SITE DETAIL REPORT

Test
9/18/2025
Test
brene
SELF ASSESSMENT

Disclaimer

The analysis, data, and reports in CSET® are provided “as is” for informational purposes only. The Cybersecurity & Infrastructure Security Agency (CISA) does not provide any warranties of any kind regarding any information contained within. In no event shall the United States Government or its contractors or subcontractors be liable for any damages, including but not limited to, direct, indirect, special, or consequential damages and including damages based on any negligence of the United States Government or its contractors or subcontractors, arising out of, resulting from, or in any way connected with this report, whether based on warranty, contract, tort, or otherwise, whether injury was sustained from, or arose out of the results of, or reliance upon the report.

CISA does not endorse any commercial product or service, including the subject of the assessment or evaluation in this report. Any reference to specific commercial products, processes, or services by trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by CISA.

The display of the CISA official seal or other CISA visual identities on this report shall not be interpreted to provide the recipient organization authorization to use the official seal, insignia or other visual identities of CISA. The CISA seal, insignia, or other visual identities shall not be used in any manner to imply endorsement of any commercial product or activity by CISA or the United States Government. Use of the CISA seal without proper authorization violates federal law (e.g., 18 U.S.C. §§ 506, 701, 1017), and is against CISA policies governing usage of the seal.

The report is prepared and intended for internal use by the organization that made the request. The contents of this report may be subject to government or private intellectual property rights. To request distribution of this report outside the organization for which it was prepared, contact the CSET Program Office. The contents of this report may be reproduced or incorporated into other reports, but may not be modified without the prior express written permission of the CSET Program Office.

Advisory

The Cyber Security Evaluation Tool (CSET®) is only one component of the overall cybersecurity picture and should be complemented with a robust cyber security program within the organization. A self-assessment with CSET® cannot reveal all types of security weaknesses, and should not be the sole means of determining an organization's security posture.

The tool will not provide a detailed architectural analysis of the network or a detailed network hardware/software configuration review. It is not a risk analysis tool so it will not generate a complex risk assessment. CSET® is not intended as a substitute for in-depth analysis of control system vulnerabilities as performed by trained professionals. Periodic onsite reviews and inspections must still be conducted using a holistic approach including facility walk-downs, interviews, and observation and examination of facility practices. Consideration should also be given to additional steps including scanning, penetration testing, and exercises on surrogate, training, or non-production systems, or systems where failures, unexpected faults, or other unexpected results will not compromise production or safety.

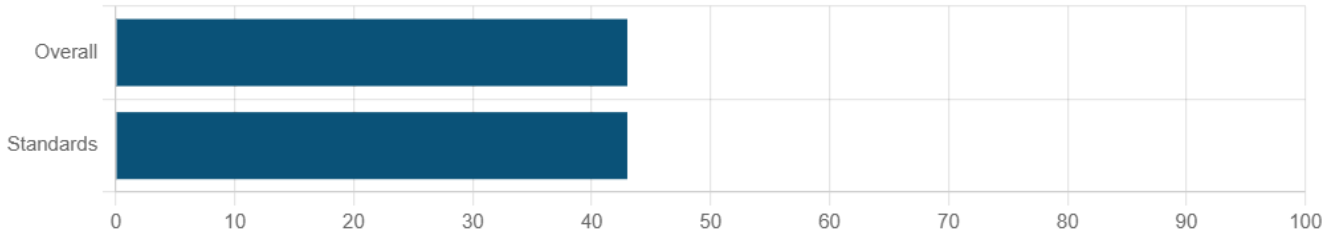
CSET® assessments cannot be completed effectively by any one individual. A cross-functional team consisting of representatives from operational, maintenance, information technology, business, and security areas is essential. The representatives must be subject matter experts with significant expertise in their respective areas. No one individual has the span of responsibility or knowledge to effectively answer all the questions.

Data and reports generated by the tool should be managed securely and marked, stored, and distributed in a manner appropriate to their sensitivity.

Site Information

Assessment Name	Test
Assessment Date	9/18/2025
Facility Name	Test
City or Site Name	Test
State, Province, or Region	Test
Principal Assessor Name	brene
Additional Notes and Comments	
Contacts	

Summary Percent Compliance



High-Level Assessment Description

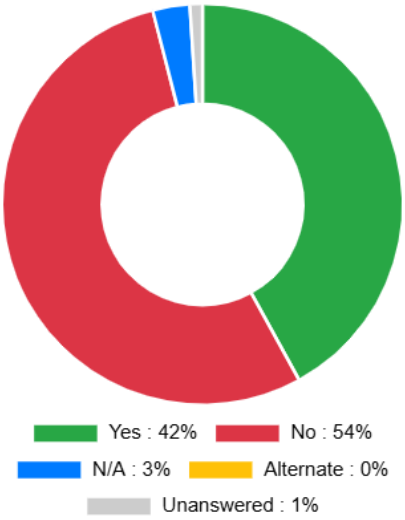
This is a test case assesment.

Executive Summary

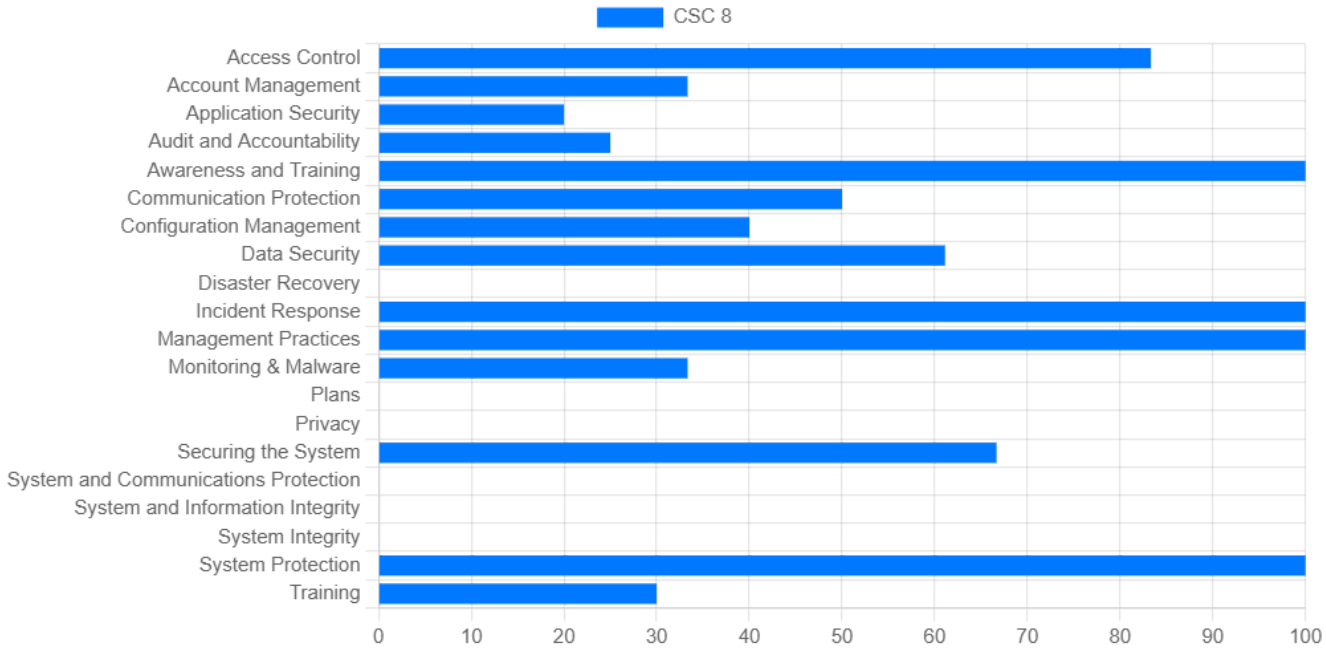
Cyber terrorism is a real and growing threat. Standards and guides have been developed, vetted, and widely accepted to assist with protection from cyber attacks. The Cyber Security Evaluation Tool (CSET) includes a selectable array of these standards for a tailored assessment of cyber vulnerabilities. Once the standards were selected and the resulting question sets answered, the CSET created a compliance summary, compiled variance statistics, ranked top areas of concern, and generated security recommendations.

Evaluation Against Selected Standards and Question Sets

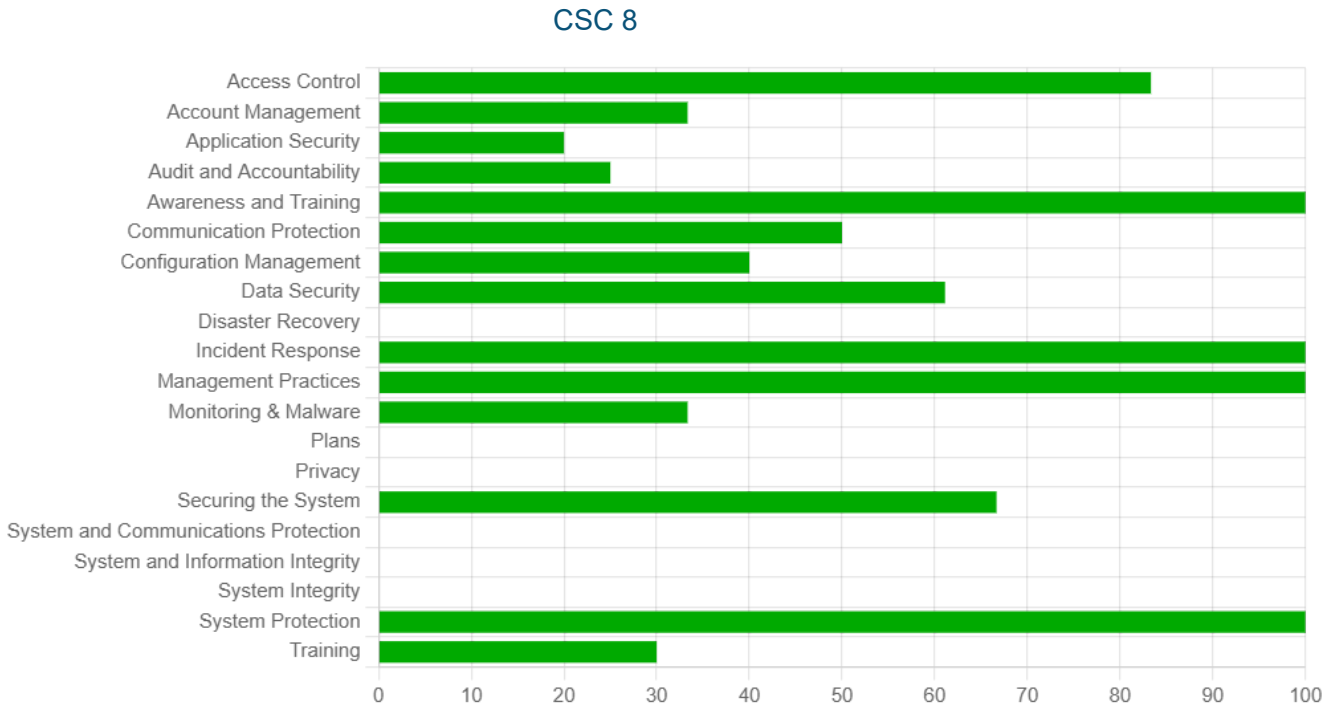
Standards Summary



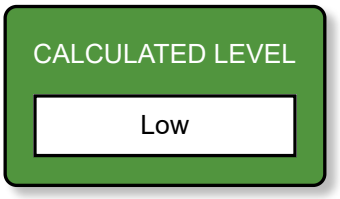
Standard or Question Set



Standards Compliance



Security Assurance Level (SAL)



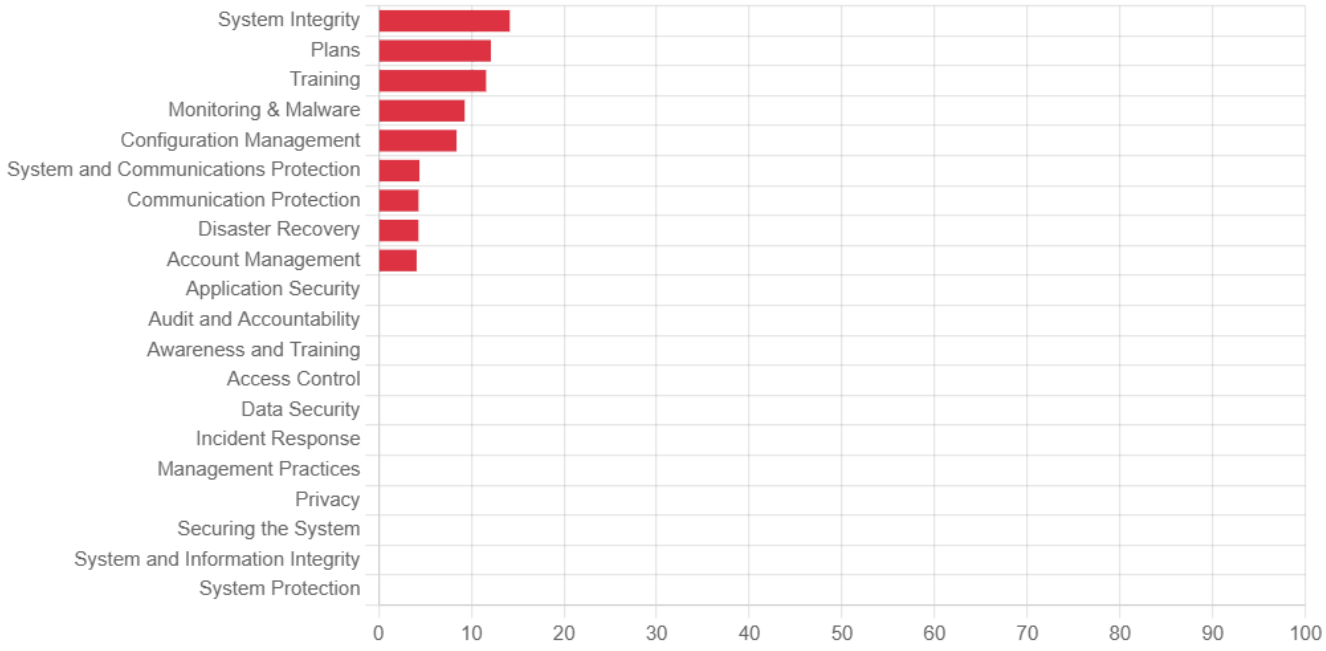
	Confidentiality	Integrity	Availability
Overall Values	Low	Low	Low

Document Library

Title	File Name
	There are no documents to display

Ranked Categories

This chart ranks the top areas of concern based on a weighted risk score. The percentages are calculated by assigning higher weights to requirements that, if not implemented, would make the system more vulnerable to easier attacks. Lower weights are assigned to requirements associated with more difficult attacks.



Summary of Ranked Questions

Each question that did not meet the required Security Assurance Level (SAL) is shown in ranking order below. The displayed levels are the SALs applicable to that question. They are: Low (L), Moderate (M), High (H), and Very High (VH). CNSSI levels are for Confidentiality (C), Integrity (I), and Availability (A). DoD Instruction 8500.2 levels are for Confidentiality (Conf) and Mission Assurance Category (MAC). They are: Classified (C), Sensitive (S), and Public (P) for Confidentiality; MAC I, II, and III for Mission Assurance Category.

Rank: 1	Access Control #2	Level: Low
Does the organization restrict privileged accounts on the information system to organization-defined personnel or roles?		No

Rank: 2	Configuration Management #1	Level: Low
Does the organization define the frequency to review and update configuration management procedures?		No

Rank: 3	Configuration Management #5	Level: Low
Does the organization review and update the information system component inventory per organization-defined frequency?		No

Rank: 4	System and Information Integrity #1	Level: Low
Does the organization monitor the information system to detect unauthorized network connections?		No

Rank: 5	Application Security #4	Level: Low
Does the organization's software inventory include the title, publisher, install date, and business purpose?		No

Rank: 6	Application Security #5	Level: Low

Is the software inventory reviewed and updated?	No

Rank: 7	Application Security #6	Level: Low
Does the organization ensure that only currently supported software is designated as authorized in the software inventory?		No

Rank: 8	Application Security #7	Level: Low
Does the organization document an exception with mitigating controls and risk acceptance for unsupported but necessary software?		No

Rank: 9	Application Security #8	Level: Low
Does the organization designate software without exception documentation as unauthorized?		No

Rank: 10	Application Security #9	Level: Low
Does the organization review their software list to verify software support?		No

Rank: 11	Data Security #6	Level: Low
Does the organization establish and maintain a data inventory?		No

Rank: 12	Data Security #8	Level: Low
Is the data inventory reviewed and updated at a defined time?		No

Rank: 13	Data Security #1	Level: Low
Are data access control lists configured based on user's need to know?		No

Rank: 14	Data Security #2	Level: Low
Does the organization apply permissions to local and remote file systems, databases, and applications?		No

Rank: 15	Data Security #5	Level: Low
Does the data retention process include both minimum and maximum timelines?		No

Rank: 16	Configuration Management #3	Level: Low
Is the configuration process for network devices reviewed and updated at a defined frequency or after significant changes?		No

Rank: 17	Configuration Management #4	Level: Low
Does the organization implement and manage a host-based firewall or port-filtering tool on end-user devices?		No

Rank: 18	Account Management #3	Level: Low
Does the organization establish and maintain an inventory of all accounts managed?		No

Rank: 19	Account Management #4	Level: Low
Does the account inventory include the person's name, username, start/stop dates, and department?		No

Rank: 20	Account Management #6	Level: Low
Does the organization require unique passwords for all assets?		No

Rank: 21	Application Security #2	Level: Low
Is the vulnerability management process reviewed at a defined frequency or with significant changes?		No

Rank: 22	Application Security #1	Level: Low
Is the remediation strategy reviewed at a defined frequency?		No

Rank: 23	Audit and Accountability #3	Level: Low
Does the organization establish and maintain an audit log management process?		No

Rank: 24	Audit and Accountability #4	Level: Low
Is the audit log management plan reviewed at a defined frequency or when significant changes occur?		No

Rank: 25	Audit and Accountability #2	Level: Low
Does the organization ensure that logging destination have adequate storage determined by the management plan?		No

Rank: 26	System and Communications Protection #2	Level: Low
Does the organization only use the latest version of browsers and email clients provided via the vendor?		No

Rank: 27	System and Communications Protection #3	Level: Low
Does the organization use DNS filtering on all assets to block malicious domains?		No

Rank: 28	Monitoring & Malware #1	Level: Low
Does the organization configure automatic updates for anti-malware signature files on all assets?		No

Rank: 29	Data Security #14	Level: Low
Is the data recovery process reviewed at a defined time or when significant changes occur?		No

Rank: 30	Data Security #16	Level: Low
Does the organization perform automated backups of in-scope assets?		No

Rank: 31	Training #4	Level: Low
Does the organization train workforce members on authentication best practices?		No

Rank: 32	Training #7	Level: Low
Does the organization train workforce members on how to identify and properly store, transfer, archive, and destroy sensitive data?		No

Rank: 33	Training #5	Level: Low
Does the organization train workforce members to be aware of causes for unintentional data exposure?		No

Rank: 34	Training #8	Level: Low
Does the organization train workforce to understand how to verify and report out-of-date software patches or any failures in automated processes and tools?		No

Rank: 35	Privacy #1	Level: Low
Does the organization establish and maintain an inventory of service providers?		No

Rank: 36	Privacy #2	Level: Low
Does the service provider inventory include all known providers, classifications, and designate a contact for each?		No

Rank: 37	Privacy #3	Level: Low
Is the service provider inventory reviewed at a defined frequency or with significant changes?		No

Rank: 38	Securing the System #3	Level: Low
Does the organization deploy a network intrusion prevention solution where appropriate?		No

Rank: 39	Plans #1	Level: Moderate
Does the organization have a Configuration Management Plan?		No

Rank: 40	System Integrity #2	Level: Moderate
Are documented practices followed for threat and vulnerability management activities?		No

Rank: 41	Monitoring & Malware #2	Level: Low
Are antivirus and malware prevention tools documented and implemented?		No

Rank: 42	Configuration Management #6	Level: Low
Does the organization maintain an asset inventory of all systems connected to the network and network devices?		No

Rank: 43	System Integrity #1	Level: Low
Does the organization deploy automated patch management tools and software update tools for operating system and software/applications on all systems for which such tools are available and safe?		No

Rank: 44	System and Communications Protection #1	Level: Low
Does the organization ensure that only fully supported web browsers and email clients are allowed in the organization?		No

Rank: 45	Communication Protection #2	Level: Low
Does the organization place application firewalls in front of critical servers to verify and validate the traffic going to the server?		Unanswered

Rank: 46	Disaster Recovery #1	Level: Low
Does the organization ensure that each system is automatically backed up on at least a weekly basis, and more often for systems storing sensitive information?		No

Rank: 47	Account Management #1	Level: Low
Does the organization establish and follow a process for revoking system access by disabling accounts immediately upon termination of an employee or contractor?		No

Rank: 48	Training #1	Level: Low
Does the organization have a security awareness program?		No

Rank: 49	Configuration Management #8	Level: Low
Does the network asset inventory also include information on whether the device is portable and/or personal device?		No

Rank: 50	Training #2	Level: Low
Are the training materials for the security awareness program updated at least annually?		No

Rank: 51	Training #3	Level: Low
Is the security awareness program mandatory for all employees?		No

Questions Comments

Communication Protection #2		
Question:	Does the organization place application firewalls in front of critical servers to verify and validate the traffic going to the server?	Unanswered
Comment:	Partialized, from network yes, no in the local windows or linux firewall.	

Alternate Justification

There are no questions with alternate justifications to display.

Questions Marked for Review

There are no questions marked for review.