IT Security Performance Auditing in Washington State

2018 PNIAF Conference

March 16, 2018

Joe Clark – Performance Auditor
Ryan Thedy – Performance Auditor

What we will cover today

- Impact of our IT security audits
- Audit program and tools we use
- Lessons learned

What we do and why

IT security audits are important to:

- Identify security gaps in state and local government IT systems
- Offer remedies and strategies to improve IT security through our recommendations

The goal: To help governments better serve Washingtonians and protect the data they hold

A sample of audit findings reveals serious problems

Procedural deficiencies

- Lack of policies and procedures
- Broken vulnerability and patch management processes
- Incomplete visibility into networks

Technical vulnerabilities

- Missing patches
- Misconfigured devices

Agency reactions demonstrate audit value

- Remediate vulnerabilities as quickly as possible
- Correct procedural deficiencies
- Prioritize security
- Agencies request audits

Building expertise within our Office

Auditors

- Lead and conduct audits; auditee relations
- Develop findings and recommendations
- Audit knowledge transfer to IT security specialists

Technical support

Solicit feedback and clarification

IT security specialists

- Review/validate findings
- Help craft findings and recommendations
- Technical knowledge transfer to auditors and auditees

Audits scoped in two parts

- **Penetration testing**
- **Leading practices assessment**
  - Critical Security Controls
    - Version 6.1

Critical Security Control assessment

Critical Security Controls (CSCs)

- Prioritized list of security measures, focused on value
- Endorsed by public and private organizations
- Surveyed WA state agencies prefer CSCs over NIST 800-53

The CSCs we use

1. Inventory of authorized and unauthorized devices
2. Inventory of authorized and unauthorized software
3. Secure configurations for hardware and software
4. Continuous vulnerability assessment and remediation
5. Controlled use of administrative privileges
11. Secure configurations for network devices

Version 7 of the Critical Security Controls is forthcoming

CSC audit program

- Measurable sub-controls to implement each CSC

- Developed procedures using AuditScripts criteria, examining three topic areas:
  - Policy
  - Implementation
  - Automation/Technical enforcement

Leading practice assessment

- **Critical Security Controls assessment consists of:**
  - Interviews
  - Observing
  - Technical testing
- **Scoping meeting(s) with auditee to discuss audit:**
  - Process
  - Needs
  - Deliverables

CSC assessment procedures – Interviews

- Participants may include:
  - CIO
  - CISO
  - IT staff
- Allocate about three hours to review each control

CSC assessment procedures – Observing

- Level of evidence depends on risk and significance
- Includes:
  - Over-the-shoulder observing
  - Screenshots
- Goal: Conduct all interviews and validation in one week

CSC assessment procedures – Technical testing

For example:

- Passwords
  - Age
- Administrator accounts
  - Excessive use?

Domain Administrators

Members are authorized to administer the domain. By default, the Domain Admins group is a member of the Administrators group on all computers that have joined a domain, including the domain controllers. Domain Admins is the default owner of any object that is created in the domain's Active Directory by any member of the group. If members of the group create other objects, such as files, the default owner is the Administrators group.

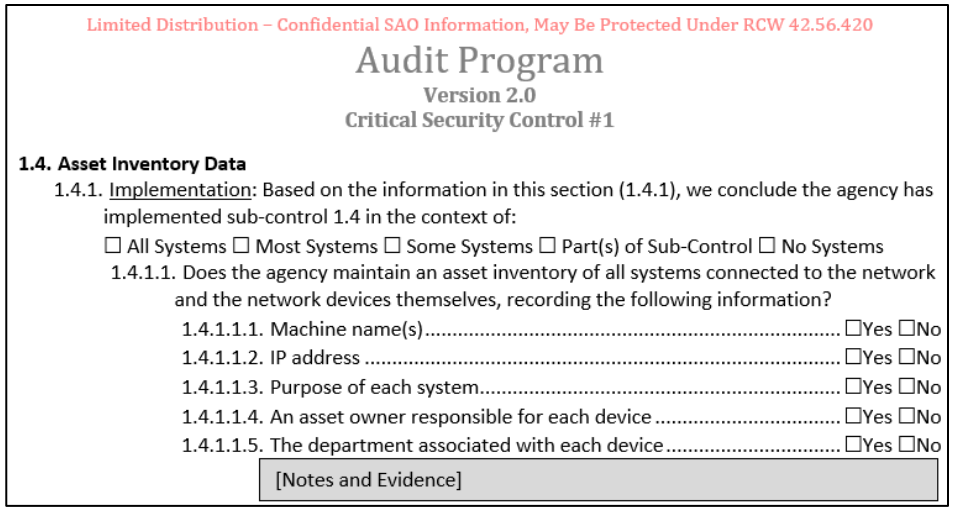
Logon ID	Name	Pwd Age (Days)	Last Logged In	No Pwd Expiry	Pwd Reversable	Pwd Not Req.
Bruce.Wayne	Bruce.Wayne	1695	3/20/2016 1:14:39 PM	True	False	False
Adam West	Adam West	1695	3/20/2016 2:59:45 AM	True	False	False
svc.SQL.GH	svc.SQL.GH	588	3/20/2016 7:40:17 PM	True	False	False
svc.backup.GH	svc.backup.GH	367	3/14/2016 7:39:37 AM	True	False	False
Dr.Pepper	Dr.Pepper	52	3/22/2016 3:07:35 AM	False	False	False
lucius.fox_Admin	Lucius.fox.Admin	43	3/22/2016 7:15:02 AM	False	False	False
Dr.Dre	Dr.Dre	23	3/19/2016 12:15:58 AM	False	False	False
barbara.gordon_admin	barbara.gordon_admin	10	3/14/2016 8:50:05 AM	False	False	False

Audit results – Overview

Deliverable	Audience
Critical Security Control assessment sheets	IT management, technical staff
AuditScripts spreadsheet	Executives, IT management, technical staff
Critical Security Control results document	Executives, IT management
Technical results (such as scans)	Technical staff

Audit results – CSC assessment sheets

- Document interviews, testing and evidence
- Include specific, detailed results
- Intended for technical staff
- Conclusions feed into AuditScripts spreadsheet



Limited Distribution – Confidential SAO Information, May Be Protected Under RCW 42.56.420

Audit Program
Version 2.0
Critical Security Control #1

1.4. Asset Inventory Data

1.4.1. Implementation: Based on the information in this section (1.4.1), we conclude the agency has implemented sub-control 1.4 in the context of:

☐ All Systems ☐ Most Systems ☐ Some Systems ☐ Part(s) of Sub-Control ☐ No Systems

1.4.1.1. Does the agency maintain an asset inventory of all systems connected to the network and the network devices themselves, recording the following information?

1.4.1.1.1. Machine name(s) ☐Yes ☐No
1.4.1.1.2. IP address ☐Yes ☐No
1.4.1.1.3. Purpose of each system ☐Yes ☐No
1.4.1.1.4. An asset owner responsible for each device ☐Yes ☐No
1.4.1.1.5. The department associated with each device ☐Yes ☐No

[Notes and Evidence]

Audit results – CSC assessment sheets

1.4. Asset Inventory Data

1.4.1. Implementation: Based on the information in this section (1.4.1), we conclude the agency has implemented sub-control 1.4 in the context of:

☐ All Systems ☐ Most Systems ☒ Some Systems ☐ Part(s) of Sub-Control ☐ No Systems

Based on the information collected in question 1.4.1.1, we conclude that the agency is **implementing sub-control 1.4 on some system**. The agency is not collecting the purpose of each system or the department associated with the system in their inventory data.

1.4.1.1. Does the agency maintain an asset inventory of all systems connected to the network and the network devices themselves, recording the following information?

1.4.1.1.1. Machine name(s) ..... ☒Yes ☐No

1.4.1.1.2. IP address ..... ☒Yes ☐No

1.4.1.1.3. Purpose of each system ..... ☐Yes ☒No

1.4.1.1.4. An asset owner responsible for each device ..... ☒Yes ☐No

1.4.1.1.5. The department associated with each device ..... ☐Yes ☒No

From interview with Boris, the inventory contains the machine name, IP address, and asset owner, which is the person with the system but may not necessarily be the person with ultimate responsibility for the system (see the full asset inventory at **F.1.143**).

Audit results – CSC assessment sheets

1.4.2. Automation/Technical Enforcement: Based on the information in this section (1.4.2), we conclude the agency has automated/technically enforced sub-control 1.4 in the context of:

☒ All Systems ☐ Most Systems ☐ Some Systems ☐ Part(s) of Sub-Control ☐ No Systems

Based on the information collected in question 1.4.2.1, we conclude that the agency is **automating/technically enforcing sub-control 1.4 on all systems** because the inventory system automatically inventories all systems connected to the production network and captures the information outlined in question 1.4.1.1. Even though the agency is not collecting all information required by sub-control 1.4, the automation of the information collecting is in place.

1.4.2.1. How is the asset inventory updated with information about new systems connected to the network?

New systems are entered into Active Directory as part of the purchasing process. Once the systems are received, the HelpDesk images the system with the standard image, which is then automatically recorded in the inventory by the inventory system. We observed one system being imaged in the helpdesk area while on-site and then visually reviewed the inventory system to verify that the system was automatically entered into the inventory after imaging.

Audit results – CSC assessment sheets

1.4.3. Documentation: Based on the information in this section (1.4.3), we conclude the agency has documentation for sub-control 1.4 that is:

☐ Approved Witten ☐ Written ☒ Partially Written ☐ Informal ☐ None

Based on the information collected in question 1.4.3.1, we conclude that the agency has **documentation that is partially written for sub-control 1.4** because the policy does not require the agency to collect the purpose of or department responsible for each system in the asset inventory.

1.4.3.1. Does the agency have documentation detailing the maintenance of an IT asset inventory, which requires the following information be recorded in the asset inventory:

1.4.3.1.1. Machine Name ..... ☒Yes ☐No

1.4.3.1.2. IP Address ..... ☒Yes ☐No

1.4.3.1.3. Purpose of each system ..... ☐Yes ☒No

1.4.3.1.4. An asset owner responsible for each device ..... ☒Yes ☐No

1.4.3.1.5. The department associated with each device ..... ☐Yes ☒No

Section 1.3 of the agency IT Security Program requires the agency to collect the machine name, IP address, and asset owner for all systems on the production network (see page 5 of the Security Program at **F.1.125**).

Audit results – AuditScripts spreadsheet

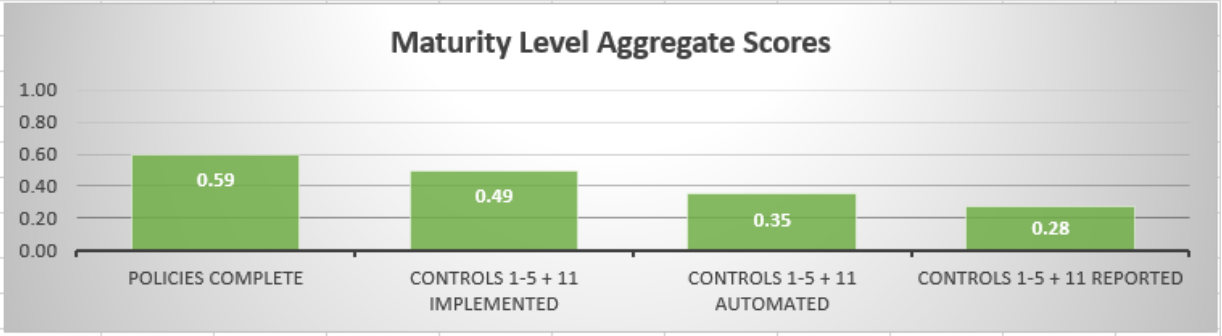
- Includes dashboard with charts/graphs
- Intended for agency technical staff and mid-level management
- Customized by our auditors

AuditScripts dashboard

AuditScripts — Critical Security Controls Initial Assessment Tool (v6.0b) — SECURITY enclave

Maturity level:	Desription:	Score:
Level One	Policies Complete	0.59
Level Two	Controls 1-5 + 11 Implemented	0.49
Level Three	Controls 1-5 + 11 Automated	0.35
Level Four	Controls 1-5 + 11 Reported	0.28
	Maturity Rating*:	**1.72**
	*Rating is on a 0-4 scale.	

Exhibit 1: Top 5 + 11 CSC Maturity Rating



Note: This tab edited for formatting and content by SAO auditors.

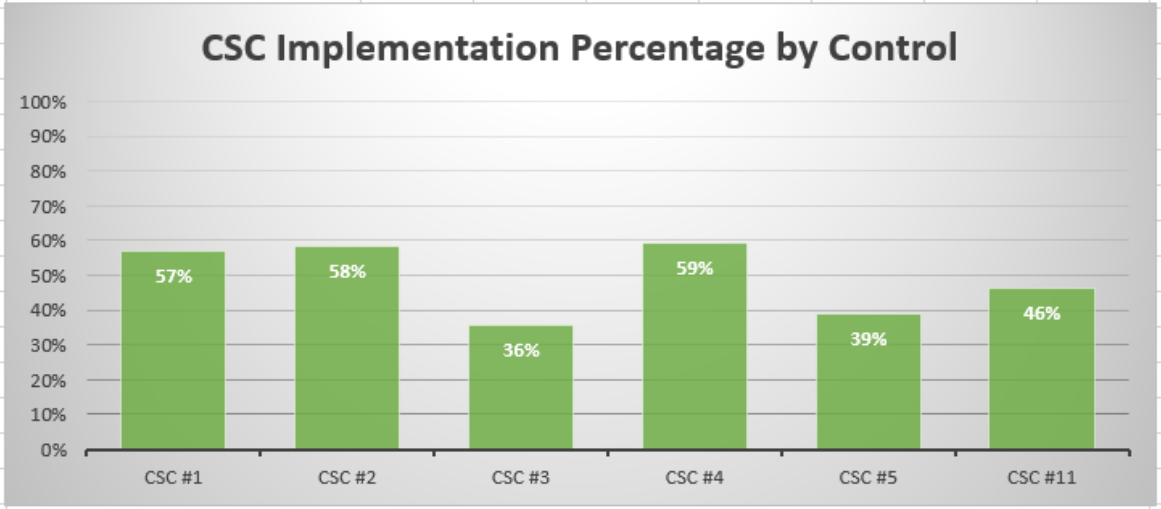
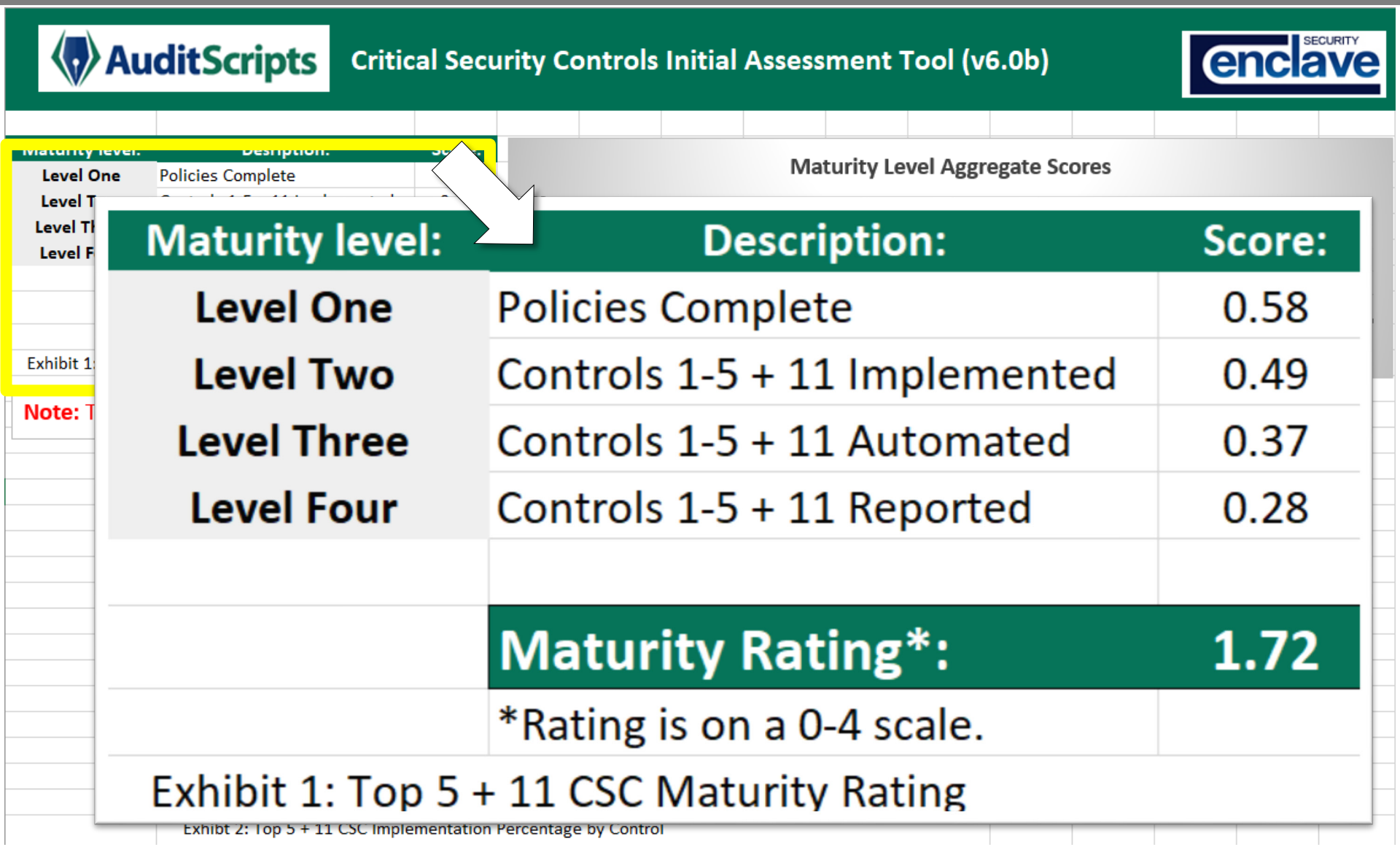


Exhibit 2: Top 5 + 11 CSC Implementation Percentage by Control

AuditScripts dashboard



AuditScripts CSC 1 worksheet

AuditScripts

Critical Security Control #1: Inventory of Authorized and Unauthorized Devices

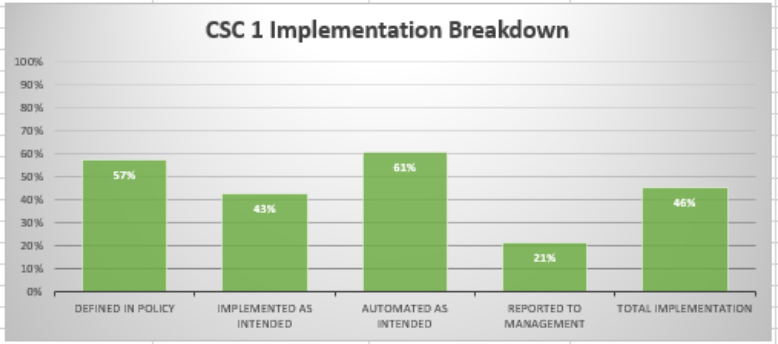
enclave SECURITY

Limited Distribution - Confidential and Proprietary SAO Information, subject to RCW 42.56.420 and RCW 42.56.270

Percent Aligned:	46%
Percent Not Aligned:	54%

Note: This tab edited for formatting and content by SAO auditors.

1. The "Percent Aligned" level was changed by SAO from "Risk Addressed."
2. The "Percent Not Aligned" level was changed by SAO from "Risk Accepted."
3. The CSC 1 Implementation Breakdown chart was added by SAO.
4. The "Control Reported to Delegated Authority" criterion (column H) was changed by SAO from "Control Reported to Business."



ID	Critical Security Control Detail	NIST Core Framework	Sensor or Baseline	Policy Defined	Control Implemented	Control Automated or Technically Enforced	Control Reported to Delegated Authority
1.1	Deploy an automated asset inventory discovery tool and use it to build a preliminary inventory of systems connected to an organization's public and private network(s). Both active tools that scan through IPv4 or IPv6 network address ranges and passive tools that identify hosts based on analyzing their traffic should be employed.	Identify	Active Device Discovery System	Approved Written Policy	Implemented on Most Systems	Automated on Most Systems	Not Reported
		Identify	Passive Device Discovery System	No Policy	Implemented on Some Systems	Automated on Some Systems	Not Reported
1.2	If the organization is dynamically assigning addresses using DHCP, then deploy dynamic host configuration protocol (DHCP) server logging, and use this information to improve the asset inventory and help detect unknown systems.	Detect	Log Management System / SIEM	Partial Written Policy	Implemented on Most Systems	Not Automated	Reported on Some Systems
1.3	Ensure that all equipment acquisitions automatically update the inventory system as new, approved devices are connected to the network.	Identify	Asset Inventory System	Written Policy	Implemented on Some Systems	Automated on All Systems	Not Reported
1.4	Maintain an asset inventory of all systems connected to the network and the network devices themselves, recording at least the network addresses, machine name(s), purpose of each system, an asset owner responsible for each device, and the department associated with each device. The inventory should include every system that has an Internet protocol (IP) address on the network, including but not limited to desktops, laptops, servers, network equipment (routers, switches, firewalls, etc.), printers, storage area networks, Voice Over-IP telephones, multi-homed addresses, virtual addresses, etc. The asset inventory created must also include data on whether the device is a portable and/or personal device. Devices such as mobile phones, tablets, laptops, and other portable electronic devices that store or process data must be identified, regardless of whether they are attached to the organization's network.	Identify	Asset Inventory System	Approved Written Policy	Parts of Sub-Control Implemented	Automated on Most Systems	Reported on Some Systems
1.5	Deploy network level authentication via 802.1x to limit and control which devices can be connected to the network. The 802.1x must be tied into the inventory data to determine authorized versus unauthorized systems.	Protect	Network Level Authentication (NLA)	Informal Policy	Not Implemented	Parts of Sub-Control Automated	Not Reported
1.6	Use client certificates to validate and authenticate systems prior to connecting to the private network.	Protect	Public Key Infrastruture (PKI)	Partial Written Policy	Parts of Sub-Control Implemented	Automated on All Systems	Reported on Some Systems

Thedy, Ryan (SAO): See question 1.4.3 of the CSC 1 assessment sheet at F.1.25

Audit results – Critical Security Controls

- **Results in brief**
  - Overall results
- **Detailed results section**
  - Explains *why* each control is important
  - What we found

CSC Results in Brief

Results in Brief

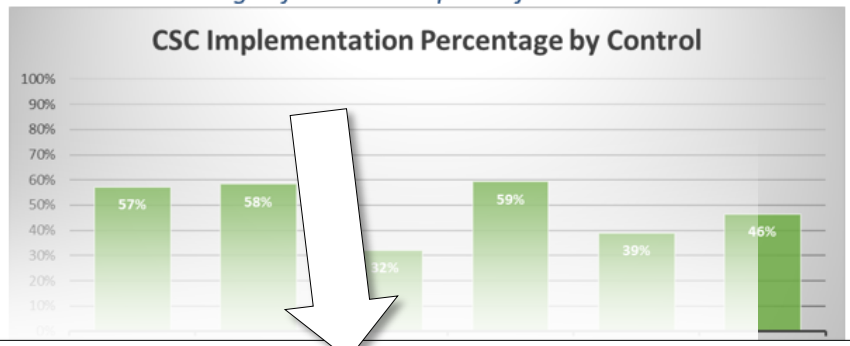
The audit of the critical security controls determine ting the six evaluated controls was 1.72 on a scale of maturity level in the six controls; Exhibit 2 the percent of each control the Entity has implemented. What the audit fou ecommendations covering each control are described in the Results section of this repor detailed analysis in Appendix C.

Maturity Rating

Exhibit 1 - Organization maturity level for the six audited controls

Maturity level:	Desription:	Score:
Level One	Policies Complete	0.58
Level Two	Controls 1-5 + 11 Implemented	0.49
Level Three	Controls 1-5 + 11 Automated	0.37
Level Four	Controls 1-5 + 11 Reported	0.28
	Maturity Rating*:	1.72
	*Rating is on a 0-4 scale.	

Exhibit 2 - Percentage of actions completed for each control



Implementation by Control

CSC Results – Control introduction

Control description

- *Does the organization have and maintain an inventory of all the devices that are connected to its network?*

Critical Security Control #1 ventory of authorized and unauthorized devices

Does the organization have and maintain an inventory of all the devices (workstations, servers, networking devices, etc.) that are connected to its network?

Why this control is important

An organization must be aware of all devices on its net servers, mobile devices, printers and network equipment). Without this knowledge, the organi awareness of risk, which could undermine its risk assessment and affect its ability to implement an effective security program.

As an example, unknown devices added to the network are unlikely to receive the same level of monitoring that known devices receive. Aside from the possibility the device may be malicious, it may not receive the necessary patches, increasing the likelihood of vulnerabilities, leading to an increased risk of compromise. Once compromised, a device can present an immediate threat to the [entity type]'s network, and can be used as a launching point for a more significant attack.

Why this control is important

CSC Results – What the audit found

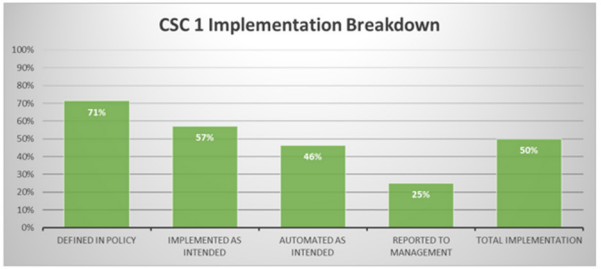
What the audit found

Overall, we conclude that the Entity has aligned its IT security controls in a way that implements 50 percent of Control #1 (see **Exhibit 4**).

The Entity maintains a partial inventory of devices on its network. One area of strength was use of an active scanner. e Entity could improve by hardware inventory with Additionally, we tested controls and observed that as able to detect d devices on the network, was able to alert personnel about those devices, and was not able twork access to those unauthorized devices within the recommended time frames. See in Appendix C for detailed results.

sting, observation, and interviews with the Entity's staff, there are multiple contributing e Entity's p lignment with Control # 1. In general, these included resource constraints, s on other s controls.

Exhibit 4- Breakdown of actions completed in Control #1



What the audit found

- Alignment percentage
- Implementation description
- Areas of strength
- Areas for improvement
- Test results

Reasons not fully implemented

Public reporting and confidentiality

- Information largely protected under state law
  - RCW 42.56.420(4)
- Yellow Book considerations (7.41 & 7.42)
- Public audit reports published with limited details
- Present high-level results to governing stakeholders
  - Joint Legislative Audit and Review Committee for state audits

Lessons learned

- Add SAO IT security specialists
- Start interviews with “Implementation” question
- Core evaluation tests will be optional
- Clearly communicate audit expectations to auditee
- Made reporting optional

References

- AuditScripts spreadsheet: http://www.auditscripts.com/free-resources/critical-security-controls/
- Center of Internet Security Critical security controls: https://www.cisecurity.org/controls/
- Additional tools listed on slides 33 & 34

State Auditor's Office website:

www.sao.wa.gov

Questions?

Contacts

Pat McCarthy
State Auditor
(360) 902-0360
Pat.McCarthy@sao.wa.gov

Scott Frank
Director of Performance Audit
(360) 902-0370
Scott.Frank@sao.wa.gov

Joseph Clark
Performance Auditor
(360) 725-5572
Joseph.Clark@sao.wa.gov

Ryan Thedy, CISA, GSIF
Performance Auditor
(360) 725-5414
Ryan.Thedy@sao.wa.gov

Tools used in our audits

- **Nessus:** https://www.tenable.com/products/nessus/select-your-operating-system
  - Gain awareness of patch levels
  - Check systems against known benchmarks
  - Gain awareness of privileged accounts
- **Lynis:** https://cisofy.com/lynis
  - Free audit tool for Linux, Unix, and Apple systems.
- **AdAssetInventory.PS1:** https://gallery.technet.microsoft.com/office/Active-Directory-Audit-7754a877
  - PowerShell script that identifies privileged accounts in AD and provides insight

More tools used in our audits

- **NetBrain:** https://www.netbraintech.com
  - Maps networks for situational awareness
  - Generates network diagram
  - Assists in configuration review
- **Nipper:** https://www.titania.com/products/nipper-studio
  - Networking auditing tool
- **CIS-CAT:** https://learn.cisecurity.org/cis-cat-landing-page
  - Center of Internet Security tool for checking CIS benchmarks