

SITE DETAIL REPORT

CONTROL SYSTEMS CYBER SECURITY EVALUATION



Homeland
Security

High Level Cyber Security Assessment

2/1/2012

Assessor: J. Doe

Disclaimer

This report is provided “as is” for informational purposes only. The Department of Homeland Security (DHS) 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 or not based upon warranty, contract, tort, or otherwise, whether or not injury was sustained from, or arose out of the results of, or reliance upon the report.

The DHS 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 DHS.

The display of the DHS official seal or other DHS 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 the Department of Homeland Security. The DHS seal, insignia, or other visual identities shall not be used in any manner to imply endorsement of any commercial product or activity by DHS or the United States Government. Use of the DHS seal without proper authorization violates federal law (e.g., 18 U.S.C. §§ 506, 701, 1017), and is against DHS’s 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

CSET® is only one component of the overall cyber security 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.

TABLE OF CONTENTS

Table Of Contents..... 4

Assessment Information.....5

Description of Assessment.....6

Executive Summary..... 6

Evaluation Against Selected Standards and Question Sets..... 8

Standards Compliance.....9

Findings And Recommendations From Basic Network Analysis.....10

Security Assurance Level (Sal) 11

Document Library..... 12

Ranked Subject Areas.....13

Summary Of Ranked Questions.....14

Question Comments And Marked For Review..... 16

Alternate Justification Comments.....17

Question Details: Key Questions..... 18

ASSESSMENT INFORMATION

Assessment Name: High Level Cyber Security Assessment

Assessment Date, (MM/DD/YYYY): 2/1/2012

Facility Name: ABC Manufacturing - Complex A

City or Site Name: Industry City

State, Province or Region: CA

Principal Assessor Name: J. Doe

Assessor E-mail: j.doe@abcm.com

Assessor Telephone: (555) 555-1212

Additional Notes and Comments:

Contact(s):

J.T. Langill
ICS Cyber Security Specialist
SCADAhacker
Outside Consultant

DESCRIPTION OF ASSESSMENT

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.

The compliance summary charts below provide a high level overview of assessment results. The Summary Percent Compliance chart shows overall security status as well as a breakdown between compliance to selected standards (known as administrative) and compliance of those components depicted on the network diagram. The next two sets of graphs provide greater detail on compliance to selected standards and component compliance.

The Areas of Concern - Top Subject and Question section lists the five areas of greatest vulnerability. Addressing these areas quickly will provide the greatest return on investment.

EXECUTIVE SUMMARY

Enterprise Evaluation Executive Summary

This analysis identifies the cybersecurity posture of Industry City, CA. The review evaluated the business systems to identify what is performed well, what can be improved, and suggests options for consideration.

The approach used in reviewing Industry City, CA's cyber systems was the Enterprise Evaluation (EE), which includes a series of questions organized in ten categories derived from international, audit community, and federal government standards, and guidelines. The findings are presented based on the responses provided during the review. Notable Good Practices represent those practices of the organization that are areas of excellence. Most Critical Aspects for Improvement represent those issues that the organization should consider remedying immediately to mitigate vulnerabilities and minimize consequences of an egregious security breach. Moderately Critical Aspects for Improvement represent those issues that the organization should consider remedying in the near future in order to mitigate vulnerabilities and minimize consequences of a security breach. Finally, Least Critical Aspects for Improvement represent those issues that the organization should consider to improve security policies or incorporate generally accepted good practices.

This report does not make recommendations as to what should be changed. Instead, the report attempts to identify both notable good practices in place at Industry City, CA as well as gaps between current practices and what is possible with appropriate resources. Industry City, CA should conduct (or reevaluate) a risk assessment to determine if any gaps should be mitigated and to what extent. This assessment should be used to support risk-based decisions on policies, plans, procedures, and business systems operations.

EE is a vulnerability assessment rather than a risk assessment. Cyber vulnerabilities can often be mitigated through physical and human security measures. Given this reality, Industry City, CA should employ a robust risk management program that not only addresses threats, vulnerabilities, and consequences via cyber means, but also physical and human aspects. For example, while issues such as the lockout of accounts are (and remain) vulnerabilities, their effects are reduced by the defense-in-depth approach of the physical and human security measures in place.

Cyber Threat: Malicious actors are increasingly acquiring information technology skills to potentially launch a cyber attack on the U.S. infrastructure. Cyber intruder groups already possess the necessary skills to launch a successful cyber attack and may be "talent-for-hire" available to terrorists, criminal organizations, and nation states. Attackers do not need to be technically savvy because free and commercial automated tools are simplifying attack methods.

Consequence of Attack On or Exploitation of Systems and Networks: If the business systems at this organization were compromised, the result could include the loss of sensitive data (e.g., intellectual capital, personal and health information) and the disruption of business operations. In addition, a compromise could provide a platform from which the process control network is attacked. Or, these networks could be exploited by malicious actors to attack other computers, facilities, and critical infrastructure through botnets.

Cybersecurity Posture (Vulnerability): A successful attack on the business systems is feasible through the Internet or other external connections (e.g., modems, wireless, portable devices, and media).

Company- or facility-specific information is often available on the Internet, and tools are readily available that automate search techniques for connections (e.g., Internet, wireless, and modems). Moreover, mature cyber attack tools (also available on the Internet) make common vulnerabilities easy to exploit by moderately skilled malicious actors unless perimeter security devices are properly configured and kept up to date (e.g., unless the option is turned off, firewalls will respond to reconnaissance attempts with information

that enables cyber attack). An estimated ten new cyber vulnerabilities are discovered every day.

A common approach to cybersecurity is to secure the perimeter, leaving the internal network as a trusted environment. The actions of insiders (intentional or unintentional) then become an issue of concern. Unfortunately, unintentional consequences, introduced to systems through good intentions of trusted insiders, are known to have caused disruptions of operational business systems. In addition, system and network vulnerabilities are becoming more widely known and trends show that untargeted attacks, such as viruses, worms, and Trojans, are more prevalent. By opening e-mail attachments or visiting compromised web-sites, unsuspecting users can introduce malicious code to otherwise well-managed systems and networks.

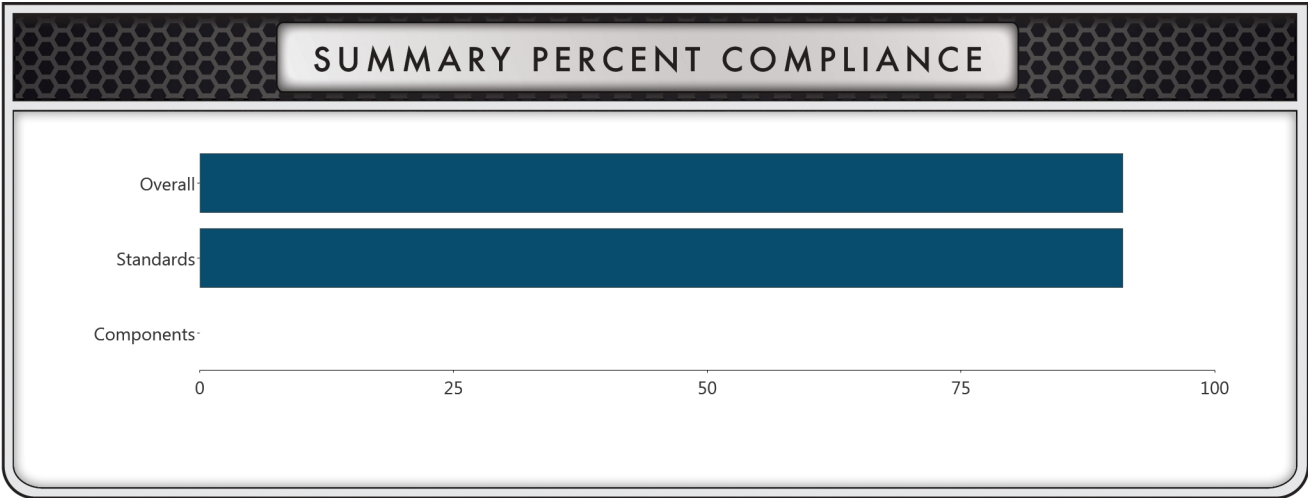
Resources are available to assist in understanding and resolving consequential cyber attacks and incidents. Among them is the United States Computer Emergency Readiness Team (US-CERT), which, in partnership with the Multi-State Information Sharing and Analysis Center (MS-ISAC), published an information paper titled “Current Malware Threats and Mitigation Strategies,” May 16, 2005. The following is an excerpt that summarizes the concern: “The nature of malicious code, or malware, (e.g., viruses, worms, bots) shifted recently... to actively seeking financial gain... [and] unfortunately, attackers have become very adept at circumventing traditional defenses such as anti-virus software and firewalls... Botnets are often the focal point for collecting the confidential information, launching Denial of Service attacks, and distributing SPAM. A bot, short for robot, is an automated software program that can execute certain commands. A botnet, short for robot network, is an aggregation of computers compromised by bots that are connected to a central ‘controller.’ ... Botnets controlling tens of thousands of compromised hosts are common...” (Source: http://www.us-cert.gov/reading_room/malware-threats-mitigation.pdf; additional information can be found at the US-CERT home: <http://www.uscert.gov/>).

Cybersecurity practices that are performed well by Industry City, CA include: [Please insert the 3 or 4 sections that are of least concern here based on results from the Detailed Findings section of the report].

Several areas of concern make possible a successful cyber attack by malicious actors or a serious cyber incident. These include: [Please insert the 3 or 4 sections that are of greatest concern here based on results from the Detailed Findings section of the report].


Industry City, CA’s most critical gaps are: [Please insert the Most Critical Aspects for Improvement here based on results from the Summary of Gaps and Options for Consideration section at the end of the report].

Company Comments
[Insert the most relevant high-level comments provided throughout the assessment here.]

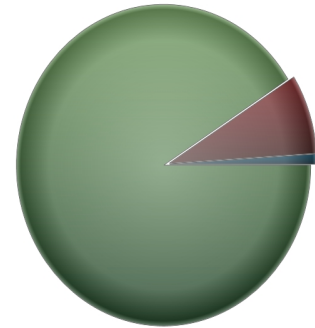


Evaluation Against Selected Standards and Question Sets

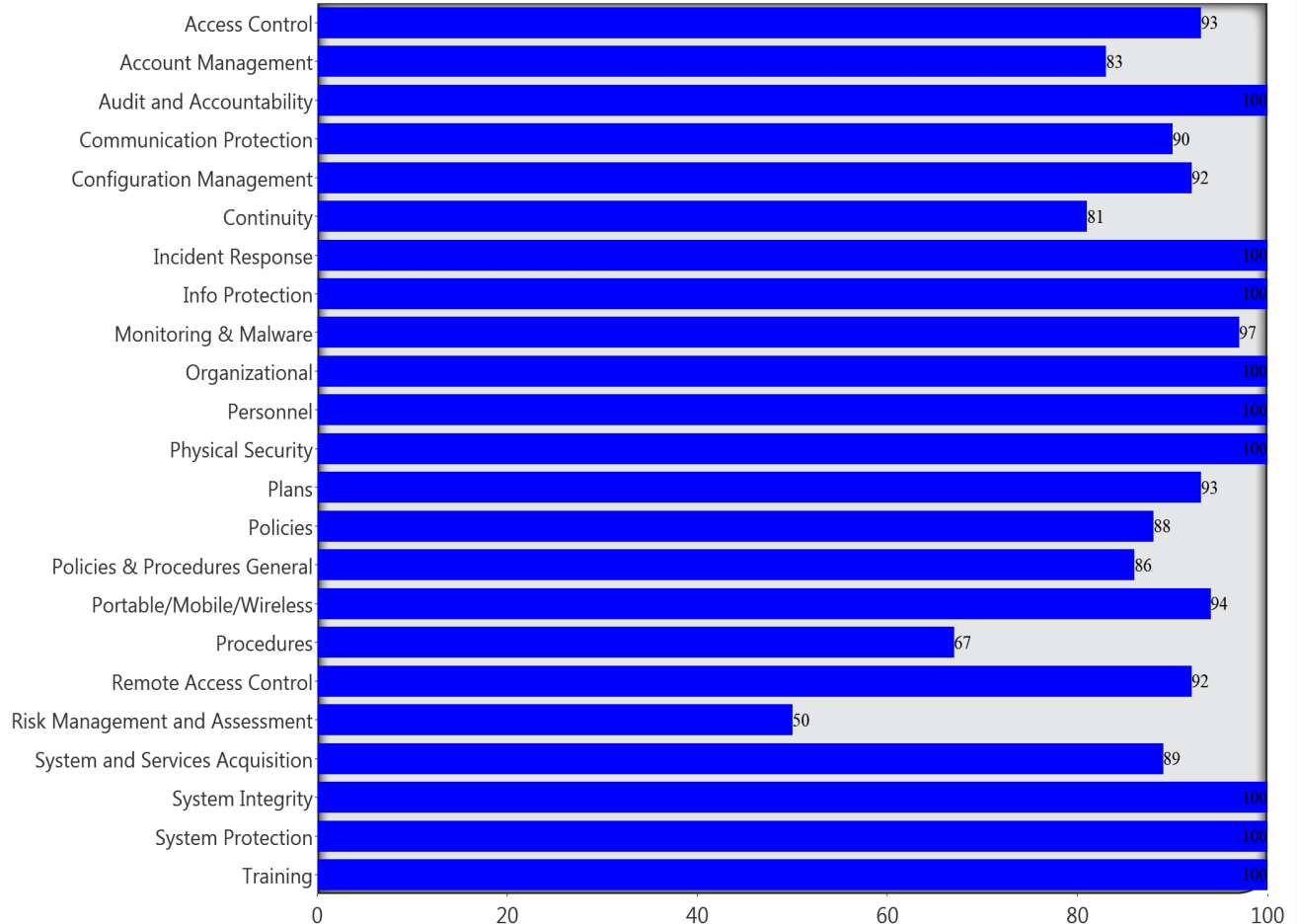
STANDARD OR QUESTION SET

 Key Questions

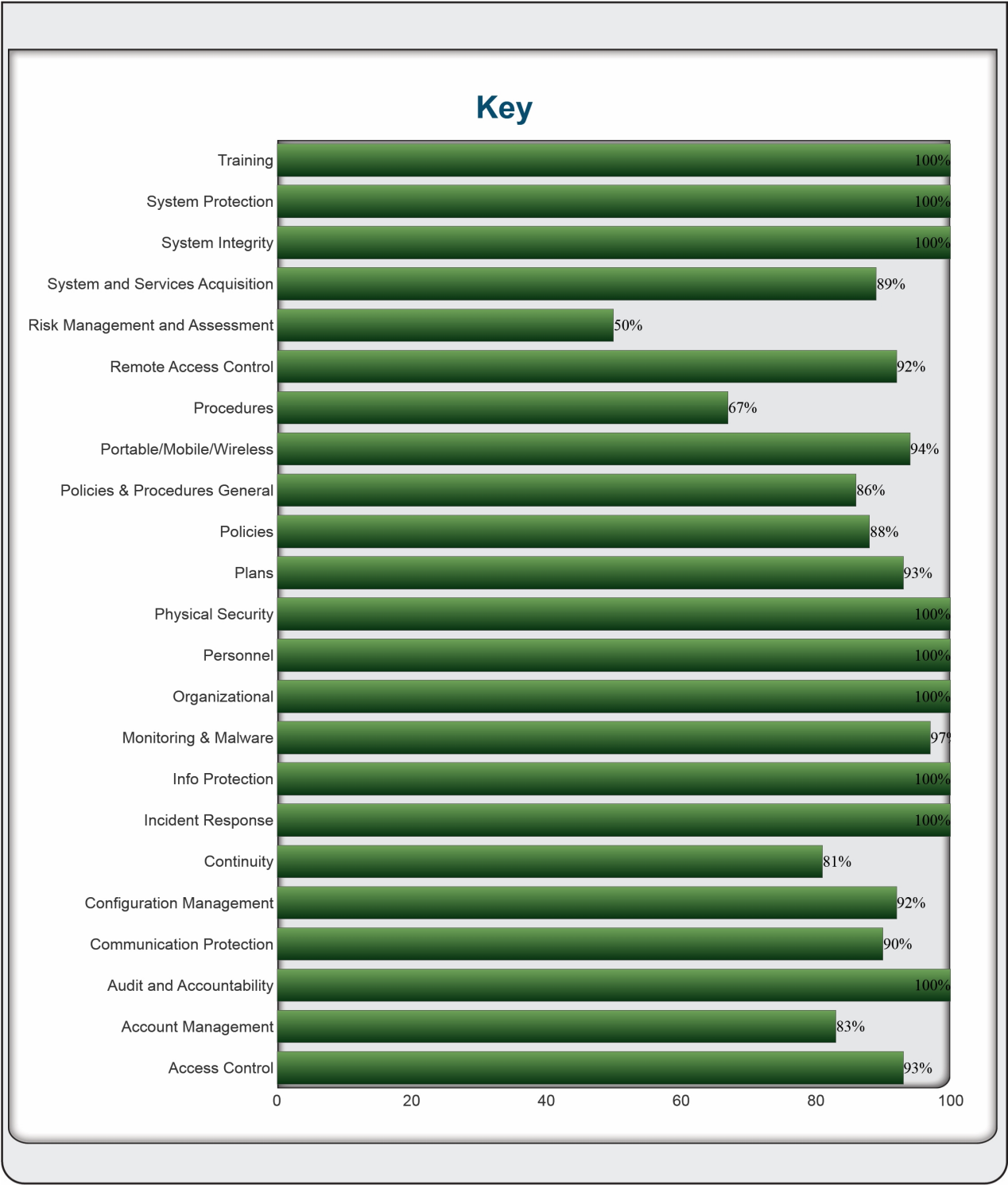
STANDARDS SUMMARY



 Yes 91
  No 8
  NA 0
  Unanswered 1



STANDARDS COMPLIANCE



FINDINGS AND RECOMMENDATIONS FROM BASIC NETWORK ANALYSIS

There are no findings or recommendations to display.

SECURITY ASSURANCE LEVEL (SAL)

Calculated Level

Moderate

	Confidentiality	Integrity	Availability
Overall Values	Moderate	Moderate	Moderate

Calculated General Security Assurance Levels

	Onsite	Offsite
Physical Injury	None	None
Hospital Injury	None	None
Death	None	None
Capital Assets	None	None
Economic Impact	None	None
Environmental Impact	None	None

NIST SP800-60 (FIPS 199) Based Security Assurance Levels

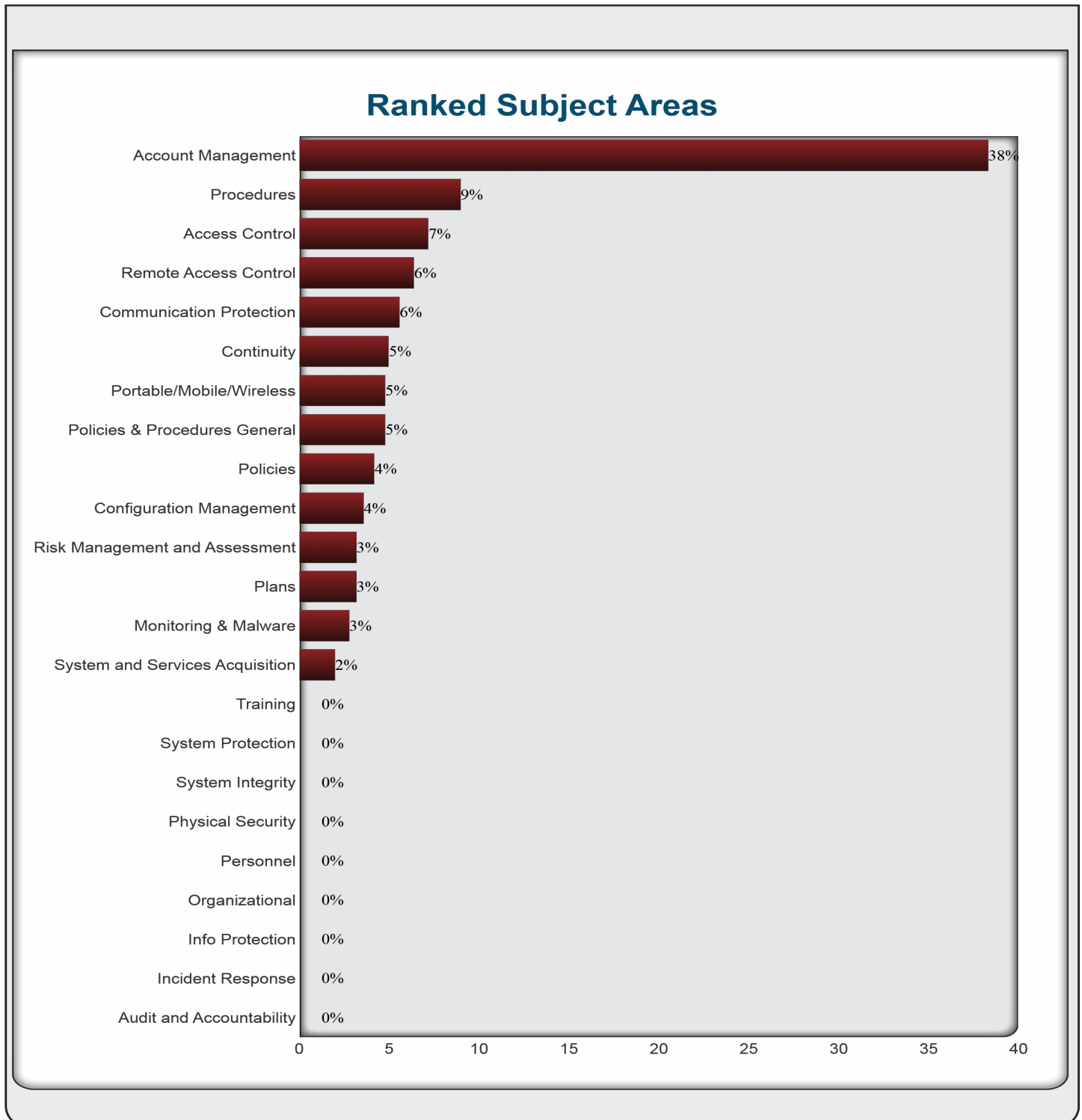
	Confidentiality	Integrity	Availability
Adjusted For System Questions	None	None	None
Information Type	None	None	None

DOCUMENT LIBRARY

Title	File Name
	There are no documents to display.

RANKED SUBJECT AREAS

This chart shows subject areas needing the most attention. Each bar represents the labeled subject area's weighted contribution so that the combined total always equals 100%. The weighted contribution includes the importance of both the question and the subject area, as well as the percentage of missed questions in that subject area.



SUMMARY OF RANKED QUESTIONS

Each question that did not meet the required security assurances level is shown in ranking order below:

Rank: 1	Access Control #9	Level: L
Do the password policies stipulate rules of complexity, based on the criticality level of the systems to be accessed?		No
Rank: 2	Account Management #28	Level: L
Is there an official assigned to authorize a user or device identifier?		No
Rank: 3	Account Management #29	Level: L
Are identifiers selected that uniquely identify an individual or device?		No
Rank: 4	Account Management #30	Level: L
Are the user identifiers assigned to the intended party or the device identifier to the intended device?		No
Rank: 5	Account Management #31	Level: L
Are previous user or device identifiers archived?		No
Rank: 6	Account Management #10	Level: M
Are automated mechanisms such as active directory used to support the management of system accounts?		No
Rank: 7	Account Management #11	Level: M
Does the system automatically terminate temporary and emergency accounts after a defined time period for each type of account?		No
Rank: 8	Remote Access Control #9	Level: M
Is remote access for privileged commands and security-relevant information authorized only for compelling operational needs and is the rationale for such access documented?		No
Rank: 9	Communication Protection #8	Level: L
Do communication cryptographic mechanisms comply with applicable regulatory requirements, policies, standards, and guidance?		No
Rank: 10	Policies & Procedures General #6	Level: L
Are security policies and procedures implemented to define roles, responsibilities, behaviors, and practices of an overall security program?		Unanswered
Rank: 11	Procedures #5	Level: L
Awareness and Training Procedure		No

Rank: 12	Portable/Mobile/Wireless #11	Level: M
Are unauthorized remote connections to the system monitored, including scanning for unauthorized mobile or wireless access points on a defined frequency and is appropriate action taken if an unauthorized connection is discovered?		No
Rank: 13	Continuity #11	Level: M
Is there transaction recovery for systems that are transaction-based?		No
Rank: 14	Plans #6	Level: L
Does the security plan align with the organization's enterprise architecture?		Unanswered
Rank: 15	Risk Management and Assessment #2	Level: L
Are the system connections monitored on an ongoing basis verifying enforcement of documented security requirements?		No
Rank: 16	Policies #1	Level: L
System Security Policy		Unanswered
Rank: 17	Procedures #2	Level: L
Security Procedure		No
Rank: 18	Continuity #1	Level: M
Are necessary communications for the alternate control center identified, and are agreements in place to permit the resumption of system operations for critical functions within a defined time period when the primary control center is unavailable?		No
Rank: 19	Continuity #2	Level: M
Is an alternate control center identified that is geographically separated from the primary control center?		No
Rank: 20	Configuration Management #6	Level: M
Are configuration-managed changes to the system audited?		No
Rank: 21	Monitoring & Malware #12	Level: M
Is the system updated to address any identified vulnerabilities in accordance with the system maintenance policy?		No
Rank: 22	System and Services Acquisition #3	Level: L
Are developmental and evaluation-related assurance requirements (acceptance testing, compliance documentation) included in system acquisition contracts based on an assessment of risk?		No

QUESTION COMMENTS AND MARKED FOR REVIEW

Question:	There are no questions with comments to display.	
Comment:		

ALTERNATE JUSTIFICATION COMMENTS

Question:	There are no questions with alternate justifications to display.	
Alternate Justification:		

QUESTION DETAILS: KEY QUESTIONS

Access Control #1	Are appropriate agreements finalized before access is granted, including for third parties and contractors?	Yes
Access Control #2	Are access agreements periodically reviewed and updated?	Yes
Access Control #3	Does the system enforce assigned authorizations for controlling electronic access to the system?	Yes
Access Control #4	Does the system employ authentication methods that meet the requirements of applicable policies, standards, and guidance for authentication to a cryptographic module?	Yes
Access Control #5	If your authentication encryption module fails can you still authenticate without creating a denial of service that impacts operational performance of system?	Yes
Access Control #6	Does the system employ multifactor authentication for network access and for access to privileged accounts?	Yes
Access Control #7	Is the concept of least privilege used to accomplish assigned tasks?	Yes
Access Control #8	Are there policies and procedures concerning the generation and use of passwords?	Yes
Access Control #9	Do the password policies stipulate rules of complexity, based on the criticality level of the systems to be accessed?	No
Access Control #10	Does the system prevent further access to the system by initiating a session lock after a defined time period of inactivity or a user initiated session lock?	Yes
Access Control #11	Does the system retain the session lock until the user re-establishes access using appropriate identification and authentication procedures?	Yes
Access Control #12	Has a signed acknowledgment been obtained from users indicating that they have read, understand, and agree to abide by the rules of behavior before authorizing access to the system?	Yes
Access Control #13	Does the system uniquely identify and authenticate organizational users?	Yes
Access Control #14	Does the system employ multifactor authentication for remote access?	Yes
Account Management #1	Are system accounts identified by account type and managed?	Yes
Account Management #2	Do system accounts have conditions for group membership?	Yes
Account Management #3	Are the access rights and privileges specified, and are authorized users identified for system accounts?	Yes
Account Management #4	Are appropriate approvals required for requests to establish accounts?	Yes
Account Management #5	Are system accounts authorized, established, activated, modified, disabled, and removed?	Yes
Account Management #6	Are system accounts reviewed on a defined frequency?	Yes
Account Management #7	Is the use of guest/anonymous accounts specifically authorized and monitored?	Yes
Account Management #8	Are account managers notified when system users are terminated; transferred, or system usage or need-to-know/need-to-share changes?	Yes

Account Management #9	Is access to the system granted based on a valid need-to-know or need-to-share as determined by official duties and satisfying all security criteria?	Yes
Account Management #10	Are automated mechanisms such as active directory used to support the management of system accounts?	No
Account Management #11	Does the system automatically terminate temporary and emergency accounts after a defined time period for each type of account?	No
Account Management #12	Does the system automatically disable inactive accounts after a defined time period?	Yes
Account Management #13	Does the system automatically audit account creation, modification, disabling, and termination actions and notify appropriate individuals?	Yes
Account Management #14	Are currently active system accounts reviewed on a defined frequency to verify that temporary accounts and accounts of terminated or transferred users have been deactivated?	Yes
Account Management #15	Are user account names different than email user accounts?	Yes
Account Management #16	Is there a mechanism in place to verify the identity whenever an authenticator (password, token) is created, distributed, or modified?	Yes
Account Management #17	Do authenticators have sufficient strength of mechanism for their intended use?	Yes
Account Management #18	Are there administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators? (e.g., passwords, tokens, cards, etc.)	Yes
Account Management #19	Is the default content of authenticators changed on system installation?	Yes
Account Management #20	Are there minimum and maximum lifetime restrictions and reuse conditions for authenticators?	Yes
Account Management #21	Are authenticators changed or refreshed periodically as appropriate for authenticator type?	Yes
Account Management #22	Is authenticator content protected from unauthorized disclosure and modification? (i.e., not transmitting over email as open text)	Yes
Account Management #23	Are users required to take, and devices implement, specific measures to safeguard authenticators?	Yes
Account Management #24	Are certificates validated for PKI-based authentication by constructing a certification path with status information to an accepted trust anchor?	Yes
Account Management #25	Is the registration process to receive a user authenticator carried out in person before a designated registration authority?	Yes
Account Management #26	Does the system enforce authorized access to the corresponding private key for PKI-based authentication?	Yes
Account Management #27	Does the system map the authenticated identity to the user account for PKI-based authentication?	Yes
Account Management #28	Is there an official assigned to authorize a user or device identifier?	No
Account Management #29	Are identifiers selected that uniquely identify an individual or device?	No
Account Management #30	Are the user identifiers assigned to the intended party or the device identifier to the intended device?	No

Account Management #31	Are previous user or device identifiers archived?	No
Account Management #32	Is access to a defined list of security functions and security-relevant information explicitly authorized?	Yes
Account Management #33	Are users of system accounts with access to a defined list of security functions or security-relevant information required to use nonprivileged accounts when accessing other system functions?	Yes
Account Management #34	Is there a division of responsibilities and separation of duties of individuals to eliminate conflicts of interest?	Yes
Account Management #35	Is the separation of duties implemented through assigned system access authorizations?	Yes
Audit and Accountability #1	Are system audit records reviewed and analyzed on a defined frequency, and are findings reported to designated officials?	Yes
Audit and Accountability #2	Is the level of audit review, analysis, and reporting within the system adjusted when a change in risk exists?	Yes
Audit and Accountability #3	Is there a frequency of auditing for each identified auditable event?	Yes
Audit and Accountability #4	Is the security audit function coordinated with other organizational entities requiring audit-related information?	Yes
Audit and Accountability #5	Are auditable events adequate to support after-the-fact investigations of security incidents?	Yes
Audit and Accountability #6	Are the events to be audited adjusted within the system based on current threat information and ongoing assessments of risk?	Yes
Audit and Accountability #7	Is the list of defined auditable events reviewed and updated on a defined frequency?	Yes
Audit and Accountability #8	Is execution of privileged functions (account creations, modifications, and object permission changes) included in the list of events to be audited by the system?	Yes
Communication Protection #1	Does the system monitor and manage communications at the system boundary and at key internal boundaries within the system?	Yes
Communication Protection #2	Are the number of access points to the system limited to allow for better monitoring of inbound and outbound network traffic?	Yes
Communication Protection #3	Is the external communication interface connections implemented with security measures appropriate to the required protection of the integrity and confidentiality of the information being transmitted?	Yes
Communication Protection #4	Does the system deny network traffic by default and allow network traffic by exception?	Yes
Communication Protection #5	Does the system prevent remote devices that have established connections (e.g., PLC, remote laptops) with the system from communicating outside that communications path with resources on uncontrolled/unauthorized networks?	Yes
Communication Protection #6	Do you encrypt communication over all untrusted communication channels?	Yes
Communication Protection #7	Are cryptographic keys established and managed using automated mechanisms?	Yes
Communication Protection #8	Do communication cryptographic mechanisms comply with applicable regulatory requirements, policies, standards, and guidance?	No

Communication Protection #9	Does the system provide mechanisms to protect the authenticity of device-to-device communications sessions?	Yes
Communication Protection #10	Does the system prevent unauthorized or unintended information transfer via shared system resources? (e.g., register, main memory, secondary storage)	Yes
Configuration Management #1	Has a current baseline configuration been developed, documented, and maintained for the system?	Yes
Configuration Management #2	Is the baseline configuration of the system reviewed and updated?	Yes
Configuration Management #3	Is there an inventory of systems and critical components and is it maintained?	Yes
Configuration Management #4	Are changes to the system authorized and documented?	Yes
Configuration Management #5	Are records of configuration-managed changes to the system reviewed and retained?	Yes
Configuration Management #6	Are configuration-managed changes to the system audited?	No
Configuration Management #7	Has an inventory of the components of the system been developed, documented and maintained that accurately reflects the current system?	Yes
Configuration Management #8	Has an inventory list of the components of the system been developed, documented, and maintained that is consistent with the system boundary?	Yes
Configuration Management #9	Has an inventory list of the components of the system been developed, documented, and maintained that is at the level of granularity deemed necessary for tracking and reporting?	Yes
Configuration Management #10	Has an inventory of the components of the system been developed, documented, and maintained that includes defined information deemed necessary to achieve effective property accountability?	Yes
Configuration Management #11	Is the inventory of system components and programming updated as an integral part of component installation, replacement, and system updates?	Yes
Configuration Management #12	Are all factory default authentication credentials changed on system components and applications upon installation?	Yes
Continuity #1	Are necessary communications for the alternate control center identified, and are agreements in place to permit the resumption of system operations for critical functions within a defined time period when the primary control center is unavailable?	No
Continuity #2	Is an alternate control center identified that is geographically separated from the primary control center?	No
Continuity #3	Are potential accessibility problems to the alternate control center identified in the event of an area-wide disruption or disaster and are explicit mitigation actions outlined?	Yes
Continuity #4	Are alternate control center agreements in place that contain priority-of-service provisions in accordance with the availability requirements?	Yes
Continuity #5	Does the alternate processing site provide information security measures equivalent to that of the primary site?	Yes
Continuity #6	Is normal operation of the system resumed in accordance with its policies and procedures after a security event?	Yes
Continuity #7	Does the continuity of operations plan address the issue of maintaining or re-establishing production in case of an undesirable interruption for the system?	Yes
Continuity #8	Do designated officials review and approve the continuity of operations plan?	Yes

Continuity #9	Does the continuity of operations plan delineate that at the time of the disruption to normal system operations, the organization executes its incident response policies and procedures to place the system in a safe configuration and initiates the necessary notifications to regulatory authorities?	Yes
Continuity #10	Is there a capability to recover and reconstitute the system to a known secure state after a disruption, compromise, or failure?	Yes
Continuity #11	Is there transaction recovery for systems that are transaction-based?	No
Continuity #12	Are backups of critical system software, applications, and data created and secured?	Yes
Continuity #13	Are backups of user-level information contained in the system performed on a defined frequency? (user account)	Yes
Continuity #14	Are backups of system-level information contained in the system performed on a defined frequency?	Yes
Continuity #15	Is the confidentiality and integrity of backup information protected at the storage location?	Yes
Continuity #16	Is backup information periodically tested to verify media reliability and information integrity?	Yes
Incident Response #1	Is an incident handling capability implemented for security incidents that include preparation, detection and analysis, containment, eradication, and recovery?	Yes
Incident Response #2	Are incident handling activities coordinated with contingency planning activities?	Yes
Incident Response #3	Are lessons learned from ongoing incident handling activities incorporated into incident response procedures?	Yes
Incident Response #4	Are automated mechanisms used to administer and support the incident handling process and to assist in the reporting of security incidents?	Yes
Incident Response #5	Is a root cause analysis initiated for the security events and any findings from the analysis submitted to the organizations corrective action program?	Yes
Info Protection #1	Do only authorized users have access to information in printed form or on digital media?	Yes
Info Protection #2	Are automated mechanisms (e.g., card or keypad entry) used to ensure and audit authorized access to media storage areas?	Yes
Info Protection #3	Is removable system media and system output marked indicating the distribution limitations, handling caveats, and applicable security markings?	Yes
Info Protection #4	Is there a list of media types or hardware components that is exempt from marking as long as the exempted items remain within the organization-defined protected environment?	Yes
Info Protection #5	Is the system media securely stored within protected areas?	Yes
Info Protection #6	Does the sensitivity of the material determine how the media are stored?	Yes
Monitoring & Malware #1	Does the system protect against or limit the effects of denial-of-service attacks based on a defined list of types of denial-of-service attacks?	Yes
Monitoring & Malware #2	Are malicious code protection mechanisms used at system entry and exit points and at workstations, servers, or mobile computing devices?	Yes
Monitoring & Malware #3	Are malicious code protection mechanisms updated whenever new releases are available in accordance with configuration management policy and procedures?	Yes

Monitoring & Malware #4	Are malicious code protection mechanisms configured to perform periodic scans of the system on a defined frequency and real-time scans of files from external sources as the files are downloaded, opened, or executed, and disinfect and quarantine infected files?	Yes
Monitoring & Malware #5	Are malicious code protection software products from multiple vendors used?	Yes
Monitoring & Malware #6	Are the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system addressed?	Yes
Monitoring & Malware #7	Are malicious code protection mechanisms centrally managed?	Yes
Monitoring & Malware #8	Does the system automatically update malicious code protection mechanisms?	Yes
Monitoring & Malware #9	Does the system prevent users from circumventing host-based malicious code protection capabilities?	Yes
Monitoring & Malware #10	Does the use of mechanisms to centrally manage malicious code protection avoid degradation of the operational performance of the system?	Yes
Monitoring & Malware #11	Are periodic security vulnerability assessments conducted according to the risk management plan?	Yes
Monitoring & Malware #12	Is the system updated to address any identified vulnerabilities in accordance with the system maintenance policy?	No
Monitoring & Malware #13	Are events on the system monitored?	Yes
Monitoring & Malware #14	Are system attacks detected? (Attacks can be detected via log monitoring, IDS system monitoring, Signature/indicators)	Yes
Monitoring & Malware #15	Is unauthorized use of the system identified? (e.g., log monitoring)	Yes
Monitoring & Malware #16	Are monitoring devices deployed strategically to collect essential information within the system to track specific types of transactions of interest?	Yes
Monitoring & Malware #17	Is the level of system monitoring activity heightened whenever an indication of increased risk exists?	Yes
Monitoring & Malware #18	Is legal counsel consulted with regard to system monitoring activities?	Yes
Monitoring & Malware #19	Are automated tools used to support near real-time analysis of events?	Yes
Monitoring & Malware #20	Are automated tools used to integrate intrusion detection tools into access control and flow control mechanisms in support of attack isolation and elimination?	Yes
Monitoring & Malware #21	Does the system monitor inbound and outbound communications for unusual or unauthorized activities or conditions?	Yes
Monitoring & Malware #22	Does the system provide a real-time alert when indications of compromise or potential compromise occur?	Yes
Monitoring & Malware #23	Does the system prevent users from circumventing host-based intrusion detection and prevention capabilities?	Yes
Monitoring & Malware #24	Are spam protection mechanisms used at system entry points and at workstations, servers, or mobile computing devices?	Yes
Monitoring & Malware #25	Are spam protection mechanisms updated when new releases are available in accordance with configuration management policy and procedures?	Yes

Monitoring & Malware #26	Is spam protection software products from multiple vendors used?	Yes
Monitoring & Malware #27	Are vulnerability scans performed for in the system on a defined frequency and randomly in accordance with company policy?	Yes
Monitoring & Malware #28	Are vulnerability scanning tools and techniques used that promote interoperability among tools and automate parts of the vulnerability management process by using standards for: (a) enumerating platforms, software flaws, and improper configurations; (b) formatting and making transparent, checklists, and test procedures; and (c) measuring vulnerability impact?	Yes
Monitoring & Malware #29	Is information obtained from the vulnerability scanning process shared with designated personnel throughout the organization?	Yes
Monitoring & Malware #30	Are vulnerability scanning tools used that include the capability to readily update the list of system vulnerabilities scanned?	Yes
Organizational #1	Are a set of rules that describes the system users responsibilities and expected behavior established and made available?	Yes
Organizational #2	Does the system design and implementation process define the security roles and responsibilities for the users of the system?	Yes
Organizational #3	Are individuals with system security roles and responsibilities identified?	Yes
Organizational #4	Is a senior security officer appointed with the mission and resources to coordinate, develop, implement, and maintain an organization-wide security program?	Yes
Personnel #1	Is a risk designation assigned to all positions and are screening criteria established for individuals filling those positions?	Yes
Personnel #2	Are position risk designations periodically reviewed and revised?	Yes
Personnel #3	Are individuals requiring access screened before access is authorized?	Yes
Physical Security #1	Are lists of personnel with authorized access developed and maintained, and are appropriate authorization credentials issued?	Yes
Physical Security #2	Are the access list and authorization credentials reviewed and approved at least annually and those no longer requiring access removed?	Yes
Physical Security #3	Is hardware (cages, locks, cases, etc.) used to detect and deter unauthorized physical access to system devices?	Yes
Physical Security #4	Is physical access monitored to detect and respond to physical security incidents?	Yes
Physical Security #5	Are physical access logs reviewed on a defined frequency?	Yes
Physical Security #6	Are results of reviews and investigations coordinated with the organization's incident response capability?	Yes
Physical Security #7	Are real-time physical intrusion alarms and surveillance equipment monitored?	Yes
Physical Security #8	Are physical access authorizations enforced for all physical access points to the facility?	Yes
Physical Security #9	Are individual access authorizations verified before granting access to the facility?	Yes
Physical Security #10	Is entry to the facility controlled by physical access devices and/or guards?	Yes
Physical Security #11	Are the areas officially designated as publicly accessible controlled in accordance with the organization's assessment of risk?	Yes
Physical Security #12	Are keys, combinations, and other physical access devices secured?	Yes

Physical Security #13	Are physical access devices inventoried on a periodic basis?	Yes
Physical Security #14	Are combinations and keys changed on a defined frequency, and when keys are lost, combinations compromised, or individuals are transferred or terminated?	Yes
Physical Security #15	Is physical access to distribution and communication lines controlled and verified?	Yes
Physical Security #16	Is physical access to output devices controlled?	Yes
Physical Security #17	Are all external system and communication connections identified and protected from tampering or damage?	Yes
Plans #1	Are the personnel qualification levels reviewed and periodically updated for personnel to make changes, conditions for allowing changes, and the approvals required for changes?	Yes
Plans #2	Security Plan	Yes
Plans #3	Continuity of Operations Plan	Yes
Plans #4	Has a risk management plan been developed?	Yes
Plans #5	Does a senior official review and approve the risk management plan?	Yes
Plans #6	Does the security plan align with the organization's enterprise architecture?	Unanswered
Plans #7	Does the security plan explicitly define the authorization boundary of the system?	Yes
Plans #8	Does the security plan describe the relationships with or connections to other systems?	Yes
Plans #9	Does the security plan provide an overview of the security requirements for the system?	Yes
Plans #10	Does the security plan describe the security controls in place or planned?	Yes
Plans #11	Is the authorizing official or designated representative who reviews and approves the system security plan specified?	Yes
Plans #12	Is the security plan for the system reviewed on a defined frequency, but at least annually?	Yes
Plans #13	Is the security plan revised to address changes to the system/environment or problems identified during plan implementation or security control assessments?	Yes
Plans #14	Does the security plan define and communicate the specific roles and responsibilities in relation to various types of incidents?	Yes
Policies #1	System Security Policy	Unanswered
Policies #2	Configuration Management Policy	Yes
Policies #3	Information and Document Management Policy	Yes
Policies #4	Awareness and Training Policy	Yes
Policies #5	Access Control Policy	Yes
Policies #6	Cryptographic Policy	Yes
Policies #7	Does the system security policy address the purpose of the security program as it relates to protecting the organization's personnel and assets?	Yes

Policies #8	Does the system security policy address the scope of the security program as it applies to all organizational staff and third-party contractors?	Yes
Policies & Procedures General #1	Are there policies and procedures for the classification of data, both electronic and paper media?	Yes
Policies & Procedures General #2	Do the data policies and procedures establish retention policies and procedures for both electronic and paper media?	Yes
Policies & Procedures General #3	Do the data policies and procedures address sharing, copying, transmittal, and distribution appropriate for the level of protection required?	Yes
Policies & Procedures General #4	Do the data policies and procedures establish access to the data based on formally assigned roles and responsibilities for the system?	Yes
Policies & Procedures General #5	Are policies and procedures in place to enforce explicit rules and management expectations governing user installation of software?	Yes
Policies & Procedures General #6	Are security policies and procedures implemented to define roles, responsibilities, behaviors, and practices of an overall security program?	Unanswered
Policies & Procedures General #7	Are security controls for third-party personnel enforced, and is service provider behavior and compliance monitored?	Yes
Portable/Mobile/Wireless #1	Are usage restrictions and implementation guidance established for organization-controlled mobile devices?	Yes
Portable/Mobile/Wireless #2	Is mobile device connection to the system authorized?	Yes
Portable/Mobile/Wireless #3	Are requirements for mobile device connection to the system enforced?	Yes
Portable/Mobile/Wireless #4	Is the capability for automatic execution of code on removable media disabled?	Yes
Portable/Mobile/Wireless #5	Are specially configured mobile devices issued to individuals traveling to locations of significant risk per policies and procedures?	Yes
Portable/Mobile/Wireless #6	Are specified measures applied to mobile devices returning from locations of significant risk per policies and procedures?	Yes
Portable/Mobile/Wireless #7	Is the use of writable, removable media restricted on the system?	Yes
Portable/Mobile/Wireless #8	Is the use of personally owned, removable media prohibited on the system?	Yes
Portable/Mobile/Wireless #9	Is the use of removable media with no identifiable owner prohibited on the system?	Yes
Portable/Mobile/Wireless #10	Does the system protect wireless access using authentication and encryption?	Yes
Portable/Mobile/Wireless #11	Are unauthorized remote connections to the system monitored, including scanning for unauthorized mobile or wireless access points on a defined frequency and is appropriate action taken if an unauthorized connection is discovered?	No
Portable/Mobile/Wireless #12	Do you employ rigorous security measures for remote sessions with administrative privileges and are they audited?	Yes
Portable/Mobile/Wireless #13	Is peer-to-peer wireless networking capability disabled except for explicitly identified components in support of specific operational requirements?	Yes
Portable/Mobile/Wireless #14	Are there use restrictions and implementation guidance for wireless technologies?	Yes

Portable/Mobile/Wireless #15	Is wireless access to the system authorized, monitored, and managed?	Yes
Portable/Mobile/Wireless #16	Is authentication and encryption used to protect wireless access to the system and the latency induced does NOT degrade the operational performance of the system?	Yes
Portable/Mobile/Wireless #17	Is the system scanned for unauthorized wireless access points at a specified frequency, and is appropriate action taken if such access points are discovered?	Yes
Portable/Mobile/Wireless #18	Is there a thorough scan for unauthorized wireless access points in facilities containing high-impact systems?	Yes
Procedures #1	Does a process exist to monitor changes to the system and conduct security impact analyses to determine the effects of the changes?	Yes
Procedures #2	Security Procedure	No
Procedures #3	Configuration Management Procedure	Yes
Procedures #4	Information and Document Management Procedure	Yes
Procedures #5	Awareness and Training Procedure	No
Procedures #6	Access Control Procedure	Yes
Remote Access Control #1	Are allowed methods of remote access to the system documented?	Yes
Remote Access Control #2	Are there usage restrictions and implementation guidance for each allowed remote access method?	Yes
Remote Access Control #3	Does remote access to the network require authentication prior to system connection?	Yes
Remote Access Control #4	Are the requirements for remote connections to the system enforced?	Yes
Remote Access Control #5	Are all the methods of remote access to the system authorized, monitored, and managed?	Yes
Remote Access Control #6	Are automated mechanisms used to facilitate the monitoring and control of remote access methods?	Yes
Remote Access Control #7	Is cryptography used to protect the confidentiality and integrity of remote access sessions?	Yes
Remote Access Control #8	Does the system route all remote accesses through a limited number of managed access control points?	Yes
Remote Access Control #9	Is remote access for privileged commands and security-relevant information authorized only for compelling operational needs and is the rationale for such access documented?	No
Remote Access Control #10	Is Bluetooth wireless networking capability disabled except for explicitly identified components in support of specific operational requirements?	Yes
Remote Access Control #11	Are there mechanisms in the design and implementation of the system to restrict access to the system from the enterprise network? (firewall, DMZ, VPN)	Yes
Remote Access Control #12	Does the system terminate a network connection at the end of a session or after a defined time period of inactivity?	Yes
Risk Management and Assessment #1	Are potential security threats, vulnerabilities, and consequences identified, classified, prioritized, and analyzed using accepted methodologies?	Yes

Risk Management and Assessment #2	Are the system connections monitored on an ongoing basis verifying enforcement of documented security requirements?	No
System and Services Acquisition #1	Are security functional requirements and specifications included in system acquisition contracts based on an assessment of risk?	Yes
System and Services Acquisition #2	Are security-related documentation requirements included in system acquisition contracts based on an assessment of risk?	Yes
System and Services Acquisition #3	Are developmental and evaluation-related assurance requirements (acceptance testing, compliance documentation) included in system acquisition contracts based on an assessment of risk?	No
System and Services Acquisition #4	Do acquisition documents require that vendors/contractors provide information describing the functional properties of the security controls employed within the system?	Yes
System and Services Acquisition #5	Does the system developer have a security test and evaluation plan?	Yes
System and Services Acquisition #6	Does the system developer have a verifiable error remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process?	Yes
System and Services Acquisition #7	Does the system developer/integrator document the result of the security testing/evaluation and error remediation processes?	Yes
System and Services Acquisition #8	Are providers of external system services required to employ security controls in accordance with applicable, policies, regulations, standards, guidance, and established service level agreements?	Yes
System and Services Acquisition #9	Is security control compliance by external service providers monitored?	Yes
System Integrity #1	Are system security alerts, advisories, and directives received from designated external organizations on an ongoing basis?	Yes
System Integrity #2	Are internal security alerts, advisories, and directives generated?	Yes
System Integrity #3	Are security alerts, advisories, and directives disseminated to a list of personnel?	Yes
System Integrity #4	Does the system monitor and detect unauthorized changes to software and information?	Yes
System Integrity #5	Is the integrity of software and information reassessed by performing, on a defined frequency, integrity scans of the system, and are they used with extreme caution on designated high-availability systems?	Yes
System Protection #1	Are the external boundaries of the system defined?	Yes
System Protection #2	Are the operational system boundary, the strength required of the boundary, and the respective barriers to unauthorized access and control of system assets and components defined?	Yes
System Protection #3	Are externally accessible system components physically allocated to separate subnetworks (DMZ) with separate, physical network interfaces?	Yes
System Protection #4	Is external access into the organization's internal system networks prevented, except as appropriately mediated? (e.g., configuration files and settings, alarm points, passwords, etc.)	Yes
System Protection #5	Is the enterprise architecture developed with consideration for security and the resulting risk?	Yes
System Protection #6	Are all critical hardware and software system components defined and documented?	Yes

Training #1	Is basic security awareness training provided to all system users before authorizing access to the system, when required by system changes and at least annually thereafter?	Yes
Training #2	Is the effectiveness of security awareness training reviewed once a year at a minimum?	Yes
Training #3	Are system security roles and responsibilities defined and documented throughout the system development life cycle, and are the individuals who have these roles and responsibilities identified and trained?	Yes
Training #4	Is security-related technical training provided before authorizing access to the system or performing assigned duties, when required by system changes and on an periodic basis?	Yes