lastly, without a clear understanding of the total cost of ownership (TCO) by application and virtual machine across the Executive Branch, there is no way to develop a financial comparison between the current- and future-state in the cloud.[6]

[5] "Cloud Strategy: Communication Deck for Senior Executives," CEB Infrastructure Leadership Council (CEB (formerly Corporate Executive Board), Gartner, n.d.).
[6] Marco Meinardi, "How to Develop a Business Case for the Adoption of Public Cloud IaaS," *Gartner*, Cloud Computing for Technical Professionals, November 21, 2018, 47; "The Application Rationalization Playbook: An Agency Guide to Portfolio Management" (Federal Chief Information Officer (CIO) Council and the Cloud & Infrastructure Community of Practice, n.d.).

CLOUD FORWARD - DECISION FRAMEWORK

Successfully implementing the *Cloud Forward* framework, will require effective decision-making, commitment, and clear alignment between agency and IT leadership. Particularly, as agencies embark upon their application modernization initiatives, evaluating their application portfolios and developing multi-year IT modernization plans for retiring legacy systems to improve service delivery. Increasingly, and with few exceptions, application modernization is synonymous with moving to the cloud.

Consequently, the decision framework that follows is foundational to the modernization of state IT systems—it provides a roadmap for the state's cloud journey by addressing key decision points and defining the core principles that will inform application- and workload-specific migrations.[4] Given that the scope of this document is inherently limited, the decision framework that follows will be further elaborated through the establishment of cloud governance, detailed implementation planning, development of agency cloud adoption toolkits, and realignment of existing EIS policies and oversight processes—future "decisions" represent unique bodies of work necessary for operationalizing the *Cloud Forward* strategy.

Table 1. Decision Point Summary

Area	*Decision Point*
Cloud-first	*Will the state adopt a Cloud-first policy?*
Security	*How will the state implement security and privacy requirements (vulnerability management, access controls…) in the cloud?*
Data Governance and Information Management	*How will state agencies govern data and manage information in the cloud?*
Application and Cloud Utilization Assessment	*How will state agencies assess new and existing applications against cloud migration and establish a baseline for current cloud utilization?*
Application Migration Strategy	*What migration strategies will agencies employ?*
Cloud Tiers	*How will state agencies decide between Software as a Service (SaaS) and other cloud tiers?*
Multi-Cloud	*Will the state pursue a multicloud strategy from the start?*
Workload Placement	*How do we select the best environment for new IT investments and existing workloads?*
Enterprise Cloud Service Brokering	*How will EIS enable state agencies to leverage cloud services?*

Cloud-First

The State of Oregon is adopting a cloud-first strategy. Cloud will be the first and preferred option for all new IT investments. In effect, for EIS and Executive Branch agencies, the question will be, "why not cloud"? However, it does not necessarily follow that all existing IT workloads will be migrated to the cloud (a common misconception), rather there is a presumption in favor of the cloud for all new IT investments. Cloud-First represents a fundamental strategic shift, as historic use of cloud has largely been opportunistic, fragmented, and typically undertaken only as a last resort; *e.g.,* inability to meet infrastructure requirements within the state data center.

Secure Cloud by Design

As the State of Oregon moves towards a cloud-defined future, there are increasing opportunities to embed risk assessment and security governance during the provisioning of cloud infrastructure environment using pre-defined templates.[7] Secure cloud by design represents a shift from paper-based policy statements and audits to the seamless integration of security policy and controls into the cloud environment itself. The shift towards secure cloud by design and the establishment of development, security and operations teams (DevSecOps) will take time and new skills, it will also require new cybersecurity strategies and tactics given the absence of the traditional physical-security perimeter.[8]

In the meantime, CSPs will be required to meet all current security and compliance standards for EIS and Executive Branch agencies. These Standards support and align with the published Statewide Information Security Plan and applicable statewide policies, including the relevant control families of the National Institute of Standards and Technology Special Publication 800-53 Revision 5 (NIST SP 800-53 R5). Consistent with the *2019 Statewide Information and Cyber Security Standards, version 1.0*, Executive Branch agencies will retain responsibility for compliance and ensuring that formal agreements are in place with CSPs and other third parties that guarantee compliance with these standards.

Without exception, major CSPs will meet and typically far-exceed these standards and requirements. However, given the unique nature and characteristics of cloud environments, it may be necessary to ensure that on-premises requirements are translated into cloud capabilities. Additionally, in partnership with EIS, agencies will need to ensure that there are individuals with the appropriate skill sets to implement and monitor the effectiveness of these controls. Lastly, for enterprise service offerings, EIS will work to negotiate enterprise-wide security agreements with major cloud services providers that agencies may leverage to demonstrate compliance with applicable security standards and controls.

As part of the Cloud Forward, Cyber Security Services will ultimately assume responsibility for or partner with the CCOI to provide:

- Continuous monitoring to detect malicious activity using vulnerability scanning tools;
- Performing risk analysis against NIST SP 800-53 R5 security controls; and

---

[7] Jayne Giezmo et al., "How CIOs and CTOs Can Accelerate Digital Transformation through Cloud Platforms," Digital (McKinsey, September 2020), https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/how-cios-and-ctos-can-accelerate-digital-transformations-through-cloud-platforms; *e.g.,* "Microsoft Compliance Offerings," accessed September 18, 2020, https://docs.microsoft.com/en-us/microsoft-365/compliance/offering-home.

[8] Giezmo et al., "How CIOs and CTOs Can Accelerate Digital Transformation through Cloud Platforms."

- Implementing security controls to identify, prevent, and detect threats using code as well as security indents and event management (SIEM) tools to automate response and recovery procedures for threats using industry-proven procedures.
- Providing cloud access security brokering (CASB) to discover and mitigate the risks associated with unapproved cloud applications (aka "shadow IT").

Working with the CCOI, CSS will also work to develop guidance for agencies on the appropriateness of CSPs for particular IT applications based on data classification and regulatory requirements leveraging the FedRAMP certification program established by the Federal Government.[9]

Data Governance and Information Management

To fully leverage current and emergent cloud capabilities, realize critical business benefits, and accelerate innovation through cloud-native services like big-data analytics, machine learning, artificial intelligence (AI), internet of things (IoT), and high-performance computing (HPC), the Cloud Forward framework recognizes the criticality of a data-informed approach to new IT investments and the migration of existing workloads.

Without effective data strategies, data governance maturity, effective data management, and classification practices and a presumption in favor of openness and interoperability, there is a substantial risk of lifting-and-shifting existing data silos, further fragmenting the state's data resources and undermining the state's ability to leverage data as a strategic asset. Without effective information management, there are also a number of attendant security and privacy risks.

Consequently, as agencies move towards a cloud-defined future, it will be necessary to align with the principles contained in the Statewide Data Strategy, partner with the state's Chief Data Officer to implement data governance, and meet the information management requirements outlined in ORS 276A.365, public records law, as well as state and federal privacy statutes governing particular kinds of data, including but not limited to:

- Healthcare Data: Health Insurance Portability and Accountability Act (HIPPA)
- Children: Children's Online Privacy Protection Act (COPPA)
- Access to Education Records: Family Educational Rights and Privacy Act (FERPA)

Enterprise Application and Cloud Utilization Assessment

In support of the Governor's IT Action Plan and as part of the EIS 2020-23 Strategic Framework, EIS is partnering with Executive Branch agencies to develop multi-year IT modernization plans for retiring legacy systems by policy area. Across the Executive Branch, state agencies maintain hundreds (and in some cases thousands) of different applications, ranging from off-the-shelf software like Microsoft Office, to highly-complex and custom-built IT systems that cost hundreds of million dollars to develop

[9] "The Federal Risk and Authorization Management Program (FedRAMP) provides a standardized government-wide approach to security assessment, authorization, and continuous monitoring of cloud services. Offering cloud service providers the opportunity to demonstrate their ability to meet Federal security requirements through standardized baselines has allowed for a flourishing marketplace of vetted providers to develop. It has also allowed agencies to adapt from arcane legacy technology to mission-centric and cost-effective cloud-based systems in a more rapid, consistent, and secure manner" Kent, "Cloud Smart."

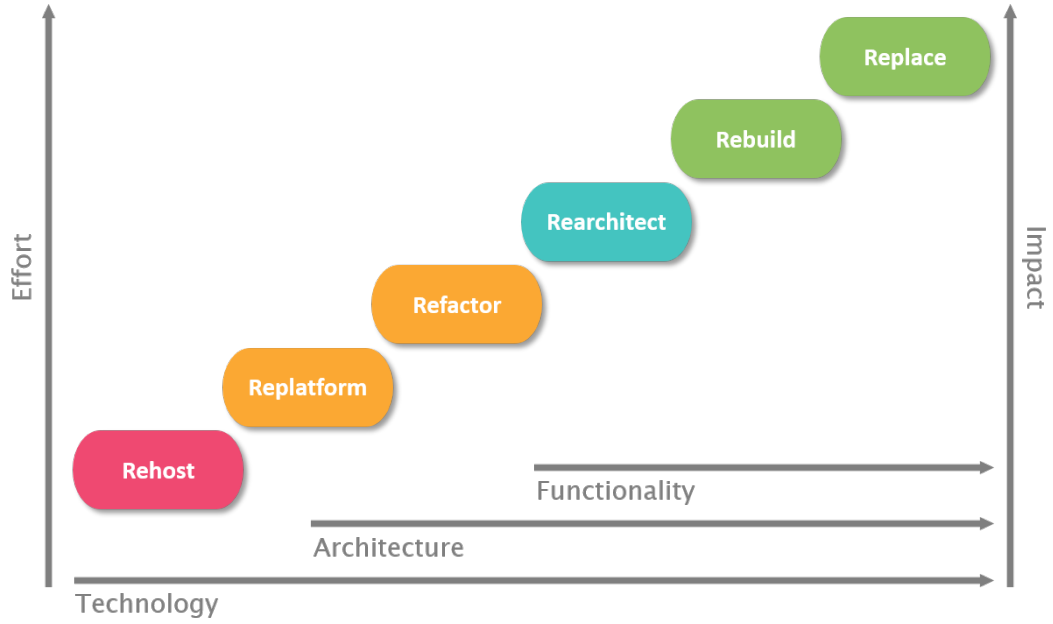
and maintain. In some cases, there is continuing reliance on 20- to 30-year-old "green screen" legacy systems developed using nearly-extinct programming languages (e.g., COBOL), whereas in other cases, agencies have already started investing in a cloud-defined future.

While traditional notions of IT modernization are limited to the migration of legacy systems to new applications or platforms (i.e., "rip and replace"), IT and application modernization increasingly encompass improved user interfaces (UI), enhanced user experience (UX), use of integration points or APIs, cloud-native or server-less infrastructure and a shift away from monolithic- to modular-IT systems comprised of loosely coupled micro-services. To support IT modernization and enterprise application rationalization, EIS is partnering with state agencies to develop an application inventory and assess current-state cloud utilization by policy area vertical—establishing a baseline for cloud adoption.

Application Migration Models

Given the anticipated variation in the age and complexity of the underlying code bases of the application portfolios maintained by agencies and across policy areas, it will be necessary to select the most appropriate migration strategy on an application- or workload-specific basis. As each application within the enterprise portfolio is evaluated for a potential migration to the cloud, there is a range of migration models available with varying timeframes, levels of effort, associated costs, attendant risks, and overall "cloud value" (i.e., business capabilities and functionality associated with cloud-native architectures) associated with each. Some of these inherent trade-offs are illustrated in the figure below.

Figure 3. Comparing Application Migration Models[10]



[10] Adapted from, Neville Cannon, "5 Steps to Make Government Legacy Modernization a Success" (Gartner, June 2, 2019).

The definitions that follow are adapted from Gartner and Info-Tech.[11]

1. **Replace.** In this model, you forego custom application development altogether and opt for a commodity SaaS. While traditionally used for commercial off-the-shelf (COTS) solutions and not always a viable option, the replacement option should be explored first as there may be new alternatives in the marketplace (i.e., buy before build).
2. **Rebuild.** In this approach, you dispense with any accumulated code and build the application from the ground up within a PaaS environment using cloud-native and agile dev-ops capabilities (e.g., low-code or no-code environment with "point-and-click" development styles). Using cloud-based application development and data platforms enables rapid prototyping, development, and scaling of modern applications that can leverage advanced analytics, artificial intelligence (AI), blockchain, the internet of things (IoT), and high-performance computing (HPC). Additionally, the use of micro-services and a modular architecture connected via well-defined APIs avoid the inherent rigidity and brittleness of monolithic legacy IT systems. While this approach takes time relative to rehosting or refactoring, it generates the greatest cloud value and reduces the time, effort, risk, and costs when compared with traditional software development and infrastructure provisioning. Despite its inherent advantages, the sunk costs fallacy can be viewed as a substantial barrier to this approach.
3. **Rearchitect.** Rearchitecting involves materially altering an application and its core architecture in-order to optimize it for the cloud and make substantial use of cloud-native capabilities within an IaaS or PaaS platform. While this approach can yield significant cloud value, it represents an ambitious undertaking, involving significant time, effort, risk, and cost.
4. **Refactor.** Sometimes referred to as *"lift, tinker and shift,"* refactoring involves modifying an application to right-size the workload and take limited advantage of cloud-native capabilities like resource scalability and discrete cloud services like databases and load balancers, without changing the core architecture of the application. At this point, the application could be moved to an IaaS environment or could be modified to leverage certain PaaS capabilities. This approach involves additional time, effort, and risk. However, it has the potential to reduce overall costs and yield nominal cloud value.
5. **Rehost.** Sometimes referred to as *"lift and shift,"* rehosting simply involves moving an application without modification (other than that required by the new hosting environment) from its current physical or virtual environment to a cloud IaaS platform. While this approach is the quickest to implement, may require minimal effort, and is typically low risk, it adds no cloud value and is often more expensive given fixed resource requirements. McKinsey characterizes "lift and shift" as a prevailing "failure mode" over the past 20 years that provides no value or significant cost reductions and often results in a collapse of support for cloud initiatives.[12]
6. **Retain.** In some cases, migration to the cloud may be infeasible and it is better to retain the application in its current state and revisit it at a later time. This approach is appropriate when assets still have useful life and considerations of time, effort, cost, risk, and cloud value weigh against migration.

---

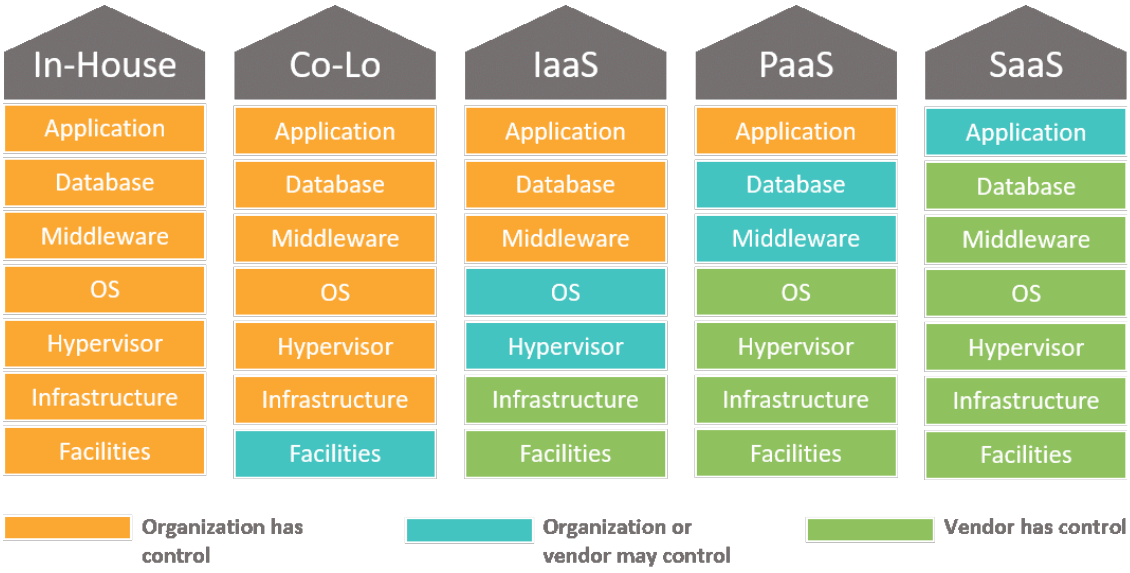
[11] Marco Meinardi, "Designing a Cloud Strategy Document," *Gartner*, Technical Professional Advice., June 30, 2019, 30; "Cloud Strategy Template" (Info~Tech Research Group, n.d.).
[12] Giezmo et al., "How CIOs and CTOs Can Accelerate Digital Transformation through Cloud Platforms."

7. **Retire.** In some cases, it may be better to simply retire the application without a replacement.

Cloud Tiers

As part of the *Cloud Forward* framework, the State of Oregon will leverage all tiers of cloud provisioning—prioritizing the use of SaaS, wherever possible. Consequently, for each application being evaluated for migration, SaaS will be the preferred cloud tier. If there are no suitable SaaS solutions available in the market, PaaS and IaaS will be considered as the next best cloud tiers for the workload in question. Again, some applications will need to be retained within the state data center under DCS management or using co-location offerings until they can be replaced or retired.

Figure 4. Cloud Tiers



By way of context, it is important to note the relative degree of control and responsibility associated with the various cloud tiers:

- **Software-as-a-Service.** The SaaS vendor is responsible for everything except for minor application configurations.
- **Platform-as-a-Service:** The customer builds the application using tools provided by the vendor.
- **Infrastructure-as-a-Service:** The customer manages OS, storage, and the application.

The graphic above depicts the relationship between control and responsibility for the cloud tiers listed above as well as on-premise providers.

Multicloud

The *Cloud Forward* strategy embraces multicloud as a guiding principle, acknowledging both the current reality and the unique value propositions and capabilities offered by leading cloud service providers—it provides access to the right technology, at the right time. Additionally, pursuing multicloud mitigates against the pitfalls of over-reliance on any single cloud service provider and the risks of vendor lock-in.

While multicloud certainly introduces operational complexity and requires modern procurement approaches, EIS envisions a phased approach. Initially, EIS will provide multicloud brokerage services using use-case based workload silos and a native tooling strategy (i.e., tools specific to each cloud service provider such as Azure Stack). In all cases, EIS cloud brokerage service offerings will be paired with clearly defined exit strategies for cloud workloads.

As EIS's cloud enablement and brokerage capabilities mature, it will work to provide dynamic multicloud service offerings using containerization strategies (e.g., kubernetes) and cross-platform tools that enable seamless shifting of workloads from one provider to another (i.e., composite and redundant multicloud).

Workload Placement

As state agencies partner with EIS to establish multi-year IT modernization plans, rationalize their application portfolios, and set a baseline for cloud adoption, they will collect information necessary to determine the appropriate placement of workloads associated with new IT investments. Workload placement—for both new IT investments and existing workloads—will be determined according to the guiding principles, migration models, and cloud tiers discussed above. Workload placement evaluations will be managed by the Cloud Center of Innovation (CCOI) in partnership with DCS under the guidance of the Cloud Services Advisory Council (CSAC), however, the prioritization of individual workloads for such evaluation will be determined by internal agency IT governance.

Figure 5. Workload Placement

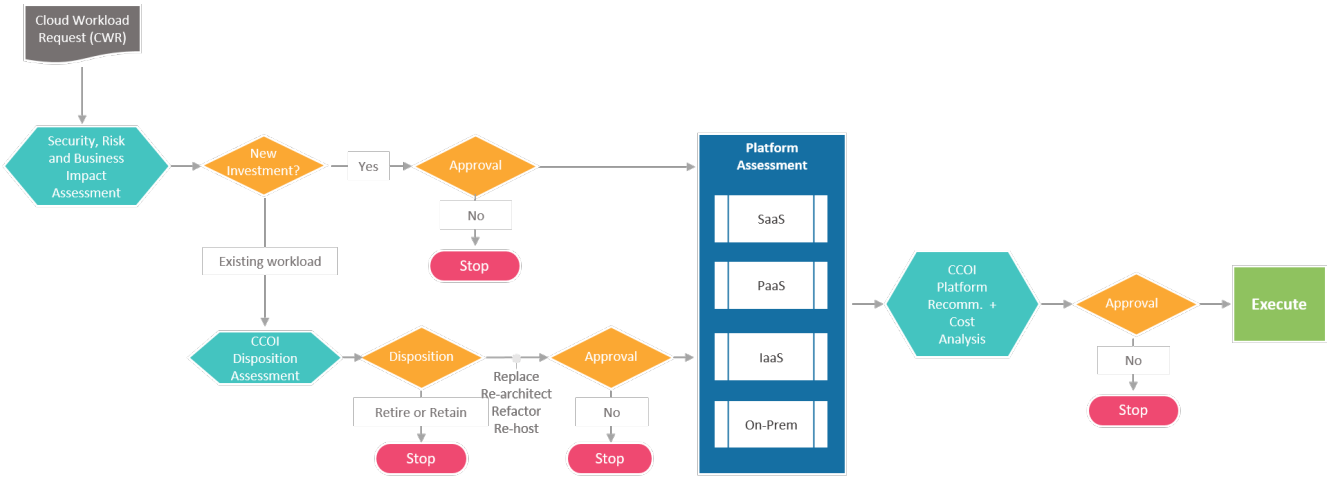


Figure 3 provides a visual framework by which each workload will be evaluated to determine the most appropriate migration model and cloud tier. When the CCOI receives an initial agency cloud workload request (CWR) they will coordinate initial security, risk, and business impact assessment. For new IT investments, if approved, the CWR will proceed immediately to a cloud tier (or platform) assessment followed by a cost analysis and a final governance determination. Whereas, in the case of existing workloads the platform assessment will be preceded by a disposition assessment to determine the most appropriate migration model and for preliminary approval. In all cases, SaaS will be the target cloud tier.

Enterprise Cloud Brokerage Services

The role of a cloud services broker is to enable customers (i.e., agency IT divisions, developers, and end-users) to quickly access and deploy cloud environments while safeguarding the interest of the enterprise through effective governance.

The evolution of DCS into the role of a cloud services broker represents a fundamental shift from its traditional focus on maintaining physical IT infrastructure and will require sustained change leadership, the acquisition of new cloud skillsets, and the development of cloud management maturity. As cloud management capabilities mature, DCS will work to blend traditional IT services, private cloud, and public cloud offerings into a seamless portfolio of service offerings. With time, end users will be increasingly able to leverage self-service portals.

At the same time, just as some agencies will be ready to take advantage of DCS cloud brokerage services, others may lack the in-house cloud expertise or desire to go it alone on their cloud adoption journey. For these agencies, DCS will act as a value-added cloud services provider, managing all aspects of an agency's IaaS and PaaS computing needs.

Together these cloud brokerage and value-added cloud services will include the following:

- **Identity.** DCS is currently synchronizing agency Active Directories to a consolidated cloud-based identity store. This cloud identity database will allow agencies to authenticate users to multiple cloud services like Microsoft 365 and Workday without creating and managing additional user accounts.
- **Security.** DCS brokered services will come with security and compliance guardrails pre-configured. Systems and services will be configured using secure, regulatory compliant, and tested blueprints. Monitoring and alerting will be integrated with Cyber Security Services (CSS) systems.
- **Network Services.** Distributed workloads require a new approach to network design as physical distance can introduce latency, security, and bandwidth constraints. DCS along with Link Oregon is building a next-gen high-speed statewide network designed with cloud services in mind (e.g., peering with major CSP and internet exchanges). Secure, high-speed network connections to cloud providers are currently under construction at DCS. These network connections will provide agencies with secure and reliable connections to critical workloads in the cloud.
- **Compute and Storage Services.** Pay as you go compute and cloud storage offer flexibility and economies of scale that reserved capacity and local storage cant. DCS will assist customer agencies with workload assessments and selection of the most cost-effective, performant, and secure solutions.
- **Cost management.** Consumption-based billing models present new challenges to accurate capacity, availability, and performance planning. DCS will monitor and work with cloud providers to adjust service configurations for optimum value.
- **Exit strategies**. Cloud workload planning and placement must also consider exit strategies. DCS will help agencies determine based on the cloud tier (IaaS, PaaS, or SaaS) what risk mitigation approaches to take. Options include moving back to on-premises, changing providers, or simply adding another provider.

CONCLUSION

As the state of Oregon embarks on its cloud migration journey, seeking to conduct the majority of the state's business using cloud-based services and infrastructure by 2025, it will require sustained leadership and true alignment between IT and business units. Fully leveraging these highly-scalable, resilient, and elastic infrastructure and technology platforms, represents a convergence of IT, business operations, and program leadership. Beyond the inherent advantages of the cloud, *Cloud Forward* provides opportunities to limit the need for long-term capital expenditures (*e.g.*, lifecycle replacement), reduce technical debt, lay the foundation for the modernization of state IT systems, and establish IT as a broker of cloud and IT services.

In working to accelerate the adoption and deployment of cloud services, EIS will provide change leadership and partner with state agencies as they work to transform the way they do business and mature their IT governance and operations for a cloud-defined future. Additionally, EIS will establish a Cloud Center of Innovation and Cloud Services Advisory Council, model best practice through the deployment of cloud-based enterprise services, mature its cloud enablement capabilities and be an engaged partner with Executive Branch agencies in accelerating cloud adoption and modernizing state IT systems to support the essential services that the people of Oregon rely on.

APPENDICES

A. Essential Characteristics of Cloud Computing

Our strategy aims to ensure that our use of cloud remains aligned with the accomplishment of our goals and not simply the use of a solution in search of a problem. Below are the five fundamental characteristics of cloud computing, as defined by the National Institute of Standards and Technology (NIST).[13]

1. **Self-Service.** Continuous striving for self-service solutions, where "self" can refer to an internal employee process or a partner end user, will allow us to speed up our service delivery as well as refocus our IT effort to strategic, high-value work.
2. **Broad Network Access.** Cloud allows IT to build services that are more accessible to end-users and members than they could be if served from the data center or a colocation facility. This allows for wide availability and, therefore, better collaboration.
3. **Resource Pooling.** Public cloud providers deliver their services to a number of clients using shared resources. This pooling of resources will allow [Organization Name] to be more efficient with our infrastructure, resulting in faster service delivery. This will also reduce/remove much of the manual work done in-house today, allowing [Organization] to refocus IT efforts toward strategic, higher-value work. Resource pooling is one of the cloud features that allow providers to undertake much of the operational work, making it possible for [Organization Name] to make better financial choices.
4. **Rapid Elasticity.** Cloud services are generally offered on a pay-as-you-go basis. When they are not being used, they can be turned off, allowing for efficiencies. This allows for scalability when needed and can reduce costs if appropriately applied.
5. **Measured Service**. Cloud services allow for simpler, detailed unit costing. This will allow us to make better financial choices by directly highlighting the cost to serve for various business units, contributing to our data-driven management approach.

B. Cloud Deployment Models

- **Public Cloud.** In a public cloud environment, a third-party provider is responsible for the underlying infrastructure stack (all the way up to the application, minus minor configurations, in a SaaS environment) and clients access the service over the public internet. The public cloud includes true multitenancy as a feature, meaning that clients share server space with other organizations. Examples of public cloud providers include Microsoft, Amazon, Google, Salesforce, and similar CSPs.
- **Private Cloud.** A private cloud includes all five of the NIST characteristics – the main difference between a private and public cloud installation is tenancy: a private cloud can exist in a provider's data center or on-premises. The only requirement is that multitenancy is internal.
- **Hybrid Cloud.** Hybridity is not merely the use of multiple clouds. True hybridity requires 1) multiple cloud instances (a pair of different IaaS providers, for example), and 2) portability between them. This can be enabled using a custom set of tools – cloud middleware – or a standardized toolset, like Microsoft's Azure Stack, or VMWare on AWS.

[13] Mell, Peter, and Timothy Grance. "The NIST Definition of Cloud Computing." *National Institute of Standards and Technology*, Sept. 2011. Web.

C. References

Brown, Kate, Nik Blosser, and Terrence Woods. “User-Friendly, Reliable, and Secure: Modernizing State Information Technology Systems and Oversight.” State of Oregon, September 24, 2018.

Cannon, Neville. “5 Steps to Make Government Legacy Modernization a Success.” Gartner, June 2, 2019.

“Cloud Strategy: Communication Deck for Senior Executives.” CEB Infrastructure Leadership Council. CEB (formerly Corporate Executive Board), Gartner, n.d.

“Cloud Strategy Template.” Info~Tech Research Group, n.d.

Giezmo, Jayne, Mark Gu, James Kaplan, and Lars Vinter. “How CIOs and CTOs Can Accelerate Digital Transformation through Cloud Platforms.” Digital. McKinsey, September 2020. https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/how-cios-and-ctos-can-accelerate-digital-transformations-through-cloud-platforms.

Kent, Suzette. “Federal Cloud Computing Strategy.” Office of Management and Budget, June 24, 2019. https://cloud.cio.gov/strategy/.

Kundra, Vivek. “Federal Cloud Computing Strategy.” Office of Management and Budget, February 8, 2011.

Meinardi, Marco. “Designing a Cloud Strategy Document.” *Gartner*, Technical Professional Advice., June 30, 2019, 30.

———. “How to Develop a Business Case for the Adoption of Public Cloud IaaS.” *Gartner*, Cloud Computing for Technical Professionals, November 21, 2018, 47.

“Microsoft Compliance Offerings.” Accessed September 18, 2020. https://docs.microsoft.com/en-us/microsoft-365/compliance/offering-home.

“The Application Rationalization Playbook: An Agency Guide to Portfolio Management.” Federal Chief Information Officer (CIO) Council and the Cloud & Infrastructure Community of Practice, n.d.

Woods, Terrence. “EIS Strategic Framework 2020-2023, Version 1.0.” State of Oregon: Enterprise Information Services (EIS), n.d.

ENTERPRISE
information services