SITE SUMMARY 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.

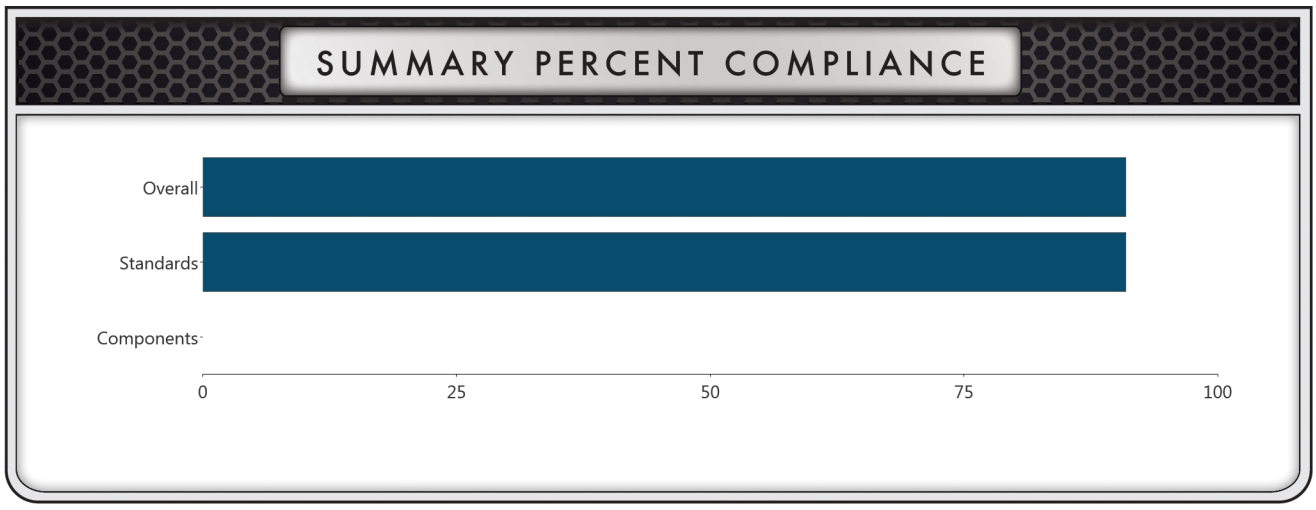
CSET® assessments cannot be completed effectively by any one individual. A cross-functional team consisting of representatives from operational, maintenance, information technology, business, and security areas is essential. The representatives must be subject matter experts with significant expertise 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

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].

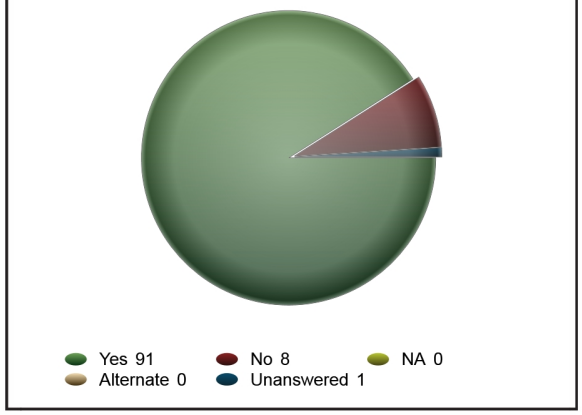
Several areas of concern make possible a successful cyber attack by malicious actors or a serious cyber incident. These include: [Please insert the 3 or 4 sections that are of greatest concern here based on results from the Detailed Findings section of the report].

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.]

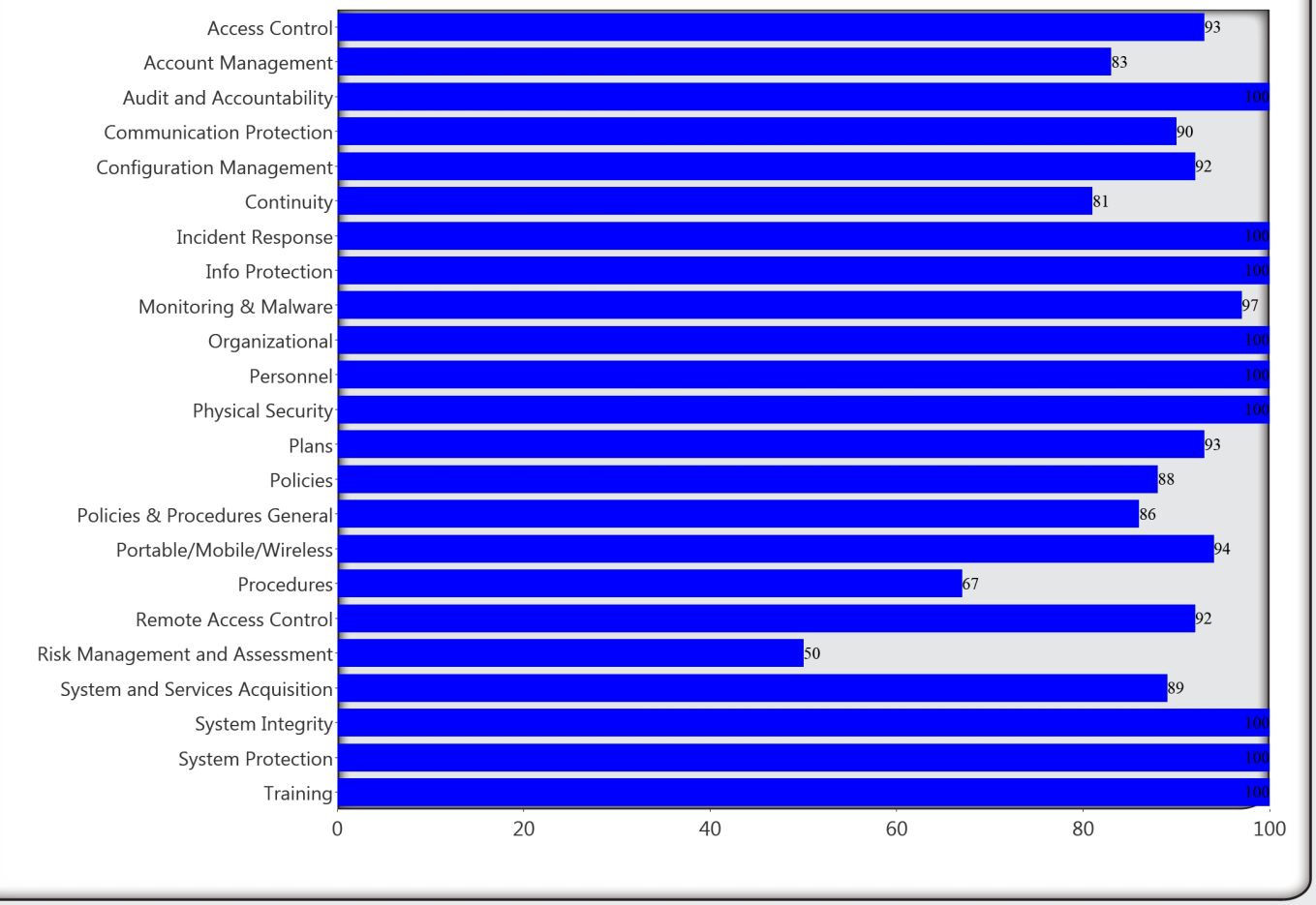
Evaluation Against Selected Standards and Question Sets

STANDARDS SUMMARY

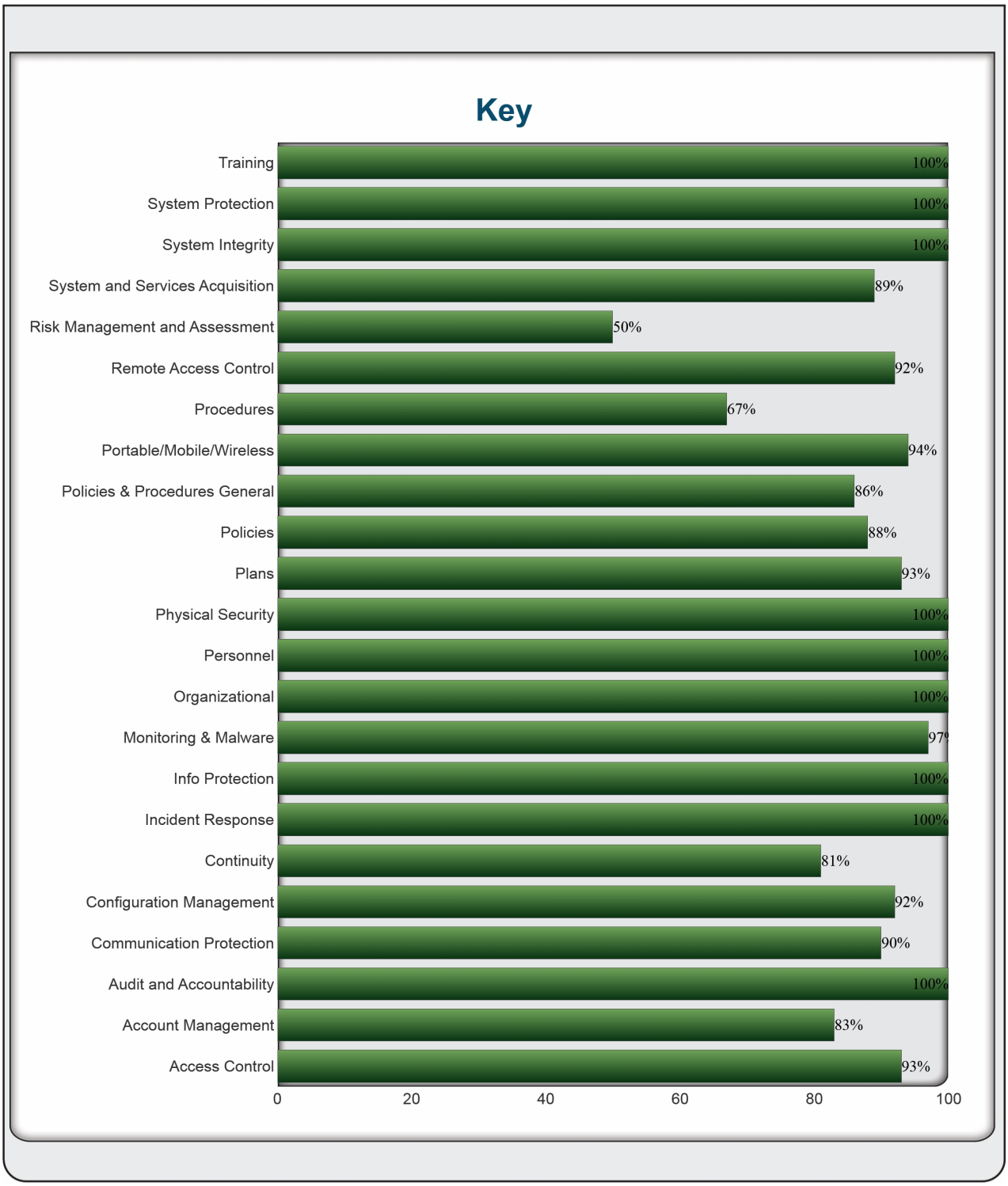


STANDARD OR QUESTION SET

Key Questions



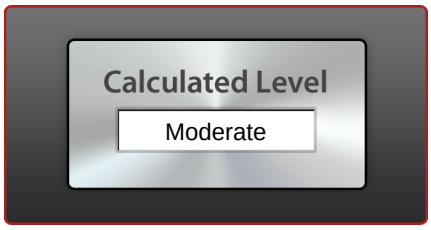
STANDARDS COMPLIANCE



FINDINGS AND RECOMMENDATIONS FROM BASIC NETWORK ANALYSIS

There are no findings or recommendations to display.

SECURITY ASSURANCE LEVEL (SAL)



	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

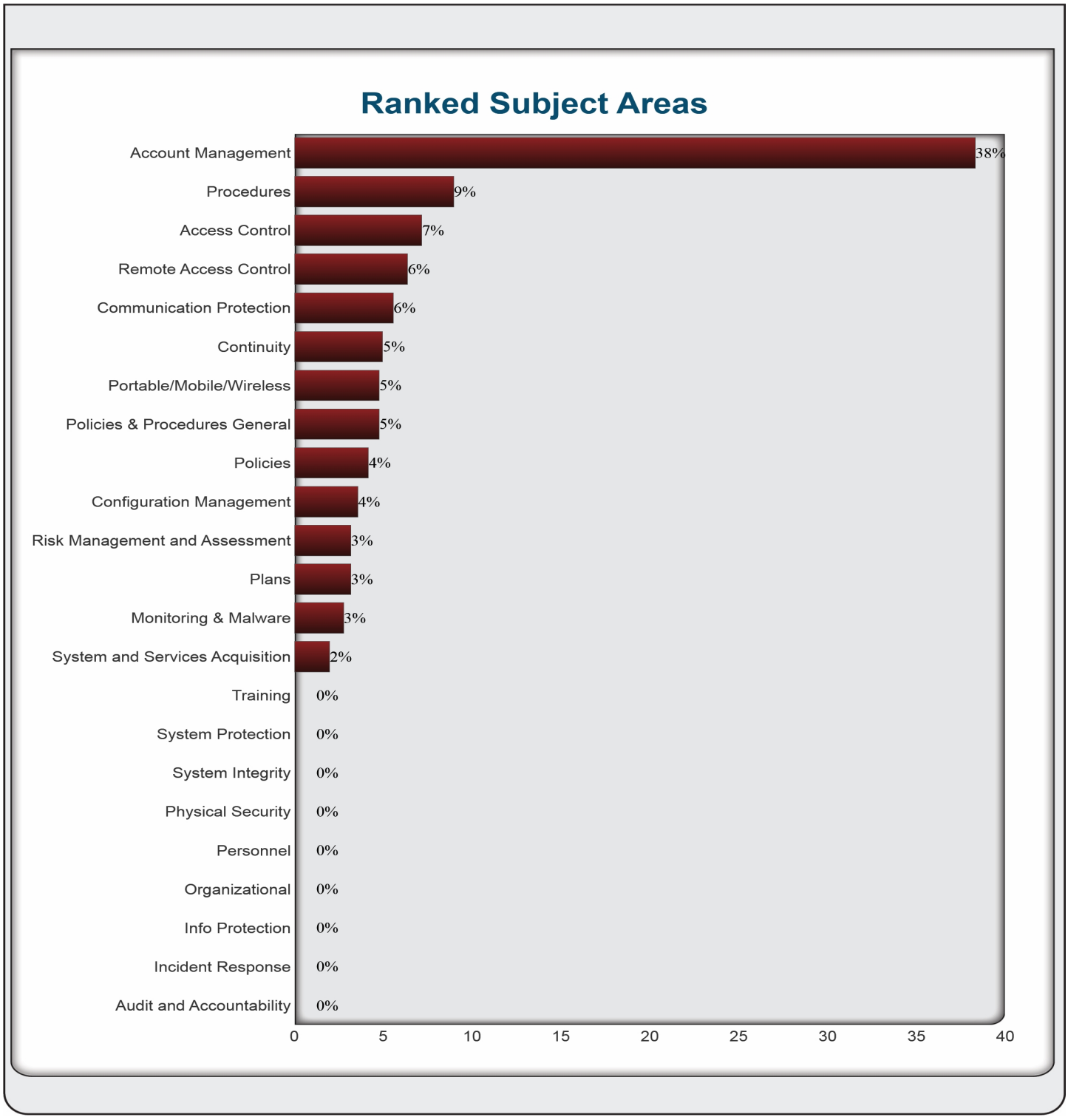
	Confidentiality	Integrity	Availability
Adjusted For System Questions	None	None	None
Information Type	None	None	None

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:		