Enterprise Evaluation

SOURCE REQUIREMENTS

CSET Release 3.0

August 12, 2010

LABEL	Requirement Text
CSVA-1	Security policies, plans, and procedures that specifically addresses business systems and related operational constraints, sensitivity issues, and processing environment issues should exist; whether they are specifically addressed in general information technology (IT) documentation or are specified in their own dedicated documentation.
CSVA-2	Security policies, plans, and procedures that specifically addresses business systems and related operational constraints, sensitivity issues, and processing environment issues should exist; whether they are specifically addressed in general information technology (IT) documentation or are specified in their own dedicated documentation. Cyber security policies, plans and procedures should be reviewed at planned intervals and if significant changes occur.
CSVA-3	Information management policies and procedures should include roles and responsibilities; data classification/sensitivity; handling and marking of documents and media; legal compliance; record retention; destruction and disposal of written records, equipment, and other media.
CSVA-4	A formal change management process should be documented and followed. Without a defined process that takes into account policy mandates, security concerns, business impact, authorization, and oversight, changes can weaken the stability and security of a system. A change management process ensures the most effective and efficient application of network and system updates, reduces the likelihood of the introduction of malicious code, and reduces the chance of human error.
CSVA-5	An individual within the facility should have the authorities and responsibilities for cyber security.
CSVA-6	Placeholder for practices related to this section that should be noted.
CSVA-7	If the organization's network is connected to networks outside of the department or organization's control, firewalls should be configured for minimum business and operational needs, and scans run to safeguard against potential vulnerabilities.
CSVA-8	Even without external connections, connectivity exists if facilities permit the use of portable electronic devices and media such as laptop computers, personal digital assistants (PDA), universal serial bus (USB) drives, compact disks (CD), or floppy disks, etc. If any of these devices can be carried into the facility by employees, contractors, or visitors; and if on-site systems and networks permit the connection of these devices, then connectivity (the possibility of transferring data) exists. Effective control over all forms of connectivity is essential to cyber security. If connected in any form, a vulnerability assessment is essential to understanding the cyber risk an organization is subject to.

CSVA-9	The concept of "least privilege" means that people or systems are only granted as much access as they need to perform their assigned job function, and no more. If someone worked in an office building and there was only one key to every floor and every room that was issued to all employees, it would be difficult to protect those valuables and resources. Instead, people are given keys to only those floors and offices that they need access to. This question seeks to find out if users are granted general, overreaching electronic and physical permissions to servers, data, and portions of a facility that may be vulnerable to attack or theft. A balance between what is good for security and what access is needed to allow business to be conducted smoothly is always the goal.
CSVA-10	Default passwords should be changed on all existing systems and devices and on new equipment when put into service.
CSVA-11	Individual user accounts are required, ensuring accountability and non-repudiation of user actions.
CSVA-12	Default passwords should be changed on all existing systems and devices and on new equipment when put into service.
CSVA-13	A complex password structure and rules should be enforced for all user and system accounts. The password requirements should be stringent enough to mandate at least five separate features of complexity which may include: limited password life, no re-use, minimum length, special characters, and an upper and lowercase character.
CSVA-14	Multi factor user identification, which refers to using more than one of the three types of identifiers in order to access a system or data, should be used. The three types of identifiers are: Something you know (e.g., an ID and password), something you have (e.g., an access card), and something you are (e.g., a fingerprint or other biometric component).
CSVA-15	In order to prevent manual and automated hack attempts on a system, repeated entry of incorrect credentials should result in a locked account. An acceptable procedure would require an account to become locked after three consecutive unsuccessful login attempts. The account would be accessible to the user only after a set amount of time had passed or by contacting a system administrator who would then reset the user's account.
CSVA-16	Many systems are connected in some fashion to other systems to share data and perform business functions. Rules governing these connections should be in place, especially when these connections are to outside networks.
CSVA-17	Many systems are connected in some fashion to other systems to share data and perform business functions. Rules governing these connections should be in place, especially when these connections are to components outside of the organization's direct control.
CSVA-18	The facility should evaluate the security status of third party groups they are connected with. Such evaluations are needed to establish the trust to do business securely and reduce the risk of negative impact on the organization. Entering into formal agreements with business partners on the security posture and expectations you have of them and they of you, gives both organizations leverage to fix weaknesses when identified.
CSVA-19	All data that has any value should be reviewed to see if encryption or protection from unauthorized access is necessary.
CSVA-20	All data that has any value should be reviewed to see if encryption or protection from unauthorized access is necessary. Sensitive data at rest that is on portable devices (e.g., laptops, PDAs, and portable storage devices and media) should be encrypted.
CSVA-21	There are multiple points in a computer network to regulate traffic using a variety of techniques. If desired, these controls can be configured to limit access by one department to another based on business and security needs.
CSVA-22	Placeholder for practices related to this section that should be noted.

CSVA-23	IT positions should be reviewed for criticality and sensitivity. Each of these roles are reviewed to determine what types and levels of sensitive materials someone filling that role will have access to and the roles then have a corresponding requirement. This information is used to determine if background checks are required.
CSVA-24	Background checks provide management with the basis for trust. Policies that limit assignments based on successful completion are the administrative security controls that can quickly and cheaply help identify the most obvious security risks based on criminal records or opportunities for compromise. Situations can change over time, and periodic reviews are needed to ensure that trust levels remain reliable.
CSVA-25	Background checks provide management with the basis for trust. Policies that limit assignments based on successful completion are the administrative security controls that can quickly and cheaply help identify the most obvious security risks based on criminal records or opportunities for compromise. Comprehensive background checks include criminal background, credit history, and lifestyle.
CSVA-26	Background checks provide management with the basis for trust. Policies that limit assignments based on a successful, timely completion are the administrative security controls that can quickly and efficiently help identify the most obvious security risks based on criminal records or opportunities for compromise.
CSVA-27	Separation of duties is a practice where roles and duties are given to separate individuals (e.g., IT Management, Systems Administration, Users, and Database Management are assigned to separate individuals), and management oversight is in place to ensure greater security and reliability.
CSVA-28	A responsive timely process is needed to ensure that all accounts are modified, de-activated, or deleted as personnel leave the company or transfer into new roles. System and application accounts, e-mail access, keys, keycards, and all other credentials should be immediately revoked upon termination of an employee without exception.
CSVA-29	More difficult than maintaining control over internal personnel is the task of ensuring all external service providers, business partners, and vendors do not compromise the security of an organization. Partner organizations should subject their personnel to your minimum security requirements if they are to have access to your facilities, systems, information, and intellectual property.
CSVA-30	Placeholder for practices related to this section that should be noted.
CSVA-31	Organization should restrict physical access to sensitive or restricted IT areas to only those with appropriate need.
CSVA-32	Organization should restrict physical access to media storage and control areas. (e.g., data storage media, telecommunication lines, etc.).
CSVA-33	Organization should monitor restricted IT and telecommunications areas for access violations, and organization should review of access logs regularly.
CSVA-34	Placeholder for practices related to this section that should be noted.
CSVA-35	Along with access credentials, users possess other knowledge of an organization that would be valuable to someone with malicious intent. Training should focus on these and other areas like prevention of internal misconduct. One of the most vulnerable aspects of a system is the human component, and leaving a gap between granting system access and awareness training could expose the organization to unnecessary risks.
CSVA-36	Training should be refreshed and reinforced on a frequent basis, as issues and trends vary. By providing regular updates to the training program, especially for those individuals in critical/sensitive positions, emerging threats can be better prepared for and guarded against.

CSVA-37	Social engineering is the process of gathering information from people rather than from machines. It is often easier to get a person to reveal passwords, security controls, or the location of unguarded materials than it is to get that data from a secure machine or storage device. In addition, companies limit the use of IT resources for numerous reasons: improper use of time can be expensive if not managed; and inappropriate Internet sites are often sources of malicious code that can infect a user's computer and from there, the entire network. By providing training in improper use, the organization reduces the risk of errors due to carelessness or lack of awareness.
CSVA-38	By tailoring training in this manner, time can be spent improving the skills of individuals with more sensitive or complex duties. For example, employees who have administrative rights to a system or access to highly sensitive materials should undergo a more in depth training process. Also, training for personnel who have access to classified or accounting systems need not be given to the entire employee population as it would provide information that may be misused.
CSVA-39	Personnel responsible for the administration of cyber systems should receive training specifically focused on those systems and their associated cyber security issues.
CSVA-40	Without penalties for misuse and a signed agreement, there are no teeth to enforcement policies and little perceived risk to employees for adverse behavior. It is historically difficult for companies to prosecute and/or otherwise enforce policies for improper use of resources if employees have not been made explicitly aware of the penalties.
CSVA-41	Placeholder for practices related to this section that should be noted.
CSVA-42	A helpdesk is often the first line of defense to resolve most end-user issues. It provides a single point of contact, a tracking and resolution system, and staff that are available based on business needs (i.e., business hours only, 24/7, etc.). Calls that require additional assistance can be escalated using a defined standard operating procedure and call tree based on the specific issue. Helpdesks are usually staffed by personnel trained in customer relationship support and have varying levels of knowledge of the systems they are supporting. There are usually documented helpdesk procedures in place that help call takers handle the calls and perform rudimentary system configuration tasks such as account resets and password resets.
CSVA-43	In the event of an emergency that might involve a system failure, a detected or active intrusion, or a virus attack, an established protocol and defined computer emergency response function limits the extent and degree of the damage. A Computer Emergency Response Team (CERT) is a group of people who are the first to be contacted in the event of an emergency and who are specially trained for their roles in the resolution of an incident. They work to identify, contain, and resolve the crisis.
CSVA-44	Firewalls and routers are put in place as preventative measures to guard a network. An IDS answers the question, "How can we tell if someone actually got through or is attempting to penetrate the protection?" An IDS will capture network or host traffic, analyze it for known attack patterns, and take specified action when it recognizes an intrusion or attempted intrusion. Recent incidents have shown an increasing trend toward attacks on both network nodes and servers which cannot be disregarded. Unintentional consequences, introduced to systems through good intentions of trusted insiders, are known to have caused disruptions of operational control systems. IDS play a key role in ensuring that threats to system security are addressed promptly, stability is maintained, and that systems are operating at maximum efficiency.
CSVA-45	Recent incidents have shown an increasing trend toward attacks on network nodes which cannot be disregarded. Log files play a key role in ensuring that threats to system security are addressed promptly, stability is maintained, and that systems are operating at maximum efficiency. The more frequent the log review, the more effective the incident response will be. Ideally logs are reviewed dynamically by an automated system with a periodic manual human review.

CSVA-46	Recent incidents have shown an increasing trend toward attacks on network nodes which cannot be disregarded. Log files play a key role in ensuring that threats to system security are addressed promptly, stability is maintained, and that systems are operating at maximum efficiency. The more frequent the log review, the more effective the incident response will be. Ideally logs are reviewed dynamically by an automated system with a periodic manual human review.
CSVA-47	Recognizing security events for what they are is a critical element in limiting the damage from cyber attacks, and consistency and diligence are keys to this as an effective practice.
CSVA-48	Making management aware of cyber security incidents and their potential for harm is of great benefit in obtaining the appropriate support and resources to effectively manage cyber security. Many events are low-order and do not rise to the level of reporting to management. These are typically the events that are handled appropriately by the firewall(s). Those that get by or that do damage need to be reported to management. The more severe the damage, the higher the reporting should be.
CSVA-49	Consider that reporting security events to external parties can have multiple benefits. For instance, by sharing incident and response information, other organizations can benefit from that experience and improve their cyber security practices; while the reporting organization can, in turn, learn from the experience and practices of others. Also, reporting information to law enforcement can be the first step in building a legal case against a suspected intruder and quickly identifying and apprehending computer criminals.
CSVA-50	Viruses, worms, Trojans, and other malicious software code proliferate on the Internet and mutate on an unpredictable basis. Malicious code is so common that without automated protection it is a near certainty that systems will be infected. Even without access to the Internet, malicious code can be introduced to an organization through actions (even unintended) of employees, support personnel, vendors, and business partners. To mitigate this risk, antivirus software is needed on every system in the organization whose architecture and application permit it. Protective software needs to download updates on a regular schedule to effectively identify new malicious code as they emerge and protect systems.
CSVA-51	With the prevalence of e-mail borne viruses and other spam messages that can include malicious software attachments, it is a best practice to apply some level of filtering that will remove attachments with dangerous file extensions. This is most effectively done at the e-mail server rather than on individual computers. Just like a physical post office does for regular mail, the e-mail server routes all messages to the recipient and is an ideal central location to apply security.
CSVA-52	The intent is to avoid practices which may be harmful to the organization, such as automatic forwarding of sensitive information and the sending of executable code. This aims to prevent valuable data from being misdirected, and/or prevent the rapid spread of e-mail-borne malicious code which can cripple a network.
CSVA-53	Placeholder for practices related to this section that should be noted.
CSVA-54	Having a detailed Contingency Disaster Recovery Plan for continuity of operations (COOP) in the event of a disaster protects against prolonged periods of system and network down time and business outages. A COOP plan is focused on preventing the interruption of critical business operations altogether, or getting business back online and functioning as quickly as necessary regardless of the cause of the interruption. Disaster Recovery Plans and Contingency Plans are subparts of the overall COOP and focus on specific activities surrounding system interruptions and how to re-establish them either at alternate sites or back at the primary site.
CSVA-55	These dependencies should be outlined in the facility's business impact analysis (BIA) as resource requirements. Priorities for recovery are one of the key factors of a successful recovery operation, and maximum allowable outage (MAO) times are one of the primary factors in setting priorities for recovery. If continuity planning is being done for one system, it must also take into account those internal and external systems which it may rely on, or which rely on it.

CSVA-56	These dependencies should be outlined in the facility's business impact analysis (BIA) as resource requirements. Priorities for recovery are one of the key factors of a successful recovery operation, and maximum allowable outage (MAO) times are one of the primary factors in setting priorities for recovery. If continuity planning is being done for one system, it must also take into account those internal and external systems which it may rely on, or which rely on it.
CSVA-57	An attack on the cyber infrastructure could occur at anytime. Therefore it is important to consider cyber security during contingency and recovery operations and during the reconstruction phase. If cyber security is not addressed in the plan then it will not receive proper attention during the recovery phase. The natural response will emphasize operability, not cyber security - which could then compromise operability.
CSVA-58	Organizations should identify disaster response roles and responsibilities for key personnel supporting the cyber infrastructure. Also, organizations should ensure that their contact information is up-to-date.
CSVA-59	There is potential for significant information loss. Consider the potential impact of the loss of one day's data for your system, and determine the cost-benefit of implementing a real time dynamic backup solution. The storage of critical data is either automated or manual. Automated storage or backup is more desirable as it is done continuously while a manual backup must be scheduled.
CSVA-60	Consideration should be given to the possibility of disaster (e.g., even small fires or floods may affect the room, tornados may affect the building, and earthquakes can have broad-reaching effects).
CSVA-61	The requirement for redundancy will vary among systems. In the case of a high availability-need system, the redundancy may come in the form of a clustered server that is always online near the main server and can instantly take over if the main machine failed for any reason. In the case of less stringent availability needs, just having spare servers in a storage room on standby that can have the backup image restored to them is adequate. For telecommunications, a backup PBX that can instantly be switched on line in case of failure, or load sharing/balancing equipment can be used to mitigate the risk of a single point of failure.
CSVA-62	Telecommunications Carriers If the sole telecommunications carrier experiences outages, then the organization's communications will be affected, with no alternative. Physical Connectivity If an entity has a single connection point to a facility then a breach in the cable near the building would likely result in a complete outage of communications. Multiple connection points offer redundancy, and should have some separation (located on opposite sides of a building). Route Diversity Contracting with different communication providers does not guarantee they use different paths for their links. Often times, one carrier is reselling service from another carrier. In such a case, a facility owner may think that the paths are diverse, but both providers are actually using the same path. Thorough data gathering from the carriers and analysis (and sometimes special agreements) maybe needed to ensure that communications paths and facilities are diverse. For more information on route diversity, please see http://www.ncs.gov/rdp.
CSVA-63	Consideration should be given to the possibility of disaster (e.g., even small fires or floods may affect the room, tornados may affect the building, and earthquakes can have broad-reaching effects). An alternate site provides the same resource in terms of physical space and infrastructure components like power and bandwidth. A hot site is one that is always online and ready for failover. A warm site has everything ready, but is not online with current data until needed. A cold site is merely space available without any equipment and can be transformed into a production site if and when required. The faster the recovery, the greater the ongoing cost to maintain..

CSVA-64	Backup telecommunications (including data) services (and their dependencies, such as power) - along with alternate sources should be obtained and tested at the primary and backup site. An alternate site provides the same communications resources and bandwidth. The faster the recovery, the greater the ongoing cost to maintain.
CSVA-65	Many things can be different than expected and training is an effective means for exposing employees to the reality of recovery operations. Updates and awareness bulletins can keep issues current and in the spotlight between training/testing sessions.
CSVA-66	Placeholder for practices related to this section that should be noted.
CSVA-67	Imbedding cyber security throughout the life cycle usually results in significant cost savings when compared to the addition of cyber security to operational systems. By integrating system security into the existing development lifecycle it will ensure that money is budgeted, personnel are designated, and requirements are gathered for security at appropriate times rather than after it is inconvenient, prohibitively expensive, or impossible. Security should be considered and provided for from system design through procurement, implementation, operation, and disposal. Purchasing or obtaining new equipment and services should always take operational security requirements into consideration, not just those for the safe and secure delivery of the product to be obtained. Requests for Proposals and Requests for Quotes often spell out minimum security safeguards and expectations of the bidders.
CSVA-68	Service Level Agreements (SLAs) with vendors and support service providers are used to establish activities and performance metrics. The intent is to ensure protection from equipment and application failure or disruption of service. The key element in an agreement is a set of services, conditions, and time-frames that are clearly defined.
CSVA-69	Placeholder for practices related to this section that should be noted.
CSVA-70	Maintaining a current inventory of the physical components of an infrastructure has numerous benefits that are increasingly realized the larger the organization. Components can be located, tracked, diagnosed, and maintained with far greater efficiency than if information about them is not documented.
CSVA-71	Vulnerabilities are not limited to critical components, and often, non-critical applications are the direct target of adversaries. Non-critical internal nodes can be used to compromise critical applications. An inventory of all internal network nodes is necessary to ensure that the facility can locate, track, and diagnose problems, and effectively maintain their network.
CSVA-72	The facility should have a comprehensive information flow diagram, showing how data moves within the infrastructure and within individual systems, thus enabling planning, diagnostic, maintenance, and security functions.
CSVA-73	The business requirement for every external network connection is needed to ensure that efforts undertaken and paths opened are consistent with business needs and priorities.
CSVA-74	Management needs an accurate picture and record of all systems currently operating in the organization, in order to determine the services required for operability. Regular reviews of what components are on the network and in use should be conducted. Security and reliability are increased if there are fewer things that can be exploited to harm an organization.
CSVA-75	An appropriate security policy is necessary to ensure that no unauthorized access channels exist and that personnel are aware of how authorized communication media should be used.

CSVA-76	New vulnerabilities are discovered frequently and zero-day vulnerabilities (those that are discovered and exploited on the same, or near to the same day) could be devastating. As new vulnerabilities are discovered in operating systems and software applications, patches and other updates are released to deal with them. Updating systems with these patches should be done on a scheduled basis and should follow a documented procedure. The complex nature of networks and systems occasionally introduces secondary vulnerabilities in the attempt to remedy another. Regular updates ensure that these also are countered in a timely and effective manner. Updates on mission critical servers and workstations should be done manually and tested before being put into operation.
CSVA-77	A formal change management process should be documented and followed. Without a defined process that takes into account policy mandates, security concerns, business impact, authorization, and oversight, changes can weaken the stability and security of a system. A change management process ensures the most effective and efficient application of network and system updates, reduces the likelihood of the introduction of malicious code, and reduces the chance of human error. All changes need to be consistent with the need for cyber security AND balanced by the priorities of management. ALL network AND application configuration changes should be reviewed by an IT security professional AND management to assess the security impact prior to the changes being implemented to the operational environment.
CSVA-78	Placeholder for practices related to this section that should be noted.
CSVA-79	Identifying and documenting critical network and system components is important for managing these items. An accurate and up to date inventory of all system components is needed to insure that software and hardware updates are timely and effectively applied.
CSVA-80	Given the constantly changing environment, cyber threats should be identified and reviewed on an ongoing basis. Some example threats include human error, theft of data, unauthorized access, alteration of data, terrorist attack, failure of environmental control systems (i.e., HVAC, humidity control, door locks, etc.), earthquakes, and floods. Most organizations follow an approved standard list that is comprehensive enough to cover the entire range of possible threats.
CSVA-81	New vulnerabilities are discovered frequently and zero-day vulnerabilities (those that are discovered and exploited on the same, or near to the same day) could be devastating. Part of the risk assessment activity should include a means to quantify the impact of a successful exploit of a weakness, including economic, physical, and public confidence, in order to rank them and conduct cost-benefit analyses to determine which weaknesses should be addressed and in which order. A Business Impact Analysis (BIA) identifies what impact a disruptive event would have on business. This could be in financial or functional terms. There are three goals for the BIA: prioritization, estimating maximum allowable downtime, and defining resource requirements and dependencies.
CSVA-82	The consequences (e.g., health and welfare, economic, and public confidence) of the exploitation of your assets, systems, and networks (used as platforms or weapons against other systems, facilities, or infrastructures) should be evaluated. This is a necessary component in establishing realistic cyber security priorities and implementing appropriate cyber security measures to reduce the probability of systems being used against other systems or other organizations. All systems that interconnect to a network and especially to the Internet are potential targets for compromise and exploitation as unsuspecting zombies in distributed denial of service attacks on other systems. Sophisticated hackers will use other systems to amass resources, to hide their malicious code, or simply take over a system from which to launch their attacks on other systems in an attempt to mask their identity and delay security officials in tracing their location and identity.
CSVA-83	Establishment and maintenance of an effective security program based on reputable sources of vulnerability information is a key practice. And, due to the exposure of legacy systems to Internet connectivity, historic vulnerabilities and solutions are often applicable and should also be considered and applied where appropriate.
CSVA-84	Potential vulnerabilities of your critical assets, systems, and networks should be identified and evaluated.

CSVA-85	The facility should identify and measure cyber security risk (including requirements, processes, and procedures) using recognized cyber security methodologies, standards, or best practices.
CSVA-86	The facility should complete a risk assessment for of critical assets, systems, and networks
CSVA-87	One of the outcomes of a risk assessment should be a cost-benefit analysis of what it would cost to address each risk versus the cost of doing nothing in relation to the benefit of the countermeasure. The overall security risk rating for each weakness takes into account the likelihood and impact of exploitation. Understanding the potential impact in monetary terms to remediate a weakness helps the organization make these determinations and prioritize them so that management can effectively allocate resources (money, personnel, equipment, etc.). Those weaknesses that are deemed not cost-effective to fix may be accepted as residual risk that do not warrant further action. Based on the outcome of the cost-benefit analysis in the risk assessment, resources should be allocated to the highest priority weaknesses that show the greatest return on investment for implementation. Although a risk may have a high likelihood and a high risk, the security countermeasure should be commensurate with the level of risk.
CSVA-88	Facilities should establish mandatory security requirements for all systems before they are put into operation, and for all operational systems throughout their lifecycle.
CSVA-89	Network and application security scans (vulnerability scans, penetration tests, authorized hardware and software scans) should be performed on at least a monthly basis and before devices are put back into operation after having been patched or upgraded. This testing attempts to guarantee the least amount of vulnerabilities possible in a system. However, just because a system configuration has followed all the required security measures and appears to be secure does not necessarily mean that it is. Frequent testing is the only way to guarantee security. Scans are usually done using a tool which generates a report while penetration testing (also known as Red Teaming) is a more in depth, controlled attack on a system in order to more accurately simulate what a hacker would attempt. Scans and testing should be done on the network infrastructure as well as on the applications themselves. The most effective time to use penetration testing is after all known vulnerabilities have been remedied (based on a risk assessment). This limits the results of the test to those issues that have not been fixed, or whose fix was ineffective, thus limiting the size of the report and the magnitude of the effort to evaluate it.
CSVA-90	Facilities should incorporate current and historic vulnerability solutions that are applicable and appropriate for its environment (e.g., firewalls are configured for minimum business or operational needs, thus ensuring that installed and newly acquired systems are as secure as feasible).
CSVA-91	The perimeter defense (i.e., routers and firewalls) should be configured to guard against reconnaissance attempts (probes, or other network scans, etc.). This practice helps prevent hackers from acquiring information about a system which can be used to look for common vulnerabilities to these products on hacker web sites throughout the Internet.
CSVA-92	The facility should have a successful and reliable program of IT audits performed by external certified IT auditors to ensure that cyber security measures are and remain effective, and that any new vulnerabilities are identified and managed. Results of audits are reported to senior management so that findings can be understood, agreed upon, and mitigated with management support.
CSVA-93	Metrics should be established and utilized to measure the effectiveness of the cyber security program, procedures, and practices. For measures to be reliable and useful, metrics should be consistently used. Metrics for cyber security effectiveness may include percent of system down time, intrusions detected and responded to, and speed of response during disaster recovery and other Continuity of Operations (COOP) tests.
CSVA-94	Placeholder for practices related to this section that should be noted.