VULNERABILITY MANAGEMENT

General Overview

There are a number of generally accepted interpretations and definitions for vulnerability management, which can be seen as the practice of identifying, classifying, remediating, and mitigating vulnerabilities, specifically those applicable to information systems. Vulnerability management has become increasingly important over the years, due to regulatory compliance mandates, along with increases in cyber security threats. Vulnerabilities within one's overall information systems landscape can cause serious harm to the confidentiality, integrity, and availability (CIA) of critical system resources, thus appropriate measures – such as starting with a well-documented vulnerability management program policy and procedure document – should be developed.

And vulnerability management is often referenced when discussing the topic of patch management and even configuration management, as all these principles seek to mitigate security issues by ensuring systems are safe and secure through continuous monitoring, software updates and hardening procedures. As for putting in place a vulnerability management program, organizations generally refer to the following model provided by Gartner, a well-known and respected organization:

- Define Policy
- Baseline the Environment
- Prioritize Vulnerabilities
- Shield
- Mitigate Vulnerabilities
- Maintain and Monitor

Additionally, other organizations within the information security industry have also offered their own vulnerability management programs, which are simply enhanced, revised, or simplified versions of the Gartner model. They all, however, share a common theme of identification and detection, prioritization, remediation, validation, and continuous monitoring. Interestingly, most vulnerability programs only tend to focus on finding software vulnerabilities – often in the context of security patches – but comprehensive vulnerability management extends to other relevant domains within an organization. The subsequent Vulnerability Management Program Policy and Procedures within the below referenced material incorporate all the major provisions as listed above, along with other supporting elements for ensuring a comprehensive and in-depth document.

As such, vulnerability management as the following:

Identifying, detecting, classifying and prioritizing, along with remediating, validating, and continuously monitoring vulnerabilities relating to critical information systems within an organization.

This in turn results in a well-established vulnerability management program consisting of the following areas:

- IDENTIFICATION | Defining Security Posture and Policies

- DETECTION | Assessing Non-Compliance and Vulnerabilities
- CLASSIFICATION and PRIORITIZATION | Determining Risk and Urgency
- REMEDIATION and VALIDATION | Removing Vulnerabilities and Confirming Security Updates
- CONTINOUS MONITORING | Proactively Assessing Vulnerabilities

Vulnerability Management Program Policy and Procedures

1.0 Overview

In accordance with mandated organizational security requirements set forth and approved by management, [company name] has established a formal Vulnerability Management Program policy and supporting procedures. This policy is to be implemented immediately along with all relevant and applicable procedures. Additionally, this policy is to be evaluated on a(n) [annual, semi-annual, quarterly] basis for ensuring its adequacy and relevancy regarding [company name]'s needs and goals.

1.0 Purpose

This policy and supporting procedures are designed to provide [company name] with a documented and formalized Vulnerability Management Program policy that is to be adhered to and utilized throughout the organization at all times. Compliance with the stated policy and supporting procedures helps ensure the safety and security of [company name] system resources. Vulnerability Management is integral to ensuring the confidentiality, integrity, and availability (CIA) of [company name]'s critical system resources, and every effort is to be made for properly identifying, detecting, classifying, and prioritizing, along with remediating, validating, and continuously monitoring such vulnerabilities.

Vulnerability management is a vital component of helping ensure the safety and security of any organization's critical system resources as growing cyber security threats are creating significant challenges and obstacles that must effectively be dealt with. The subsequent policies and procedures relating to vulnerability management initiatives for [company name] strive to ensure the overall confidentiality, integrity, and availability (CIA) of the organization's network.

1.0 Scope

This policy and supporting procedures encompasses all system resources that are owned, operated, maintained, and controlled by [company name] and all other system resources, both internally and externally, that interact with these systems.

- Internal system resources are those owned, operated, maintained, and controlled by [company name] and include all network devices (firewalls, routers, switches, load balancers, other network devices), servers (both physical and virtual servers, along with the operating systems and applications that reside on them) and any other system resources deemed in scope.

- External system resources are those owned, operated, maintained, and controlled by any entity other than [company name], but for which these very resources may impact the confidentiality, integrity, and availability (CIA) and overall security of the aforementioned description of "Internal system resources".

- When referencing the term "users", this includes any individual that has been granted access rights by [company name] to various system resources and has went through all required provisioning steps. Users typically include, but may not be limited to, the following: employees, consultants, vendors, contractors, along with local, state, and federal personnel.

- For purpose of this policy, vulnerability management is defined as the following: The practice of identifying, classifying, remediating, and mitigating vulnerabilities, specifically those applicable to information systems.

1.0 Policy

[Company name] is to ensure that the vulnerability management program policy adheres to the following conditions for purposes of complying with the mandated organizational security requirements set forth and approved by management:

IDENTIFICATION | Defining Security Posture and Policies

An essential component of any vulnerability management program is to comprehensively identify and define the security posture of the organization as a whole. Increasing cyber security threats, regulatory compliance mandates, the implementation of best practices, and other important operational and security considerations are to be identified when defining such a posture. Ultimately, a well-conceived vulnerability management program for [company name] is one that ensures the confidentiality, integrity, and availability (CIA) of the organization's information systems landscape, which includes all critical system resources. Vulnerability management programs – often confined to only conducting internal and external scans, along with penetration testing, and remediating such issues – are to also include identifying and detecting, classifying and prioritizing, remediating, validating, and continuously monitoring vulnerabilities relating to the following:

- **User Access Rights:** Ensuring users have access rights commensurate to one's roles and responsibilities within the organization is a constant challenge, given the continuous user provisioning and de-provisioning processes undertaken, the numerous systems requiring access for such users, along with requests for changes and modifications in access rights. As for access rights for all users – ranging from end-users of system resources, to I.T. personnel with elevated | super-user access rights, they are to be assigned on a "need to know" basis, one that incorporates Role Based Access control (RBAC), whereby users are granted permissions based on defined roles for specific systems. Additional components of access rights policies – formally known as the user identity, provisioning, & access rights lifecycle – are to include the following:

    - Utilizing provisioning and de-provisioning documentation for on-boarding and off-boarding all users, such as authorization forms and checklists, termination forms and checklists, etc.
    - Establishing appropriate password complexity rules and account lockout thresholds on all system resources accessed by users.
    - Enforcing appropriate segregation of duties for users having access to [company name] system resources.

- **Configuration Standards:** Provisioning, hardening, securing and locking-down all critical system resources within [company name] is crucial for ensuring a baseline of information security, one that can be built upon over time by continuous monitoring and updating of such systems with security patches. For the various system resources, industry leading provisioning,

hardening, securing, and configuration procedures are to be utilized at all times, which requires obtaining specific hardening guidelines from vendors and various associations, such as the following:

- SANS
- NIST SP 800 Publications
- United States Computer Emergency Readiness Team (US-CERT)
- National Security Agency (NSA) hardening documents
- CIS Security Benchmarks Division
- OWASP
- Vendor specific hardening guidelines
- MITRE community driven information security consortiums

Additionally, from a scope perspective, configuration standards are to include provisioning, hardening, securing and locking-down all network devices (i.e., firewalls, routers, switches, etc.), operating systems, applications (such as database installations, web server applications, etc.), along with internally developed software applications.

- **Network Architecture and Topology:** Insecure network topologies and weak security architectures – even if the systems themselves are properly secured and hardened – can result in significant vulnerabilities for the organization. For example, a firewall by itself serving as the main filtering point for traffic - even when properly provisioned – serves only as a single layer of security without other layered or Defense in Depth initiatives. Utilizing industry leading security devices, such as intrusion detection systems (IDS), load balancers, file integrity monitoring (FIM) software, specialized firewalls (such as layer 7 web application firewalls), and other essential tools is a requirement for protecting system resources and other information assets. As such, all [company name] network topology documents are to be reviewed and kept current on a regular basis for helping establish layered and well-fortified information security architecture.

- **Network Vulnerabilities:** The use of internal and external vulnerability scanning procedures, along with network layer and application layer penetration tests are a critical component of [company name]'s vulnerability management program. Scanning and penetration testing are highly effective in identifying critical security threats, and are one of the most important components of [company name]'s vulnerability management program. As such, these security tools and methodologies are to be utilized on a consistent basis, both for purposes of any regulatory compliance mandates, along with implementing best practices for proactive network vulnerability analysis.

Ultimately, an important component of developing a comprehensive vulnerability management program requires [company name] to adequately address the following major issues and constraints:

- **Vulnerabilities:** Software flaws or a misconfiguration that may potentially result in the weakness in the security of a system within the organization's system resources.
- **Remediation:** The three (3) primary methods of remediation are (1) installation of a software patch, (2) adjustment of a configuration setting and (3) removal of affected software.

- **Threats:** Threats are capabilities or methods of attack developed by malicious entities to exploit vulnerabilities and potentially cause harm to a computer system or network.

DETECTION | Assessing Non-compliance and Vulnerabilities

The aforementioned policies serve as the organization's baseline for security posture, one that helps ensure the confidentiality, integrity, and availability (CIA) of [company name]'s information systems landscape. Policy directives are only as good as the initiatives put in place to enforce such measures, therefore, a comprehensive assessment relating to non-compliance and vulnerabilities is to be undertaken on all critical system resource relating to the following:

User Access Rights: The organization's entire user identity, provisioning, & access rights lifecycle is to be assessed for ensuring confirmation and existence of the following:

- Documented policies and procedures detailing the provisioning and de-provisioning process for all users accessing [company name] system resources.
- User provisioning and de-provisioning forms and supporting checklists, templates as needed for documenting such activities.
- Implementation of Role Based Access Control (RBAC) for users accessing [company name] system resources.
- Appropriate segregation of duties for [company name] system resources.

Configuration Standards: The organization's entire provisioning, hardening, securing and locking-down methodologies are to be assessed for ensuring confirmation and existence of the following:

- Configuration standards have been appropriately identified, reviewed, and approved, by authorized I.T. personnel within [company name].
- Actual configuration standards documentation – such as guides, checklists, forms, and other supporting hardening material – exist and are kept either in hard copy or electronic format.
- All critical system resources within [company name] have been adequately provisioned, hardened, secured and locked-down in accordance with the stated configuration documentation on file. Note: The phrase "All critical system resources" pertains to the following: all network devices (i.e., firewalls, routers, switches, etc.), operating systems, applications (such as database installations, web server applications, etc.), along with internally developed software applications.

Network Architecture and Topology: The organization's network security architecture and supporting topology documents are to be assessed for ensuring confirmation and existence of the following:

- The use of various industry leading tools and protocols for ensuring a layered, Defense in Depth strategy is utilized for protecting [company name]'s information systems landscape. Such tools are to include, but are not limited, to the following: intrusion detection systems (IDS), load balancers, file integrity monitoring (FIM) software, specialized firewalls (such as layer 7 web application firewalls), and others.
- Updated, accurate, and detailed network topology documents, such as schematics, flowcharts, multi-layered diagrams, and others. Additionally, such documentation is to be version and date stamped, and reviewed by authorized I.T. personnel for accuracy.

Network Vulnerabilities: The organization's vulnerability scanning and penetration testing initiatives are to be assessed for ensuring confirmation and existence of the following:

- Vulnerability scans – from a scope perspective - include both internal and external scans for all relevant and critical system resources, for purposes of implementing best practices initiatives, along with complying with regulatory compliance mandates.
- Scans are scheduled to run automatically at pre-determined dates and times throughout the calendar year, with all results being immediately reviewed and assessed as necessary.
- Penetration tests – from a scope perspective - include both network layer and application layer tests on all relevant environments, for purposes of implementing best practices initiatives, along with complying with regulatory compliance mandates.

Once all assessments have been thoroughly undertaken for the aforementioned areas, instances of non-compliance and the applicable vulnerabilities related to each are to be documented accordingly in the Vulnerability Management Worksheet, resulting in a classification of such issues, along with a prioritization schedule for remediation.

CLASSIFICATION and PRIORITIZATION | Determining Risk and Urgency
All instances of non-compliance and the related vulnerabilities are to be classified and prioritized accordingly in the following manner within the [company name] Vulnerability Management Worksheet:

1. Area for which non-compliance was identified (1. User access rights. 2. Configuration standards. 3. Network architecture and topology. 4. Network vulnerabilities).
2. Specific issue or concern.
3. Assigned risk ranking and urgency for remediating of non-compliance and related vulnerabilities, such as the following:

    - **High:** The threat source is highly motivated and sufficiently capable; controls to prevent the vulnerability from being exercised are ineffective.
    - **Medium:** The threat source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.
    - **Low:** The threat source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.

A risk rating deemed HIGH, is one that "The threat source is highly motivated and sufficiently capable; controls to prevent the vulnerability from being exercised are ineffective", and the impact of such a threat poses serious harm to critical [company name] system resources. As for the deployment of security patches, they are to be commenced in the following manner:

- **High:** 0 – 24 hours.
- **Medium:** Within thirty (30) days.
- **Low:** Within ninety (90) to one-hundred-eighty (180) days.

Because vulnerabilities identified through internal and external scans, along with network layer and application layer penetration tests often are the most critical– in terms of immediate needs that must be

met for mitigating security threats – they are to be first in line for remediation (unless exceptions are noted). This requires following [company name]'s documented patch management policy and procedures, which outlines the necessary steps for assessing, testing, and deploying security patches. Furthermore, documenting one's classification and prioritization initiatives for vulnerability management requires having a current asset inventory of all major system resources, such as spreadsheets, and other necessary forms, checklists, and templates detailing essential information as discussed above.

REMEDIATION and VALIDATION | Removing Vulnerabilities and Confirming Security Updates

All issues of non-compliance and related vulnerabilities are to be remediated in accordance with the scheduled risk rating and urgency parameters previously noted. This requires authorized I.T. personnel to undertake all necessary measures for ensuring the confidentiality, integrity, and availability (CIA) of [company name]'s information systems landscape. Additionally, all relevant information is to be documented within the [company name] Vulnerability Management Worksheet, which should include specific security and technical measures undertaken to correct such issues, along with procedures initiated for confirming the removal of vulnerabilities (i.e., testing systems, re-scanning IP addresses, etc.). Specifically, for vulnerabilities found when conducting internal and external scans and network layer and application layer tests, these procedures are to be re-performed in a timely manner for ensuring such issues have been removed.

CONTINUOUS MONITORING | Proactively Assessing Vulnerabilities

Threats to an organization's information systems landscape and all critical system resources is dynamic in nature, always evolving – ultimately creating enormous challenges for [company name] – for which these challenges must be met. It is the policy of this organization that all major areas identified for purposes of vulnerability management (1. User access rights. 2. Configuration standards. 3. Network architecture and topology. 4. Network vulnerabilities) are to be regularly monitored in a way that helps in proactively identifying such vulnerabilities. Specifically the following is to apply:

- **User Access Rights:** Periodic review of the entire user identity, provisioning, & access rights lifecycle, with findings, analysis, and recommendations reported to senior management within [company name].
- **Configuration Standards:** Periodic review of critical system resources for ensuring the applicable hardening standards are in fact being applied as required, with findings, analysis, and recommendations reported to senior management within [company name].
- **Network Architecture and Topology:** Periodic review of the entire [company name] security architecture for ensuring a layered, Defense in Depth approach is being utilized, with findings, analysis, and recommendations reported to senior management within [company name].
- **Network Vulnerabilities:** Structured schedule for automated internal and external scans to be performed, along with network layer and application layer penetration tests, with findings, analysis, and recommendations reported to senior management within [company name].

Monitoring for issues of non-compliance and related vulnerabilities is extremely critical, as it allows [company name] to address security issues in a proactive manner, helping mitigate harm and damage to the organization's critical system resources.

1.0 Procedures

[Company name] has developed and implemented a comprehensive vulnerability management process, which encompasses the following categories and supporting activities listed below. These policy directives will be fully enforced by [company name] for ensuring the patch management initiatives are executed in a formal manner and on a consistent basis for all specified systems.

Note: The "Policy" sections contained within this specific policy and procedure document simply state general best-of-breed practices that should be in place. However, the "Procedures" sections list and describe the actual steps to undertake for ensuring compliance with the aforementioned policies. As such, look upon the policies as statements, formal guidelines, and the general framework for a particular subject matter. As for the procedures, these are the actual processes, steps, workflow activities and supporting initiatives that illustrate how the actual policies are implemented. In summary, policies state what are to be done, while procedures show you how they are done.

Additionally, if you want to provide any more information that's relevant to each section listed below, please use the "Additional Information" box [shown under each section], as this allows you to document any additional evidence of the procedures undertaken for meeting adherence with the stated policies. All information in light blue text should be deleted as this information is merely stated for reference purposes.

IDENTIFICATION | Defining Security Posture and Policies

User Access Rights

For User Access Rights, please describe in detail the following: (1). How your organization actually incorporates the concept of Role Based Access Control (RBAC). (2). What specific procedures are in place for provisioning and de-provisioning users – such as what is the process, and what forms are actually used. (3). What are your password complexity rules and account lockout policies for directories used to authenticate against. (4). And any other information you feel is relevant.

Additional Information
General Notes | Comments:

Configuration Standards

For Configuration Standards, please describe in detail the following: (1). What specific provisioning and hardening documents (i.e., vendor supplied documents, internally developed checklists, etc.) are used by your organization for the following areas:

- Routers:
- Switches:
- Firewalls:
- Operating Systems:
- Applications (Database instances, web server applications, etc.):
- Internally developed software applications:

- Other (i.e., printer software, etc.):

Additional Information
General Notes | Comments:

Network Architecture and Topology

For network architecture and topology, please describe in detail the following: (1). What specific security provisions and safeguards have been put in place – such as layered security | Defense in Depth measures, etc., for ensuring a secure and well-fortified architecture?

Additional Information
General Notes | Comments:

Network Vulnerabilities

For network vulnerabilities, please describe in detail the following: (1). What type of vulnerability scans are conducted (i.e., internal, external), on what environments, and how often? (2). What type of penetration tests are conducted (i.e., network layer and application layer), on what environments, and how often?

Additional Information
General Notes | Comments:

DETECTION | Assessing Non-compliance and Vulnerabilities

Consistent with the above stated policies for "DETECTION", your organization will need to undertake comprehensive measures for actually detecting what vulnerabilities exist in relation to the following areas:

- User Access Rights
- Configuration Standards
- Network Architecture and Topology
- Network Vulnerabilities

In essence, the baseline assessment conducted in the "Identification" phase must now be assessed for compliance, with non-compliance documented accordingly for the next phase, which is

"CLASSIFICATION and PRIORITIZATION". Please use the Vulnerability Management Worksheets listed below or simply state what your actual procedures are for assessing compliance, along with documenting non-compliance.

Additional Information
General Notes | Comments:

CLASSIFICATION and PRIORITIZATION | Determining Risk and Urgency

Once you've detected non-compliance and related vulnerabilities, they will need to be documented accordingly for the next phase, such as the specific issue or concern and the applicable risk ranking given to such issues. Please use the Vulnerability Management Worksheets listed below or simply state what your actual procedures are for assessing classifying and prioritizing issues of non-compliance and related vulnerabilities.

Additional Information
General Notes | Comments:

REMEDIATION and VALIDATION | Removing Vulnerabilities and Confirming Security Updates

Your organization will need to undertake comprehensive measures for actually remediating and confirming validation with vulnerabilities that exist in relation to the following areas:

- User Access Rights
- Configuration Standards
- Network Architecture and Topology
- Network Vulnerabilities

Please use the Vulnerability Management Worksheet listed below or simply state what your actual procedures are for remediation and validating the respective remediation efforts.

Additional Information
General Notes | Comments:

CONTINOUS MONITORING | Proactively Assessing Vulnerabilities

Please state what practices are in place regarding the continuous monitoring of vulnerabilities relation to the following areas:

- User Access Rights
- Configuration Standards
- Network Architecture and Topology
- Network Vulnerabilities

Please use the Vulnerability Management Monitoring document listed below or simply state what your actual procedures are for continuous monitoring.

Additional Information
General Notes | Comments:

Vulnerability Management Worksheet – User Access Rights

IDENTIFICATION | Defining Security Posture and Policies		
	List of Baseline Security Posture and Policies	**General Notes, Comments, Recommendations**
(1).	Documented policies and procedures detailing the provisioning and de-provisioning process for all users accessing [company name] system resources.	
(2).	User provisioning and de-provisioning forms and supporting checklists, templates as needed for documenting such activities.	
(3).	Implementation of Role Based Access Control (RBAC) for users accessing [company name] system resources.	
(4).	Appropriate segregation of duties for [company name] system resources.	
(5).	Please insert other baseline security posture and policies	
(6).	Please insert other baseline security posture and policies	
(7).	Please insert other baseline security posture and policies	
(8).	Please insert other baseline security posture and policies	
(9).	Please insert other baseline security posture and policies	
(10.)	Please insert other baseline security posture and policies	

DETECTION | Assessing Non-compliance and Vulnerabilities			
	Baseline Security Posture	**Procedures Used for DETECTING Compliance**	**Compliant: YES or NO and any other Relevant Comments**
(1).	Documented policies and procedures detailing the provisioning and de-provisioning process for all users accessing [company name] system resources.		
(2).	User provisioning and de-provisioning forms and supporting checklists, templates as needed for documenting such activities.		
(3).	Implementation of Role Based Access Control (RBAC) for users accessing [company name] system resources.		
(4).	Appropriate segregation of duties for [company name] system resources.		
(5).	Please insert other baseline security posture and policies		
(6).	Please insert other baseline security posture and policies		
(7).	Please insert other baseline security posture and policies		
(8).	Please insert other baseline security posture and policies		
(9).	Please insert other baseline security posture and policies		
(10.)	Please insert other baseline security posture and policies		

CLASSIFICATION and PRIORITIZATION | Determining Risk and Urgency			
	Baseline Security Posture Requiring CLASSIFICATION and PRIORITIZATION	**Specific Issue or Concern**	**Risk Ranking (High, Medium, Low) and Urgency**
(1).	Documented policies and procedures detailing the provisioning and de-		

	provisioning process for all users accessing [company name] system resources.		
(2).	User provisioning and de-provisioning forms and supporting checklists, templates as needed for documenting such activities.		
(3).	Implementation of Role Based Access Control (RBAC) for users accessing [company name] system resources.		
(4).	Appropriate segregation of duties for [company name] system resources.		
(5).	Please insert other baseline security posture and policies		
(6).	Please insert other baseline security posture and policies		
(7).	Please insert other baseline security posture and policies		
(8).	Please insert other baseline security posture and policies		
(9).	Please insert other baseline security posture and policies		
(10.)	Please insert other baseline security posture and policies		
REMEDIATION and VALIDATION | Removing Vulnerabilities and Confirming Security Updates			
	Baseline Security Posture Requiring REMEDIATION	**Specific Security and Technical Measures Undertaken for REMEDIATION of Issues**	**Procedures Initiated for VALIDATION of the Removal of Vulnerabilities**
(1).	Documented policies and procedures detailing the provisioning and de-provisioning process for all users accessing [company name] system resources.		
(2).	User provisioning and de-provisioning forms and supporting checklists, templates as needed for documenting such activities.		
(3).	Implementation of Role Based Access Control (RBAC) for users accessing [company name] system resources.		
(4).	Appropriate segregation of duties for [company name] system resources.		
(5).	Please insert other baseline security posture and policies		
(6).	Please insert other baseline security posture and policies		
(7).	Please insert other baseline security posture and policies		
(8).	Please insert other baseline security posture and policies		
(9).	Please insert other baseline security posture and policies		
(10.)	Please insert other baseline security posture and policies		
CONTINOUS MONITORING | Proactively Assessing Vulnerabilities			
	Baseline Security Posture Requiring CONTINUOUS MONITORING	**Specific Security and Technical Measures Undertaken for CONTINUOUS MONITORING**	**General Notes, Comments, Recommendations**
(1).	Documented policies and procedures detailing the provisioning and de-provisioning process for all users accessing [company name] system resources.		
(2).	User provisioning and de-provisioning forms and supporting checklists, templates as needed for documenting		

	such activities.		
(3).	Implementation of Role Based Access Control (RBAC) for users accessing [company name] system resources.		
(4).	Appropriate segregation of duties for [company name] system resources.		
(5).	Please insert other baseline security posture and policies		
(6).	Please insert other baseline security posture and policies		
(7).	Please insert other baseline security posture and policies		
(8).	Please insert other baseline security posture and policies		
(9).	Please insert other baseline security posture and policies		
(10.)	Please insert other baseline security posture and policies		

Vulnerability Management Worksheet – Configuration Standards

IDENTIFICATION | Defining Security Posture and Policies		
	List of Baseline Security Posture and Policies	**General Notes, Comments, Recommendations**
(1).	Industry approved configuration standards are to measurers for properly provisioning, hardening, securing and locking-down all network devices.	
(2).	Industry approved configuration standards are to measurers for properly provisioning, hardening, securing and locking-down all operating systems.	
(3).	Industry approved configuration standards are to measurers for properly provisioning, hardening, securing and locking-down all applications, such as database installations, web server applications, etc.	
(4).	Industry approved configuration standards are to measurers for properly provisioning, hardening, securing and locking-down all internally developed applications.	
(5).	Please insert other baseline security posture and policies	
(6).	Please insert other baseline security posture and policies	
(7).	Please insert other baseline security posture and policies	
(8).	Please insert other baseline security posture and policies	
(9).	Please insert other baseline security posture and policies	
(10.)	Please insert other baseline security posture and policies	

DETECTION | Assessing Non-compliance and Vulnerabilities			
	Baseline Security Posture	**Procedures Used for DETECTING Compliance**	**Compliant: YES or NO and any other Relevant Comments**
(1).	Industry approved configuration standards are to measurers for properly provisioning, hardening, securing and locking-down all network devices.		
(2).	Industry approved configuration standards are to measurers for properly provisioning, hardening, securing and locking-down all operating systems.		
(3).	Industry approved configuration standards are to measurers for properly provisioning, hardening, securing and locking-down all applications, such as database installations, web server applications, etc.		
(4).	Industry approved configuration standards are to measurers for properly provisioning, hardening, securing and locking-down all internally developed applications.		
(5).	Please insert other baseline security posture and policies		
(6).	Please insert other baseline security posture and policies		
(7).	Please insert other baseline security posture and policies		
(8).	Please insert other baseline security posture and policies		
(9).	Please insert other baseline security posture and policies		
(10.)	Please insert other baseline security posture and policies		

CLASSIFICATION and PRIORITIZATION | Determining Risk and Urgency			
	Baseline Security Posture Requiring	**Specific Issue or Concern**	**Risk Ranking (High, Medium, Low)**

	CLASSIFICATION and PRIORITIZATION		and Urgency
(1).	Industry approved configuration standards are to measurers for properly provisioning, hardening, securing and locking-down all network devices.		
(2).	Industry approved configuration standards are to measurers for properly provisioning, hardening, securing and locking-down all operating systems.		
(3).	Industry approved configuration standards are to measurers for properly provisioning, hardening, securing and locking-down all applications, such as database installations, web server applications, etc.		
(4).	Industry approved configuration standards are to measurers for properly provisioning, hardening, securing and locking-down all internally developed applications.		
(5).	Please insert other baseline security posture and policies		
(6).	Please insert other baseline security posture and policies		
(7).	Please insert other baseline security posture and policies		
(8).	Please insert other baseline security posture and policies		
(9).	Please insert other baseline security posture and policies		
(10.)	Please insert other baseline security posture and policies		
	REMEDIATION and VALIDATION | Removing Vulnerabilities and Confirming Security Updates		
	Baseline Security Posture Requiring REMEDIATION	**Specific Security and Technical Measures Undertaken for REMEDIATION of Issues**	**Procedures Initiated for VALIDATION of the Removal of Vulnerabilities**
(1).	Industry approved configuration standards are to measurers for properly provisioning, hardening, securing and locking-down all network devices.		
(2).	Industry approved configuration standards are to measurers for properly provisioning, hardening, securing and locking-down all operating systems.		
(3).	Industry approved configuration standards are to measurers for properly provisioning, hardening, securing and locking-down all applications, such as database installations, web server applications, etc.		
(4).	Industry approved configuration standards are to measurers for properly provisioning, hardening, securing and locking-down all internally developed applications.		
(5).	Please insert other baseline security posture and policies		
(6).	Please insert other baseline security posture and policies		
(7).	Please insert other baseline security posture and policies		
(8).	Please insert other baseline security posture and policies		

(9).	Please insert other baseline security posture and policies		
(10.)	Please insert other baseline security posture and policies		
	CONTINOUS MONITORING | Proactively Assessing Vulnerabilities		
	Baseline Security Posture Requiring CONTINUOUS MONITORING	**Specific Security and Technical Measures Undertaken for CONTINUOUS MONITORING**	**General Notes, Comments, Recommendations**
(1).	Industry approved configuration standards are to measurers for properly provisioning, hardening, securing and locking-down all network devices.		
(2).	Industry approved configuration standards are to measurers for properly provisioning, hardening, securing and locking-down all operating systems.		
(3).	Industry approved configuration standards are to measurers for properly provisioning, hardening, securing and locking-down all applications, such as database installations, web server applications, etc.		
(4).	Industry approved configuration standards are to measurers for properly provisioning, hardening, securing and locking-down all internally developed applications.		
(5).	Please insert other baseline security posture and policies		
(6).	Please insert other baseline security posture and policies		
(7).	Please insert other baseline security posture and policies		
(8).	Please insert other baseline security posture and policies		
(9).	Please insert other baseline security posture and policies		
(10.)	Please insert other baseline security posture and policies		