**Application Risk Management Implementation Plan**

- **Create a list of Cybersecurity Implementation controls discussed in class for**

- Application Data Handling
    - Database Management System – For data storage and retrieval purposes a 3rd party DBMS is used along with applications.
    - Data Storage – It is crucial that the data at rest is encrypted under classified or unclassified system categories.
    - In-Memory Data Handling – All sensitive data should be removed from memory and encrypted when not in use.
    - Data Transmission – It is crucial that the data in transit is encrypted under classified or unclassified system categories.
    - Data Integrity – Integrity Checks should be performed on all files to ensure that the files have not been modified in any way.
    - Data Marking – Information Disclosure can be avoided by marking all sensitive data as non-public data.

- Authentication
    - Server Authentication – Any server authentication requires DoD PKI credential and certificates or from other authorized entities.
    - User Authentication – All user authentication requires DoD PKI credential and certificates or from other authorized entities
    - Signed Code Identification – DoD PKI mobile code certificates are used for the signing process and should be validated before their execution on a workstation.
    - Standalone Application Authentication – The network services and application services are not used by these applications and are protected by OS authentication.
    - Server Application Authentication – These applications are used for providing services to remote users.
    - Client Application Authentication – Like standalone applications, these are too protected by OS authentication.
    - Combination Client Server Application Authentication – These Client and Server components have their own authentication requirements.
    - Application Component Authentication – Access to these application components by users should be first authenticated and then authorized.
    - PKI Certificate Validation – Validation checks should be performed regularly for ensuring its proper use, trust and expiration.
    - Password Complexity and maintenance – Strict password policies should be enforced for highly sensitive applications.
    - Credential protection – Credential protection should include OS level protection, file access protection, encryption, and hashing.

- Cryptography
    - Symmetric Ciphers – The encryption and decryption of sensitive data is performed using the same cryptographic key.
    - Message authentication codes, hashes – MAC's and hashes of the data can be performed to avoid data tampering and ensures confidentiality.
    - Digital Signatures – Digital signatures can be useful to provide data authentication and ensuring data integrity.

- User Accounts
    - Application Accounts – Application accounts are paramount and require the same level of protection as OS and databases.
    - Application Sessions – Strict session limits in terms of user and sessions per user should be implemented to avoid attacks like DOS.
    - Access Control – Access control and user authorization policies can be used to safeguard against many application related attacks.
    - Excessive Privileges – Permissions and ACL policies should be implemented to limit attack that use excessive privileges.

- Input Validation
    - Integer Overflows – To prevent integer overflows, techniques like static analysis and input sanitization can be done to allow only good data to pass.
    - Format String vulnerability – Static analysis tools, input validation can be used to defend against format string vulnerability.
    - Command Injection Vulnerability – malicious code can be injection into a vulnerable application, and this can wreak havoc.
    - Buffer Overflows – There are many safeguards like using memory safe and type safe programming languages and secure coding practices to minimize buffer overflows.
    - Canonical Representation – Applications can be compromised by attackers by canonical representation vulnerability in web pages. These can be avoided by setting strict Access control policies like permissions and ACLs.
    - Hidden Field Vulnerability – By removing hidden elements and not using them to store values this vulnerability can be prevented.
    - Information Disclosure – There are several information security policies which can be implemented to minimize information disclosures.
    - Race condition – By minimizing the use of global variables and using thread safe versions of functions this vulnerability can be prevented.

- Auditing
    - Notify the User on login – All the details like date and time, IP address, no of login attempts should be notifies to the respective users.
    - Access to need-to-know information – All the information like date and time, IP address, no of login attempts will be used for auditing

    - Classified audit record content – Strict application auditing policy should be implemented regardless if it is implemented in an application or an external device.
    - Mobile code – There are 3 categories of mobile code established by the DoD.
    - Web Services – Vulnerabilities for classified and unclassified systems can be managed by industry standards like OASIS and W3C. Apart from these secure network policies protocols should also be followed.

- Configuration Management
    - Software CM – Managing the versions of all components thereby controlling the software is known as software Configuration Management.
    - Release Manager – Release Manager is tasked with the role of configuration management.

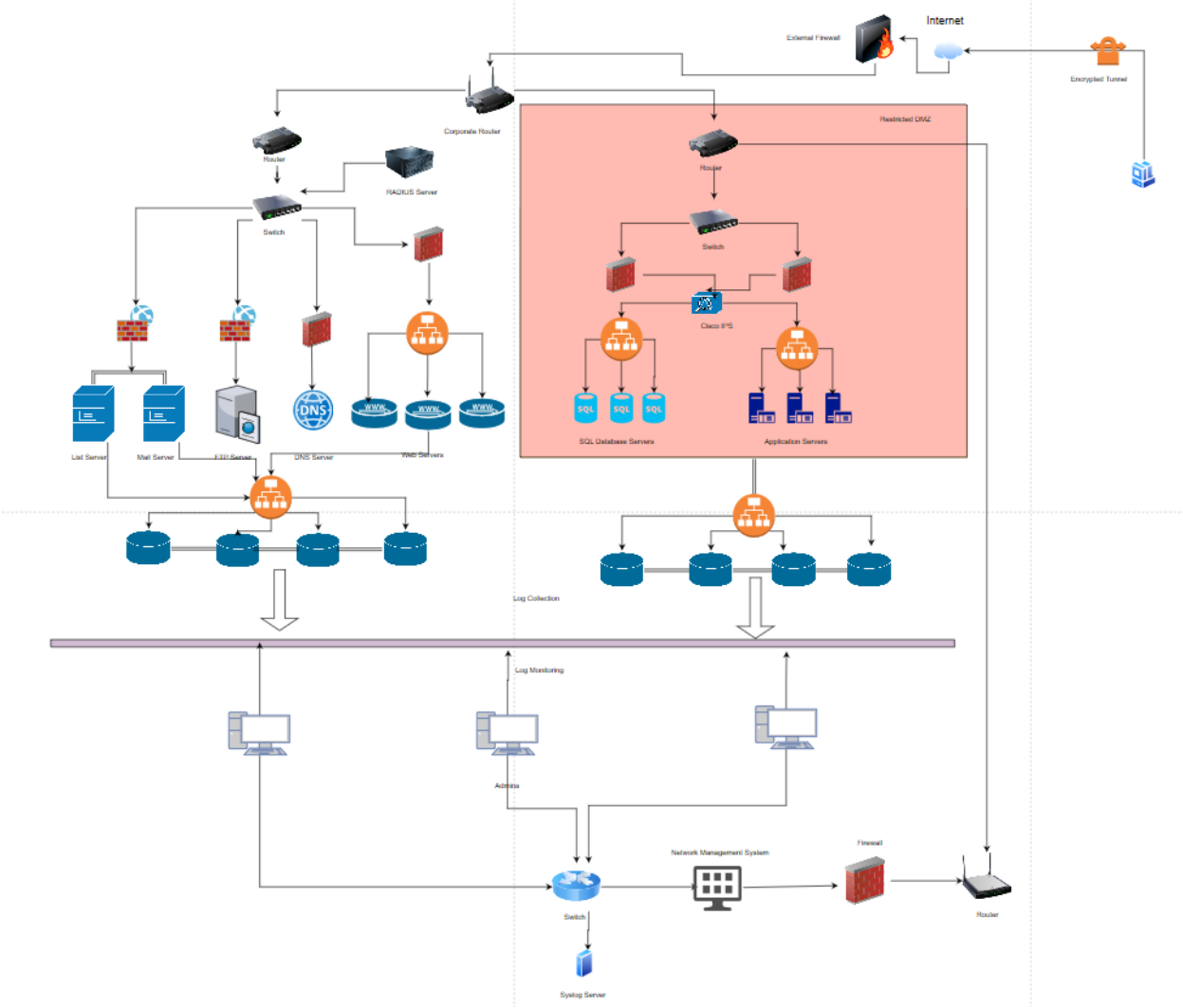
- Testing
    - Plans and Procedures – Documentation outlining the plans and procedures for testing and a schedule of all the tests to be undertaken.
    - Fuzzy testing –Fuzzy testing is a technique used to find coding errors and loopholes in an application by inputting random data.
    - Code Reviews – Code Review is performed by fellow programmers to uncover any coding errors.
    - Automated Tools – Automated tools can be employed to discover any unknown vulnerabilities.
    - Third party and open source catalog – Org can use 3rd party and open source components like Synopsis or black duck software.
    - Web Application Vulnerability Scanners – These scanners can help discover any unknown potential vulnerabilities and provides suggestions for remediating them.

- Deployment
    - Documentation – The documentation requires to cover items like plan, threat model, ports and protocols guide etc.
    - Maintenance – There must be regular check of updates and software which is no longer under maintenance is removed.
    - Denial of Service – Malicious Attempts can be made to exhaust system resources; hence proper security controls should be in place.
    - Audit Trail Monitoring – Audit trials should be properly monitored for any malicious attempts.
    - Audit Log Retention – Audit logs should be retained for longer intervals for analysis and investigative purposes.
    - Audit Trail Protection – All audit logs should be encrypted to safeguard them from malicious users.
    - Recovery and Contingency Planning – Code recovery and contingency planning should be in place in case of any disaster.

- Account Management – Unused or unnecessary accounts should be removed.
- Deployment Infrastructure – Proper Deployed infrastructure should be in place for additional protection and business continuity.

- **Create a network topology diagram for your company.**

The Network Topology diagram stays the same as it follows defense-in-depth approach. The Network Topology diagram consists of a restricted DMZ. Here, there are several SQL database servers and Application Servers. The distribution of workloads across multiple servers is achieved by load balancers. Inside the Restricted DMZ are two stateful inspection firewalls to monitor malicious traffic. There is also a Cisco IPS to identify and block malicious activities. This is connected to a router which is in-turn connected to a corporate router. The other servers like the Mail server, FTP server, DNS Servers and Web servers are connected to packet filter firewalls. The log collection from all the servers is done by the log collectors. There are several admins to monitor and analyze the collected logs for malicious activities. A RADIUS server is implemented to authenticate remote users securely. A syslog server is also implemented for easy configuration of all logging devices. The clients can connect through IPsec encrypted tunnel and share data securely.




➢ **Create a list of Cybersecurity Implementation controls that exist at your company**

- Application Data Handling
    - Database Management System – Database Management System is a system for managing databases and lets its users perform Data manipulation functions. There are several databases used along with its respective applications.
    - Data Storage – In my company, all data at rest is encrypted under type 1 encryption.
    - Data Transmission – In my company, all data in transit is encrypted under type 1 encryption.
    - Data Integrity – In my company, data Integrity Checks are performed at regular intervals on all files to ensure that the files have not been modified in any way.

- Authentication
    - Server Authentication – DoD PKI credential and certificates are required for server authentication when dealing with government projects.
    - User Authentication – DoD PKI credential and certificates are required for user authentication when dealing with government projects.
    - Signed Code Identification – DoD PKI mobile code certificates are used for the signing process and should be validated before their execution on a workstation.
    - Standalone Application Authentication – 2FA is implemented for standalone application authentication.
    - Server Application Authentication – In my company, these provide services to remote users and the users are authenticated via 2FA.
    - Client Application Authentication – 2FA is implemented for standalone application authentication.
    - Application Component Authentication – In my company, access to these application components by users should be first authenticated by 2FA and then authorized via permissions and ACLs.
    - Password Complexity and maintenance – All the employees have their own passwords and its company policy that the passwords should be changed every 30 days. Also, a password must contain an uppercase, a lowercase and a numeric. Additionally, last 3 previously used passwords cannot be used again
    - Credential protection – In my company the credentials are stored outside the database for protection.

- Cryptography
    - Symmetric Ciphers – The encryption and decryption of sensitive data is performed using the same cryptographic key.
    - Digital Signatures – Digital signatures using Type 1 algorithms are used in my company.

- User Accounts
    - Application Accounts – Several application accounts are used in my organization for a group of applications
    - Access Control – Access control and permissions are the primary form of authorization in my organization.

- Input Validation
    - Integer Overflows – My company uses secure coding practices and tools like SafeInt Library to prevent integer overflows and other errors like divide by zero.
    - Format String vulnerability – Many Static analysis tools and security controls like Format_Guard can be used to defend against this vulnerability.
    - Command Injection Vulnerability – Several safeguards like implementing least privileges, input sanitization techniques and using whitelist validation can prevent this vulnerability.

    - Buffer Overflows – There are many safeguards implemented in applications at my company against buffer overflows like ASLR, DEP, SEHOP etc. These controls can however make the attack difficult. To prevent these overflows, one should follow secure coding practices and input validation techniques.
    - Canonical Representation – Boundary checking mechanisms and input validation can prevent such vulnerabilities.
    - Hidden Field Vulnerability – By removing hidden form fields this vulnerability is prevented.
    - Information Disclosure – There are several information security policies at my organization against this vulnerability.
    - Race condition – Applications in my company use different locking schemes to prevent race conditions.

- Auditing
    - Notify the User on login – In my company all users are notified of all the details like date and time, IP address, no of login attempts.
    - Access to need-to-know information – My organization uses all need to know information for auditing purposes.
    - Mobile code – My company follows DoD category 3 policies for general use and DoD category 1 policies when dealing with government projects.
    - Web Services –Industry standards like OASIS and W3C are used in my company for managing vulnerabilities for classified and unclassified systems.

- Configuration Management
    - Software CM – Regular checks are performed in my company for updates and controlling of changes in the software.
    - Release Manager – There are a few Release Managers in my organization responsible for all the configuration management.

- Testing
    - Plans and Procedures – All the documentation regarding plans and procedures are readily available at my organization.
    - Fuzzy testing – All the applications which are used at my company are testing thoroughly using various kinds of tests which include fuzzy tests.
    - Code Reviews – All the applications which are used at my company are reviewed by many programmers and security experts.
    - Web Application Vulnerability Scanners – Vulnerability scanners like Scuba are employed at my org. to check for vulnerabilities.

- Deployment
    - Documentation – All the required documentation like System Security plan, threat model, ports and protocols guide etc. are readily available at my company.
    - Maintenance – Checks for patches and updates are conducted every month and any software which is no longer maintained is removed.
    - Denial of Service – There are several information security controls and policies in place against denial of service attacks.
    - Audit Trail Monitoring – All the audit trails are monitored both actively and passively and its access is controlled by strict Access controls policies and permissions.
    - Audit Log Retention – All Audit logs are retained for a period of 2 months in my company for analysis and investigative purposes.
    - Audit Trail Protection – All audit logs are encrypted at my company.
    - Recovery and Contingency Planning – All critical software is backed up and stored securely for recovery purposes.
    - Account Management – Regular checks are performed, and any unused or unnecessary accounts are removed.
    - Deployment Infrastructure – Additional servers, databases and other infrastructure are in place for additional protection and business continuity.

- **Compare the Implementation controls discussed in class with your company's existing Cybersecurity Implementation controls**

| Implementation Controls | Status |
|---|---|
| **Application Data Handling** | |
| Database Management System | Implemented |
| Data Storage | Implemented |
| In-Memory Data Handling | NOT Implemented |
| Data Transmission | Implemented |
| Data Integrity | Implemented |
| Data Marking | NOT Implemented |
| **Authentication** | |
| Server Authentication | Implemented |
| User Authentication | Implemented |
| Signed Code Identification | Implemented |
| Standalone Application Authentication | Implemented |
| Server Application Authentication | Implemented |
| Client Application Authentication | Implemented |
| Combination Client Server Application Authentication | NOT Implemented |
| Application Component Authentication | Implemented |
| PKI Certificate Validation | NOT Implemented |
| Password Complexity and Maintenance | Implemented |

| | |
|---|---|
| Credential Protection | Implemented |
| **Cryptography** | |
| Symmetric Ciphers | Implemented |
| Message Authentication codes, Hashes | NOT Implemented |
| Digital Signatures | Implemented |
| **User Accounts** | |
| Application Accounts | Implemented |
| Application Sessions | NOT Implemented |
| Access Controls | Implemented |
| Excessive Privileges | NOT Implemented |
| **Input Validation** | |
| Integer Overflows | Implemented |
| Format String vulnerability | Implemented |
| Command Injection Vulnerability | Implemented |
| Buffer Overflows | Implemented |
| Canonical Representation | Implemented |
| Hidden Field Vulnerability | Implemented |
| Information Disclosure | Implemented |
| Race condition | Implemented |
| **Auditing** | |
| Notify the User on login | Implemented |
| Access to need-to-know information | Implemented |
| Classified audit record content | NOT Implemented |
| Mobile code | Implemented |
| Web Services | Implemented |
| **Configuration Management** | |
| Software CM | Implemented |
| Release Manager | Implemented |
| **Testing** | |
| Plans and Procedures | Implemented |
| Fuzzy testing | Implemented |
| Code Reviews | Implemented |
| Automated Tools | In Progress |
| Third party and open source catalog | NOT Implemented |
| Web Application Vulnerability Scanners | Implemented |
| **Deployment** | |
| Documentation | Implemented |
| Maintenance | Implemented |
| Denial of Service | Implemented |
| Audit Trail Monitoring | Implemented |
| Audit Log Retention | Implemented |
| Audit Trail Protection | Implemented |
| Recovery and Contingency Planning | Implemented |
| Account Management | Implemented |
| Deployment Infrastructure | Implemented |

- **Create a list of critical assets in $ that exist in your company**

  Data is the most important asset at our company.
  Some of the critical assets are:
  Patients health records: Maintaining Patients health records is crucial to our organization. It will cost millions if there is any breach involving patient's health records.

  Client Information: Doctors and patient's information are one of the crucial assets. Damage control will cost millions if there are any data leaks.

  Employee Information: It consists of HR records. Damage control and credit monitoring services would cost the company millions of dollars of there is a breach.

  Organization Reputation: Positive Reputation for a corporation is essential for building trust and is one of the critical assets. It is intangible.

  Network Devices and software: There are numerous network devices and software which could be categorized as critical assets. As Data is the most important asset, servers like SQL database are the most critical assets at our organization. Other important assets include Servers, firewalls, routers, Cisco IPS etc. These network devices and applications cost hundreds of thousands of dollars.

| S. No | Asset | Value (Approx.) |
|---|---|---|
| 1 | Patient Health Records | $200 Million |
| 2 | Client Information | $100 Million |
| 3 | Employee Information | $10 Million |
| 4 | Organization Reputation | Intangible |
| 5 | Network Devices | $5 Million |

- **Create a list of potential vulnerabilities for critical assets where Cybersecurity Implementation Controls are missing**

  - In my company the data in memory is not cleared after its use. This may lead to range of vulnerabilities including data being read or altered by malicious users.
  - Data Marking policies are not implemented at my company. This can lead to leak of sensitive information and IP data
  - As strict PKI validation policies are not followed, this can undermine the effectiveness of PKI certificates.
  - Hashes are not used in my company, instead encrypted passwords are stored. This can be a vulnerability if the attacker manages to gain access to keys which are not cleared from memory.
  - Session limits like time limits, limits on users and sessions in use are not implemented in my company.

- **Create a list of potential threats to your company that could exploit vulnerabilities of critical assets.**

    - Denial of service and other attacks are possible through multiple logons as there are no session limits implemented.
    - As data in memory is not managed properly, a range of attacks would be possible from prediction of patterns to reconstruction of RSA and AES keys.
    - Several broken authentication attacks are possible as Message authentication codes and hashes are not implemented.
    - As PKI validation policies are not implemented properly, denial of service and many attacks against PKI are possible.
    - As DoD policies are followed only when dealing with government projects, during general use the code may be replaced by a malicious code.

- **Create a list of potential risks for critical assets where Cybersecurity Implementation Controls are missing**

    - Denial of Service: DOS attacks are a possibility due to absence of application sessions and PKI validation policies. This can have a high impact as providing services to the organization is paramount.
    - Unauthorized access: Due to the poor in-memory data handling policies, unauthorized access is a possibility after the attacker learns about the cryptographic keys from the memory.
    - Disclosure of sensitive information: Absence of data marking can lead to disclosure of sensitive information and IP data.
    - Data Integrity and Authenticity can be compromised as message authentication codes and hashes are not used.
    - Data confidentiality can be compromised as data in memory can be accessed by a malicious user.

- **Provide a list of recommended Hardening Prevention controls and policies for each recommended control that should be created to reduce vulnerability probabilities and thus mitigate the identified risks (it is not required to write detailed policies) – Risk Prevention Strategy.**

    - All the data in memory should be cleared after use and all the data should also be encrypted in memory when not in use.
    - Data marking policies should be implemented to avoid risk of information disclosure.
    - PKI certificates validation should be enforced properly for the ascertain the effectiveness of PKI certificates.
    - Message authentication codes and hashes should be implemented to ensure data confidentiality, integrity and availability.

- Session limits should be implemented to avoid DOS and other attacks.

- **Provide a list of recommended Hardening methods and policies for critical assets that should be implemented to reduce asset risk impact and thus mitigate the identified risks and increase resilience (it is not required to write detailed policies) – Risk Response Strategy**

  - Security controls like ACL's and permissions should be implemented for applications with excessive privileges.
  - Automated tools should be implemented for testing which maximizes the chances of finding coding errors and other vulnerabilities.
  - Combination of client server application authentication should be implemented to streamline the process of authentication.
  - Classified Audit record content should be followed to classify and prioritize audit events.
  - Use of open source catalog can be helpful in developing secure applications and testing policies should also be implemented by open source software.

- **Create a detailed policy for the Application Service Provider Standards control using a SANS template as provided in class**

**Consensus Policy Resource Community**

# Web Application Security Policy

**Free Use Disclaimer:** *This policy was created by or for the SANS Institute for the Internet community. All or parts of this policy can be freely used for your organization. There is no prior approval required. If you would like to contribute a new policy or updated version of this policy, please send email to policy-resources@sans.org.*

**Last Update Status:** *Updated June 2014*

## 1. Overview

Web application vulnerabilities account for the largest portion of attack vectors outside of malware. It is crucial that any web application be assessed for vulnerabilities and any vulnerabilities be remediated prior to production deployment.

## 2. Purpose

The purpose of this policy is to define web application security assessments within

company. Web application assessments are performed to identify potential or realized weaknesses because of inadvertent misconfiguration, weak authentication, insufficient error handling, sensitive information leakage, etc. Discovery and subsequent mitigation of these issues will limit the attack surface of company services available both internally and externally as well as satisfy compliance with any relevant policies in place.

## 3. Scope

This policy covers all web application security assessments requested by any individual, group, or department for the purposes of maintaining the security posture, compliance, risk management, and change control of technologies in use at company.

All web application security assessments will be performed by delegated security personnel either employed or contracted by company. All findings are considered confidential and are to be distributed to persons on a "need to know" basis. Distribution of any findings outside of company is strictly prohibited unless approved by the Chief Information Officer.

Any relationships within multi-tiered applications found during the scoping phase will be included in the assessment unless explicitly limited. Limitations and subsequent justification will be documented prior to the start of the assessment.

## 4. Policy

4.1 Web applications are subject to security assessments based on the following criteria:

a) New or Major Application Release – will be subject to a full assessment prior to approval of the change control documentation and/or release into the live environment.

b) Third Party or Acquired Web Application – will be subject to full assessment after which it will be bound to policy requirements.

c) Point Releases – will be subject to an appropriate assessment level based on the risk of the changes in the application functionality and/or architecture.

d) Patch Releases – will be subject to an appropriate assessment level based on the risk of the changes to the application functionality and/or architecture.

e) Emergency Releases – An emergency release will be allowed to forgo security assessments and carry the assumed risk until such time that a proper assessment can be carried out. Emergency releases will be designated as such by the Chief Information Officer or an appropriate manager who has been delegated this authority.

4.2 All security issues that are discovered during assessments must be mitigated based upon the following risk levels. The Risk Levels are based on the OWASP Risk Rating Methodology. Remediation validation testing will be required to validate fix and/or mitigation strategies for any discovered issues of Medium risk level or greater.

a) High – Any high-risk issue must be fixed immediately, or other mitigation strategies must be put in place to limit exposure before deployment. Applications with high-risk issues are subject to being taken off-line or denied release into the live environment.

b) Medium – Medium risk issues should be reviewed to determine what is required to mitigate and scheduled accordingly. Applications with medium risk issues may be taken off-line or denied release into the live environment based on the number of issues and if multiple issues increase the risk to an unacceptable level. Issues should be fixed in a patch/point release unless other mitigation strategies will limit exposure.

c) Low – Issue should be reviewed to determine what is required to correct the issue and scheduled accordingly.

4.3 The following security assessment levels shall be established by the InfoSec organization or other designated organization that will be performing the assessments.

a) Full – A full assessment is comprised of tests for all known web application vulnerabilities using both automated and manual tools based on the OWASP Testing Guide. A full assessment will use manual penetration testing techniques to validate discovered vulnerabilities to determine the overall risk of all discovered.

b) Quick – A quick assessment will consist of a (typically) automated scan of an application for the OWASP Top Ten web application security risks at a minimum.

c) Targeted – A targeted assessment is performed to verify vulnerability remediation changes or new application functionality.

4.4 The current approved web application security assessment tools in use which will be used for testing are:

- <Tool/Application 1>
- <Tool/Application 2>
- …

Other tools and/or techniques may be used depending upon what is found in the default assessment and the need to determine validity and risk are subject to the discretion of the Security Engineering team.

## 5. Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-through, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Web application assessments are a requirement of the change control process and are required to adhere to this policy unless found to be exempt. All application releases must pass through the change control process. Any web applications that do not adhere to this policy may be taken offline until such time that a formal assessment can be performed at the discretion of the Chief Information Officer.

## 6. Related Standards, Policies and Processes

OWASP Top Ten Project

OWASP Testing Guide

OWASP Risk Rating Methodology

## 7. Definitions and Terms

None.

## 8. Revision History

| Date of Change | Responsible | Summary of Change |
|---|---|---|
| June 2014 | SANS Policy Team | Updated and converted to new format. |
| | | |

| Version | Revision Date | Author |
|---|---|---|
| V1.0 | 11/17/2019 | Abhishek Ningala |