OREGON | Office of the State
Chief Information Officer

2016

OSCIO Statewide IT Assessment

THE STATE OF INFORMATION TECHNOLOGY IN OREGON

INTRODUCTION

Table of Contents

Introduction

As we all know, changing citizen expectations coupled with the failed launch of Cover Oregon have increased interest in state IT oversight and service delivery—reflected in the passage of HB 3099 (Chapter 807, Oregon Laws 2015) which became fully operative on January 1, 2016. Among its many provisions, HB 3099 also directed Office of the State CIO (OSCIO) to conduct several biennial assessments, including: a review of state agencies compliance with the OSCIO's rules, policies and standards; a market analysis of the state data center; and recommendations regarding the establishment of new shared and utility services. Pursuant to ORS 291.039(4)(a) our Office presents these findings to the Governor and the Joint Legislative Committee on Information Management and Technology (JLCIMT).

In support of these reporting requirements, our Office conducted a statewide survey focused on IT asset management with an emphasis on IT infrastructure and IT personnel. These themes were underscored in a memorandum from JCLIMT memorandum, dated February 11, 2016, that specifically identified the following concerns:

- *"Apparent or actual agency non-compliance with IT-related statutes, State CIO rules and policies, or stated expectations related to IT Investment Review and Approval and Information Security, and the need for the Office of the State CIO to establish rules, policies, and standards related to IT procurement. (Note: ORS 291.990 Penalties - is an available remedy)"*
- *"The need to assess and determine how to best reorganize and stabilize the Enterprise Technology Services unit's Service Catalog and associated rates, while incorporating managed services (e.g., the statewide voice services contract) and brokered cloud services (e.g., Infrastructure as a Service - IaaS) offerings into the mix of services that the Office of the State CIO provides to state agencies and other customer organizations."*
- *"The current distribution/decentralization of responsibility and accountability for information security across the enterprise."*
- *"Agencies that currently utilize, maintain, support, and who are considering the submission of budget requests to sustain or enhance their own computer rooms (small data centers) at their agency's."*

Unlike previous assessment and benchmarking efforts, such as the 2012 Hackett Group study, the intent of the survey was to capture the current state of IT from the vantage point of a typical agency CIO. In adopting this stance, our Office hoped to reduce the reporting burden and gain greater insight into the opportunities and challenges faced by the IT organizations within each agency.

Additionally, it is worth noting that the assessment has and will continue to inform the development of policy-area Information Resource Management (IRM) plans. The policy-area IRM plans build on agency IT strategic plans and proposed project portfolios for 2017-19 that align with the Governors initiatives. The policy-area IRM plans will be presented during the 2017 Legislative Session.

INTRODUCTION

GENERAL NOTES

The OSCIO Statewide IT Survey was distributed in May of 2016 and agencies were provided just over three months to complete it. The survey was announced in several forums, including: during an All Agency Director's Meeting and the 2017-19 Budget Kick-Off and was distributed to both agency and IT leadership. Additionally, Strategic Technology Officers for each of the policy-area segments were available to answer questions and provide technical assistance. The survey itself included 48 questions (Appendix A) related to the following topics, including:

- IT Finance
- IT Personnel & Staff Augmentation
- Infrastructure
- Application Portfolios
- IT Operations
- Telecom & Network Expenses
- IT Security
- IT Strategy, Planning, Project and Portfolio Management
- OSCIO Policy Compliance

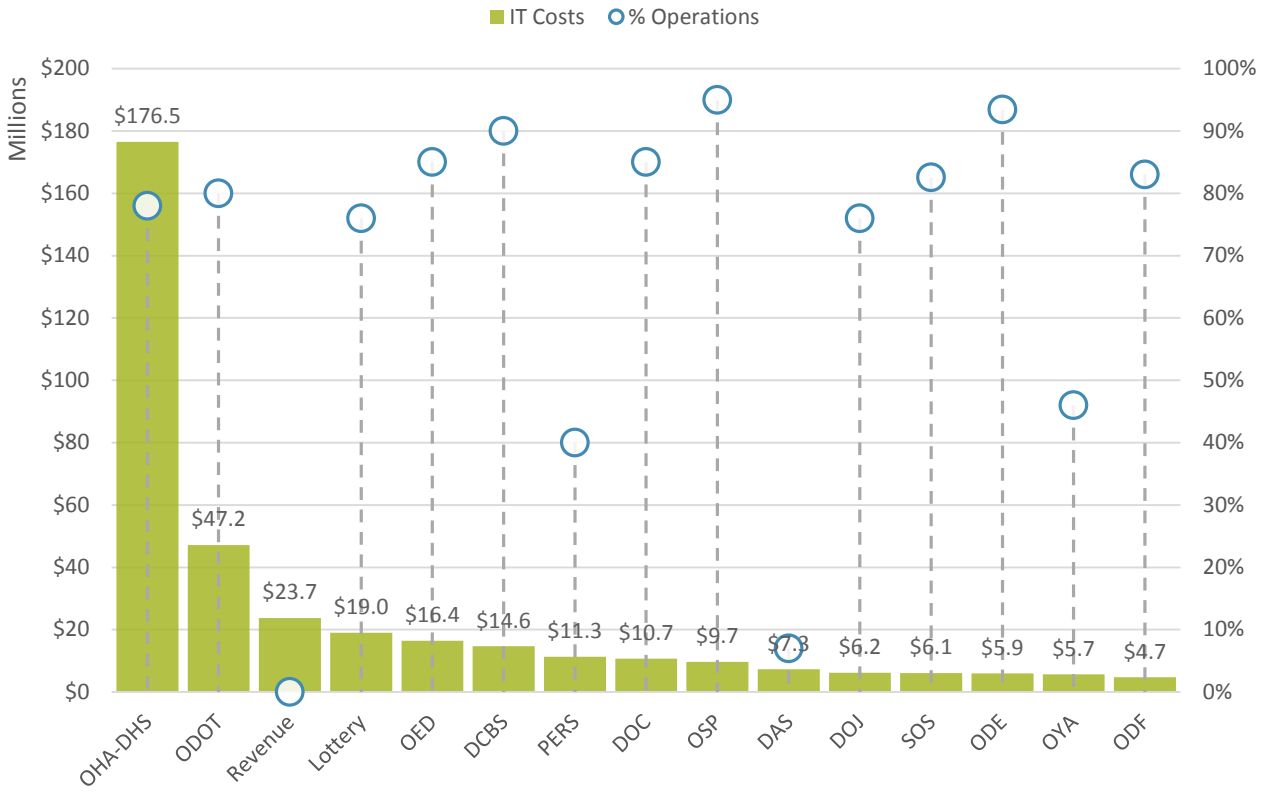
There were 58 responses representing 59 agencies (the Office of Information Services submitted a joint-response on behalf of the Department of Human Services and the Oregon Health Authority). In addition to Executive Branch agencies, there were responses from several exempt agencies, including the Secretary of State and Oregon State Library. No responses were received from agencies within either the Legislative or Judicial Branch. Given these omissions and the limitations of self-reporting, the overall figures and trends are by definition under-inclusive. However, despite these limitations the assessment findings offer a statewide perspective and provide insight into the challenges and opportunities faced by agency IT leaders in Oregon.

IT Finance

The overall reported IT spend was just over $391 million with an average of about $6.8 million per agency. The top 15 agencies in terms of their IT budgets account for nearly 93% of the total agency IT spend. The largest single category of IT spend by functional area was within client devices and peripherals (*e.g.,* desktops) at just over $61.6 million. The second and third most significant areas in terms of IT spend were related to servers at just over $25.7 million and $20.1 million on networking infrastructure.

The ratio of IT budgets spent on IT operations and maintenance was 70% on average. Typically, the lower this figure the better because it represents investments in new capabilities as opposed to time spent fixing antiquated or obsolete equipment. That said, there were many agencies who spent 90% or more of their IT budgets on operations or maintenance. The chart on the following page summarizes the aggregate IT spend and proportion spend on maintenance and operations for the top 15 respondents, representing 16 agencies.

Fig. 1 - Average IT Costs & Operations



IT Personnel & Staff Augmentation

In terms of overall staffing profiles, the majority of agencies have relatively few IT staff. Of the 59 respondents, 8 agencies reported having no dedicated IT staff and 30 respondents indicated that their IT staff was between 1 and 10 individuals. Just as with IT finance, a few of the top tier agencies account for the vast majority of IT personnel within the state—namely, OHA-DHS, ODOT and DAS. There are only 9 agencies with IT staffs that exceed 50 individuals. Figure 2 summarizes the overall IT staffing profiles.

Fig. 2 – IT staffing profiles

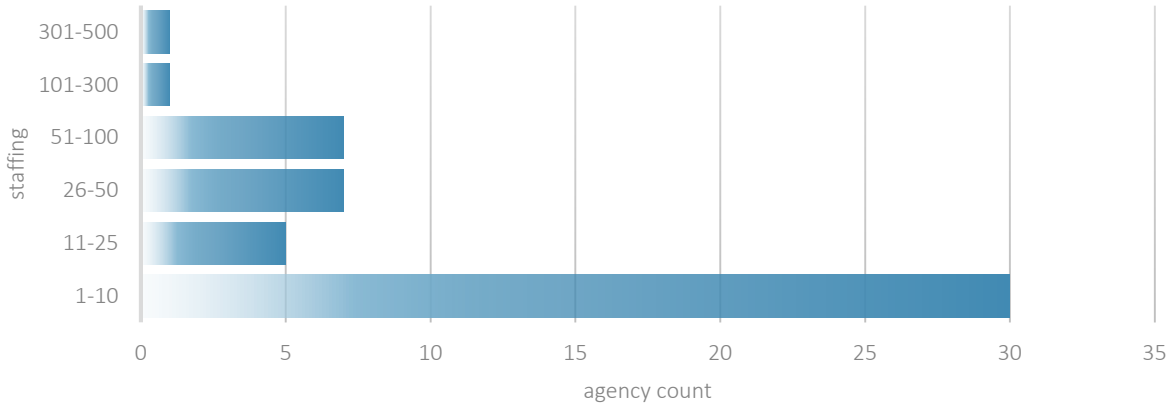
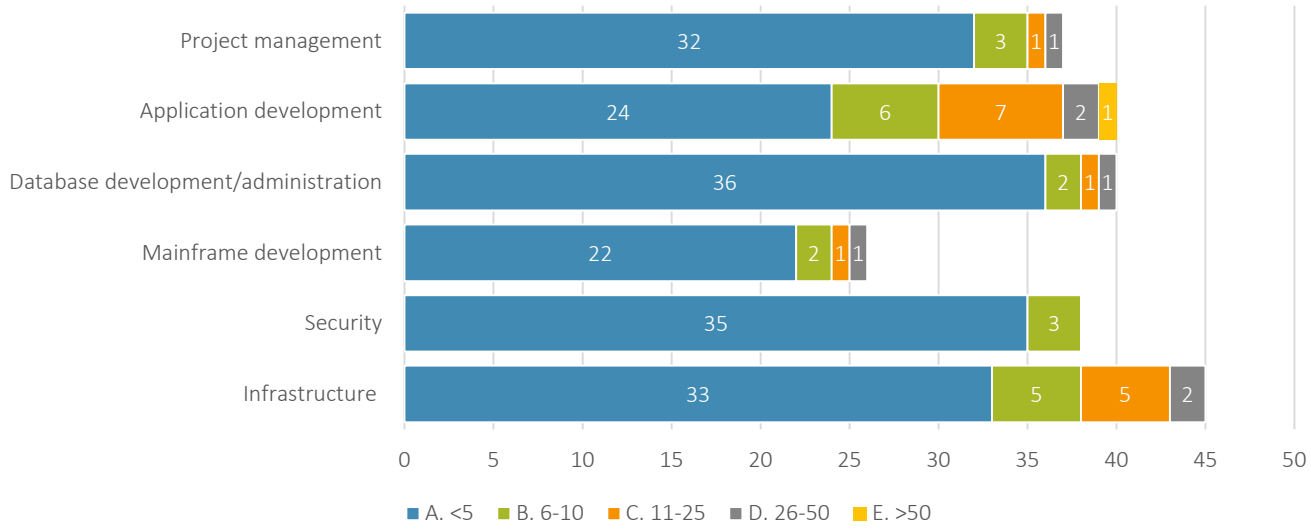


Figure 3 disaggregates the overall IT staffing profiles by functional areas, including: infrastructure, security, mainframe, database development, applications development and project management. An interesting finding was the predominance of IT infrastructure staff. Defined so as to include mainframe maintenance, network and servers. Of the 59 respondents, there were 45 who had IT staff working within this functional area. In 12 cases, the agency had 6 or more IT staff working within this area. Somewhat unsurprisingly, the next most significant functional areas represented were application development and database administration. The chart below provides additional detail.

Fig. 3 – IT staffing by functional area



In addition to identifying the functional composition of their IT staffs, agencies were also asked to identify the number retirements they anticipate within the next five years by functional area. Again, infrastructure looms large. Of the 45 agencies who have IT infrastructure staff, 35 of them anticipate that they will be losing staff to retirement. Similarly, 18 agencies or about 30 percent, identified infrastructure as a critical IT skills gap within their organization—followed by security and project management.

Fig. 4 – IT staffing + retirements

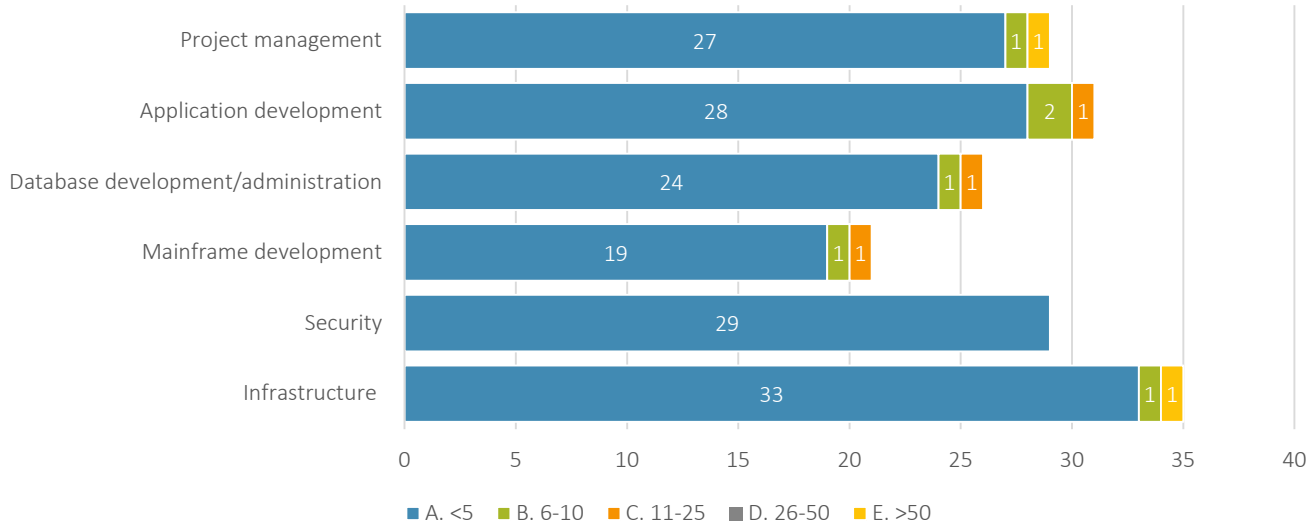
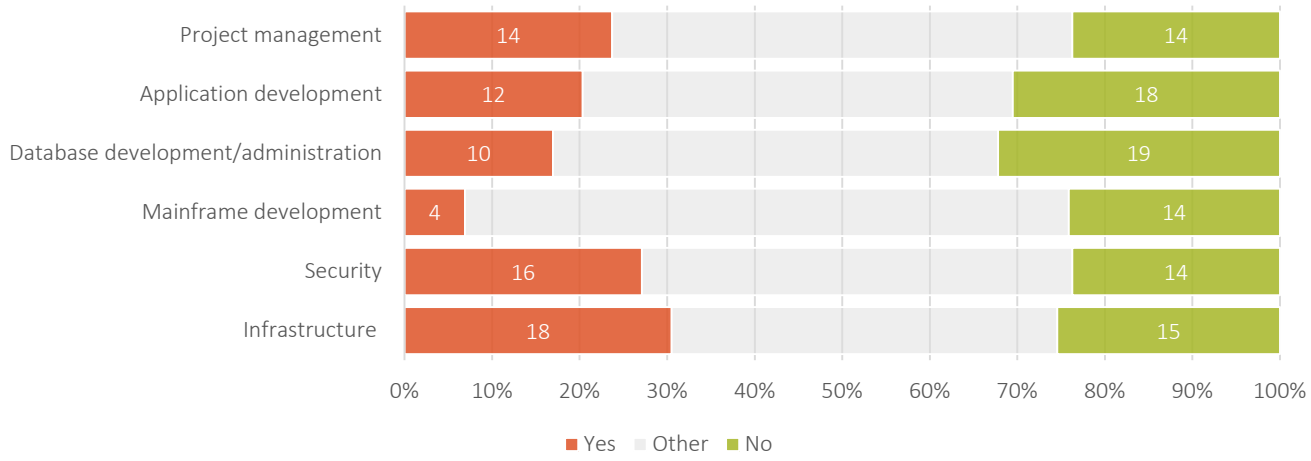
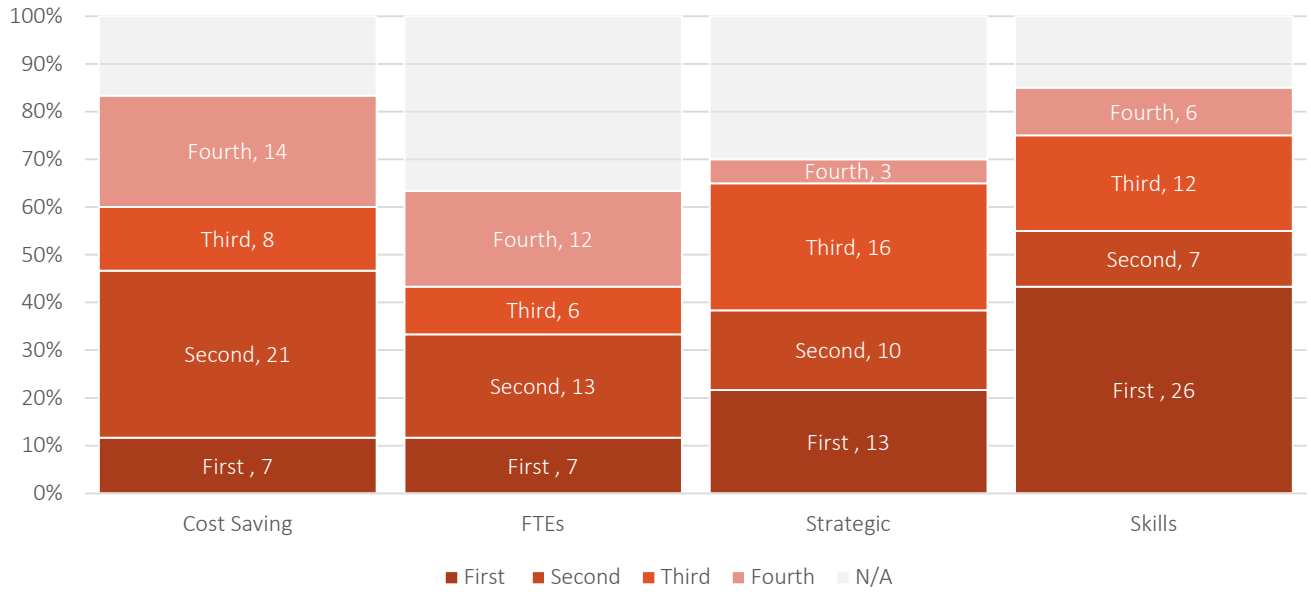


Fig. 5 – IT skill gaps by functional area



In addition to asking agencies about their internal IT staff, the survey also asked agencies to force-rank their reasons for outsourcing IT service. The four reasons included: cost savings, insufficient position authority (*i.e.,* full time equivalent positions (FTE)), strategic considerations and skills gaps. In most cases, agencies identified a lack of in-house skills as the most frequent and important reason for outsourcing IT services. Interestingly, while cost savings ranked second in overall responses, it was seldom ranked as the most important reason—typically, it was ranked second.

Fig. 6 – reasons for outsourcing IT services by priority



IT Infrastructure

In attempting to determine the overall IT infrastructure footprint for the state of Oregon, the survey sought information regarding the number of non-ETS data centers in use by agencies, the total number of installed servers supported within their agency and the square footage consumed by these agency-based infrastructure activities. The term "data center" was broadly defined, using the same definition as was used in the 2012 Hackett Report.[1] Of the 59 respondents, 42 had at least one or more data centers. There was a total of 106 separate data centers (an average of 2.36 per agency), though the Oregon Youth Authority and Department of corrections skewed the average with 35 and 17 data centers respectively. The majority of respondents (32) had only one data center.

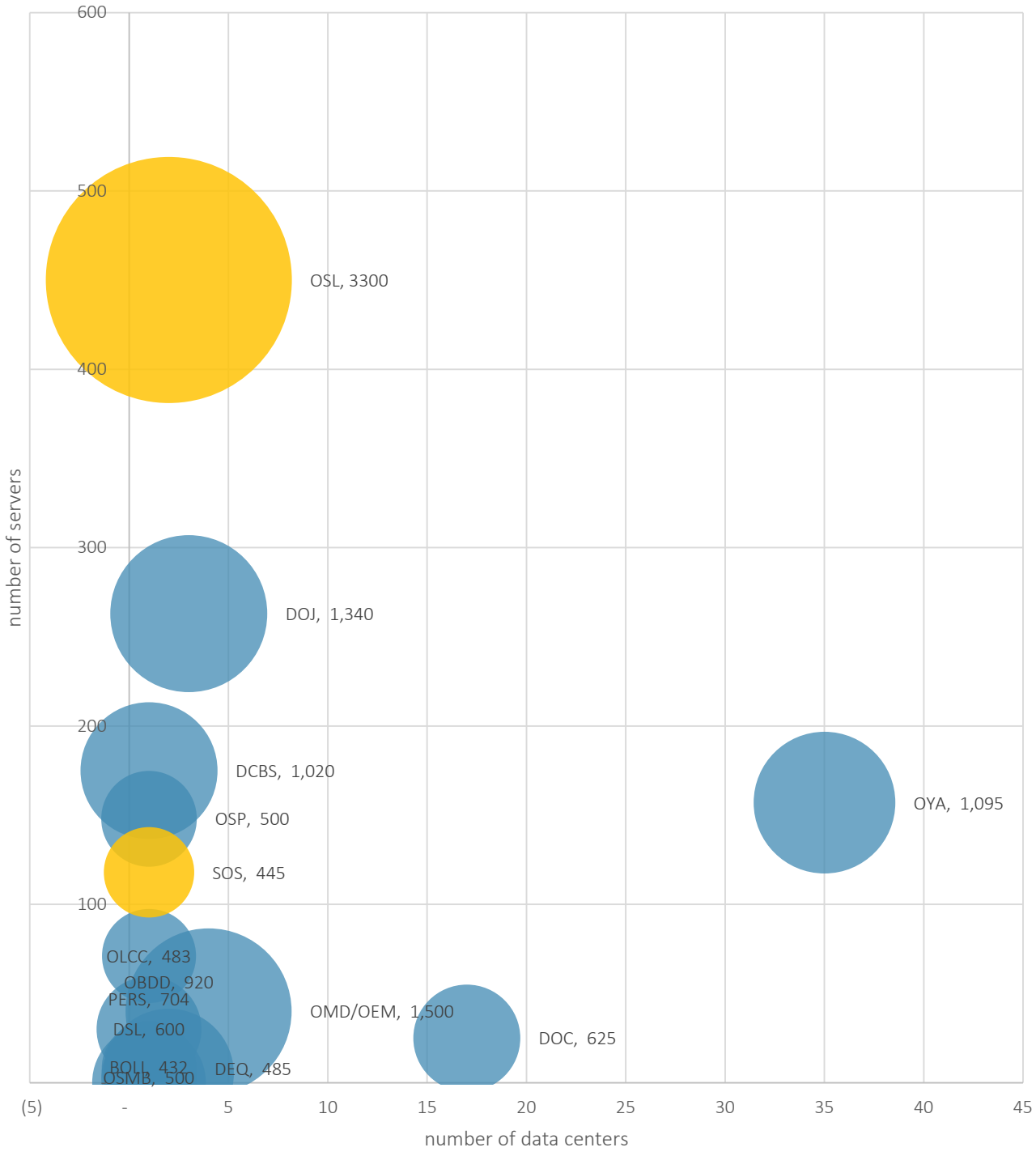
In terms of servers, there were a total of 2,204 individual servers being supported within agencies—an average of 45.4 per agency. In this case, the Oregon State Lottery had the most significant infrastructure footprint with 450 individual servers—they were followed by the Department of Justice (263 servers), the Department of Business and Consumer Services (175 servers), the Oregon Youth Authority (157 servers) and the Oregon State Police (148 servers).

As for the number of square footage consumed by data-center operations, the figures largely align with the server totals. Overall, there were 18,008 square feet being consumed by data-center operations with an average of 353 square feet per agency. Again, the Oregon State Lottery predominates with 3,300 square feet being consumed by data center operations. One observation regarding data-center operations, is the extent to which public safety agencies loom large in terms of IT infrastructure. Five public safety agencies were among the top 10 agencies in terms of space dedicated to data center operations, including: the Office of Emergency Management/Oregon Military Department (1,500 ft^2), the Department of Justice (1,340 ft^2), the Oregon Youth Authority (1,095 ft^2), Department of Correction (625 ft^2) and Oregon State Police (500 ft^2).

The chart on the following page summarizes the infrastructure footprint for the top 15 agencies based on square footage. The x-axis covers the number of data centers, the y-axis provides the number of servers and the area of the bubbles corresponds to the square footage.

[1] *"Data Center" – a facility, which may be a room in a building or an entire building, that is specifically configured to support and house hardware. In the past, data centers have frequently been associated with mainframe computers, where the mainframe is housed in a data center for protection and extra electricity and air-conditioning that is needed. However, communication equipment and file servers are also frequently kept in a data center to protect them. For example, if the facility is used to house agency applications, count it as a data center.*

Fig. 7 – IT infrastructure footprints (top 15)

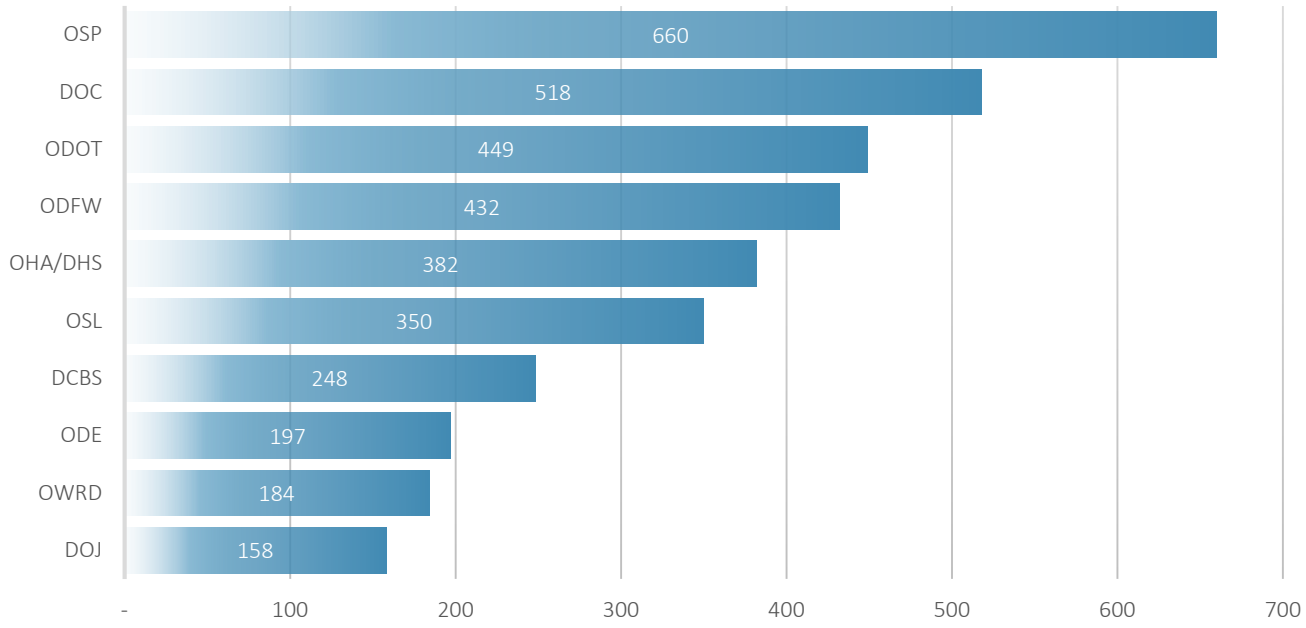


Application Portfolios

To assess the statewide application portfolio, the survey asked a variety of questions regarding the number of unique applications supported within agencies, the types of applications being supported and the primary database platforms in use. In terms of individual-agency application portfolios, the gross number of unique applications being supported was 4,762 with an average of 82.1 per agency. However, this number likely includes a great deal of duplication. Unfortunately, due to the heterogeneous nature of the responses given to the follow-up questions regarding the names of discrete applications, it is not possible to eliminate duplicate entries and develop a cross-agency portfolio view. Similarly, with its emphasis on hardware and peripherals, reporting from the IT Asset Management policy and procedures provide limited insight into the statewide application portfolio. Based on the 2012 Hackett Report, the number of unique applications is likely somewhere between 2,000 and 2,500—still a substantial number that drives increased costs through complexity.

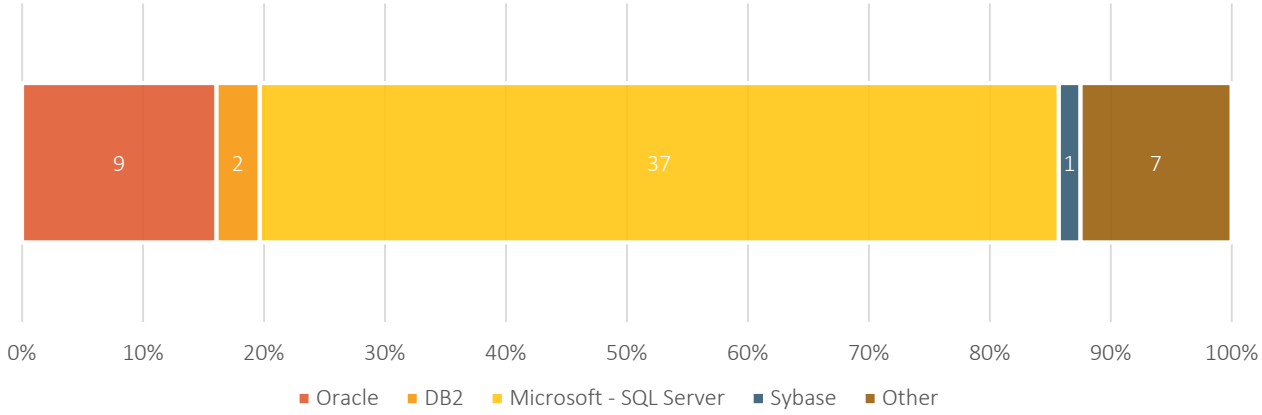
Among the top ten agencies, in terms of application portfolio size, the number of applications ranged between 158 and 660. The agency with the most reported unique applications was the Oregon State Police (660) followed by the Department of Corrections (518) and Department of Transportation (449).

Fig. 8 – application portfolios (top 10)



Turning to the database platforms, Microsoft SQL server represents the predominant database platform with 37 respondents identifying it as their primary database platform. The second most predominant platform was Oracle with 8 respondents identifying it as their primary platform.

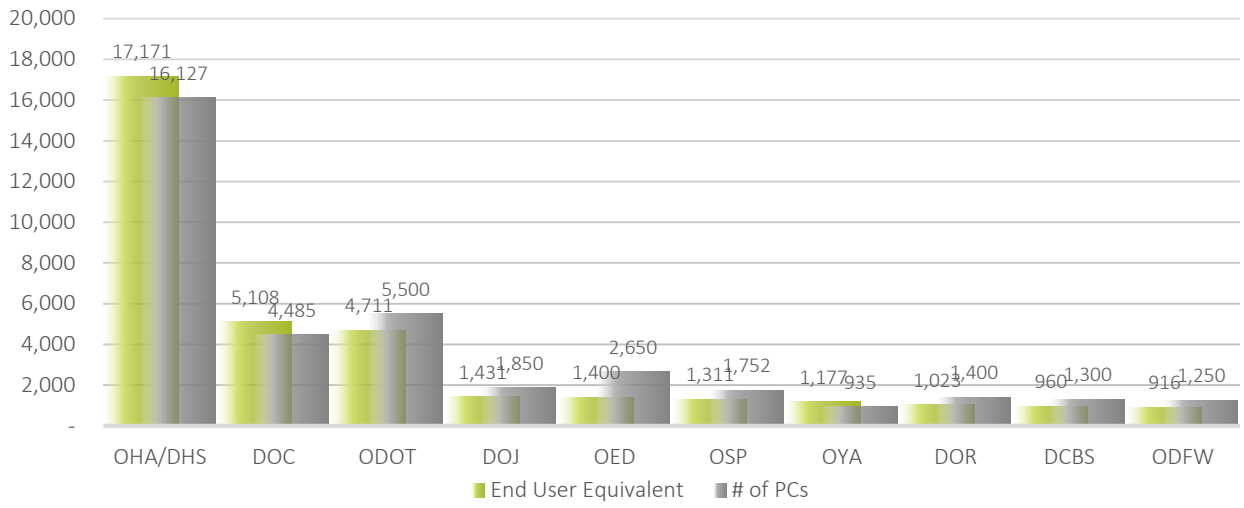
Fig. 9 – primary database platforms by agency



IT Operations

In evaluating IT operations, the survey asked questions regarding the current IT support model, programming language and cloud services deployment. In total, state agencies support 42,223.5 end-user-equivalents (EUE), with an average of 754 EUEs per agency. The EUE definition was taken from the 2012 Hackett Report and is intended to account for part-time and seasonal workers.[2] Increasingly, there is no longer a one-to-one correspondence between the number of employees and devices deployed within an agency. In some cases, an individual may have multiple devices, whereas in other cases, multiple individuals may share a device at a common workstation. The total number of devices supported exceeded the number of EUEs by nearly 4,000 at 45,997 total devices for an average of 793.05 per agency. The chart below summarizes the support model for the top 10 agencies in terms of EUEs.

Fig. 10 – IT operations and support



[2] ***"IT End User"*** *– An individual (typically either an employee or contractor) that spends at least 10% of his or her time using a business provided, funded, supported computing device that is part of an agency's IT infrastructure (i.e. desktops, laptops, hand held devices, etc.) to support his or her business function. The user must have direct access to internal applications / systems to execute specific transactions on behalf of the organization. The end user count does NOT include users of manufacturing process control or shop floor control systems. The end user count does NOT include users of CAD / CAM systems. The end user count does NOT include "casual" users of voice response systems, cell phones, and pagers. The end user count MAY include "OTHER" users that are not employees or contractors (i.e. agents / brokers / dealers / distributors, supply chain partners), but ONLY if they are using a computing device provided, funded, and supported by the business at least 10% of their time, and use enterprise applications / systems to execute specific business transactions. Only count end users once even if each end user has multiple devices. Shared devices used in multiple labor shifts or for groups of people should be counted as a single end user per shift. Do not count each user separately since the device is shared. Network printers should NOT be counted as a workstation. Example: There are 4 nurses using one PC at a nurse's station in a hospital. You would count this as 1 end user, NOT 4. If this scenario occurs across shifts, you should count this as 3 end users, NOT 12. POS workstations and kiosks may be counted as a single end user if the workstation or kiosk is in use at least 10% of the time. Do not separately count each user of the workstation or kiosk.*

Turning to cloud services deployment, the majority of respondents had either partially migrated to the cloud (24) or we're actively evaluating cloud services (21). The remaining agencies were either early adopters or not actively evaluating cloud services, including: 5 agencies who were already highly invested in the cloud. In terms of specific cloud offerings, email and collaboration were most popular, followed by disaster recovery and office productivity software (*e.g.*, Office 365). With the multi-state multiple award cloud services procurement from the National Association of State Procurement Officers (NASPO) ValuePoint program, we are likely to see a major increase in the number of cloud service deployments within the next year. Furthermore, ETS is currently evaluating a full transition to Office 365—thereby retiring the on-premises Enterprise Email offering and moving approximately 20 agencies into the cloud.

Fig. 10 – current status of cloud migration

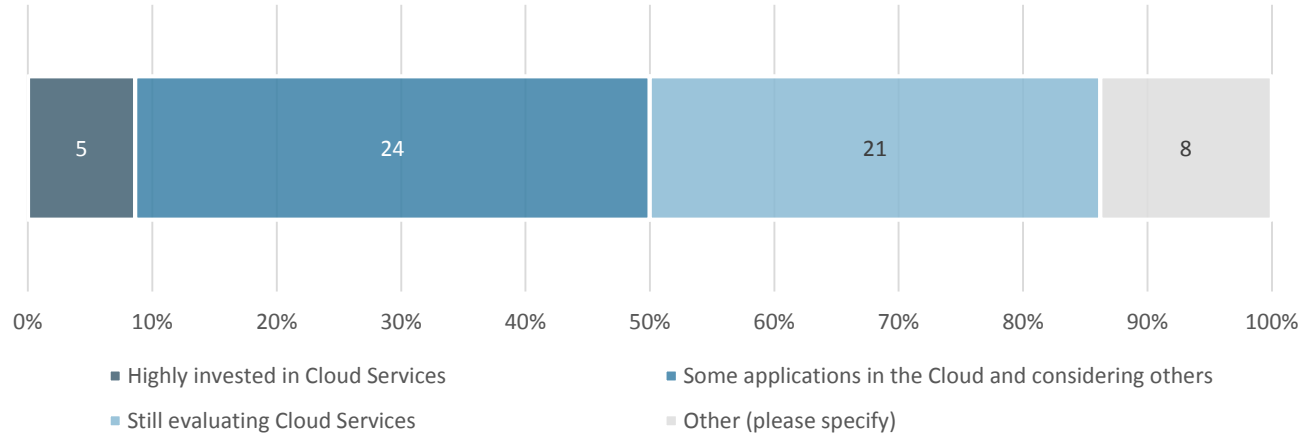
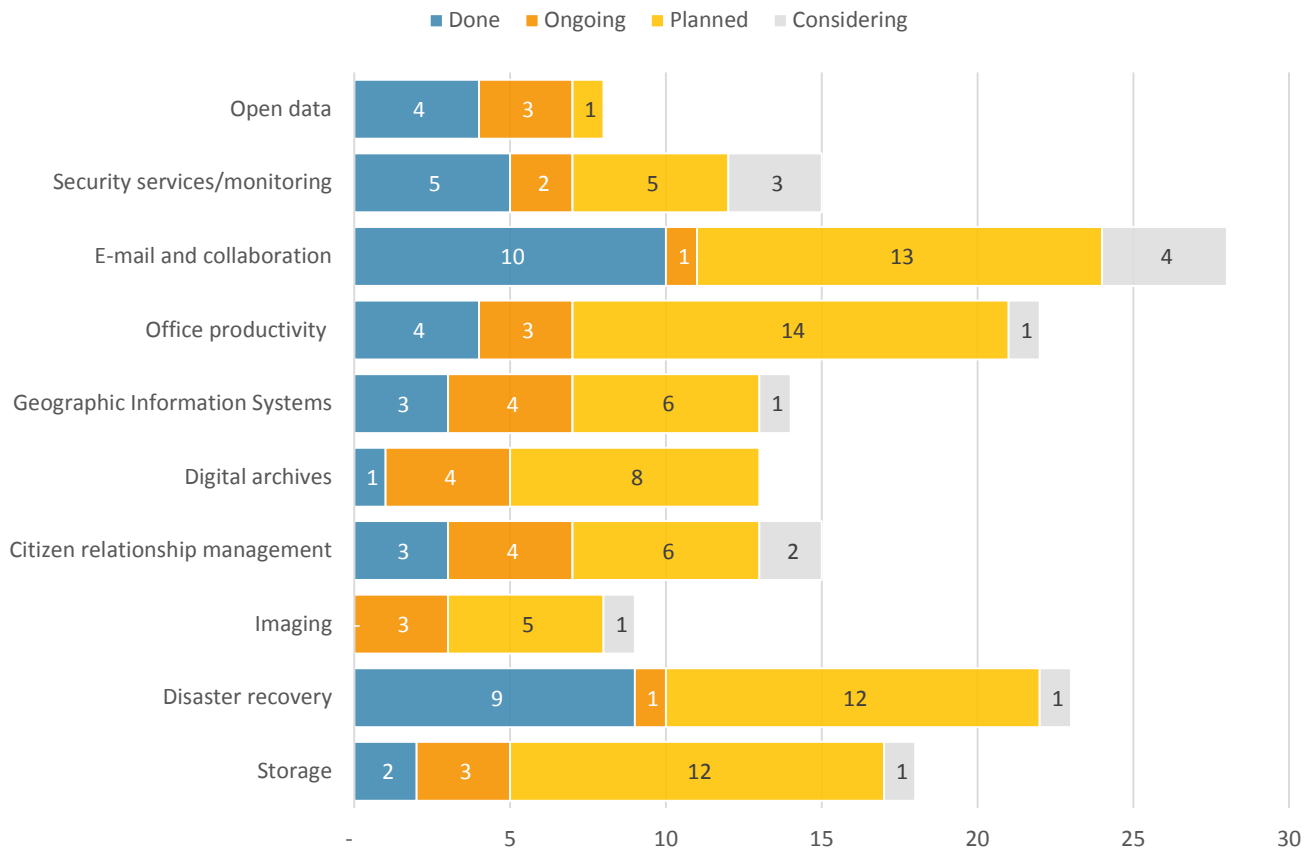


Fig. 11 – number of agencies leveraging specific cloud solutions



Telecom & Network Expenses

Turning to telecommunications and network expenses, the state of Oregon paid an estimated $26.9 million last year for the Executive Branch and responding agencies alone. According to the survey responses, the state paid nearly $8.5 million for voice services, $8.1 million for wireless, $8.9 million for data network charges and $1.4 million in equipment. While figures for the remainder of the state may be estimated using specific account numbers within the budgeting system, these do not provide disaggregated figures for the categories reported above—particularly, for the breakdown of wireless and voice. That said, looking at the telecommunications spending for the top 10 reporting agencies is instructive. There is substantial variance between each of these agencies, in terms of the proportion of expenses allocated to each category. Additionally, it is important to note that these figures exclude the one-time implementation costs associated with project MUSIC (mobilizing unified systems for integrated communications).

Fig. 12 – aggregate telecom and network expenses (reported)

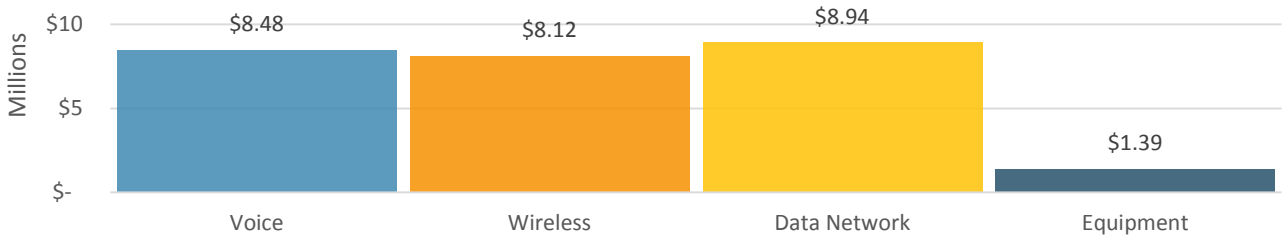
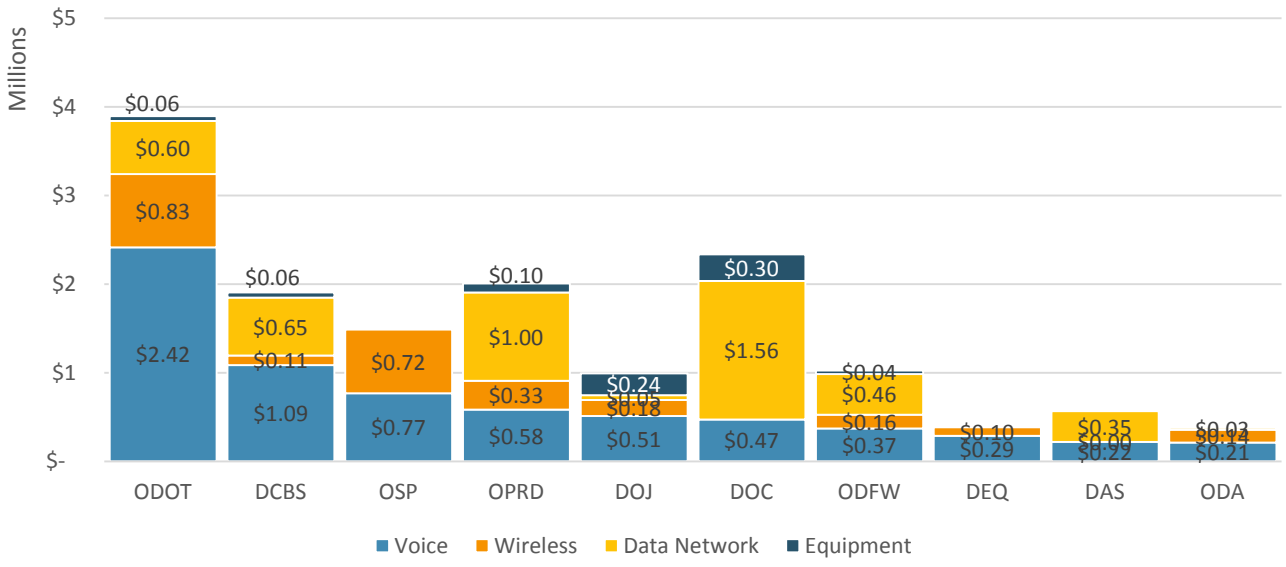


Fig. 13 – telecom and network expenses (top 10)



IT Security

With respect to IT security, the survey indicates that role-based security is implemented to a high- or medium-degree within most agencies. Additionally, the survey indicates that few agencies have experienced breaches. As for the impact of these events on daily operations, the majority of agencies reported no impact or minimal impact. Unfortunately, these findings reflect the limitations of both self-reporting and the survey questions employed—these findings provide little insight into the overall security posture or risk profile of any one agency. Furthermore, in the absence of a common framework such as the NIST Cybersecurity Framework, there is no way to identify the presence of absence of specific controls or standards. Fortunately, the release of the statewide security audit by the Secretary of State and the implementation of the statewide agency-by-agency risk-based security audit being undertaken pursuant to Executive Order 16-13, "Unifying Cyber Security in Oregon" will provide actionable insights into the security posture of the state as a whole. With that said, the survey findings were as follows.

Fig. 14 – implementation of role-based security

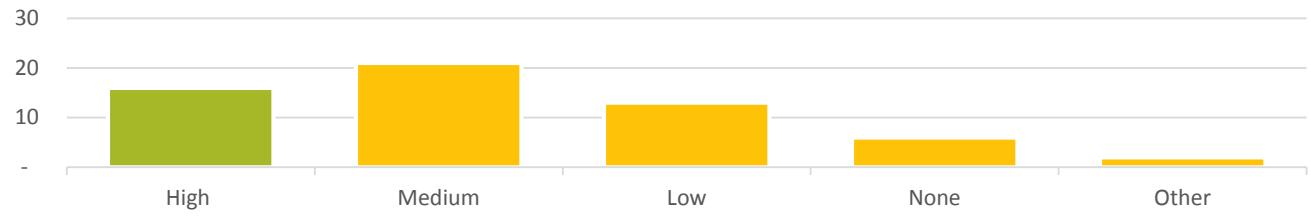


Fig. 15 – IT security incidents

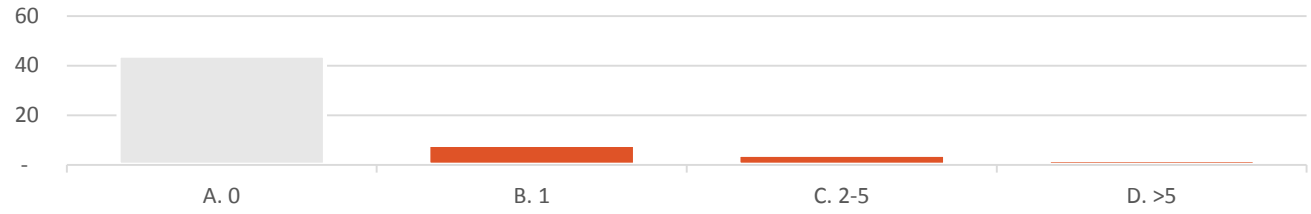
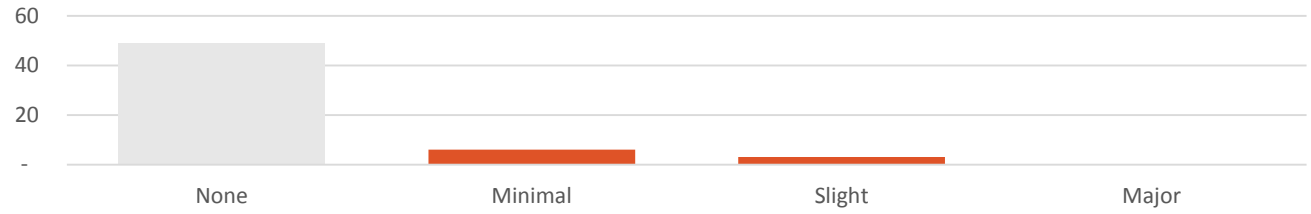


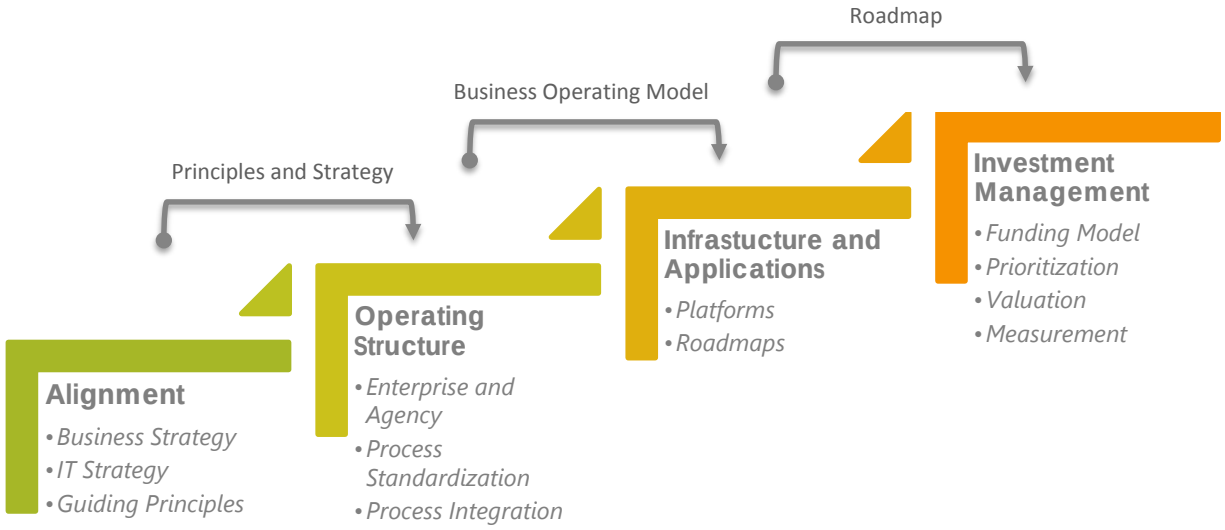
Fig. 16 – impact of IT security incidents



IT Strategy, Project and Portfolio Management

The following questions attempted to assess the relative maturity of IT strategy development and project and portfolio management—to put it another way, is IT working on the right things and delivering value? In its 2015 report, "*Is State IT Working on the Right Things?,"* NASCIO found that many states cannot afford to maintain their current portfolio of IT services, that past investments have resulted in unnecessary complexity, and that there is continuing misalignment between business strategy and IT decision-making. The report identified four components of effective IT decision-making, including: alignment, operating structure, infrastructure and applications, and investment management (the NASCIO model, is summarized below).

*Fig. 17. **NASCIO.** Components for effective IT decision-making*



IT STRATEGY + ALIGNMENT

With respect to IT strategy or "alignment," agencies reported a high-degree of formal alignment between the business of state government and the development of IT capabilities, with around 85% of agency CIOs, reporting that their IT strategic plans we're formally endorsed by agency leadership and nearly 70% reporting close alignment between their IT strategy and agency business plans. That said, only about a third of agencies have implemented a formal and structured process for IT strategy development. Additionally, in most cases, IT strategies are only updated upon request. Furthermore, just under 60% of agencies report that agency leadership is "always" or "often" engaged during the development of their IT strategic plans. Lastly, agencies report only a moderate degree of stakeholder engagement regarding the development of their IT strategic plans—only about 25% reported a high degree of stakeholder engagement.

Fig. 17 – IT strategy development maturity

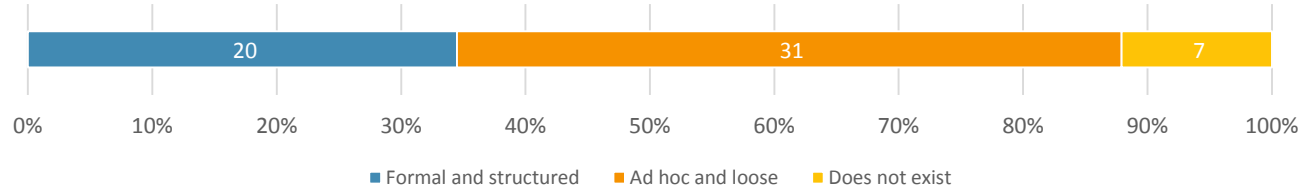


Fig. 18 – frequency of IT strategy updates

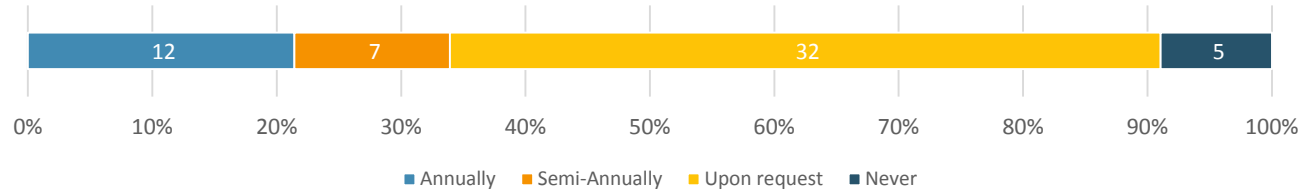


Fig. 19 – frequency of executive engagement on IT strategy

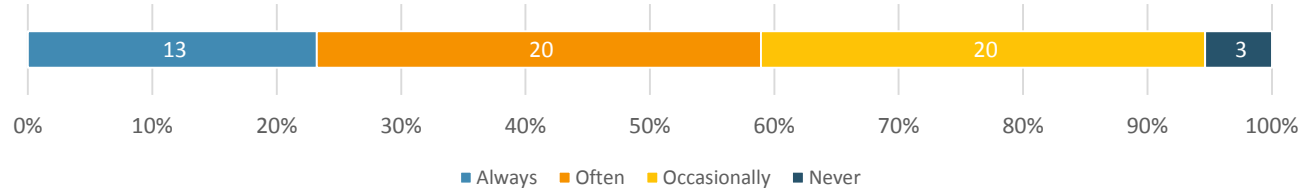


Fig. 20 – criticality of IT to agency business functions

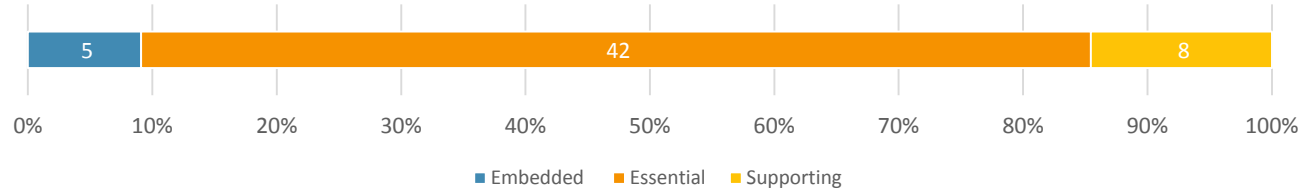


Fig. 21 – formal executive support for IT strategy

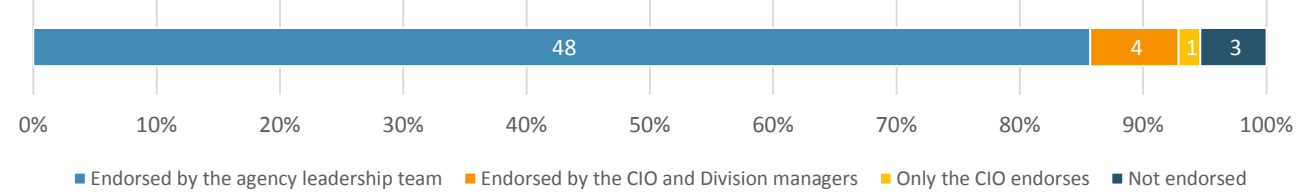


Fig. 22 – degree of alignment between agency strategic plan and IT strategy

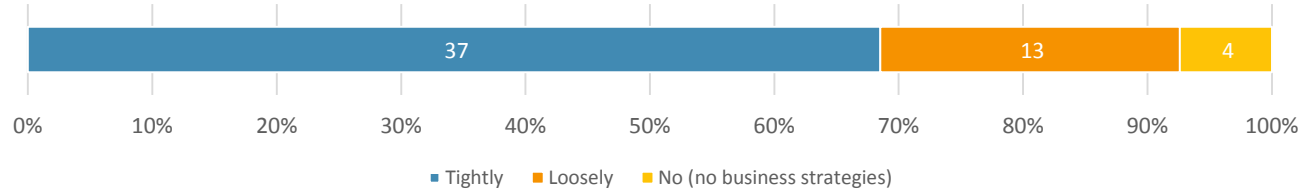


Fig. 23 – extent to which IT strategy supports internal agency, cross-agency and external functions (insularity)

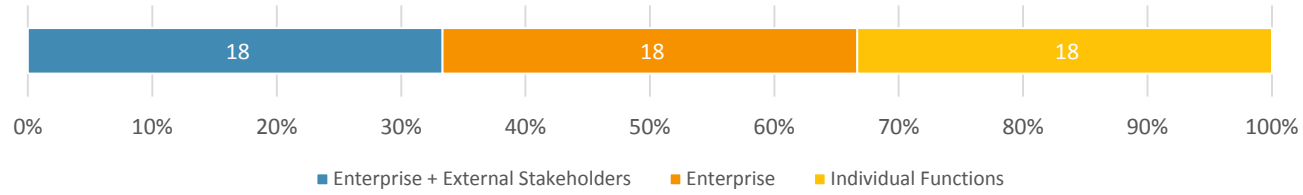
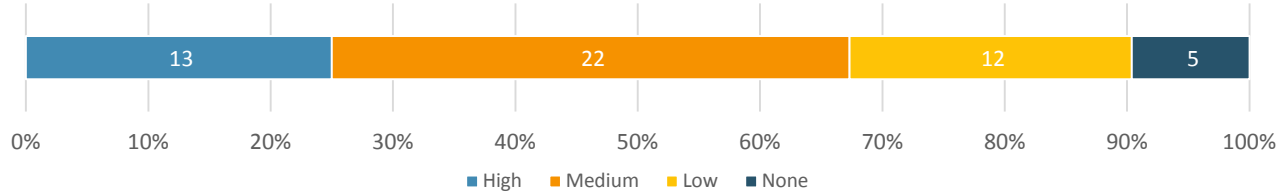


Fig. 24 – stakeholder engagement in IT strategy development



PROJECT AND PORTFOLIO MANAGEMENT

Turning to project and portfolio management and value delivery, these questions are primarily focused on three key metrics—on-time project delivery, budget variance and the degree to which the IT projects achieve required specifications. For reporting agencies, the unweighted average for project reporting metrics were as follows: 74% of all IT projects were delivered on time; 89% were delivered on-budget; and 89% were delivered according to specification. Of course, these unweighted averages fail to account for the number of projects undertaken or the number that were closed during the reporting period, the size of the agency (*e.g.,* number of FTE or budget size) or the risk or complexity associated with a particular project (*e.g.,* cost, number of agency interfaces, associated shadow systems or the number of unique function points).

The historical absence of a common methodology and system of record have undermined the transparency of project reporting metrics. Furthermore, only 25% of agencies report a "high" degree of post-project validation of project metrics. Absent post-project validation of the schedule, budget and specification variance, the reporting metrics have limited value.

Going forward, the Enterprise Project and Portfolio system will provide a system of record and consistent project metrics and baselines—albeit, only for IT projects exceeding $1 million or those that have been required to comply with Stage Gate review. Ultimately, our Office hopes to mature project and portfolio management practices within agencies as part of their internal governance and as part of the oversight model.

Fig. 25 – project reporting metrics (average)

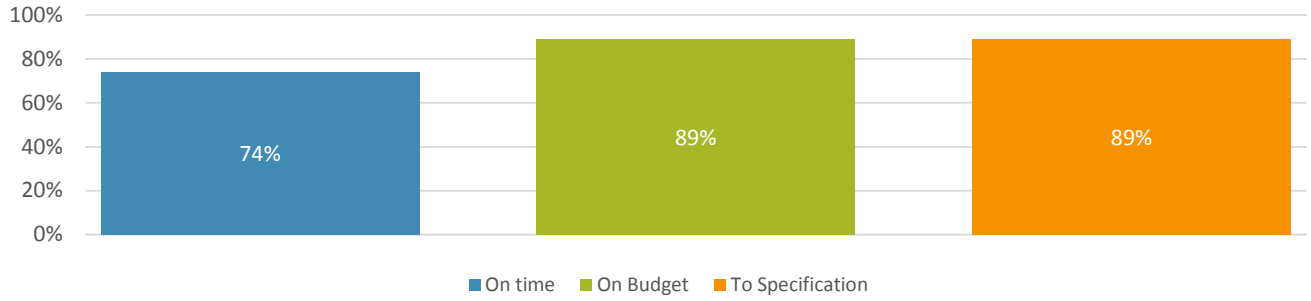


Fig. 25 –metrics by reporting agency for projects completed in the last year

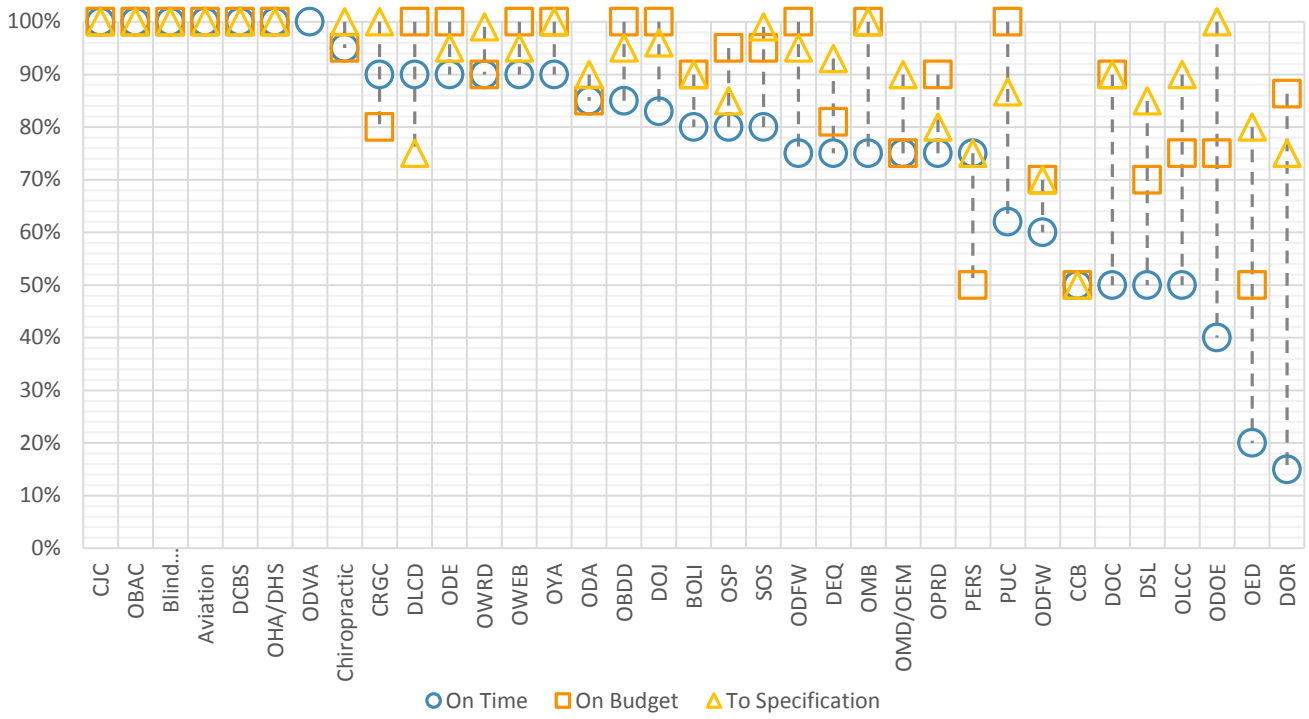
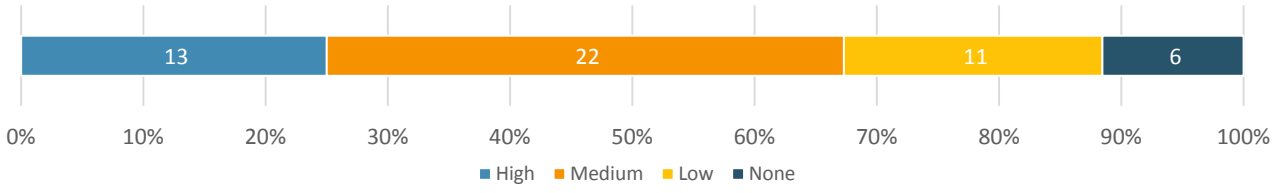


Fig. 26 – post-project validation of metrics (time, budget and specification)



OSCIO Policy Compliance

The OSCIO policy compliance section of the IT survey asked questions regarding three policies, including: business continuity planning, IT asset management and the portable device policy. As previously discussed, the survey provided little insight into IT security operations. The IT security policies that are currently in place are in effect "policies on policy"—they provide little insight into the risk posture of individual agencies or provide a comprehensive framework for managing enterprise IT security functions. Following the implementation of the statewide agency-by-agency risk-based security audit being undertaken pursuant to Executive Order 16-13, "Unifying Cyber Security in Oregon," our Office anticipates a re-write of existing IT security policies and will also seek to define the elements that will constitute the service catalog for the Enterprise Security Office going forward.

BUSINESS CONTINUITY PLANNING

Business continuity planning (BCP) entails the development of contingency plans in the case of a major event that impacts and agency's ability to deliver core services—it is critical for resilience planning and ensuring delivery of citizen services when they are needed most. Beyond the backing up of key systems and data, it requires a deep understanding of an agency's various system, their interdependencies, and requires systematic prioritization of key functions and the systems that support them.

According to the survey, when it comes to BCP, more than 30% of agencies have no or little BCP documentation. Of the remaining two-thirds, a slight majority have completed "medium" amount of documentation with just under 30% having completed a "high" amount of BCP documentation. When it comes to testing BCP protocols or updating existing documentation, 22 agencies have never tested their BCP protocols and 18 agencies have not completed a test in more than 24 months. While agencies report updating their BCP documentation more often than they test them, these figures are only marginally better with 19 agencies reporting that they have not updated their BCP documentation in more than 24 months. As for the results of recent BCP tests, only one agency indicated that they successfully tested their protocols without problems. In several cases, the test could not be completed.

Turning to the use of backup sites, nearly 60% of agencies are using a backup site. However, in the absence of BCP documentation there is no guarantee that an agency will be able to restore systems or recover their work.

Fig. 27 – documentation of business continuity planning (BCP)

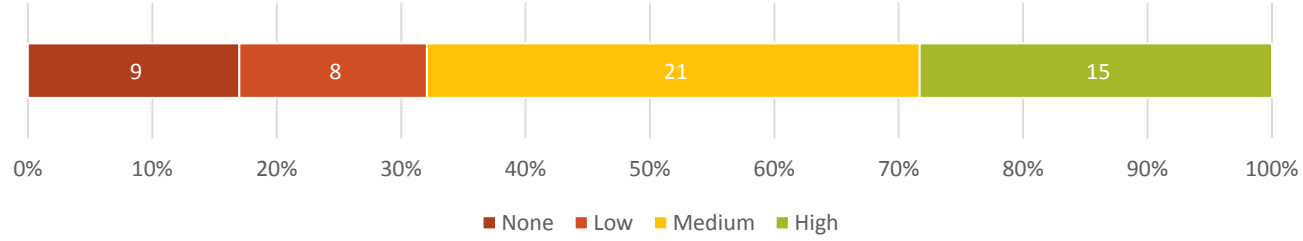


Fig. 28 – frequency of BCP testing and updates

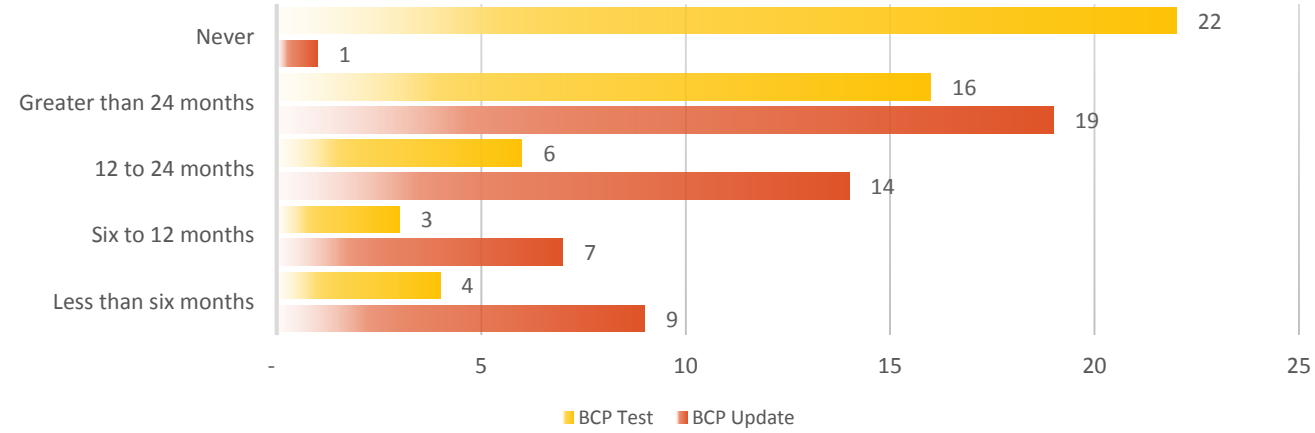


Fig. 29 – results of recent BCP tests

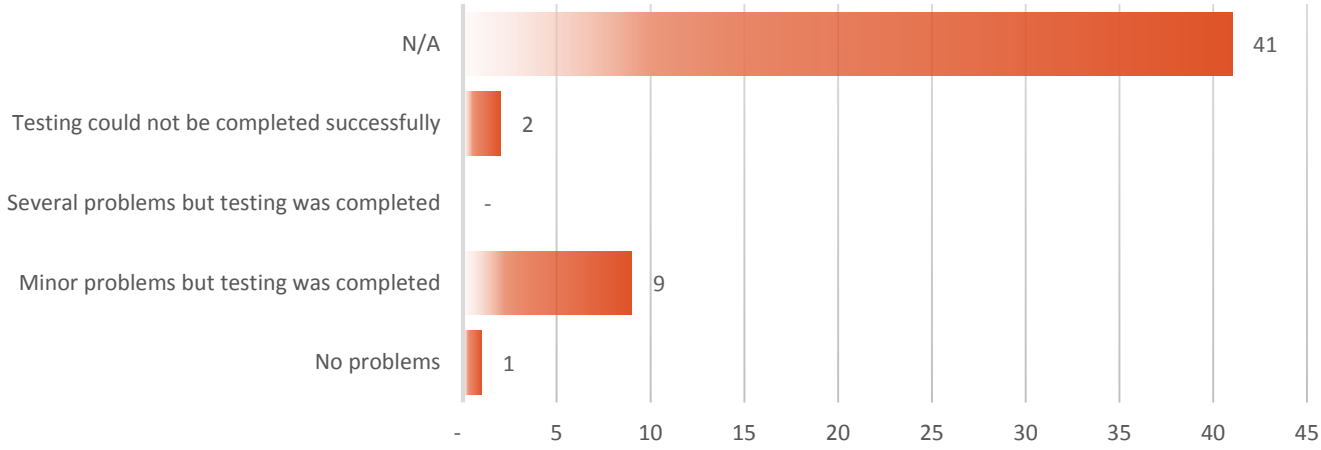
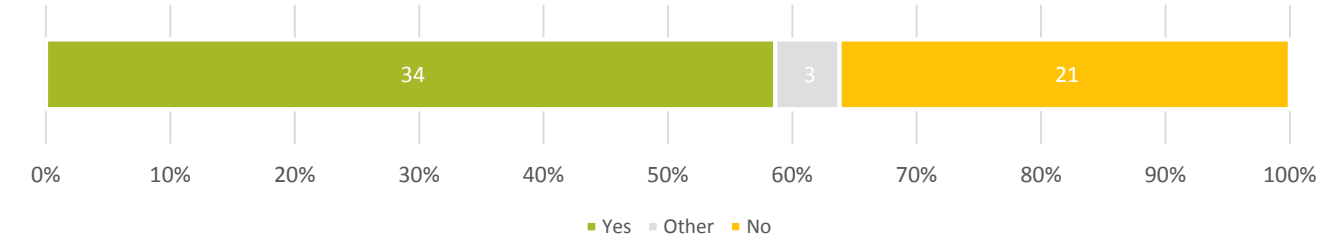


Fig. 30 – use of a backup site



IT ASSET MANAGEMENT (ITAM)

The basic premise of IT asset management is that it is difficult, if not impossible, to optimize IT investments without understanding your current inventory and distribution of assets. A comprehensive ITAM program should provide insight into the distribution of IT spending by category and individual component type in real-time, enabling more efficient purchasing and optimization of existing assets and licenses—applying equally across hardware, software and services. Furthermore, such a program and the tools it relies on would enable the determination of the costs associated with operations and maintenance for a particular system or application.

The current ITAM policy requires that agencies have a program in place, that they identify and ITAM coordinator and periodically submit a spreadsheet listing desktop components and peripherals, as well as the associated inventory tag numbers. Reporting on software and licensing is not currently required.

Our Office is currently conducting a pilot in software-asset-management (SAM) as a service, with an emphasis on license optimization—redeploying existing licenses that are underutilized and cancelling maintenance on applications that are only used on a limited basis. The pilot will cover all of the licenses deployed within the state data center and potentially one other agency. Additionally, the pilot has sought industry insight into best practices within IT asset management.

Ultimately, getting a handle on the state's asset and application portfolio, will enable the state of Oregon to protect itself from negative audit findings related to the unauthorized deployment of software licenses. Most recently, an audit by Microsoft identified several million dollars' worth of unauthorized SQL Server installed throughout the state. While centralizing purchasing of these specific licenses at ETS will go a long way in mitigating this particular audit finding, use of a SAM as a service or an implementation of an enterprise IT Asset Management tool would enable our Office to better optimize our IT asset portfolio.

In terms of compliance with the current policy, nearly 70% of agencies report implementation of the program. Additionally, the majority of agencies report that they have updated their asset inventories in the last six months.

Fig. 31 – IT asset management (ITAM) program implementation

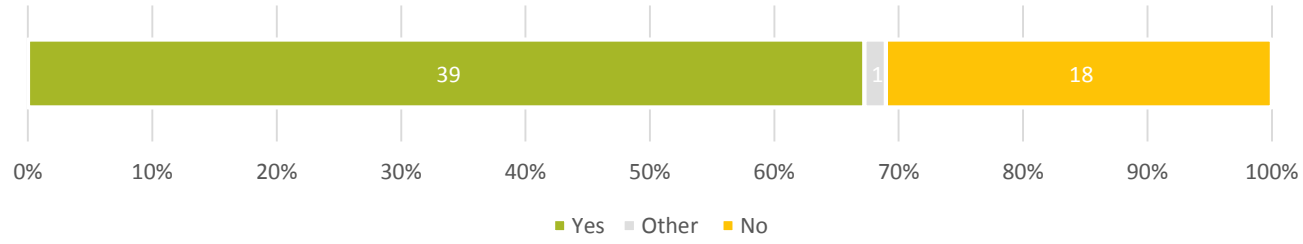
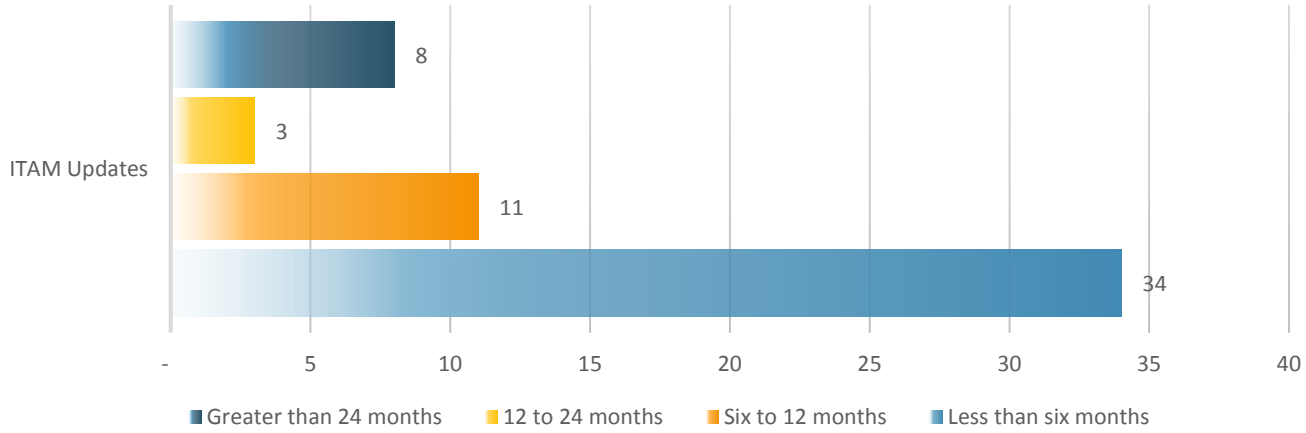


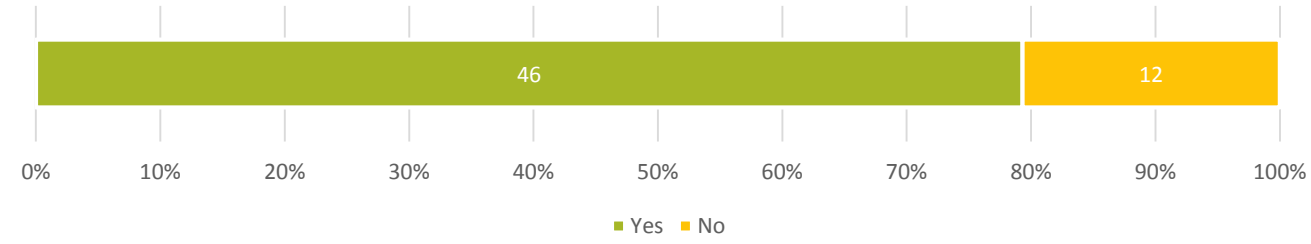
Fig. 32 – most recent ITAM update



PORTABLE DRIVES POLICY

The portable drives (*e.g.,* thumbdrives) policy requires agencies to have a policy in place to minimize the risks associated with portable drives. Based on the survey, nearly 80% of agencies are in compliance with the current policy.

Fig. 32 – portable drives policy



Appendix A. Survey Questions

1. Please identify your agency and primary contact.

2. What were you total IT Costs for the last fiscal year (including expense and depreciation)?

3. What percentage of your IT spending is represented by operations and maintenance?

4. Total Spending by Infrastructure Functional Area
    a. Mainframe
    b. Servers
    c. Storage
    d. Client and peripherals
    e. IT Helpdesk
    f. Data Networking
    g. Voice Telecom
    h. Security

5. What is the annual facilities and overhead costs (e.g., rent, building depreciation, utilities, etc.) for the IT processes provided by your agency?

6. What is your total IT staff?
    a. 1-10
    b. 11-25
    c. 26-50
    d. 51-100
    e. 101-300
    f. 301-500

7. What is your organization's IT staffing profile relative to the following IT staffing functions (number, proficiency, retirement eligibility and critical skills gaps)?

8. What is the appropriate answer for tenure, experience, and turnover for the following IT employees?

9. What is your IT spend per employee?
    a. Employees
    b. Contractor outsourced

10. What is the percentage of IT employees versus total employees within your organization

11. Ranks your agency's reasons for outsourcing technology?
    a. Cost savings
    b. FTEs reduced/re-deployed

c. Strategic or competitive advantage
d. Lack of in-house skills or capabilities
e. Other

12. How many data centers (internal hardware hosting facilities) are supported within your agency? (Reconciled) (Grid)

13. How many installed servers are supported within your agency?

14. How many square feet of floor space is consumed by data center operations within your agency?

15. How many unique applications does your agency support? (Note: Count Office Suite as one)

16. List the name of each unique application included in the number reported in the prior question.

17. What is your current email system and provider?

18. How many technology platforms does your group support? (Grid)
    a. Application Servers (Number)
    b. Integration Brokers (Number)
    c. Portals (Number)
    d. Workflow Engines (Number)
    e. Document/Content Management (Number)
    f. Business Intelligence / Data Warehousing Platforms (Number)
    g. Data Management Tools (Number)
    h. # of which are OpenSource (Number)

19. How many different database platforms are being utilized by the entire organization?

20. Which database platform is your primary?
    a. Oracle
    b. DB2
    c. Microsoft - SQL Server
    d. Sybase
    e. Other

21. How many end users do you currently support within your agency?

22. How many individual PCs are supported by your agency?

23. How many programming languages does your group utilize?

    Programming language refers to the coding language used to develop, enhance or execute a business application. The number of languages is counted based on unique language names only, and does not include

different versions of the same language. Examples of programming languages include COBOL, Fortran, Assembler, ABAP, RPG, C, Visual Basic, Java, etc.

24. What is your agency's status regarding the implementation of cloud services?
    a. Highly invested in Cloud Services
    b. Some applications in the Cloud and considering others
    c. Still evaluating Cloud Services
    d. Other

25. What categories of service have you migrated or plan to migrate to the cloud? (Done, Ongoing, Planned)
    a. Storage
    b. Disaster recovery
    c. Imaging
    d. Citizen relationship management
    e. Digital archives
    f. Geographic Information Systems
    g. Office productivity software (e.g., word processing)
    h. E-mail and collaboration
    i. Security services/monitoring
    j. Open data

26. What are the total current year telecom expenses?
    a. Voice usage charges (Currency)
    b. Wireless (data and voice) usage charges (Currency)
    c. Data network and usage charges (include VoIP) (Currency)
    d. Equipment cost (exclude capitalized expenses) (Currency)

27. To what degree is role based security implemented throughout the enterprise?
    a. None
    b. Low
    c. Medium
    d. High

28. How many security breaches were detected for any unauthorized/improper access during the benchmark period?
    a. 0
    b. 1
    c. 2-5
    d. >5

29. What impact did security breaches have on the daily operations?
    a. None
    b. Minimal
    c. Slight

d. Major

30. To what degree does an IT strategy exist within your agency?
    a. Formal and structured
    b. Ad hoc and loose
    c. Does not exist

31. How often is your IT strategy updated?
    a. Semi-Annually
    b. Annually
    c. Upon request
    d. Never

32. How often is IT leadership engaged in agency strategy discussions and decisions?
    a. Never
    b. Occasionally
    c. Often
    d. Always

33. How critical is IT to the execution of the agency's business strategy?
    a. Embedded - IT related products and services are our business
    b. Essential - IT capabilities are critical systems essential to our business
    c. Supporting - IT is primarily back office support to our core business

34. Is the IT Strategy endorsed by senior agency leadership team?
    a. Not endorsed
    b. Only the CIO endorses
    c. Endorsed by the CIO and Division managers
    d. Endorsed by the agency leadership team

35. Is the IT Strategy built upon / aligned with defined agency strategic priorities?
    a. No (no business strategies)
    b. Loosely
    c. Tightly

36. Is the IT Strategy holistic and integrated?
    a. Individual Functions
    b. Enterprise
    c. Enterprise + External Stakeholders

37. To what degree are program unit stakeholders actively involved in developing and updating the IT strategy?
    a. None
    b. Low
    c. Medium

d. High

38. Of the total IT projects completed, what percentage are completed on time, on budget, and to specifications?
    a. On time
    b. On Budget
    c. To specification

39. Upon completion, are projects/ programs reviewed to validate the original business case (both costs and benefits) and lessons learned fed back to improve methodologies and tools?
    a. None
    b. Low
    c. Medium
    d. High

40. To what extent is your Business Continuity plan formally documented?
    a. None
    b. Low
    c. Medium
    d. High

41. When was the last time the Business Continuity plan was updated?
    a. Less than six months
    b. Six to 12 months
    c. 12 to 24 months
    d. Greater than 24 months

42. When was the last time the Business Continuity plan was tested?
    a. Less than six months
    b. Six to 12 months
    c. 12 to 24 months
    d. Greater than 24 months

43. How successful was the most recent test of the Disaster Recovery plan?
    a. No problems
    b. Minor problems but testing was completed
    c. Several problems but testing was completed
    d. Testing could not be completed successfully

44. Do you have a backup site?
    a. Yes
    b. No

45. Do you have an IT Asset Management (ITAM) in place?
    a. Yes

b. No

46. Who is your ITAM Coordinator?

47. When was the last time your IT Asset Inventory was updated?
    a. Less than six months
    b. Six to 12 months
    c. 12 to 24 months

48. Do you have policies and procedures in place for controlling portable and removable storage devices, including: identifying what assets may or may not be stored on such devices and approved methods for securing that information?
    a. Yes
    b. No