
UNDERSTANDING THIS REPORT

The purpose of this quarterly update is to demonstrate the current and ongoing impact of the State of Oregon's unified cyber security approach. This report shows adoption of key risk-reducing services provided by Cyber Security Service (CSS) along with additional metrics associated with select services.

CSS is comprised of the following sections:

Security Operation Center (SOC) provides detection and response services, enterprise vulnerability management support and CIS Controls-based services supporting cyber hygiene.

Network Security (NETSEC) provides the core technical security infrastructure and related service offerings that agencies rely on to effectively support their mission. Network Security Services manage software, hardware, processes, and procedures to ensure all data and communications are appropriately secured for availability and access.

Governance Risk and Compliance (GRC) provides identity and protection security services that support the confidentiality, availability, and integrity of Information systems that allow agencies to meet their business missions while supporting the following security categories; Business Environment, Governance, Risk Assessment & Management Strategy, along with Awareness & Training, Data Security, and Information Protection Processes & Procedures.

Services provided by CSS are broken down into the following categories:

Security Operations Center (SOC)

- Monitoring and Detection Services
- Vulnerability Management Services
- Incident Response Services
- Additional SOC Services

Governance Risk and Compliance (GRC)

- Information Security Awareness & Training
- Cyber Security Risk Assessment
- Business Information Security

Network Security (NETSEC)

- Network Security - Firewall
- Network Security - Virtual Private Network
- Network Security - Web Applications Firewall

For a complete list of CSS Services, please refer to the CSS Services Catalog. For a more detailed description of services found in this report, please refer to Appendix A - *Service Descriptions* at the end of this document.

NOTE: The label of 'Agency' or 'Agencies' used throughout this document refers to the eighty (80) State Agencies, Boards and Commissions included in the EIS Policy areas. For a list of these agencies, boards and commissions, please refer to Appendix B at the end of this document. [Source: EIS Policy Areas and Agency Assignments]

METRICS REPORT CONTENT

The metrics area of this report is broken down by CSS Sections. For each CSS Section, the first two bar charts measure how well CSS is executing against the stated vision of providing a unified approach to cybersecurity. Both of these common two bar charts for each Section demonstrate “known” adoption of services documented in the CSS Service Catalog.

BAR CHART 1: ADOPTION OF SERVICES BY AGENCIES

Shows the percentage of adoption by all state agencies where **each agency is weighted equally** and is based on coverage for the stated service. For example, if 20 of the 80 agencies (regardless of agency size) adopted a service it will show as 25% adoption.

Coverage options include the following:

1. Agency is utilizing the CSS-provided service.
2. Agency is using their own equivalent of the CSS-provided service.
3. Agency is using a third-party equivalent of the CSS-provided service.
4. Agency has no known coverage related to the CSS-provided service.
5. Agency has documented no need for the equivalent of the CSS-provided service.

An example of #5 above might include scanning services for Internet-facing systems, when an Agency does not have any systems that are internet-facing.

For the initial iteration of this report, and to the best of its ability, CSS will document and report to each agency the CSS documented coverage for each service and request any needed clarifications.

BAR CHART 2: RISK REDUCTION IMPACT (NUMBER OF POSITIONS AFFECTED)

Shows the percentage of adoption by all state agencies where each agency is **weighted based on the number of positions in that agency** and is based on coverage for the stated service. For example, if the total number of positions for all 80 agencies was 40,000 and four (4) agencies adopted a service AND the total number of positions for those four agencies was 20,000, then the service will show as 50% adoption.

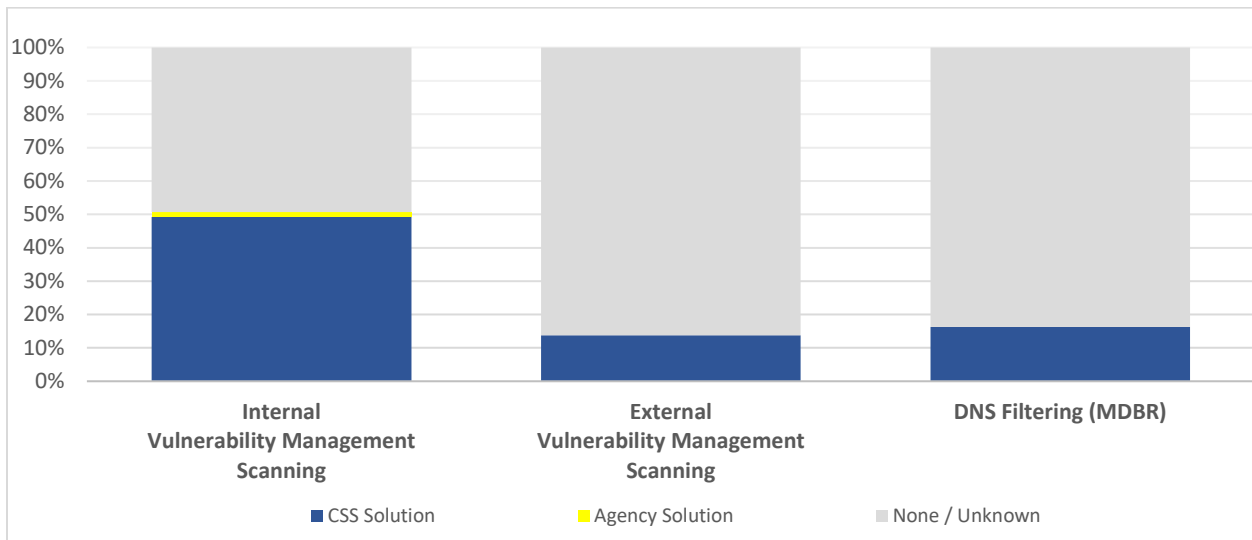
Coverage options are the same as Bar Chart 1 above.

SERVICE-SPECIFIC METRICS

This sub-section measures the operational effectiveness of a particular CSS service relative to specific execution goals. For example, these metrics might be used to show how service implementations are meeting service commitments and where improvements in efficiency, staffing levels or service scope may need to be adjusted. Other examples include tactical measurements of strategic significance in driving service-related risk reduction. Additional descriptions are included for each such metric in the body of the report.

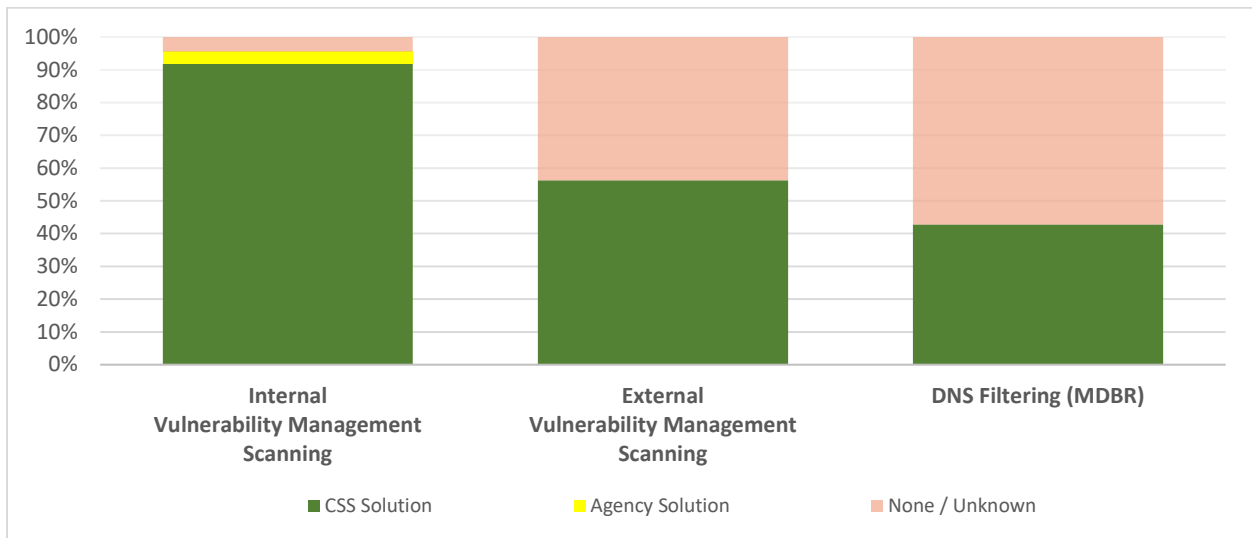
CSS SECTION: SECURITY OPERATIONS CENTER (SOC)

ADOPTION OF SERVICES BY AGENCIES



The above chart shows the percentage of adoption by all state agencies where **each agency is weighted equally** and is based on coverage for the stated service. For example, if 20 of the 80 agencies (regardless of agency size) adopted a service it will show as 25% adoption.

RISK REDUCTION IMPACT (PERCENTAGE OF TOTAL POSITIONS IN ALL AGENCIES)



The above chart shows the percentage of adoption by all state agencies where **each agency is weighted based on the number of positions in that agency** and is based on coverage for the stated service. For example, if the total number of positions for all 80 agencies was 40,000 positions, and four (4) agencies adopted a service AND the total number of positions for those four agencies was 20,000, then the service will show as 50% adoption.

SOC - SERVICE-SPECIFIC METRICS

The current service-specific metrics for the SOC are focused on agency preparation and effective interoperation between the CSS SOC and agency IT operations. The goal and associated timeline for each metric is included below.

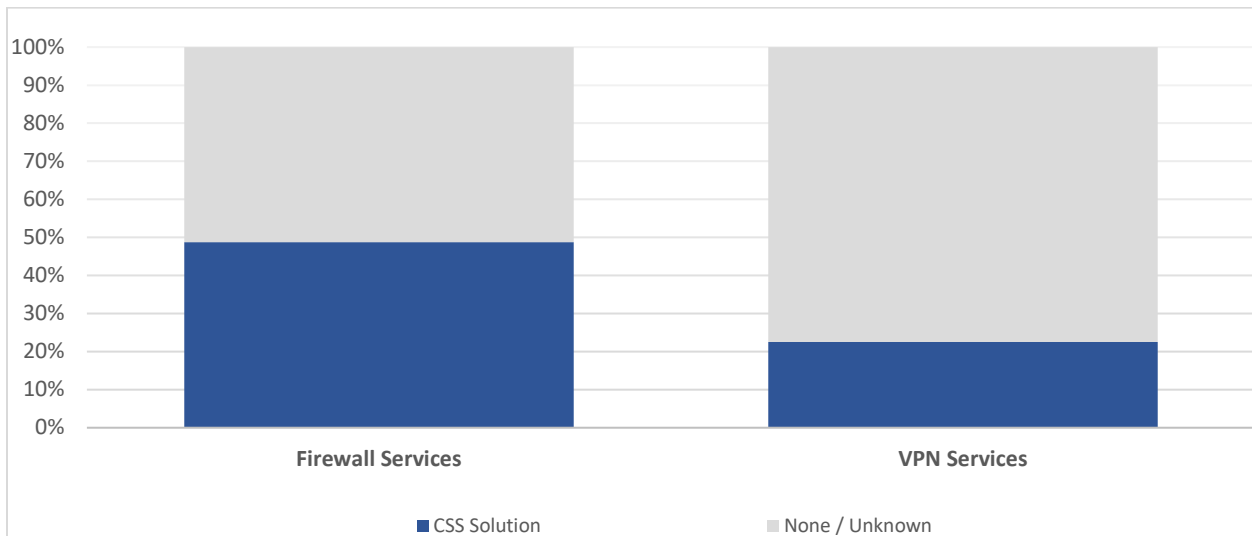
INCIDENT RESPONSE PREPAREDNESS

Rapid detection and response is the difference between an intrusion and a breach. The following metrics demonstrate agency preparedness with regards to their ability to receive and process threat intelligence, potential incidents and advisories. All of the following use the same methods of calculation as charts #1 (each agency is weighted equally) and #2 (weighted by positions).

Weighted (by positions)	Service-Specific Metric Description and Goal
Unweighted (Percentage of all Agencies)	
75.5%	Agency Point of Contact (POC) established with CSS SOC for communication of potential security incidents, security incidents, and cyber security advisories relating to current threats and vulnerabilities. Goal of 100% by September 2021.
51.3%	
51.6%	Agency has a published Incident Response Plan. Requirements: DAS Statewide Policy 107-004-52 [General Info (1)(b)] DAS Statewide Policy 107-004-120 [General Info (1)(b)] Statewide Information Security Plan (2018) – 16.1 2019 SW Standards - IR-8 - Incident Response Plan (a) Goal of 100% by December 2022.
18.8%	
1.4%	Agency has completed an Incident Response tabletop exercise within the past three years, or has one scheduled in the next 6 months, validating their published Incident Response Plan. Requirements: DAS Statewide Policy 107-004-52 [General Info (1)(b)] DAS Statewide Policy 107-004-120 [General Info (1)(b)] 2019 SW Standards - IR-3 - Incident Response Testing (a) Goal of 50% by December 2022.
2.5%	

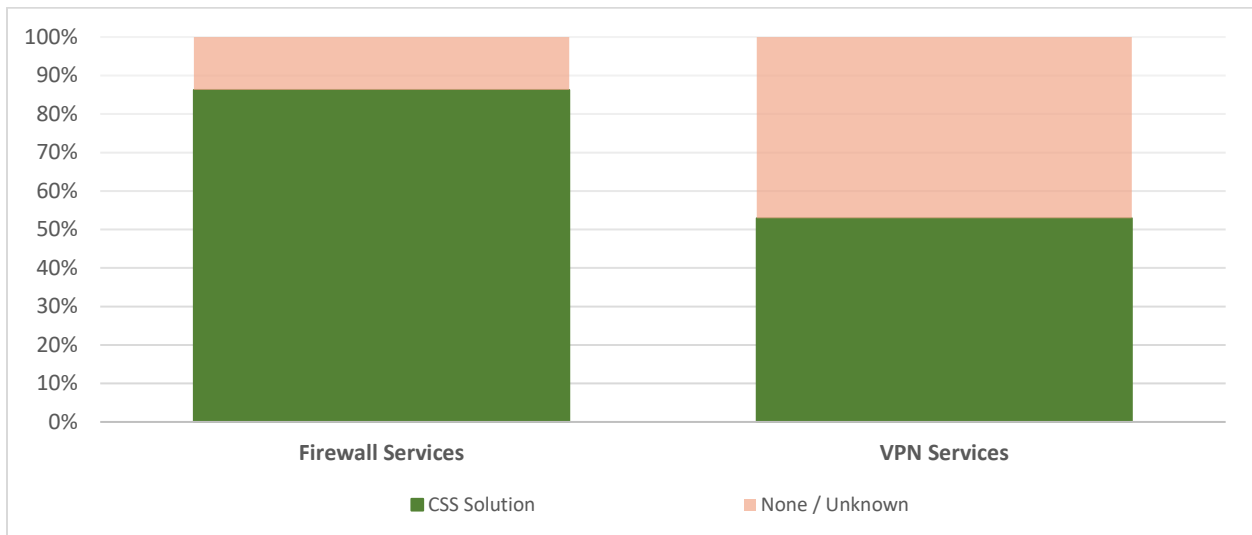
CSS SECTION: NETWORK SECURITY (NETSEC)

ADOPTION OF SERVICES BY AGENCIES



The above chart shows the percentage of adoption by all state agencies where *each agency is weighted equally* and is based on coverage for the stated service. For example, if 20 of the 80 agencies (regardless of agency size) adopted a service it will show as 25% adoption.

RISK REDUCTION IMPACT (PERCENTAGE OF TOTAL POSITIONS IN ALL AGENCIES)



The above chart shows the percentage of adoption by all state agencies where *each agency is weighted based on the number of positions in that agency* and is based on coverage for the stated service. For example, if the total number of positions for all 80 agencies was 40,000 positions, and four (4) agencies adopted a service AND the total number of positions for those four agencies was 20,000, then the service will show as 50% adoption.

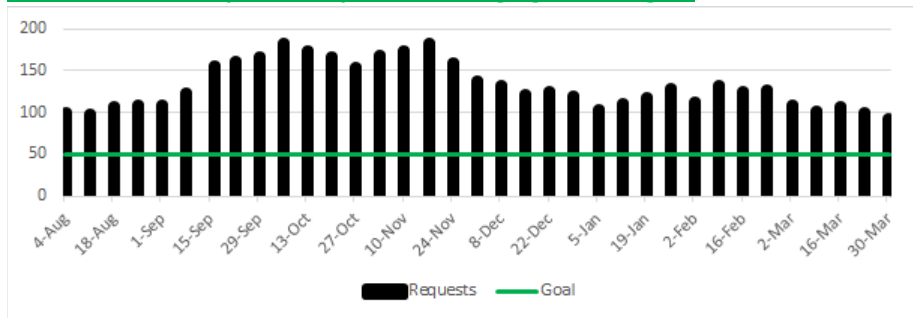
NETSEC - SERVICE-SPECIFIC METRICS

OPERATIONAL EFFECTIVENESS

Operational effectiveness measures specific execution goals for the network security team in meeting service commitments and efficiently deploying resources.

Effectively managing the ticket queue ensures customer requests are not unduly stalled and that the current active load on the team is managed to a level that allows them to maintain a highly responsive, high quality level of service.

Network security tickets queue backlog against targets

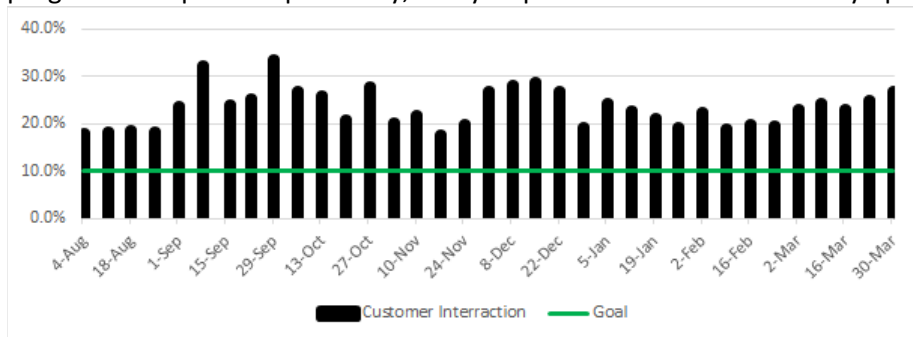


This measure evaluates how well the network security team manages the customer ticket queue against targets.

- Target is 50 open requests
- Current 12 week average is 151 or 66% over target

% Network security tickets awaiting customer interaction

This measure evaluates how well the network security team maintains customer interactions on the progress of requests. Specifically, every request should receive a timely update within a 7-day period.

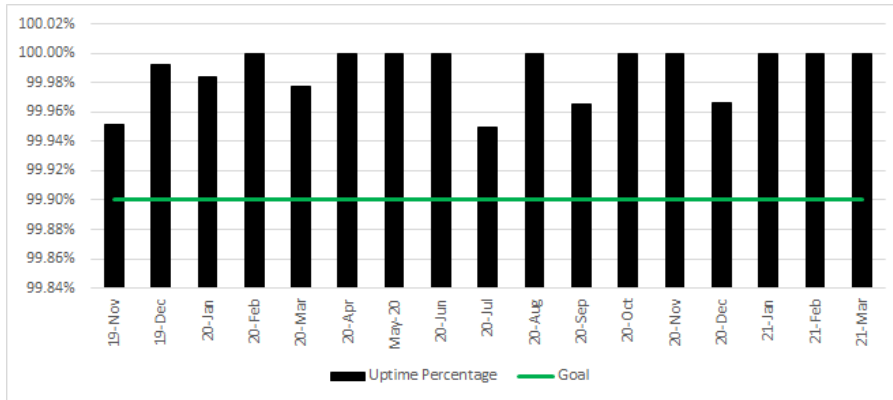


- Target is 10% tickets awaiting customer interaction (>7 days)
- Current 12 week average is 24% or 57% over target

% Network security uptime related to network security activity

This measure tracks the network security team’s contribution to State network uptime, an essential measure of the team’s execution quality. Uptime is deducted whenever there is a State network outage attributable in whole or in part to the network security team.

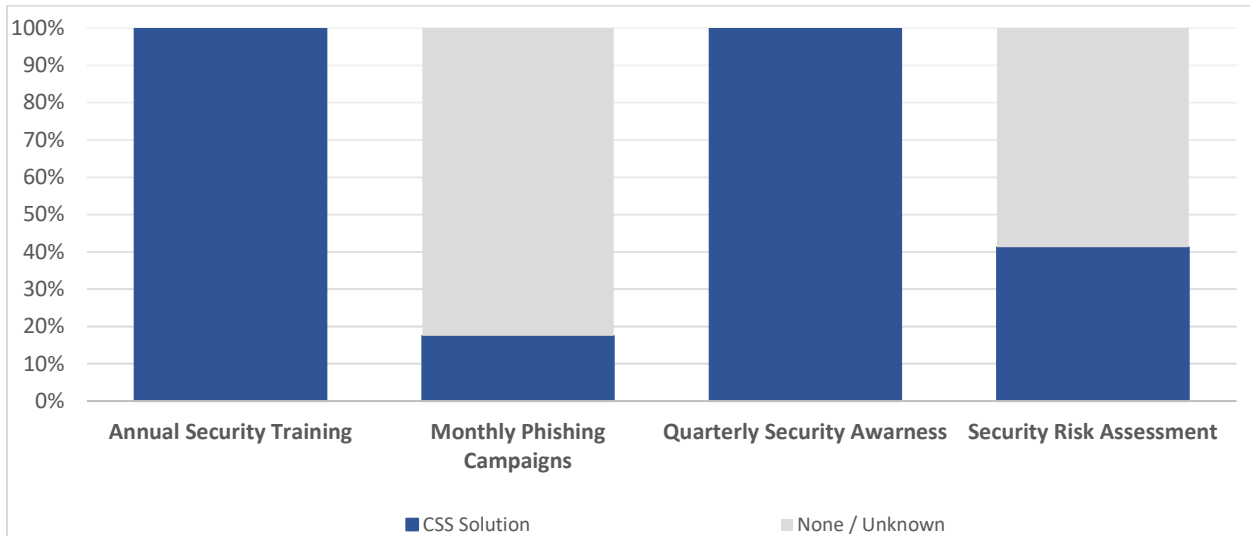
Scope: Current measurement is conducted at the state’s perimeter firewall



- Target uptime is 99.9% or better
- Current 12 month average uptime is 99.99%, goal exceeded

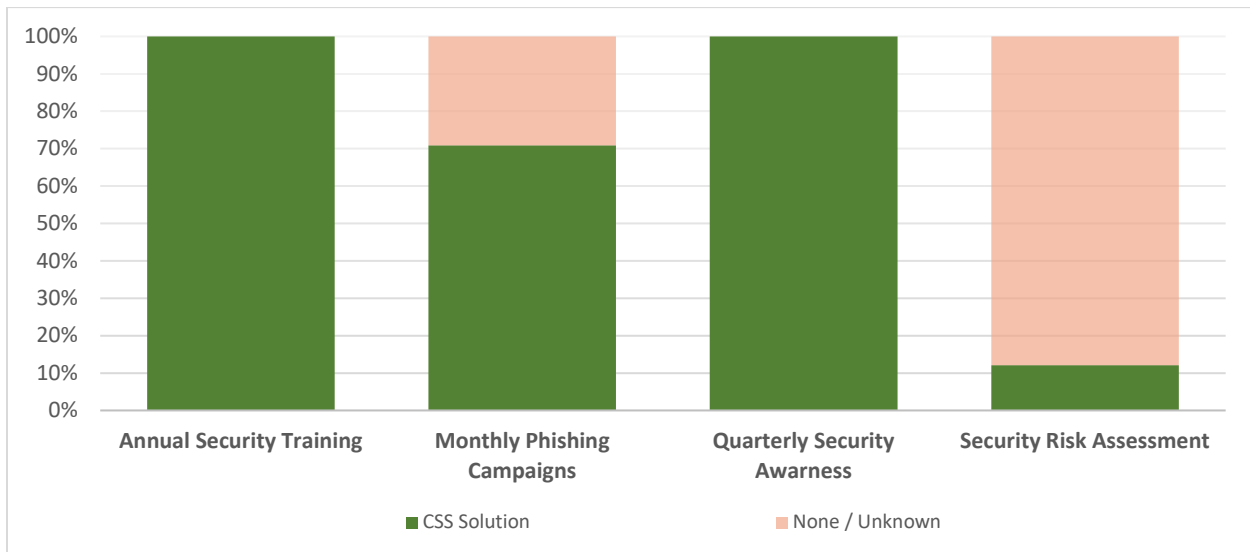
CSS SECTION: GOVERNANCE RISK AND COMPLIANCE (GRC)

ADOPTION OF SERVICES BY AGENCIES



The above chart shows the percentage of adoption by all state agencies where **each agency is weighted equally** and is based on coverage for the stated service. For example, if 20 of the 80 agencies (regardless of agency size) adopted a service it will show as 25% adoption.

RISK REDUCTION IMPACT (PERCENTAGE OF TOTAL POSITIONS IN ALL AGENCIES)



The above chart shows the percentage of adoption by all state agencies where **each agency is weighted based on the number of positions in that agency** and is based on coverage for the stated service. For example, if the total number of positions for all 80 agencies was 40,000 positions, and four (4) agencies adopted a service AND the total number of positions for those four agencies was 20,000, then the service will show as 50% adoption.

GRC - SERVICE-SPECIFIC METRICS

% Information Security & Awareness Training (ISAT) Participation

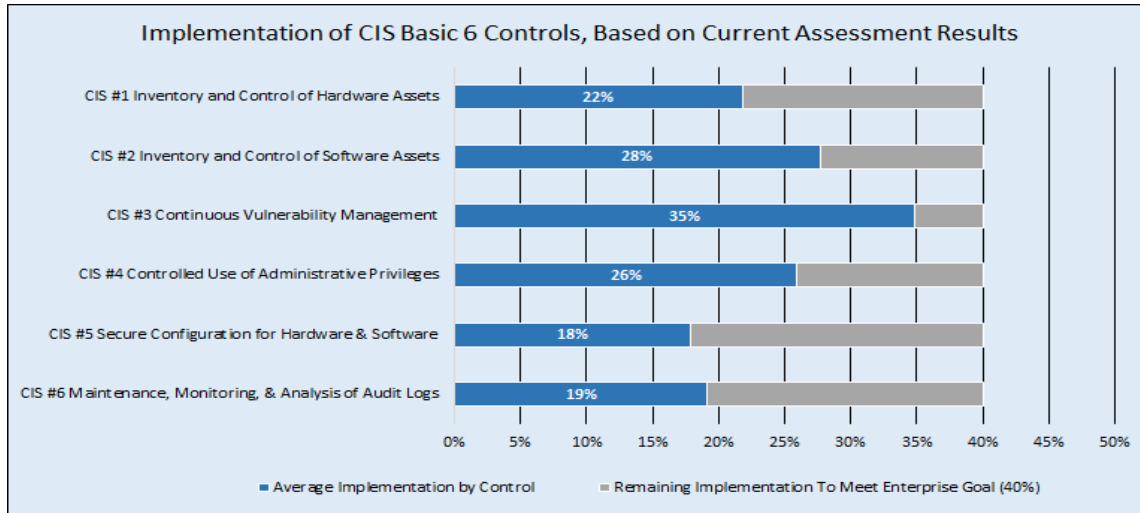
These ISAT measures track the Enterprise Agency participation in the ISAT program. The overall strategy of the ISAT program is one of positive engagement, providing training and awareness that people want to take to help them not only at work, but in their personal lives. The phishing awareness program, also known as a phishing simulation program, is a customizable training and awareness program that provides the opportunity for more focused training opportunities to help reduce organizational risk.

Scope: The metrics included in the graph below include data pertaining to: phishing for the 13 agencies currently participating in the EIS Phishing Awareness Program for Quarter #1 2021; ReportAPhish; ISAT monthly awareness content; and the annual EIS Information Security Training.

ISAT Metric	Frequency	Jan 2021	Feb 2021	Mar 201
Enterprise Annual Training Completion	Monthly	n/a	n/a	n/a
Awareness Reinforcement Video Views	Monthly	3379	3512	3044
Enterprise Security Culture Strength	Annually	67%	n/a	n/a
Enterprise Phishing Number of Targets	Monthly	18480	18592	18735
Enterprise Phishing Successful Delivery	Monthly	18198	18271	18380
Enterprise Phish Prone %	Monthly	26%	9%	40%
Enterprise Phishing Fails	Monthly	4652	1698	7318
Phishing Repeat Responders	Monthly	15	34	154
Simulations reported to ReportAPhish	Monthly	336	137	402
Other reported to ReportAPhish	Monthly	38	33	36
SPAM reported to ReportAPhish	Monthly	107	191	155
Phishing reported to ReportAPhish	Monthly	54	118	86
Phishing reported to agency help desks	Monthly	1273	497	1910

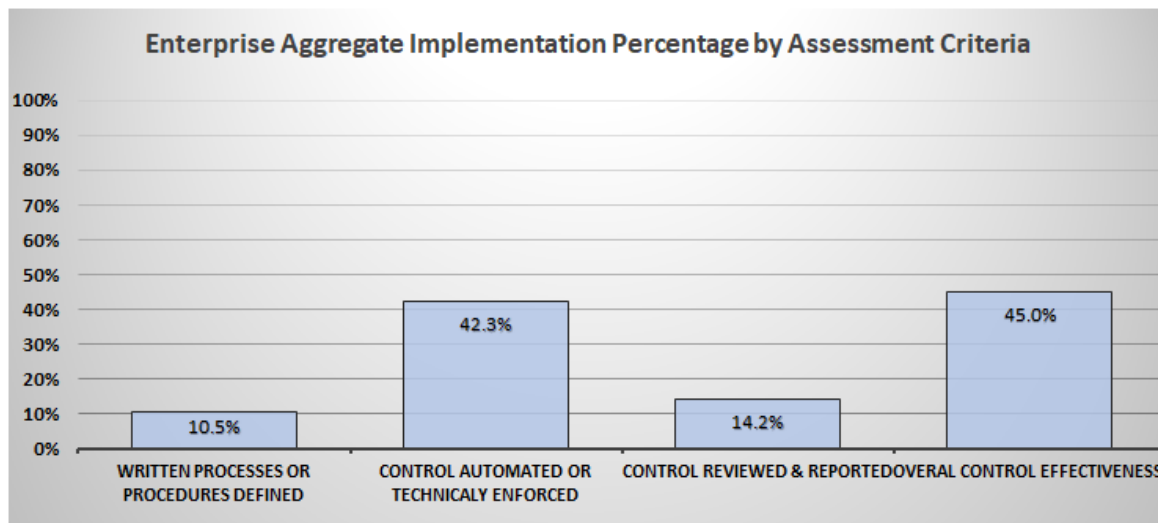
% Risk Assessment: Agency Implementation against the CIS Basic 6 Controls

This Risk Assessment measure tracks the aggregated data based on Executive Branch Agencies (for this Quarter #1 report 27 agencies included) that have been assessed against the Implementation of the CIS Basic 6 Controls.



% Risk Assessment: Agency Implementation by Assessment Criteria

This Risk Assessment measure tracks the aggregated Agencies (for this Quarter #1 report 27 agencies included) implementation of the CIS Basic 6 Controls based on the assessment criteria utilized in the assessment; (1) Written Processes & procedures; (2) Control Automated or Technically Enforced; (3) Control Reviewed & Reported; & (4) Overall Control Effectiveness.



Appendix A - Service Descriptions

Service Name	Service ID	Service Description
Internal Vulnerability Management Scanning	VMS-2	Provide infrastructure and technical support to agencies in support of active scanning of specific hosts and/or IP network ranges in their environment. The service includes prioritization of vulnerabilities to be addressed using a risk-based rating approach monthly reports for Agency leadership.
External Vulnerability Management Scanning	VMS-7	Provide a continuous assessment of the “health” of agency internet-accessible assets by checking for known vulnerabilities and weak configurations. This service coordinates unauthenticated external scanning of state assets utilizing the CISA Cyber Hygiene program.
Malicious Domain Blocking and Reporting (MDBR)	SOCA-1	Prevent IT systems from connecting to harmful web domains, helping limit infections related to known malware, ransomware, phishing, and other cyber threats. This service can block the vast majority of ransomware infections by preventing the initial outreach to a ransomware delivery domain.
Firewall Services	FW-1	Firewall configurations creates network connectivity through a series of ports and protocols.
VPN Services	VPN-1	Remote-access VPNs allow secure access to State resources by establishing an encrypted tunnel across the Internet. The ubiquity of the Internet, combined with today’s VPN technologies, allows organizations to cost-effectively and securely extend the reach of their networks to authorized staff, to any place, at any time.
Annual Security Training	ISAT-1	Develop, conduct, and maintain a statewide general security awareness training program.
Monthly Phishing Campaigns	ISAT-2	Conduct, and maintain phishing simulation program.
Quarterly Security Awareness	ISAT-3	Conduct, and maintain quarterly security awareness campaigns.
Security Risk Assessment	CSRA-1	Provide biannual information security risk assessments against CIS Controls to gauge the health of the security program, provide lists of strengths and weaknesses, and suggest a roadmap and plans to improve the security posture.

Appendix B – EIS Defined Agencies by Policy Area

Administration & Business Services

Accountancy, Board of (BOA)
Administrative Services, Department of (DAS)
Advocacy Commissions Office, Oregon (OACO)
Appraiser Certification and Licensure Board (ACLB)
Architect Examiners, Oregon State Board of (ORBAE)
Construction Contractors Board (CCB)
Consumer and Business Services, Dept. of (DCBS)
Employment Relations Board (ERB)
Governor, Office of the (GOV)
Labor and Industries, Bureau of (BOLI)
*Lottery, Oregon State (OSL)
Public Employees' Retirement System (PERS)
Revenue, Department of (DOR)
*Secretary of State (SOS)
Tax Practitioners, Oregon Board of (OBTP)
*Treasurer, State (OST)
**Exempt by Statute*

Education

Education, Department of (ODE)
Higher Education Coordinating Commission (HECC)
State Library of Oregon (SLO)
Teacher Standards and Practices Commission (TSPC)

Healthy People

Blind, Commission for the (OCB)
Chiropractic Examiners, Oregon Board of (OBCE)
Dentistry, Oregon Board of (OBOD)
Human Services, Department of (DHS)
Health Authority, Oregon (OHA)
Long Term Care Ombudsman (LTCO)
Massage Therapists, Oregon Board of (OBMT)
Medical Board, Oregon (OMB)
Medical Imaging, Oregon Board of (OMBI)
Mental Health Regulatory Agency (MHRA)
Mortuary and Cemetery Board, Oregon (OMCB)
Naturopathic Medicine, Oregon Board of (OBNM)
Nursing, Oregon State Board of (OSBN)
Occupational Therapy Licensing Board (OTLB)
Optometry, Oregon Board of (OBO)
Patient Safety Commission, Oregon (OPSC)
Pharmacy, Oregon Board of (OBOP)
Physical Therapists Licensing Board, Oregon (OPTLB)
Psychiatric Security Review Board (PSRB)
Social Workers, Board of Licensed (BLSW)
Speech-Language Pathology & Audiology, Bd of (BSPA)
Veterinary Medical Examining Board, Oregon (OVMEB)

Natural Resources

Agriculture, Oregon Department of (ODA)
Columbia River Gorge Commission (CRGC)
Energy, Department of (DOE)
Environmental Quality, Department of (DEQ)
Examiners for Eng. and Land Surveying, Bd of (OSBEELS)
Fish and Wildlife, Oregon Department of (ODFW)
Forestry, Department of (ODF)
State Board of Geologist Examiners (OSBGE)
Geology and Mineral Industries, Dept. of (DOGAMI)
Land Conservation and Development (DLCD)
State Landscape Architects Board (OSLAB)
Landscape Contractors Board (LCB)
Land Use Board of Appeals (LUBA)
Lands, Department of State (DSL)
Marine Board, Oregon State (OSMB)
Parks and Recreation, Oregon Department of (OPRD)
Public Utility Commission (PUC)
Water Resources Department (WRD)
Watershed Enhancement Board, Oregon (OWEB)

Public Safety

Corrections, Department of (DOC)
Criminal Justice Commission (CJC)
Government Ethics Commission (GEC)
Justice, Department of (DOJ)
Liquor Control Commission, Oregon (OLCC)
Military Department, Oregon (OMD)
Parole and Post-Prison Supervision, Board of (BOPPPS)
Police, Department of State (OSP)
Public Safety Standards & Training, Dept of (DPSST)
Racing Commission (ORC)
Youth Authority, Oregon (OYA)

Transportation & Economic Development

Aviation, Department of (ODA)
Business Development Department, Oregon (OBDD)
Employment Department (OED)
Housing and Community Services Dept, Oregon (HCS)
Real Estate Agency (REA)
Transportation, Oregon Department of (ODOT)
Travel Information Council (TIC)
Veterans' Affairs, Department of (ODVA)