Enterprise Information Resource Management Strategy (EIRM)

2017-2022

Accountable, Customer-centered, Collaborative and Innovative

May 2018
## Contents

- Message from the State CIO
- Guiding Principles
- EIRM Retrospective
- OSCIO's Roles and Functions
- Goal 1. Maturing IT Resource Management
- Goal 2. IT Supply Chain Management
- Goal 3. Data Utility
- Goal 4. Information Security
- Goal 5. Capacity Management
- Recent OSCIO-Related Legislation
- Agency Information
Message from the State CIO

Dear Colleagues,

In February of 2015, I released the 2015-20 Enterprise Information Resource Management (EIRM) Strategy. It was a strategy for its time and one that emphasized IT Governance and a coordinated system of support for agencies throughout the consult, design and build phases of the IT project lifecycle. The strategy encompassed a number of initiatives, including the development of the Joint OSCIO/LFO Stage Gate Model, deployment of an enterprise project and portfolio management (PPM) tool, and service reviews to identify opportunities for shared and utility services.

The Office of the State CIO (OSCIO) continues to build on these initiatives and remains committed to the principles underlying the February 2015 EIRM, however, events in recent years have expanded the responsibilities of our Office to include state data center operations, enterprise IT security, data governance and IT portfolio management. While this expanded mandate can largely be attributed to legislative action—e.g., HB 3099 (2015) and SB 90 (2017)—it can also be traced to a renewed interest in IT governance, increased emphasis on IT operations, and strong leadership on IT security within the Governor’s Office.

A June 2017 assessment conducted by the Governor’s Office found that the majority of stakeholders interviewed lacked a clear understanding of how the State of Oregon makes or prioritizes IT investment decisions and what criteria are used. The assessment also found confusion regarding how agencies make their own IT investment decisions, with some stakeholders expressing concerns that agencies may not be using best practices in their prioritization of IT initiatives. These assessment findings coupled with an expanded OSCIO mandate and recent legislative actions underscored the need to revise the February 2015 strategy.

The 2017-22 EIRM that follows contextualizes recent developments, embraces the OSCIO’s new operating model and provides for an expanded mission and vision, coupled with supporting values and five major goals, including:

1. **Maturing IT Resource Management**—mature enterprise and ensure agency internal IT governance to enable project prioritization and stewardship of IT resources based on business alignment, cost, ROI, and risk
2. **IT Supply Chain Management**—build trusted partnerships through collaboration to identify, procure and pilot new Enterprise services, and establish agency Centers of Excellence
3. **Data Utility**—utilize data as a strategic asset to improve service delivery, facilitate cross-agency collaboration, identify cost savings and enhance transparency
4. **Information Security**—unify cybersecurity to improve customer service for Oregonians while ensuring those systems are secure and resilient
5. **Modernization**—engage Enterprise Leadership to develop a roadmap for capacity management to help position the enterprise for the future

Each of these goals is supported by specific objectives, supporting actions, short- and long-term impact statements and key metrics—many aimed at providing a baseline data for recent legislative actions (e.g., open data). I look forward to working with everyone as we transition from project-by-project oversight model to a more holistic approach to information resource management.

Sincerely,

Terrence Woods
Acting Chief Information Officer, State of Oregon
Guiding Principles

In leveraging the potential of information technology to transform service delivery in Oregon State government, policy and technology leaders need to adhere to guiding principles that will lead to successful and measurable outcomes. The following principles are aligned with the Enterprise Leadership Team’s original vision for Enterprise Information Resource Management (EIRM) implementation.

| Alignment        | Understand the business and objectives of state leaders and constituents
|                  | Ensure IT capabilities are aligned with the business needs of state government and its customers |
| Transparency & Oversight | Enable transparent IT financial management and effective management of IT resources |
| Maturity         | Mature IT governance to support effective IT resource management and project delivery |
| Optimization     | Provide services to citizens in the most cost-effective manner possible
|                  | Leverage shared services across government to increase value, eliminate unnecessary duplication and reduce costs |
| Simplicity       | Ensure that proposed solutions provide a measurable impact and value to solve an identified problem
|                  | Standardize the IT environment by leveraging existing state-owned solutions and shared services to reduce redundancy and complexity |
| Innovation       | Partner with program and policy leaders in leveraging innovative and cost-effective technology solutions to address the state’s business problems |
| Iterative Refinement | Define incremental approaches to solution design and implementation—“the progressive reduction of uncertainty” |
| Adaptive         | Encourage project planning and solution designs that are responsive to emergent challenges and opportunities |
| Measured Value   | Pursue solutions with a clear business case that make government more accessible and responsive to Oregonians
|                  | Substantiate tangible return on investments in technology that meet or exceed the expectations of program and policy sponsors |
| Security         | Secure state systems and ensure that they are resilient and ready for the future |
EIRM Retrospective

In 2014, a new framework for Enterprise IT Governance (EITG) was developed and the EITG Steering Team was established. The IT governance framework differentiates between utility services, shared services, and unique agency functions. Comprised of the State CIO, staff from the OSCIO, the Governor’s office, and members from the Enterprise Leadership Team; the EITG Steering Team was charged with identifying and prioritizing the implementation of shared and utility services (defined below).

**shared service**

Implementation of a shared solution that meets a common policy area or business function, generates business value for two or more agencies and enables them to fulfill their core mission, provided:
- The shared solution is not coextensive with an existing or planned utility service;
- Two or more agencies have developed a resource-sharing agreement to sustain the shared service that includes one or more of the following: financing, staffing, hardware, software or support;
- Partner agencies derive mutual benefit from the shared solution; and
- Partner agencies agree upon a common approach to implementation, delivery, maintenance, and governance.

**utility service**

Utility services are those where it makes good business sense to have a single supplier for all users when balancing:
- Economies of scale;
- The need for one integrated system;
- A strong need for uniformity;
- Core business objectives are not impacted by a lack of customization;

A service can also be declared a utility for compelling policy reasons. A utility service has a “community benefit” whether or not everyone takes advantage of the service. Customers of utility services may be local government entities, individual state agencies and other public entities that may choose how much to purchase, but for any of the reasons cited above the choice of suppliers is limited to one source.
JOINT OSCIO/LFO STAGE GATE

In 2014, the State CIO, in cooperation with the Legislative Fiscal Office (LFO), established the Joint OSCIO/LFO Stage Gate process—an incremental funding and project oversight model for major IT initiatives exceeding $1 million or posing substantial risk. In the words of G.M. Winch, the underlying rationale of stage gating is the "progressive reduction of uncertainty." This is accomplished through "external" review of the IT initiative and its progress to date (performance), evaluation of its near-term plans, validation of resource commitments and an assessment of the initiatives readiness to go forward. Factors influencing Stage Gate endorsements, include: quality parameters (i.e., how well is the project being executed?); operational feasibility (i.e., are there appropriate resources and can the project be completed on time?); and economic viability (e.g., return on investment (ROI) or net present value (NPV)).

stage gate
/stāj/ /găt/ noun

1. formal review conducted at prescribed points in a project life-cycle for the purpose of controlling project risk, monitoring scope changes and maintaining stakeholder engagement

2. conceptual and operational models that provide key communication opportunities for moving a project from idea to closure (project to program)
HB 3099 (2015) & OSCIO REDesign

Prior to the passage of HB 3099 (2015), the DAS Director retained substantial authority over state IT operations and policy—as a DAS employee and direct report, the State CIO lacked independence and possessed only nominal authority over statewide IT policy. Under this model, the State CIO’s division consisted of 34 positions—a group whose responsibilities were limited to IT project oversight, security standards, data collection for geographic information systems and pilot implementation of an IT Governance framework. Furthermore, the State CIO had no authority over IT service delivery within ETS—a division with 225 positions that reported to the Deputy DAS Director. Consequently, there was a fundamental disconnect between statewide IT policy and service delivery.

Following the discovery of statewide network vulnerabilities in March of 2015, the Governor restructured leadership over statewide IT policy and operations, temporarily assigning operational responsibility for ETS to the State CIO. The reassignment and delegation of joint authority over statewide IT policy and operations were made permanent under HB 3099, which designated the State CIO as an independent official, directly responsible to the Governor as the primary advisor on statewide IT policy and operations. Among other provisions, the bill codified an incremental funding and development process for IT projects over $1 million (i.e., Stage Gate review) and provided a delegation of authority over enterprise IT and telecommunications projects.

With enhanced authority over increasingly complex IT and telecommunications projects and vendor relationships, added responsibility for IT service delivery at ETS, and a growing backlog of remediation measures to mitigate statewide security vulnerabilities, the Office of the State CIO required a new direction. By clarifying the role of the State CIO and ensuring alignment between statewide IT policy and operations, HB 3099 provided a unique opportunity to reaffirm the OSCIO’s commitment to enabling state agencies and partner jurisdictions to better serve Oregonians—mitigating security vulnerabilities and threats, optimizing IT investments across the enterprise of state government, ensuring financial transparency and aligning service delivery with industry best practices.

Among other provisions, HB 3099 established the Joint OSCIO/LFO Stage Gate within the statute. However, it is important to note that the State CIO still lacks formal authority to stop or cancel a project, once the project has gone into execution and been appropriated funding. In addition, the legislation provided the State CIO with independent procurement authority, oversight responsibilities, and contract enforcement capabilities. The OSCIO delegation of independent authority over IT procurement and enterprise IT and telecommunications project (from inception through project lifecycle) includes:

- the ability to suspend or modify project implementation;
- cancel or modify a procurement, contract, or price agreement;
- modify the scope of an initiative prior to the award of a contract or price agreement;
- enforce the terms and conditions of a contract or price agreement (e.g., “call for cure”); or
- elect to be named as a party or third-party beneficiary to any contract or price agreement.

As part of this commitment and to fulfill the intent of HB 3099, the OSCIO adjusted its organizational structure a previously described, enabling a renewed focus on data center operations, development of
enterprise security capabilities, effective management of IT vendor relationships and implementation of the IT governance framework.

**E.O. 16-13, “UNIFYING CYBER SECURITY IN OREGON” AND SB 90 (2017)**

Governor Brown’s Executive Order 16-13, “Unifying Cyber Security in Oregon” (EO 16-13) represented a fundamental shift in how the state of Oregon approaches IT security. EO 16-13 was the first step towards addressing persistent IT security vulnerabilities and represents the next phase of Oregon’s IT security evolution. It has enabled the implementation of a statewide agency-by-agency risk-based security assessment and remediation program that informed legislative deliberations. While implementing change is inherently disruptive, OSCIO has made the continuity of IT security operations a top first priority—keeping the majority of IT security personnel, protocols, and tools in place while working to strengthen the statewide community of IT security professionals.

In February 2017, the Governor introduced SB 90. The bill recognizes that information security is woven into the fabric of public trust and that Oregon requires a long-term multi-sector cyber strategy that leverages the private-sector expertise of Oregon’s cyber-related industries, enables information sharing, anticipates cyber disruptions and builds capacity across the state with our local government partners and school districts. SB 90 and the Cyber Oregon initiative seek to enhance Oregon’s cybersecurity through four measures, including:

- Enhancing state government IT security by unifying IT security functions and personnel within the Executive Branch—permanently extending, E.O. 16-13, “Unifying Cyber Security in Oregon”;
- Establishing the Oregon Cybersecurity Advisory Council to enable information sharing and cyber workforce development;
- Laying the foundation for the development of a Cybersecurity Center of Excellence; and
- Enabling Oregon to compete for cyber grant funding and engage in cross-sector cyber initiatives through public-private partnerships.

**ORACLE SETTLEMENT**

In September of 2016, the State of Oregon reached a settlement with Oracle that included both cash and in-kind elements—ending protracted litigation related to the failed launch of Cover Oregon that had already cost the state nearly $25 million in legal fees. The settlement has afforded the state a unique opportunity to modernize many of its aging statewide and agency legacy systems through a 5-year unlimited license agreement (ULA) on the PeopleSoft ERP, the Hyperion Enterprise Financial Planning suite, the Business Intelligence suite and a host of enterprise-class database, data integration, and middleware components. The major ULA components are summarized below:

- The PeopleSoft Enterprise ERP suite is a comprehensive set of integrated end-to-end business software packages that enable organizations to enhance productivity by integrating administrative systems, streamlining operations, providing a single source of truth and enabling real-time analytics. Each individual application within the PeopleSoft suite is designed to interact
with every other application, including Financial Management, Supplier Relationship Management, Enterprise Service Automation (ESA), Human Capital Management (HCM) and Customer Relationship Management (CRM) among others.

- The **Hyperion Enterprise Financial Planning** suite is a portfolio of software packages focused on improving financial management, reporting, and analysis. The suite includes products designed to assist financial management, budgeting, planning, financial forecasting, financial reporting, database management and business intelligence.

- The **Business Intelligence** suite is set of software tools designed to enable interpretation of large volumes of data by providing analytics and insights that empower data-driven decision-making. The suite includes products that enable business performance management, statistical analysis and data visualization among other tools.

Though the ULA represents a major opportunity for the state of Oregon, it will require a substantial investment of effort, time and money to realize its value. The value of the ULA will be determined by what the state of Oregon is capable of implementing over the next five-years, the value of the ULA (assuming full implementation) could easily exceed $100 million. A 10-year modernization plan prepared by KPMG estimated that the state would need to spend between $490-515 million to implement a fraction of the software contained in the ULA.

The OSCIO has and will continue to work with agencies to identify opportunities to upgrade our existing Oracle products (Oracle databases in particular). Additionally, the state data center (ETS) is working to set up test environments (“sandboxes”) for business intelligence applications, and evaluating opportunities to deploy middleware and other back-end solutions; however, the decision to implement any of the more than 200 product components available under the ULA is a business decision.
Following the passage of HB 3099 (2015) the Office of the State CIO (OSCIO) re-structured in order to enable a renewed focus on data center operations, development of enterprise security capabilities, effective management of IT vendor relationships and further maturation of the IT governance framework. The resulting OSCIO redesign led to the establishment of four distinct programs, including the Strategic Technology Office; Enterprise Shared Services; Enterprise Technology Services; and the Enterprise Security Office.

**Strategic Technology Office (STO)**

The Strategic Technology Office (STO) is key in implementing the IT Governance Framework which includes oversight and portfolio management of all major IT investments. Using a standard framework and statewide policies the office will work with agencies to identify and resolve IT project issues and strike a balance between central delivery and agency flexibility. The staff serve as advisors, making recommendations for agency alignment with enterprise strategies and architecture; project management and IT governance; industry best practices and agency business goals. The Strategic Technology Office looks for solutions and cost-sharing opportunities across multiple agencies and offers alternate solutions to business problems. The office helps facilitate efficient decision making, policy and statutory adherence and provides tools and assistance agencies in achieving project success.
**Enterprise Shared Services (ESS)**

The Office of Enterprise Shared Services (ESS) manages a number of programs, including E-Government, the Statewide QA Program, the Geospatial Enterprise Office (GEO), the Oregon Transparency Program, and the State Interoperability Program. The central theme of these programs being the development of shared service models and management of long-term strategic vendor relationships—e.g., the state of Oregon’s e-Government partnership NIC-USA. Additionally, ESS has partnered with DAS Procurement in development of a joint IT Supply Chain Management program (“Basecamp”). Unlike the traditional approach to IT procurement, future statewide IT price agreements will be driven by the establishment of a comprehensive and cohesive enterprise technology architecture that ensures interoperability, while minimizing cost and disruption to current systems (i.e., a technology reference model). Ultimately, BaseCamp will provide a single point of reference for legacy, core, and leading technology services—aggregating purchasing power across the state, reducing application and infrastructure complexity and deepening the IT talent pool.

**Enterprise Technology Services (ETS)**

Enterprise Technology Services (ETS) is the shared services provider for computing and network infrastructure relied on by state agency IT support organizations. As a shared services provider of information technology infrastructure, ETS operates as an external service provider. ETS’ primary customer base is state agency IT shops responsible for developing innovative solutions aimed at automating the business operations that support Oregonians. The operations of ETS are guided by a business-centric governance structure. The infrastructure services supported by ETS are local and wide area network connectivity, storage management, computer hosting, disaster recovery and enterprise email.

**Enterprise Security Office (ESO)**

The Enterprise Security Office brings together all enterprise security - governance, policy, procedure, and operations - under a single accountable organization. This will allow for end-to-end direction setting and execution for enterprise security. The team will be composed of a Policy and Controls Section for setting enterprise security policy and developing associated controls to ensure compliance; a Solutions Section for driving enterprise security architecture; a Services Section for delivering day-to-day enterprise security operations in the data center; and a Security Operations Center (SOC) for providing dedicated, real-time security monitoring and response across the enterprise. In addition, the ESO will staff Business Information Security Officers for each major sector of the executive branch, established specifically to help agency leaders with strategic planning and risk-based decision making related to information security.
Goal 1. Maturing IT Resource Management

State government in Oregon is increasingly challenged to do more with less. Like other states, Oregon can no longer afford to maintain its current portfolio of IT services, past investments have resulted in unnecessary complexity and there is continuing misalignment between business strategy and IT decision-making. Effective IT governance and project and portfolio management maturity are critical for ensuring alignment between business and IT and prioritizing agency-specific and enterprise investment decisions.

OBJECTIVE 1. IT GOVERNANCE. Collaborating To Ensure IT Decision-Making Supports Long-term Agency and Enterprise Business Strategies

IT governance is about accountability and is a formalized process for making, communicating, and implementing IT investment decisions. It is a combination of three high-level aspects, including governance mechanisms, decision domains and approaches to decision making. Put differently, “What decisions must be made?”; “who will make these decisions?”; “How will decisions be made?” and “What is the process for monitoring results?” IT governance requires sustained executive leadership and repeatable processes to ensure alignment between organizational strategies and objectives.

Project and portfolio management (PPM) is a critical practice of IT governance; enabling cross-project visibility, project prioritization and benefits realization, enterprise architecture, asset and investment management and increased IT oversight and quality assurance. PPM facilitates the following processes:

- Scenario planning to address emergent business needs;
- Development of long-term IT investment strategies to meet business needs; Identification of shared service opportunities and duplicative project requests;
- Management of business-aligned portfolio segments to define opportunities within policy areas selection and prioritization of programs and projects;
- Balancing of resources and demand for strategic capacity planning;
- Balancing demand in order to ensure effective resource prioritization and load leveling; and
- Oversight of stage gate and workflow compliance; and

Challenge

IT project failures can frequently be traced to a lack of effective IT governance at the agency-level. In some cases, agency planning for projects and resources lags behind operational priorities or legislatively directed tasks and the biennial budget process. Absent governance and effective IT decision-making, agency IT initiatives will remain at risk due to a lack of business alignment, limited executive support, the absence of accountability and the inability to resolve competing priorities stemming from capacity constraints and resource contention.

1 NASCIO, “Is State IT Working on the Right Things”
A recent assessment by the Governor’s Office found that the majority of stakeholders interviewed lacked a clear understanding of how the State of Oregon makes or prioritizes IT investment decisions and what criteria are used. Furthermore, confusion also extended to how agencies make their own IT investment decisions. Some stakeholders expressed concerns that agencies may not be using best practices in the prioritization of IT.

At the enterprise-level, while there is general familiarity with the Enterprise Leadership Team (ELT) and the Enterprise IT Governance (EITG) steering team, it is not clear how these bodies work in the identification, deployment or operation of utility and shared services.

**Supporting Actions**

- **Develop** a process map in coordination with the Governor’s Office, EITG, ETS CUB and ELT that clarifies the processes, decision rights and expectations supporting project delivery and supports the development of an executive-level IT dashboard that provides centralized and transparent project status reporting.

- **Clarify** decision-making regarding the designation, funding, deployment, and operation of utility and shared services.

- **Establish** roles for Senior IT Portfolio Managers in developing agency IT strategic plans to assist in the alignment of IT and business across the enterprise.

- **Engage** with agencies to establish, formalize or document their internal IT Governance processes, and to identify best practices among agencies.

- **Draft** an OSCIO statewide policy on IT Governance that requires periodic submission of agency IT Strategic Plans; development and documentation of agency internal IT governance policies and procedures; adoption of agency project prioritization models; use of the Enterprise Project and Portfolio Management Tool to support agency-specific and enterprise project prioritization; and periodic submission of ranked IT project portfolios.

- **Develop** a scalable project and portfolio prioritization model based on best practices that considers strategic alignment, impact, cost, benefits realization (e.g., ROI) and risk that can be adapted to agency-specific needs.

- **Develop** an enterprise project and portfolio prioritization model based on best practices that considers alignment with the Governor’s priorities, cost, benefits realization (e.g., ROI) and risk.

**Impact**

**Short-term.** IT investment and decision-making informed by best practices that include the right people and perspectives from business and IT.

---

GOAL 1. MATURING IT RESOURCE MANAGEMENT

Long-term. Reduced risk, effective governance, and stewardship of IT resources and increased alignment with the Governor’s policy and program priorities.

Metrics

1.1 Agency IT Strategic Plans. Percentage (%) of agencies that have developed and submitted current agency IT Strategic Plans to the OSCIO.

1.2 Agency IT Governance. Percentage (%) of agencies (>25.00 FTE) that have developed and submitted documentation of their current internal IT Governance model.

1.3 Project Prioritization Portfolio Model. Percentage (%) of agencies (>25.00 FTE) that have developed and submitted their current portfolio prioritization model.

1.4 Agency Project Portfolio. Percentage (%) of agencies (>25.00 FTE) that have submitted their bi-annually ranked IT project portfolios.

1.5 PPM Maturity. Average PPM Maturity among agencies (>25.00 FTE)—i) unweighted, and ii) weighted by FTE.

OBJECTIVE 2. IT FINANCIAL MANAGEMENT

IT delivery may rely on internal agency resources, be purchased from the Oregon State Data Center (SDC) or through IT vendors. The costs for these resources may be detailed in various agency budget categories and accounting objects, may be embedded within individual program units, or mistakenly mischaracterized as non-IT expenditures. Additionally, IT initiatives may rely on a blend of state and federal funds.

Increasing budgetary constraints, legacy systems modernization, and increasing IT costs, heightens the need for aligning the cost of ETS services with industry best practices. Providing actual cost transparency, meaningful benchmarks, and actionable metrics for both business units and IT departments will aid agencies in projected IT budget development. In recent years, financial management of Enterprise IT aids in establishing the foundation for effective cost allocation and rate development.

While the IT chart of accounts, general ledger and other sources of financial and labor data are critical to determining the true cost of IT, effective IT financial management practices require mature IT asset management, a real-time and accurate inventory of IT infrastructure, hardware and software licensing entitlements and effective lifecycle management.

Challenge

The cost allocation methodologies and rates used to recover the costs of running the SDC remain a challenge. There is limited data on the total cost of ownership within the SDC. Gaining this detailed information is the first step to align with best practices and mature IT financial and asset management.

A recent review of software licensing entitlements and compliance, limited to only four vendors (IBM, Microsoft, CA and Hitachi), identified between $4-10 million in potential cost avoidance and compliance risk—mainly, through active maintenance of licensing metric tools and aligning licensing entitlements with the number of deployments actually required (i.e., over deployment or “surplus” licenses). In 2016, a
GOAL 1. MATURING IT RESOURCE MANAGEMENT

Microsoft audit found ~$3.7 million worth of MS SQL improperly deployed throughout the state (these licenses are now centrally managed by the SDC). Furthermore, under the terms of the 5-year Oracle Unlimited Licensing Agreement, the State of Oregon will need to be in a position to certify all of its licensing entitlements or risk substantial financial exposure. Ultimately, effective financial and assess management practices represent critical components of financial risk management and the business of IT.

Supporting Actions

✓ **Initiate and Implement** an asset management solution within the SDC (pending 2019-21 Legislative Funding).

✓ **Require** all agencies and SDC with IT initiatives amounting to or exceeding $150,000 to enter project costs (including internal labor) into the Enterprise Project Portfolio Management tool to identify the total costs of ownership (real value) and benefit realizations of their projects.

✓ **Identify** the detailed total cost of SDC services by 2019-21 biennium.

✓ **Align** processes to IT financial management best practices.

**Impact**

**Short-term.** Increase detail of accounting to better capture the actual SDC costs, allowing the state to better forecast and evaluate future technology needs. Increase insight and transparency to cost information on agency large IT projects.

**Long-term.** More accurate information for budget decision makers to prioritize future project funding, including better data about the current status and anticipated growth.

**Metrics**

1.6 **Application and Service Costs.** The total costs associated with the delivery of each SDC service delivered.

1.7 **Infrastructure Costs.** IT infrastructure costs per unit (e.g., server instance or data storage) more closely aligned to established targets and benchmarks.

OBJECTIVE 3. QUALITY ASSURANCE (QA). Implementing a Risk-based Approach to Third-Party QA Requirements

The OSCIO Quality Assurance (QA) program was established to encourage quality by design by engaging with agencies in planning for quality and risk management, improving the quality of project delivery, facilitating contracting for third-party QA consulting services, providing QA education and training, and reporting on major IT projects in execution (Stage 4).

**Challenge**

Until the passage of SB 87 (2017), the requirement for independent quality assurance (QA) applied to all IT projects exceeding $5 million without regard to risk—a one size fits all approach that denied the OSCIO discretion regarding the actual need for QA services and added unnecessary QA overhead to low-risk
GOAL 1. MATURING IT RESOURCE MANAGEMENT

projects. Additionally, in the case of low-dollar-high-risk projects or those staffed by internal resources, there was an argument against requiring QA oversight. Lastly, the requirement for independent (i.e., third-party) QA undermined the OSCIO’s internal capacity to perform QA functions.

Supporting Actions

✓ Develop policies and procedures to document and provide annual reporting to the Joint Legislative Committee on Information Management and Technology regarding IT initiatives exceeding $5 million where the OSCIO determined that independent QA was not necessary.

✓ Enhance the visibility of quarterly QA reporting by requiring the Quarterly Major IT Projects report available on request and providing a public-facing website dashboard of all projects within the QA portfolio.

✓ Align level of QA with project risk factors

✓ Expand the capacity of the OSCIO QA program to meet statewide needs

Impact

Short-term. Enhancing the OSCIO’s internal QA capacity and capabilities and elevating the role of quality management within IT project delivery through a flexible and risk-based approach to independent QA that scales to accommodate both high-dollar and low-dollar projects.

Long-term. Improved IT project outcomes in terms fewer failed IT projects, higher quality IT systems and cost avoidance through reduction of re-work and bug fixes.

Metrics

1.8 QMS Capacity. The independent QMS portfolio in terms of individual contracts, projects costs, and function points.

1.9 QA Exceptions. The number of QMS exceptions issued for IT projects exceeding $5 million.
GOAL 2. IT SUPPLY CHAIN MANAGEMENT

Goal 2. IT Supply Chain Management

In 2014, the current IT governance framework was established. The framework differentiates between unique-agency functions (or “bespoke”), shared services and utility services, and acknowledges that the majority of IT initiatives are currently best-managed at the agency-level—particularly, where such initiatives are governed by statute or unique Federal requirements.

Shared services provide central access points for defined, IT-supported business functions across multiple business units within the state. This approach improves operational efficiency, optimizes service delivery, lowers costs, and can harmonize operations and culture. Rather than simply consolidating duplicate capabilities, it changes the relationship between business and IT for better government outcomes.

While the clarification of decision-making regarding the designation, funding, deployment, and operation of utility and shared services is a critical component of maturing IT resource management, OSCIO will continue to support the coordination and identification of shared and utility services through the OSCIO Broadband Initiative, our IT Supply Chain Management Program (“Basecamp”) and work to encourage agency centers of excellence (e.g., business intelligence and analytics).

OBJECTIVE 1. OregonFIBER Partnership

Now recognized as the fourth utility, broadband is viewed as a critical component of community infrastructure, enabling innovation and new opportunities in education, health, and economic development. Communities who find themselves on the wrong side of the digital divide will increasingly struggle to recruit and retain businesses, provide quality education and deliver healthcare innovations such as “telemedicine.”

Agencies rely on voice and data networks to access information, communicate, and deliver services to other government agencies, business partners, and citizens. Network technologies provide the foundation for voice and data services to navigate within and across agencies, and to reach constituents throughout the state. OSCIO initiated a request for proposals (RFP) for last-mile and regional connectivity. At the same time, we have partnered with Oregon’s four research universities in the development of a new high-speed (100 Gbps) core research network.

Challenge

Employees and citizens increasingly expect continuous connectivity to conduct work and business at higher quality, greater capacity and faster speeds; however, upgrading aging network infrastructure is often costly. Meanwhile, the pressure is being placed on networks as vast amounts of data are being transferred

---


4 Oregon State University (OSU), the University of Oregon (UO), Oregon Health and Science University (OHSU) and Portland State University (PSU).
over the state's IT infrastructure to deliver essential services. Oregon spends a disproportionate amount of money to provide executive branch agencies with broadband services—managing over 1,400 Wide Area Network (WAN) circuits on individual contracts with no aggregation of services or economies of scale. Requesting new service may take months, as each new circuit needs to be scoped, engineered and bid individually, with vendor pricing and responsiveness varying widely.

Supporting Actions

- **Leverage** the collective buying power of the State and our Research University Partners
- **Increase** bandwidth
- **Standardize** pricing terms across the state or by region
- **Upgrade** data networks to ensure that capacity is able to support emerging technologies for the secure transmission of data, voice, and video
- **Optimize** use of existing network infrastructure
- **Reduce** transaction costs

Impact

**Short-term.** A reliable network infrastructure, resulting in faster access to applications and increased employee productivity.

**Long-term.** Increased adoption of newer technologies, including unified communications (integrated, real-time communication including voice, chat, and video), cloud, and mobile solutions, enabling the transformation of service delivery for the benefit of all Oregonians.

Metrics

2.1 **Availability.** Maximum bandwidth availability by circuit
2.2 **Average Cost/MB.** Average cost per MB (in aggregate and by agency)
2.3 **Total Measured Resource Consumption (MRC).** Total MRC (in aggregate and by agency)
2.4 **Network Capacity.** Number of days during the last quarter (90 days) where network utilization exceeded 75 percent (%) of total available capacity
2.5 **Public Fiber.** Amount of publically owned fiber in miles

OBJECTIVE 2. IT SUPPLY MANAGEMENT

The IT Supply Chain Management Program—“BaseCamp”—was designed to enable the state of Oregon to meet the increasing demand for information technology related products and services by coordinating statewide IT procurements, aggregating the purchasing power of the state and partner jurisdictions, establishing a technology reference model for lagging, core and leading IT products and services, and implementing a comprehensive vendor management framework.
GOAL 2. IT SUPPLY CHAIN MANAGEMENT

Challenge

While the State of Oregon is already transitioning to new models of service delivery for its information technology (IT), application and telecommunications needs, there is a growing recognition that traditional approaches to IT acquisition and vendor management are increasingly inadequate—given emergent technology, changes in the IT marketplace, the increasing sophistication of IT procurement, and the resulting vendor relationships. Traditional approaches to statewide technology procurement in Oregon can be characterized as ad hoc, insular and reactive.

- **Ad hoc.** Agencies typically requested one-off IT procurements without regard to statewide needs, and DAS Procurement Services fulfilled these requests one procurement at a time—increasing the cost, risk, and potential of inefficiencies.

- **Insular.** Agencies typically relied on in-house expertise to craft their statements of work rather than leveraging the resources and experience of other agencies—undermining the potential common solutions and further fragmenting the state’s IT spend and reliance on old service delivery models.

- **Reactive.** Traditionally, there has been little in the way of proactive vendor management or relationship management—resulting in disjointed vendor relations, the absence of performance management and contract-level engagement.

Supporting Actions

- **Align** all IT procurement opportunities and strategic procurements with the Oregon Technology Reference Model
- **Ensure** all statewide IT procurements include a performance work statement—outlining performance measures and public disclosures
- **Increase** engagement with partner jurisdictions through continued stakeholder outreach, vendor contacts, conference participation, surveys, and active procurements
- **Accelerate** the number of high-value statewide IT procurements available to state agencies and partner jurisdictions
- **Reduce** the number of ad hoc agency-specific IT procurements
- **Publish** vendor scorecards and performance data on a quarterly basis
- **Leverage** market research and performance data to drive customer value

Impact

**Short-term.** Increasing the number of high-value statewide IT price agreements available and increasing the utilization of these agreements by agencies and partner jurisdictions. Driving value by leveraging statewide purchasing power and proactive vendor management.

**Long-term.** Realignment of the IT procurement portfolio towards statewide IT price agreements and simplification of the State’s IT operating environment.
Metrics

2.6 Engagement. The number of unique visits to the Basecamp website over the last 90 days.

2.7 Procurements. The number of Basecamp opportunities identified that are active procurements and the average number of days required to complete the procurement process.

2.8 Volume. The volume of IT products and services (in dollars) procured by state agencies and partner jurisdiction under statewide agreements initiated by Basecamp.
Goal 3. Data Utility

Data has become a critical strategic asset, informing agency business processes and decisions. Implementing strategies to obtain greater benefit from data will provide improved service delivery across the enterprise and to the citizens of our State. While most agencies are mature in the traditional organization, administration, governance, and management of their data, there are opportunities for innovation that come from open data and data analytics.

OBJECTIVE 1. GEOSPATIAL FRAMEWORK DATA

The Oregon Legislature recognizes the importance of geospatial framework data, and through the passage of HB 2906 (2017), has committed to the collection and dissemination of geospatial “framework” data—typically, foundational and trusted data elements that serve multiple sectors, are organized into 15 geospatial themes, developed using agreed-upon standards and maintained through collaborative stewardship. Increasingly, datasets with locational elements (e.g., addresses or tax lot IDs) constitute an essential component of the business of government.

Prior to the passage of HB 2906, the Oregon Geographic Information Council (OGIC) operated pursuant to Executive Order 00-02, “Oregon Geographic Information Council,”—in effect since February 1st, 2000. HB 2906 established the Council within statute under the authority of the OSCIO, re-balanced the Council’s membership with increased local government representation, provided for the appointment of a State Geographic Information Officer (SGIO) and required the sharing of certain geospatial data elements (“framework data”) between public bodies beginning in 2020.

Challenge

According to a 2006 OGIC study, Oregon State and local government waste $200 million annually through unnecessary and duplicative geospatial data collection and management. However, in the absence of consequential incentives, mutual purpose and effective governance, concerns over privacy/confidentiality, liability and cost recovery represent substantial impediments to data sharing between public bodies. The Council needs to establish governance and funding mechanisms to address these concerns in order to increase the collection and public-sector availability of geospatial framework data.

Supporting Actions

- **Appoint** a State Geographic Information Officer
- **Recruit** new local government and non-profit representation for the Council
- **Establish** working subgroups to resolve outstanding concerns regarding privacy/confidentiality, liability and custodianship through revised licensing agreements and model intergovernmental agreements (IGAs)
- **Build** a secure high-availability central geospatial data library
GOAL 3. DATA UTILITY

✓ **Develop** a policy option package for Oregon Geographic Information Council Fund for 2019-21 Governor’s Budget that would fund the collection of geospatial framework data through competitive grants

✓ **Partner** with the Oregon Watershed Enhancement Board to streamline grant applications

**Impact**

Short-term. Increase geospatial data-sharing between public bodies and reduce unnecessary expenditures on data collection and management.

Long-term. Establishment of a central geospatial data warehouse that includes all framework data elements, that is freely available to public bodies and that enables the transformation of the business of government.

**Metrics**

3.1 **Availability.** Percentage (%) of geospatial framework data elements available within the central geospatial data library

3.2 **Standards.** Percentage (%) of geospatial framework data elements covered by an OGIC standard

3.3 **Availability.** Percentage (%) of geospatial framework data elements available through a cloud-based GIS platform or service

**OBJECTIVE 2. OPEN DATA**

The Oregon Legislature has long recognized the importance data as a strategic asset, however, with the passage of HB 3361 (2017) it has enabled the state to unlock the value of public data through standards that enable the public to search, extract, organize and analyze high-value datasets—enhancing transparency through proactive release and providing the foundation for shared insight and innovation. A redesigned Oregon open data portal—data.oregon.gov—will promote government transparency, encourage citizen participation and better enable the efficient use of public resources.

**Challenge**

While the state of Oregon was a pioneer in establishing its open data portal in 2011, progress has slowed due to resourcing and lack of data available through the portal. This in part is due to the current operating model where data is made available on a case-by-case basis at the individual discretion of state agencies. The lack of sharing “public” data even among state agencies and between divisions within the same agency, requires extensive negotiation of complex data sharing agreements and reinforces programmatic silos.

A related issue is the underutilization of data as a strategic asset due to a lack of common data standards and of an enterprise data inventory—limiting collection and dissemination of open data, cross-agency analysis, reducing interoperability, and frustrating business intelligence initiatives and data-driven decision making.
GOAL 3. DATA UTILITY

From the public perspective, the absence of an enterprise data inventory does not build trust in transparency. Oregonians are currently not aware of what data is available and cannot make meaningful requests for that data. Whereas from an agency perspective, the lack of such an inventory may result in duplication of effort and lost opportunities. In addition, in the absence of an accurate and well-managed portfolio of data assets, state agencies cannot make meaningful determinations regarding their cybersecurity risk profile.

**Supporting Actions**

- **Appoint** a Chief Data Officer
- **Establish** an Open Data advisory group
- **Develop** an Enterprise Data Strategy
- **Publish** and Open Data Standard
- **Draft** a technical standards manual
- **Develop Educational program around Data Management Maturity and new state standards**
- **Coordinate** the collection of an enterprise data inventory and make summary information publicly available
- **Develop** statewide policies and procedures to support Open Data and publishing to the State’s web portal

**Impact**

**Short-term.** Reduced frequency of open records requests and staff time spent responding to requests by making agency data available for stakeholder consumption.

**Long-term.** Increased cooperation and performance through transparency, data quality and sharing, accountability, and public engagement.

**Metrics**

- **3.4 Data Inventory.** Percentage (%) of agencies (>25.00 FTE) that have submitted their data inventories
- **3.5 Data Publication.** Number of high-value datasets (to be defined in policy) published

**OBJECTIVE 3. DATA STRATEGY**

The state possesses an untapped asset in the data it collects and stores. To make it useful, the state must improve its approach to data management, which requires agencies to develop and execute data management and governance structures, practices, and procedures that properly manage the full data lifecycle. A coordinated, enterprise approach to data management promotes the availability of consistent, secure, accurate, timely, and accessible information.
GOAL 3. DATA UTILITY

Challenge
With growing data volumes and increased data complexity, the job of data management is more challenging than ever. Oregon government must improve data management and governance practices to fully realize the benefits that data can provide. Concerns regarding security, accuracy, integrity, ownership, usage rights and volume of data all contribute to the complexity of managing the state’s information.

Supporting Actions
Require Agencies to:

- **Implement** uncomplicated internal data governance structures aligned with the new state standards to guide agency-wide data decisions.
- **Develop** data management policies and procedures to improve the integrity and usefulness of agency data.
- **Promote** standardization and interoperability of systems through a master data management plan.

Impact

**Short-term.** A clearer understanding of data, identification of areas for improvement, and identification of a reduction of duplicative data collection efforts.

**Long-term.** Reduced storage and operating costs, reduce duplication, improved retrieval, and usefulness of data in support of business processes and decision making, and improved data protection and transparency.

Metrics

3.6 **Data Strategy.** Percentage (%) of agencies that have developed and submitted current agency data strategies to the OSCIO

3.7 **Data Management Maturity.** Average DMM Maturity among agencies (>25.00 FTE)

OBJECTIVE 4. DATA ANALYTICS

Data analytics is the science of examining raw data with the purpose of obtaining information and drawing conclusions from the data. As the amount of data available to the state continues to grow, so does the opportunity for agencies to use data analytics to guide important decisions. As analytical tools mature and become commonplace, agencies will benefit from timely data mining strategies that inform decision making.

Challenge
Traditionally, agencies look for answers in static, rather than dynamic, data. If managed and mined properly, data can inform the agency on areas needing improvements, such as work processes and
customer satisfaction. Knowledge gathered from data analytics can enhance both immediate responses and long-term strategic planning.

**Supporting Actions**

- **Obtain** executive and program-area buy-in to cultivate good, agency-wide data practices that improve data quality
- **Develop** and seek expertise and tools to successfully begin a data analytics program
- **Evaluate** and refine analytics strategies and decision-making processes
- **Begin standardizing** enterprise data analytics solutions that can be leveraged across agencies and aggregated for state-wide metrics, reporting, dashboards, and predictive analytics

**Impact**

**Short-term.** Reduced risk associated with decision making, and identify areas for cost savings and improvement.

**Long-term.** Improved business processes, planning ability, customer service and data-driven decision making.

**Metrics**

- **3.8 Data Sharing Agreements.** Current number of data sharing agreements in effect (baseline determination)
- **3.9 Analytics Solutions.** Current number of data analytics solutions and the costs per license (baseline determination)
- **3.10 Data Storage.** Cost reductions associated with elimination of duplicative data storage
Goal 4. Information Security

At a fundamental level, information security is about trust—as public servants and custodians of public data, we owe Oregonians a duty to protect their personal information. Regardless of agency mission or size, Oregonians rightfully expect their government to use technology to improve customer service while ensuring those systems are secure and that personal information is subject to consistent protections. Citizen expectations of privacy, should not hinge on the agency with whom they are transacting—be it the Department of Motor Vehicles or Department of Fish and Wildlife (ODFW).

Objective 1. Unifying Enterprise Security Operations

With the passage of SB 90 (2017), the mission of the ESO will be “unifying cybersecurity to improve customer service for Oregonians while ensuring those systems are secure, resilient and ready for the future.” In working to realize this mission, the ESO has identified four focus areas that build on the work associated with the implementation of EO 16-13, including i) proactive, holistic risk management; ii) open empowered culture of security; iii) resilient it architecture; and iv) rapid detection, response, and recovery. The unified strategy recognizes that IT security is a public good and that we are more resilient when we stand together—pooling our cybersecurity resources and shifting our approach from a model of risk transfer and assignment of blame to a proactive enterprise security approach.

Fig. _ Enterprise Security Office. Strategic House
Challenge

Recent IT security breaches, persistent vulnerabilities, non-compliance with IT security-related OARs and statute and the most recent Secretary of State audit findings demonstrated that Oregon’s decentralized model for IT security was failing. In some agencies, there were clear capacity gaps, a legacy of disinvestment and an overly risk-tolerant approach to the cyber risks facing our state. More problematic however is the asymmetric nature of IT security risk, where the vulnerabilities of smaller and under-resourced agencies put larger state agencies and local government partners at risk.

Supporting Actions

- **Restructure** the ESO to accommodate the addition of 35 new positions and IT security responsibilities transferred pursuant to SB 90 (2017)
- **Draft** a new Statewide Security Plan (last updated in 2009)
- **Conduct** regular NIST-based IT security assessments encompassing IT infrastructure, external applications, application security and Level-4 data handling
- **Implement** vulnerability management across the enterprise and deploy internal scanning across all Executive Branch end-points
- **Build** a culture of security through education and awareness activities
- **Revise** statewide IT security policies to support a new Statewide Security Plan
- **Establish IT** security risk governance model that supports overall IT governance and ensures rapid, informed and documented IT security decision making

Impact

**Short-term.** Improvements to the security posture of state agencies through regular risk assessments, cyber hygiene, remediation of vulnerabilities and enhanced employee awareness and ESO staffing capabilities—reducing risk to the agency, its data and citizen information.

**Long-term.** An open, empowered culture among all Executive Branch employees that supports: proactive, holistic risk management; the implementation of resilient IT infrastructure; and rapid detection, response, and recovery.

Metrics

1. **Risk Assessments.** Percentage (%) of agencies that have undergone an information security risk assessment in the last 2 years
2. **External Application Scans.** Percentage (%) of agencies that have undergone an external application scan in the last 2 years
3. **Internal Infrastructure Scans.** Percentage (%) of agencies that have deployed internal scanning infrastructure and have conducted scans in the last 90 days

---

GOAL 4. INFORMATION SECURITY

4.4 **Critical Vulnerabilities per Host (CPH).** Average number of critical vulnerabilities per networked device (in aggregate and by agency)

4.5 **Vulnerability Scan Quality.** Percentage (%) scans completed in last 90 days that were “high quality”

4.6 **Policy.** Number of statewide IT security policies that have not been revised or reviewed in the last 2 years

OBJECTIVE 2. CYBERSECURITY CENTER OF EXCELLENCE

Information security is woven into the fabric of public trust—we owe Oregonians a duty to protect their personal information and ensure systems are secure. At the same time, Oregon requires a long-term multi-sector cyber strategy that leverages the private-sector expertise of Oregon's cyber-related industries, enables information sharing, anticipates cyber disruptions and builds capacity across the state and with our local government partners and school districts.

Beyond unifying IT security functions and personnel within the Executive Branch of state government—extending Executive Order, 16-13 “Unifying Cyber Security in Oregon”—SB 90 established the Cybersecurity Advisory Council within the Office of the State Chief Information Officer (OSCIO). SB 90 also provided a legal framework for establishing an Oregon Cybersecurity Center of Excellence (CCoE) and requires the OSCIO to return with a detailed CCoE proposal within 2 years.

The cross-sector Cybersecurity Center of Excellence is part of a broader Cyber Oregon initiative and is intended to adopt a collective impact model that brings together Oregon’s Cyber-related industries, universities and local governments to improve Oregon’s overall cybersecurity ecosystem and statewide security posture.

**Challenge**

Under the traditional approach to IT security, there is a tendency to focus on individual agency needs and the transfer of risk, leaving others to take care of themselves. However, cyber threats neither respect nor acknowledge the jurisdictional boundaries separating the bodies that comprise Oregon’s public sector. While community institutions may fall outside the traditional ambit of state cybersecurity, our interdependence and shared information systems render individual and isolated interventions insufficient—we are more resilient when we stand together.

**Supporting Actions**

- **Identify** the membership of the Cybersecurity Advisory Committee
- **Convene** the Cybersecurity Advisory Committee and charge empower them to articulate a shared vision for an Oregon Cybersecurity Center of Excellence (CCoE)
- **Conduct** a cross-sector cybersecurity capabilities, resources and needs assessment that supports the development of a CCoE through comparative policy analysis, surveys, focus groups, identification of funding opportunities and stakeholder outreach
GOAL 4. INFORMATION SECURITY

✓ Raise public awareness through the Cyber Oregon initiative—a public-private campaign supported by a vendor-neutral website that taps into the expertise of Oregon’s cyber-related industries through tools, tips, news, social media and other online forums

✓ Propose legislation and funding to make the Oregon CCoE a reality and serve as a model for other states

Impact

Short-term. Articulation of a shared vision for an Oregon Cybersecurity Center of Excellence (CCoE); increased public awareness of cybersecurity; development of a public-facing vendor neutral clearinghouse of cybersecurity information; and crafting of a Legislative concept and funding model to support the CCoE.

Long-term. Establishment of a CCoE with a sustainable funding and operations model that enjoys widespread support among Oregon’s cyber-related industries, universities, local governments and schools—providing a forum for sharing threat intelligence and best practices, encouraging the development of a diverse talent pool for Oregon’s cyber-related industries through public-private sector partnerships and internships, establishment of an Oregon Civilian Cyber Corps, and development of scalable public-sector threat monitoring and response capabilities.

Metrics (potential)

4.7 Cyber Readiness Index. The Cyber Readiness Index 1.0 (CRI) as modified by Spidalieri (2015), a comprehensive, comparative, experience-based methodology created to evaluate a state’s maturity and commitment to cybersecurity.

4.8 Need. The percentage of survey respondents that indicate agreement with the need for the services associated with a CCoE (CPS Assessment will provide baseline data).

4.9 Awareness. The number of unique visits to the <Cyber OREGON> website over the last 90 days; the number of newsletters and/or cyber alerts subscribers; and the

4.10 Commitment. The number private-sector commitments in terms of letters of support; staff time dedicated to the CCoE; and financial contributions to the <Cyber OREGON> initiative.

4.11 Engagement. The number of small business, local government and education cybersecurity consulting engagements conducted under the auspices of the CCoE.

4.12 Workforce. The number of internship placements associated with the CCoE and/or Federal Cybersecurity Scholarships for Service.
GOAL 5. CAPACITY MANAGEMENT

Goal 5. Capacity Management

The internet revolution and consumerization of information technology (IT) has fundamentally altered the ways in which consumers expect to engage with organizations, both private and public. Consumers and citizens alike increasingly expect real-time, easy to use mobile transactions. However, there is an increasing disconnect between these expectations and Oregon’s disparate and antiquated environment. Legacy systems are more difficult and costly to maintain. They are less resilient and carry a higher degree of security risk. Yet they cannot be easily replaced due to cost, limited expertise, and complexity of the systems.

OBJECTIVE 1. SDC POWER

The State Data Center (SDC) has provided Information Technology infrastructure to state agencies and local government since January 2007. More than seven years after the state embarked on building its own data center and consolidating a substantial portfolio of agency IT needs and services into a single provider, the state’s IT infrastructure needs have outpaced available capacity. The original 11 Computing and Network Infrastructure Consolidation (CNIC) agencies’ workload, have utilized available capacity and the customer demand to date for data center service has been met through virtualization and modernization of the computing environment within the SDC. While the SDC is currently working to free up stranded electrical capacity, it has effectively reached the limits of its initial capacity.

Challenge

In order to limit the initial capital outlay, the design of the SDC facility was such that the core mechanical infrastructure (generators, electrical switchgear, cooling infrastructure) of the building was only built to meet at 50% of its’ total capacity, with the intent to double that capacity to accommodate increasing future demand. Absent additional power, the SDC IT infrastructure will either need to remain within existing agency facilities or relocated using third-party data center space through brokered agreements—underutilizing the capabilities of the state’s own purpose-built data center.

Supporting Actions

- **Build-out** core mechanical infrastructure to increase available power capacity and redundancy
- **Install** vented chimneys on all servers within data halls to reduce cooling costs (pending available funding)
- **Implement** hot/cold aisle containment to further increase energy efficiency
- **Provide** a co-location (self-managed) service offering to agency customers
- **Reduce** the number of non-SDC data centers
GOAL 5. CAPACITY MANAGEMENT

Impact

Short-term. Additional SDC capacity enabling the establishment of a co-location service offering and enhanced physical security and recovery of the state’s data.

Long-term. Increased utilization of the SDC resulting in cost avoidance associated with non-SDC data centers, greater efficiencies and lower costs for current SDC customers.

Metrics

5.1 Capacity. Increase total electrical capacity to meet demand
5.2 Consumption. Increase total electricity consumed
5.3 Utilization. Increase number of agency (Executive Branch) servers migrated to the SDC
5.4 Cost Avoidance. Capital costs and operations and maintenance avoided as a result of agency migration to the SDC

OBJECTIVE 2. CLOUD SERVICES ENABLEMENT

Cloud technology provides an alternative to traditional IT delivery models. Cloud computing—a model that enables on-demand network access to resources—has the potential to change the way the state does business. This convenient, as-needed delivery of services eases the burden for capital expenditures and has the potential to minimize time to deployment for SDC and its customers.

Challenge

Concerns regarding security, system interfaces, legacy architecture, and procurement keep the SDC from advancing cloud implementation beyond basic applications.

Supporting Actions

✓ Develop a comprehensive strategy that will guide cloud deployments, then pilot infrastructure solutions in the cloud with a goal of easing the burden on aging infrastructure and quickly address agency growth while reducing capital outlay.
✓ Increase use of Basecamp cloud contracts and statement of work templates to determine where to start and to implement solutions.

Impact

Short-term. Benefit from the consolidated buying power of the state, and increase utilization of cloud services.

Long-term. Realized benefits of cloud services through cost-effective solution design and replacement of unsupported legacy systems.

Metrics

5.5 Cost: Increased return on investment through more service offerings, faster time to market and potential cost savings for agencies.
5.6 **Adoption**: Reduced reliance on on-premise hardware, while reducing the States need for capital outlay for IT infrastructure.

**OBJECTIVE 3. LEGACY SYSTEM RISK MANAGEMENT**

Agencies are facing the next step in modernizing business capabilities, replacing numerous legacy systems to move toward a more collaborative and interoperable state government. As agencies transition from traditional practices to innovative solutions, they will need to evaluate current and ongoing investments in legacy systems and consider the scalable services of cloud and the efficiencies of shared services. Legacy modernization, cloud, and shared services will continue to increase in impact. Determining which services to use, with whom to share services, and how to get there may not be easy, but is essential to the future success of state agency IT.

**Challenge**

Legacy systems modernization remains a challenge for agencies due to decreasing vendor support for end-of-life systems and limited funding and staff to maintain them and plan for their replacement. A statewide effort is now underway to help agencies identify and upgrade unreliable systems, but it will take planning, time, and ample resources before the state can resolve this challenge. In the meantime, systems and data are at risk.

**Supporting Actions**

- **Establish a process to evaluate** cloud services and commercial off-the-shelf solutions before building custom applications.
- **Conduct** regular security audits through the CISO of unsupported systems and legacy systems to identify high-risk systems, and establish a roadmap for prioritizing issues and upgrading unsupported software.
- **Create** an inventory of all legacy systems and their data sets as a baseline for a roadmap moving toward modernization.

**Impact**

**Short-term.** Improved repeatable, adaptable methodologies to standardize and prioritize legacy system modernization. Insight into current landscape and data into risk exposure.

**Long-term.** Future roadmap for moving state off non-supported, at-risk systems. A statewide architecture structure that easily grows with business needs, rather than a depreciable asset.

**Metrics**

- **5.7 Legacy Systems.** Inventory of all current legacy systems to serve as a baseline.
- **5.8 Agency Migration Strategy.** % of agencies with a documented plan in place to replace and retire legacy systems.
5.9 **Enterprise Migration Strategy.** Criteria and prioritization process through Enterprise IT Governance to address most at-risk systems
Recent OSCIO-Related Legislation

**SB 87 (2017)**
The bill amended ORS 291.035(2) (a) so that the Office of the State CIO has the discretion to determine whether an IT project exceeding $5 million does not require independent quality assurance (QA) services. It also maintained a statutory presumption requiring independent QA, unless there was an explicit determination that QA was not required.

**SB 88 (2017)**
The bill amended ORS 182.128 (4) and (5), reduced the quorum requirements for the Electronic Government Portal Advisory Board (EPAB) from a majority of the entire advisory board to a majority of its voting members. Additionally, the bill amended ORS 182.126(1) and ORS 182.132(3)(a) and (b) by substituting the term "convenience fee" with "portal provider fee".

**SB 90 (2017)**
The bill unified IT security functions and personnel within the Executive Branch of state government—extending Executive Order, 16-13 "Unifying Cyber Security in Oregon." Additionally, the bill established Cybersecurity Advisory Council within the Office of the State Chief Information Officer (OSCIO), and it provided the legal foundation for establishing an Oregon Cybersecurity Center of Excellence (CCoE) through public-private-partnership enabling language and by enabling the OSCIO to obtain grant funding. Lastly, the bill requires the OSCIO to return with a detailed CCoE proposal within 2 years. The cross-sector Cybersecurity Center of Excellence is part of a broader Cyber Oregon initiative and is intended to adopt a collective impact model that brings together Oregon’s Cyber-related industries, universities and local governments to improve Oregon’s overall cybersecurity ecosystem and statewide security posture.

**HB 2906 (2017)**
The bill establishes the Oregon Geographic Information Council (OGIC) under statute; provides for sharing of geospatial data ("framework data") between public bodies beginning in 2020; requires the appointment of a State Geographic Information Officer (SGIO) by the Office of the State CIO; requires the SGIO to maintain, secure and provide access to a central geospatial data library for the purpose of sharing geospatial framework data; and establishes the Oregon Geographic Information Council Fund with biannual reporting requirements on funds expended.

**HB 2946 (2017)**
The bill amended ORS 184.483 (7) (a) (b) and (d), significantly expanding the range of transparency reporting to include revenue, expenditure, and budget data for the following entities: semi-independent state agencies, public universities, statewide programs operated by public universities, and any public corporation designated in statute. Directs State Chief Information Officer to include links on the Oregon Transparency website (http://www.oregon.gov/transparency) to the data, per established standards, in the format requested. Also, allows other entities to request that links to their websites be posted.
**HB 3361 (2017)**

The bill establishes the position of Chief Data Officer (CDO) within the Office of the State CIO. Directs CDO to establish an Open Data standard for the management of data as a strategic asset and proactive release of publishable data, develop an enterprise data and information strategy, and maintain a web portal for the release of publishable data. Requires state agencies to comply with the Open Data Standard and to release publishable data on the data.oregon.gov web portal.
Agency Information

Office of the State Chief Information Officer
155 Cottage St., Salem, OR
Tel 503.378.3175
Fax 503.378.3795
www.oregon.gov/das/OSCIO