RAPID7

Critical Security Controls Assessment Overview

[Managed Services - MDR

[#Your Name]
Customer Advisor

[#DATE]

Agenda

- Introduction to CSC
- The CSC Assessment Process
- CSC Scoring & Recommendations
- Q&A

CSC Overview

- **What is CSC:**
  - The Critical Security Controls (CSC) is a prioritized set of actions recommended by the Center for Internet Security (CIS) to prevent and mitigate cyber attacks.
- **Purpose of CSC:**
  - The CSC is designed to help organizations protect their critical assets and data from cyber threats by identifying the most important security measures to implement.
- **Importance of CSC:**
  - With the increasing frequency and sophistication of cyber attacks, it is more important than ever for organizations to have a strong security program in place.
  - The CSC provides a practical and effective framework for organizations to follow in order to improve their security posture and reduce the risk and impact of future cyber attacks.

The CSC Assessment Process

- **What is a CSC assessment?**
  - The CSC assessment is a two-hour systematic evaluation of an organization's security program to determine the level of implementation and effectiveness of the controls.
- **What is the purpose of CSC assessments?**
  - The purpose of a CSC assessment is to identify areas of weakness in an organization's security posture, and provide recommendations on implementing appropriate security controls to protect against potential threats.
- **What is the outcome of CSC assessments?**
  - After a CSC assessment, the organization will receive a personalized summary with a compilation of the results of the assessment, which provides recommendations for improving the security posture. The organization can then use this information to make informed decisions about where to allocate resources and focus their security efforts.

Recommendations for Improving Compliance with the CSC

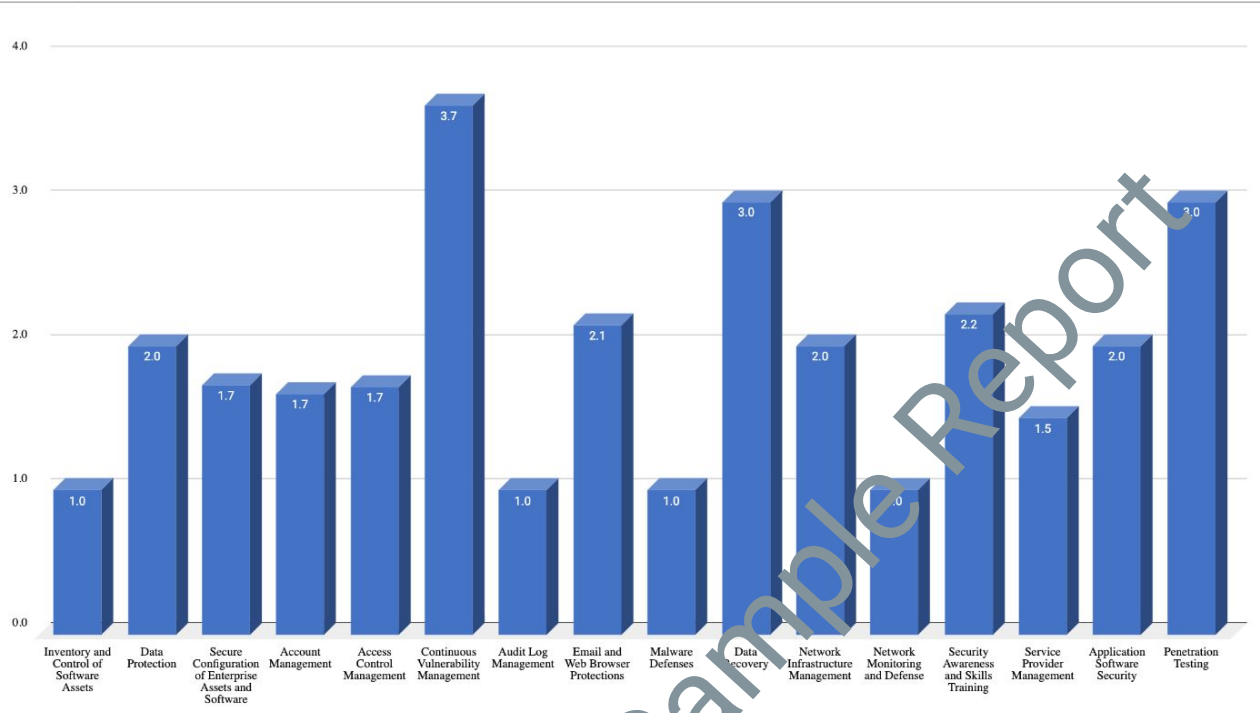
- **Assign a dedicated team for this project**
  - Designating a cross-functional team of key stakeholders to oversee the implementation and maintenance of the CSC assessment will help to ensure that the controls are properly implemented and that the security posture is continuously monitored and updated.
- **Conduct regular assessments**
  - Regular assessments of the CSC implementation will help to identify any gaps or areas for improvement, and provide an opportunity to update the controls as necessary to stay ahead of new threats.
- **Maintain an incident response plan**
  - Having a well-defined incident response plan in place will help the organization quickly and effectively respond to any security incidents that occur, reducing the risk of damage and helping to ensure a prompt recovery.

CSC Scoring

Description	Score
0 - Control not in place | Do Not Do/Do Not Have	0
1 - Control partially in place | No Policy/Procedure - Informal Practice Only | No one responsible	1
2 - Control in place | Have Written Policy/Procedure - Not Followed | No clear responsibility	2
3 - Control in place | Policy/Procedure Partially Implemented | Assigned Responsibility	3
4 - Control in place | Policy/Procedure Fully Implemented, Reviewed & Updated Annualy | Assessed	4
5 - Control in place | Policy/Procedures Fully Implemented, Tested, & Control Monitored | Assessed	5

CSC Control - Protect

Protect Controls	Score
Inventory and Control of Software Assets	1.0
Data Protection	2.0
Secure Configuration of Enterprise Assets and Software	1.7
Account Management	1.7
Access Control Management	1.7
Continuous Vulnerability Management	3.7
Audit Log Management	1.0
Email and Web Browser Protections	2.1
Malware Defenses	1.0
Data Recovery	3.0
Network Infrastructure Management	2.0
Network Monitoring and Defense	1.0
Security Awareness and Skills Training	2.2
Service Provider Management	1.5
Application Software Security	2.0
Penetration Testing	3.0
CSC Protect Controls Score	**1.9**



Recommendations

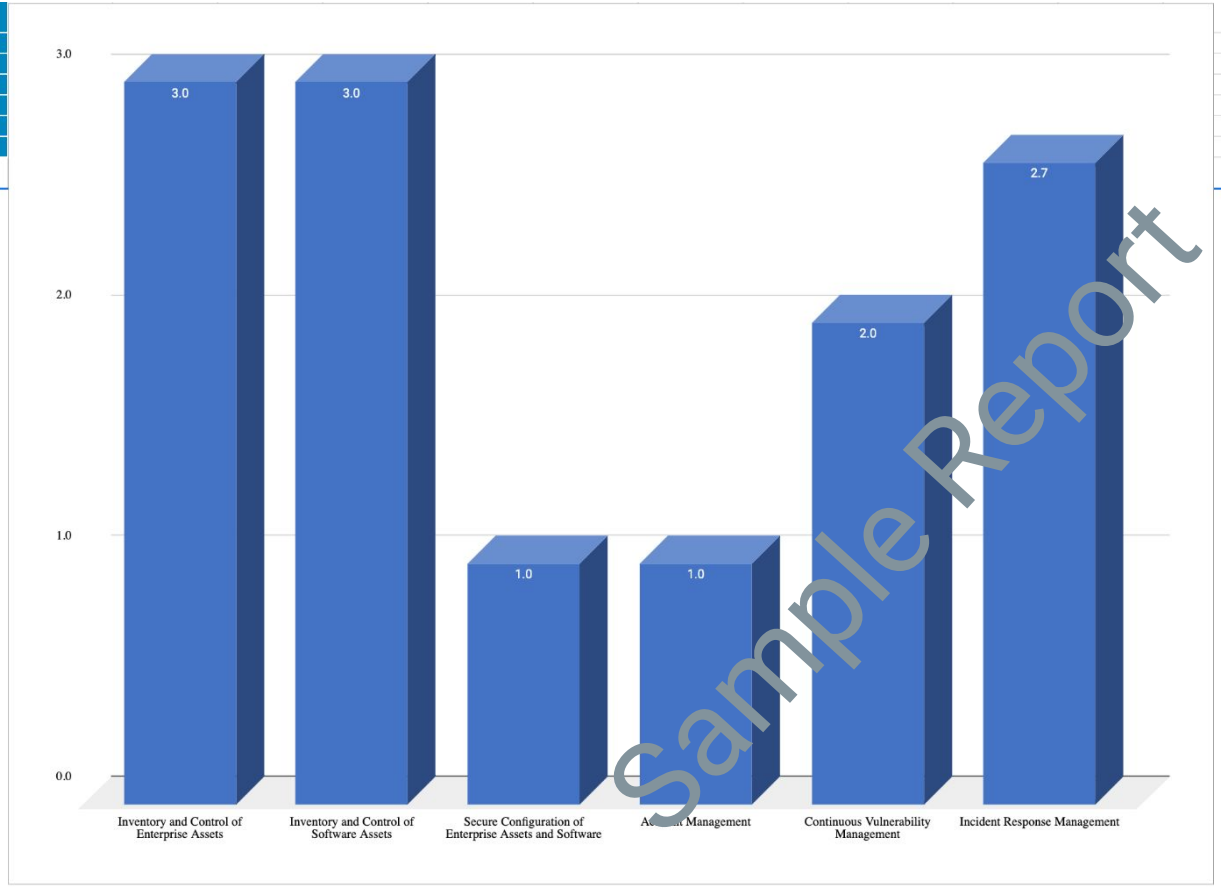
6.4 Users: Require MFA for remote network access.

9.2 Network: Use DNS filtering services on all enterprise assets to block access to known malicious domains.

10.1 Devices: Deploy and Maintain Anti-Malware Software

CSC Control - Respond

Respond Controls	Score
Inventory and Control of Enterprise Assets	3.0
Inventory and Control of Software Assets	3.0
Secure Configuration of Enterprise Assets and Software	1.0
Account Management	1.0
Continuous Vulnerability Management	2.0
Incident Response Management	2.7
CSC Respond Controls Score	**2.1**



Recommendations

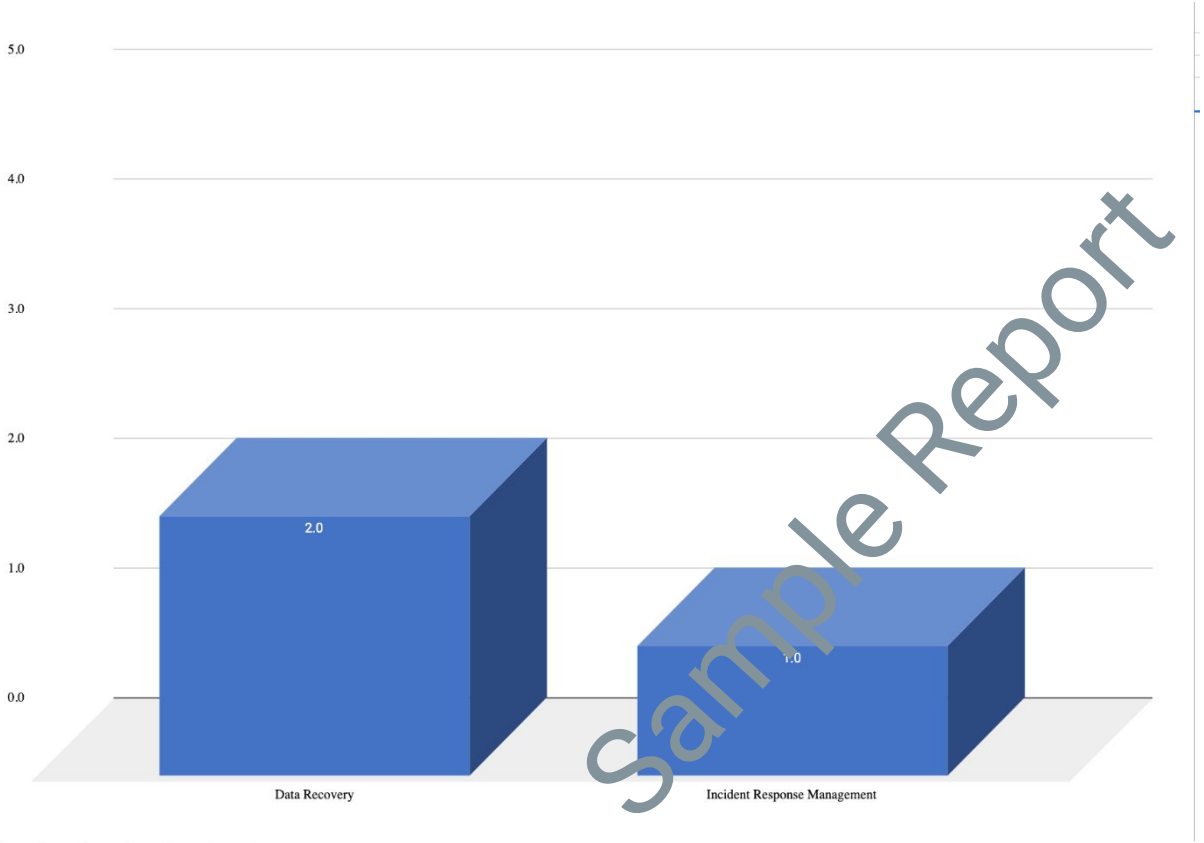
7.2 Applications: Establish and maintain a risk-based remediation strategy documented in a remediation process, with monthly, or more frequent, reviews.

17.4 Establish and maintain an incident response process that addresses roles and responsibilities, compliance requirements, and a communication plan. Review annually, or when significant enterprise changes occur that could impact this Safeguard.

17.5 Assign key roles and responsibilities for incident response, including staff from legal, IT, information security, facilities, public relations, human resources, incident responders, and analysts, as applicable. Review annually, or when significant enterprise changes occur that could impact this Safeguard.

CSC Control - Recover

Recover Controls	
Data Recovery	2.0
Incident Response Management	1.0
CSC Recover Controls Score	**1.5**



Recommendations

11.4 Data: Establish and maintain an isolated instance of recovery data. Example implementations include, version controlling backup destinations through offline, cloud, or off-site systems or services.

17.7 Plan and conduct routine incident response exercises and scenarios for key personnel involved in the incident response process to prepare for responding to real-world incidents. Exercises need to test communication channels, decision making, and workflows. Conduct testing on an annual basis, at a minimum.

Q&A