CYBER HYGIENE

WHITEPAPER BY THE IJIS INSTITUTE

IJIS INSTITUTE

Acknowledgments

This document is a product of the IJIS Institute; a private nonprofit collaboration network that brings together innovative thinkers from the public and private sectors, national practice associations, and academic / research organizations working together to solve public sector mission, information sharing, policy, and technology challenges.

We would like to extend a special thanks to ***Melanie Sankaran from Aventiv Technologies, Inc.*** who led the development of this whitepaper in support of the IJIS Institute's Corrections Advisory Committee and the IJIS Institute's Cyber Security Task Force.

IJIS Institute Cyber Task Force Members

Armando Aleman
American Cyber Systems Company

Jay Kaine
Motorola Solutions

Jim Emerson
National White Collar Crime Center

Collin Evans
Analysts International

Jason Franks
Mission Critical Partners

Jeramy Cooper-Leavitt
Aventiv

Kirk Lonbom
Microsoft

Dave McClure
PERF

Michael Melore
IBM

Anil Sharma
IBM

Maria Thompson
Amazon Web Services

Stacey Wright
Cyber Resiliency Services

Cyber Crime Support Network

Larry Zorio
Mark43

IJIS Institute Corrections Advisory Committee Members

Fred Roesel

Marquis Software

John Daugherty

Montana Department of Corrections

Brian Mattson

Microsoft

Kimberly Ramm

Fairfax County Sheriff's Office

Tom Herzog

Tom Herzog Consulting

Tanya Stauffer

Analysts International

Lisa Burlingame

Oklahoma Department of Corrections

Mary Beth Carroll

SAS Institute

Joe Russo

American Parole & Probation Association

Steve Viefhaus

Securus Technologies

James Meyers

Richland County Sheriff's Office

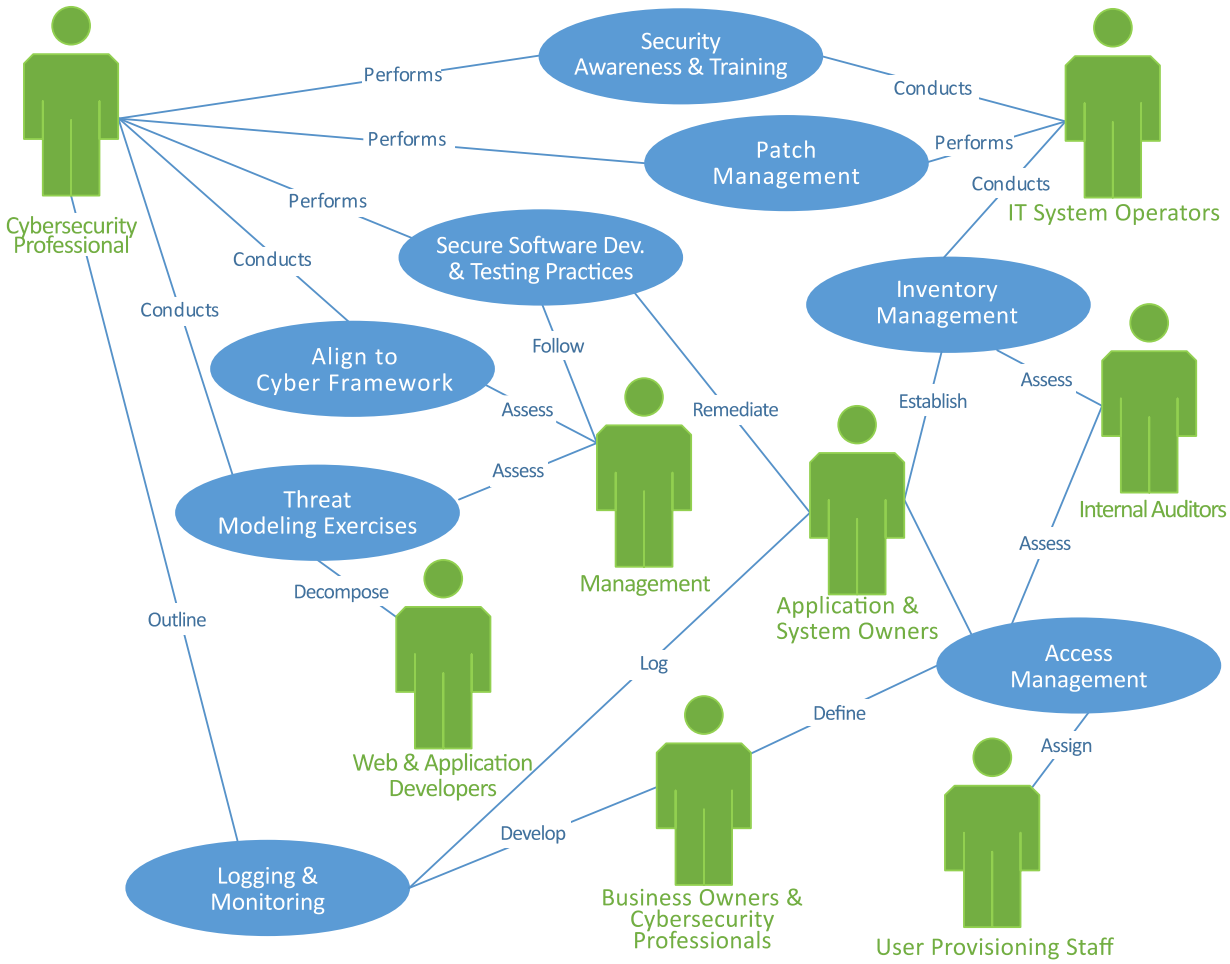
Cyber hygiene refers to the steps to improve the online security of a system and maintain system health. Implementing cyber hygiene is to adopt a security-focused mindset and develop safeguards, processes, and procedures to protect systems from cybersecurity threats.

The purpose of this whitepaper is to provide guidance when evaluating and maintaining the security of an application, system, and data. Justice and Public Safety systems often contain information that is subject to various regulations and requirements regarding the protection of data and the integrity of the systems where it resides. Understanding the fundamentals outlined in this whitepaper provides guidance on how agencies evaluate if the proper safeguards and controls exist along with their effectiveness for the proper protection of information. This whitepaper outlines key considerations, but by no means covers the breadth or depth when building and maintaining cyber hygiene. The concepts and fundamentals outlined can be used as a starting point, reference, and guidepost.

Additionally, the success of responding to a cybersecurity incident through detecting, analyzing, containing, eradicating risk, and successful recovery is predicated upon a solid cybersecurity program and incident response plan. This is discussed at the end of this whitepaper in Appendix B: Incident Management & Response.

Industry-recognized and common Information Security frameworks mentioned in this whitepaper are outlined below and more detail can be found in Appendix C: References & Resources. The importance of alignment to the cybersecurity framework provides a common language and taxonomy that ensures not just practitioners, but also auditors and industry partners, are interpreting the same language. In addition, the outcome is a strong cybersecurity program, that if followed with continuous diligence and attention, can help protect the viability of the agency and its data.

Cyber Hygiene Use Case Diagram



USE CASE SPECIFICATION: SELECT A CYBERSECURITY FRAMEWORK

Select a Cybersecurity Framework to align against.

Associated Actor	Relationship	Description
Cybersecurity Professional	Performs and Implements	Some agencies or companies may not have a dedicated Cybersecurity professional on staff. In this case, outsourced resources, or Internal IT and or Risk professionals should be utilized.
Management	Reviews and Determines Risk Acceptance	Management reviews identified gaps and determines the appropriate level of risk acceptance for a given exposure.

FLOW OF EVENTS

Align to a Framework – Determine a Cyber framework that best aligns with the business.

- ◊ Data Provided: Selected Cybersecurity Framework

Detail
Each information security framework has a similar control family and suggested action as it relates to the protection of data. If there are any government or regulatory requirements as it pertains to your business/organization, choosing a complementary framework is recommended. Information Security standards and requirements for the security of data and systems should be followed to achieve and maintain required compliance. Each of the 12 sections in this chapter can be referenced back to a cybersecurity framework control family and/or data security standard.

Conduct a Gap Analysis to Identify Control Weaknesses – Determine information security gaps within each control area. For example, if a control is met in some places, but possibly not everywhere across an organization or system, document the gap in the control.

- ◊ Data Provided: Control Weakness Gap Analysis

Create a Roadmap of Prioritized Risks That Need to Be Remediated – Review the comprehensive list of identified gaps in the framework control areas. For example, if there is a control gap that is missing vs. one that is partially met, a risk decision can be made on which gap to prioritize first.

- ◊ Data Provided: Prioritized Remediation List

Establish a Risk Acceptance Process for Any Risks That Are Not Remediated – Some control gaps might be at an acceptable risk level for the organization. When that occurs,

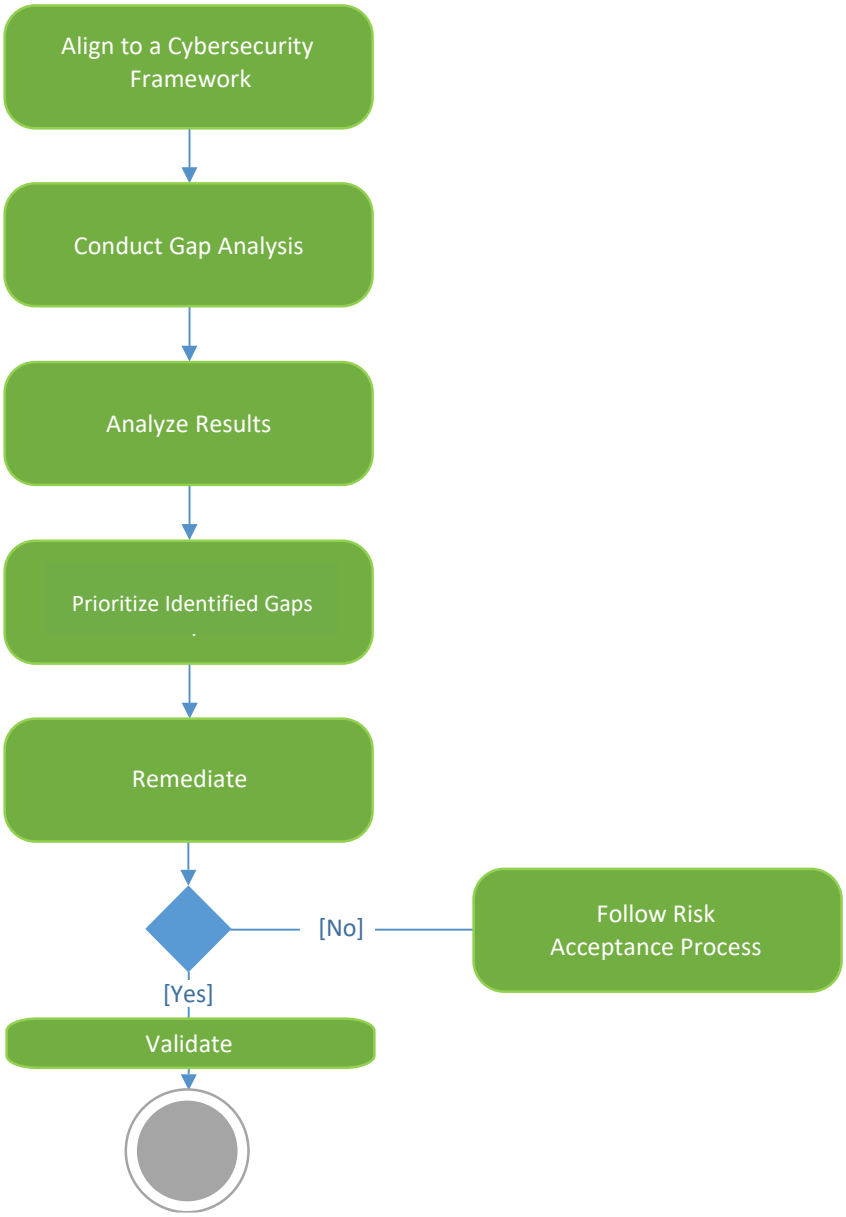
it is best to document via a risk acceptance process, including the right level of management authority to approve and sign off on the acceptance of risk.

- ♢ Data Provided: Documented process for the Acceptance of Risk

Review Gap Analysis At least Bi-Annually for Progress Towards Risk Reduction – Ongoing review of control gaps and progress should be reviewed at a minimum bi-annually. Any accepted risks should also be reviewed at least annually to ensure the risk should continue to be accepted, or due to current threat models, be prioritized for remediation.

- ♢ Data Provided: Updated Control Weakness Gap Analysis, Updated Prioritized Remediation List, Accepted Risk Document

Cybersecurity Framework Activity Diagram



USE CASE SPECIFICATION: INVENTORY MANAGEMENT

Implementing a reliable inventory of all IT systems, applications, and supporting hardware is the first step in defining the scope of a cybersecurity program.

Associated Actor	Relationship	Description
IT System Operator	Documents Systems	IT System Administrators document the operating system, middleware, and hardware for each system
Application Owner	Documents Applications	Application Owners document the applications they support and develop
Cybersecurity Professional	Utilizes inventory	Cybersecurity professionals utilize the inventory to apply the proper security protections and controls
Internal Auditor	Validates	Validate the inventory process and accuracy of the inventory

FLOW OF EVENTS

Create a Repository Containing Inventory and Purpose – Create a repository that contains the inventory and purpose of all IT systems including servers, workstations, underlying supporting hardware, and assigned network IP addresses.

The inventory should be stored in a place accessible to job functions that are responsible for system health, operation, and security. Changes and updates to the inventory should be restricted to a single function, such as IT to maintain the integrity of the information.

◊ Data Provided: Single IT Asset Inventory

Establish System Owners for Each System Within the Inventory – Establish system owners for each system within the inventory. A system owner is responsible for updating information such as operating system, IP address and function.

◊ Data Provided: Documented System Owner for each system in the IT Asset Inventory

Establish Application Owners for All Applications Within the Inventory – Application owners should be designated for all applications and associated with the underlying system in which they function.

This is important as common cyber hygiene functions, such as patch management, rely on both the application owner and system owner to work together. Additionally, if there is an issue with the application, a system owner may not be able to properly diagnose and fix the issue. Similarly, if there is a hardware or operating system issue, it may impact the availability of the application. Both roles play a key role in agreeing on acceptable maintenance windows and the expected availability of both the application and system. Therefore, both System and Application owners must be listed in the IT asset inventory.

- ◊ Data Provided: Documented Application Owner for each system in the IT Asset Inventory

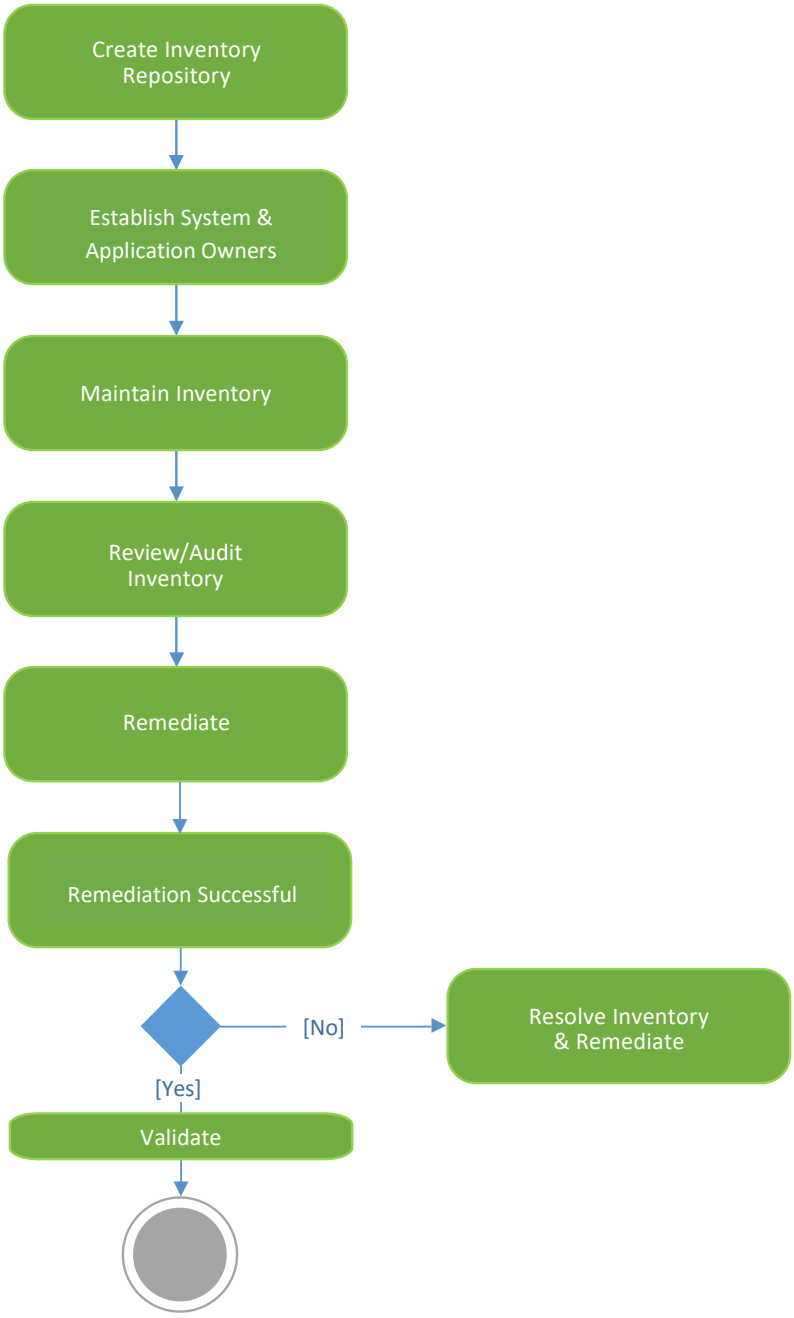
Develop a Process to Maintain Inventory – IT asset inventories need to be maintained to ensure the accuracy and integrity of the data. When a new system or application is introduced before it is in production, the inventory must be updated. When a system or application is decommissioned, create a step to update the inventory accordingly.

- ◊ Data Provided: Documented Maintenance Process and Procedure for IT Assets

Develop a Process to Review the Inventory for Accuracy At Least Annually – Have an independent function not responsible for maintaining the inventory, such as Internal Audit, complete an audit of what is in inventory, and the processes used to maintain the integrity of the data. Utilization of IT management and vulnerability reports can be helpful to compare what systems are audited vs. inventoried vs exist on the network.

- ◊ Data Provided: Documented process and procedure review

IT Systems Inventory Management Activity Diagram



USE CASE SPECIFICATION: ACCESS MANAGEMENT

Access control is a necessary component of data security that prescribes what users are allowed to access and use information and resources. Protecting data from unauthorized access is a means to ensure the integrity and confidentiality of the data and underlying system.

Associated Actor	Relationship	Description
Cyber Security Professional	Performs	Review the appropriateness of application and system access
User Provisioning Staff	Provisions	User Provisioning Staff assign rights to systems and applications based on role or job function
Application Owner	Creates User Roles	Application owners create roles with specific access rights to an application
Internal Audit	Audits	Internal Audit or independent third-party reviews users assigned to roles based on their job function and data access requirements
Business Owner/User	Documents Roles	Business owners outline specific roles needed to perform various job functions

FLOW OF EVENTS

Define User Roles – Cybersecurity professionals and/or identity and access management professionals work with business owners to understand user roles including application administration roles that support business processes.

- ◊ Data provided: Documented list of User roles for each application

Assign Users – Once roles are defined, specific users of the application should be assigned to a role within the application, allowing access to data and resources only needed to do the assigned business process.

Outline Requirements – If a role does not exist that matches a business process or data access permission, outline requirements for role creation with the application owner or third-party vendor and assign users to the newly created role. This ensures application and data access is restricted appropriately.

◊ Data provided: Documented new role definition and access rights

Review Users – Conduct a review of application users, job roles at least annually certifying all user access to data is appropriate. This review should also include making sure that previously employed users who are no longer with the organization have been properly removed from accessing the application.

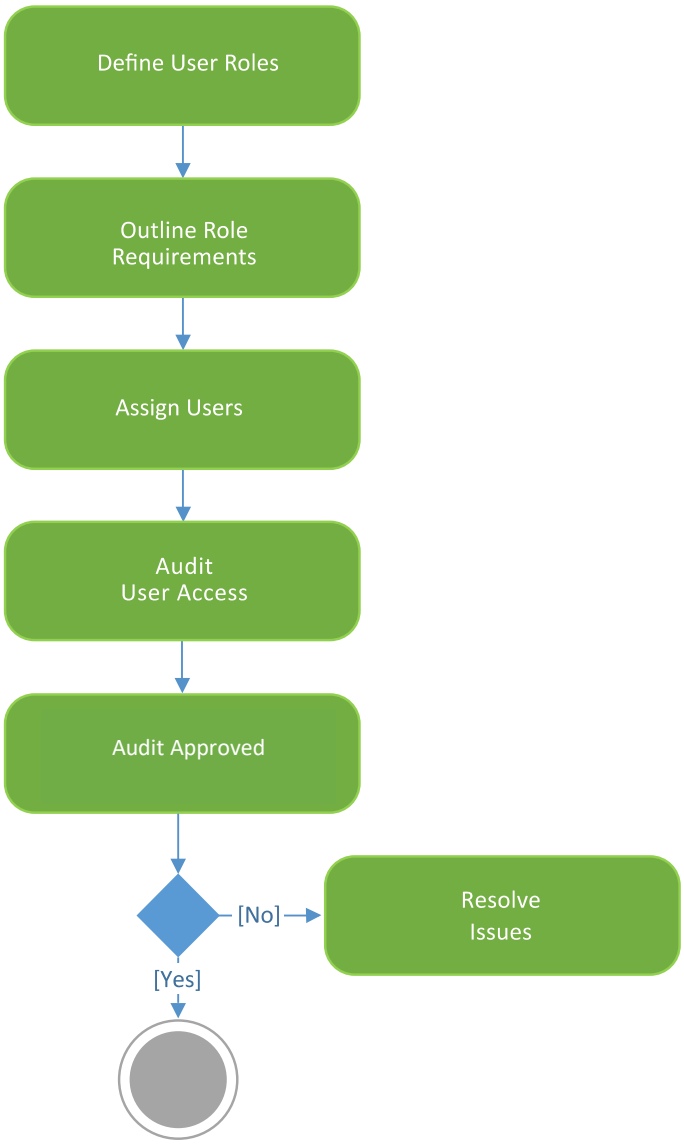
Application users should be removed from applications upon termination of employment (voluntary or involuntarily).

If a user termination process does not exist, it should be created and then incorporated as part of the periodic user access review process. This will validate the effectiveness of the termination and user de-provisioning process.

Any user that has changed roles within the organization should have existing access rights reviewed and updated as appropriate to the new role.

◊ Data provided: Documented User Access Review Process for each Application

Access Management Activity Diagram



USE CASE SPECIFICATION: LOGGING AND MONITORING

The purpose of an application and system log is to capture user activities and events. Log monitoring is the action of reviewing system and application logs to help identify attempts or the success of unauthorized activities. It is close to impossible to confirm the security of a system without having a trail of what, when and how a system was accessed.

Associated Actor	Relationship	Description
Application and System Owner	Develops and Implements	Application owners develop user and event logs as part of application development System Owners implement logging in the underlying operating systems
Networking Team	Assists	Networking teams assist the Security Operations Center to ingest logs centrally
Security Operations Center (SOC)	Reviews and Monitors	SOC team monitors activity on the network, applications, and operating systems for anomalous behaviors
Outsourced Information Security Provider	Reviews and Monitors	If there is not a dedicated Security Operations Center within the agency, outsource the function to a third-party provider
Business Owner	Outlines Business Processes	Business owners outline business processes to help develop user activities to be captured in logs.

FLOW OF EVENTS

Outline Business Processes – Outline business processes for each application to be monitored. Ensure user actions are recorded in logs generated by both the application and the underlying operating system, including any middleware.

- ◊ Data provided: Documented Outline of each business process for an application

Develop Use Case Requirements – Develop threat use case requirements on what should be recorded in log data based on business processes and normal vs. abnormal user behavior. Most Commercial

Off the Shelf (COTS) applications have default logging of user and system activities that can be enabled, or already enabled. This provides an audit trail of what happened when a particular user was logged into the system or application and what actions were performed.

◊ Data Provided: Documented use case for abnormal and expected user behavior

Inventory existing logs – Take inventory of what log files are available and if any need to be created or customized based on the business process or function of the application.

◊ Data provided: Inventory list of logs available from both the application and system

Generate/Gather Logs – Work with SOC and Networking teams to ensure logs generated from the systems are ingested into a central logging solution and accessible for at least 90 days. It is not important that all logs remain readily available or online. Logs may be archived due to size limitations and other potential storage requirements. Archiving logs protect logs from overwriting current log data. It is recommended archived logs are saved for at least 180 days before purging. Reference any applicable regulatory or information security standards, such as PCI, for specific logging requirements.

◊ Data provided: Inventory list of logs available from both the application and system

Determine Normal and Anomalous Behavior – Application owners should work with the SOC to determine what normal and anomalous behavior is. This provides important threat use case data that should be written in logs from systems, applications. For example, if there are repeated user authentication requests within a rapid time, this could signify an active threat of unauthorized access to the system. Therefore, it is important to create an alert that will trigger should that behavior exist in the logs so it can be investigated. There could be several standard threat use cases in what a user, or system account should and should not do.

One way to determine what to write in a log, is to put yourself in mind of an investigator. If there are repeated login attempts, it is important to know what application(s) or system(s) the attempts took place, what user account(s) were attempting to login, if any were successful, over what time and from what source IP address.

◊ Data provided: System and Application Logs, Documented use cases for abnormal and unexpected user behavior

Develop Automated Use Case Monitoring – Use cases should be developed and entered in a monitoring and alerting solution. If there is not an automated system that is available to correlate log files against threat use cases, it will be necessary to do regular log file reviews to try and identify any anomalous behavior patterns. The risk in a manual log review is potentially increased time of detection of a suspicious event, and thus increased time to respond and recover. Therefore, in this case, it is recommended that an outsourced provider perform this function for the agency or company.

Review Triggering Events – All triggered alerts on any threat use case rules that gets triggered should be reviewed and investigated. It is important to document what was reviewed, the procedures used to

investigate and the outcome or resolution of the triggered event.

Continue to build and tweak use cases as application functionality and or new business processes get introduced. If a threat use case alert gets triggered multiple times for the same behavior that is deemed a false-positive for example, review the rules used to trigger the alert and investigate, then make any needed adjustments. This will help tune the alerting system and ensure time and energy is spent on important events, making the process increasingly efficient and effective.

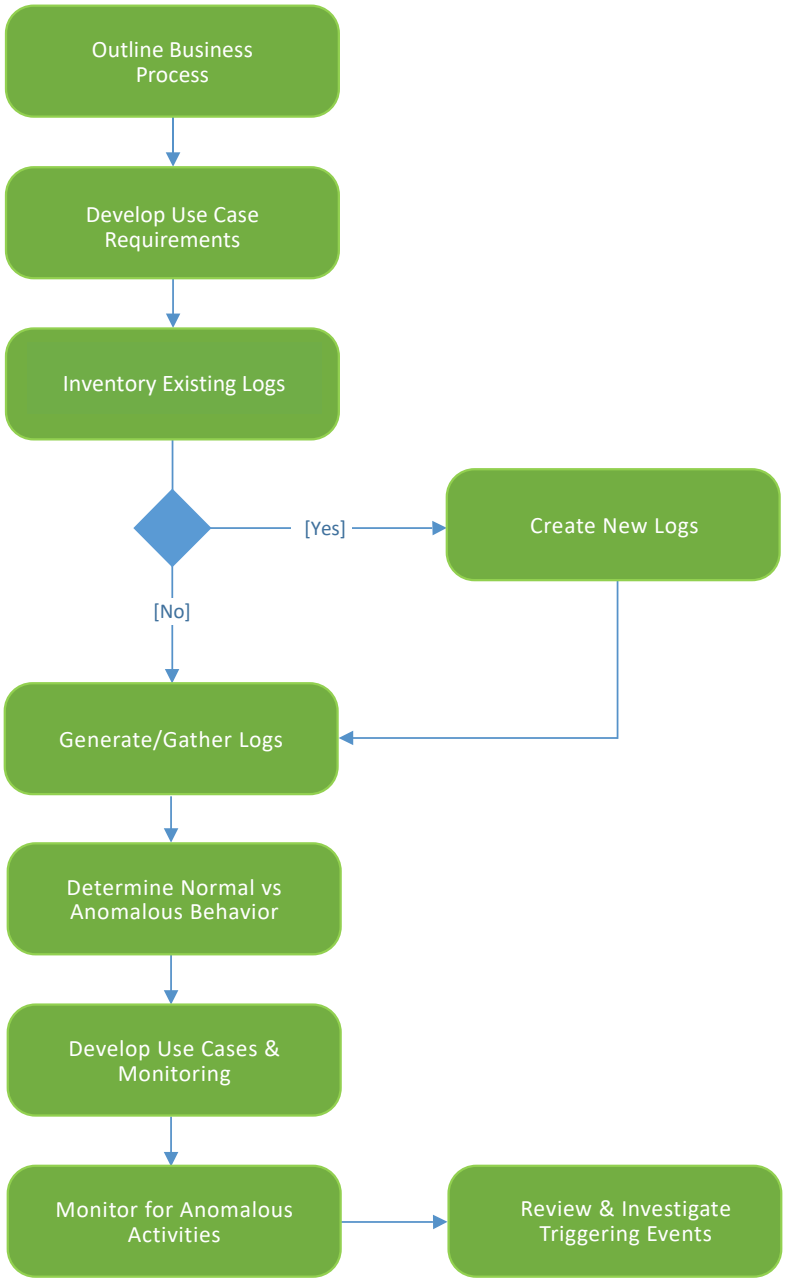
- ♢ Data provided: Application and/or operating system logs

There are many different log analysis solutions ranging from free to paid solutions. This by no means is a comprehensive list. What is important to consider when investing both time and money into a solution is that it is a good fit for the agency. To clarify, solutions considered and invested in should support the technologies and applications running at the agency. Log management solutions can either be outsourced to a managed security solution partner (MSSP) or supported by agency staff. Having the properly trained resources who understand both how to use the technology and what kinds of activities to log and look for is what is most important.

Reference of Common Log Analysis Solutions:

- ♢ Sematext https://sematext.com/logsene/
- ♢ SolarWinds Log and Event Manager https://www.solarwinds.com
- ♢ Splunk https://www.splunk.com
- ♢ LogDNA https://logdna.com

Logging and Monitoring Activity Diagram



USE CASE SPECIFICATION: PATCH MANAGEMENT

Patch Management is the process to update operating systems, third-party Commercial Off the Shelf (COTS) applications, middleware, and firmware. Vendors publish known vulnerability fixes in patch updates. Patches should be applied when issued to help secure the system, application, and environment.

Vulnerability Management is the control that is auditing the patch management process in an automated way. Vulnerability scans are run against system names and/or IP addresses to determine information such as application version, misconfiguration parameters, or settings.

To deem the effectiveness of a Patch Management program is to conduct regular Vulnerability scans. If the team responsible for patching has patched some or part of the relevant systems, this should be reflected in the output of the vulnerability scan showing systems still vulnerable and not patched properly.

It is recommended that all Patch Management actions and vulnerability scans are documented and approved via a formal change management process. In addition, all systems in the environment and/or network should be included as part of the Patch Management and Vulnerability Management Policy and Procedures.

Associated Actor	Relationship	Description
IT Operations Staff	Patches	IT Operations staff applies vendor patches and works with application owners to ensure applications are not inadvertently affected
Application Owner	Business Functionality Tests	Application Owners test and confirm the functionality of the application is not negatively impacted due to an applied patch
Cybersecurity Professional	Validates and Tests	Cybersecurity professionals validate and test that patches have been properly applied by running vulnerability management scans.
Outsourced Cybersecurity Professional	Validates and Tests	If there are not internal cybersecurity resources available, outsource to a trusted third party.

FLOW OF EVENTS

Establish a Patch Management Policy – Receive security patch updates from third-party vendors.

◊ Data provided: Patch Management Policy

Review The Risk Criticality of the patch – This is a very important step during the patch and vulnerability management process. If there is a critical risk that is addressed in a patch published by a third-party vendor, it is important for the agency to identify what systems are affected, including where they are located on the network. Utilizing the system inventory discussed in the above section is an essential resource to identify system information. If a system is exposed to the Internet, the risk of the vulnerability being exploited by an attacker is most likely higher than if the system was located on the internal network behind firewalls and other mitigating controls and security defenses.

◊ Data provided: Develop a list of affected systems requiring the patch

Prioritize Order – Prioritize the order of what gets patched first based on criticality and risk including the acceptable time to remediate per policy.

◊ Data provided: Document prioritization of patch management processes and procedures

Test Patches – Test patches in test and/or lower IT environments first before patching production. This is a very important step as some patches might negatively affect the application that is running on the system and therefore more time for testing is needed.

◊ Data provided: Validation of application functionality after patch

Run Vulnerability Tool – Run a vulnerability management tool against the environment and determine what if any vulnerabilities exist.

Review Missing Patches – Review and investigate any patches that did not properly get applied and determine root causes.

Repatch – Repatch any necessary systems.

◊ Data provided: Vulnerability report

Rerun Vulnerability Scan – Rerun the vulnerability scan validating that all system patches have been properly applied. Some systems may not be able to be patched for various reasons. Some applications may not allow for an allowable downtime window where the system would be off-line for patching. Other reasons can include the hardware or software are out of date, and therefore cannot accept additional patches per the outdate version of the software or firmware that is running.

Investigate any mitigating controls that might reduce the risk of the vulnerability if patching is not available. Common mitigating controls include additional network access control lists (ACLs) and further restriction of user access until upgrading applications or operating systems to current and vendor supported versions is possible.

◊ Data provided: Vulnerability report validating patch process

Document Systems Not Patched – Systems or applications that are not patched according to the stated Patch Management Policy timelines should be documented and reviewed by Management. Outcomes should be documented in the case of a risk

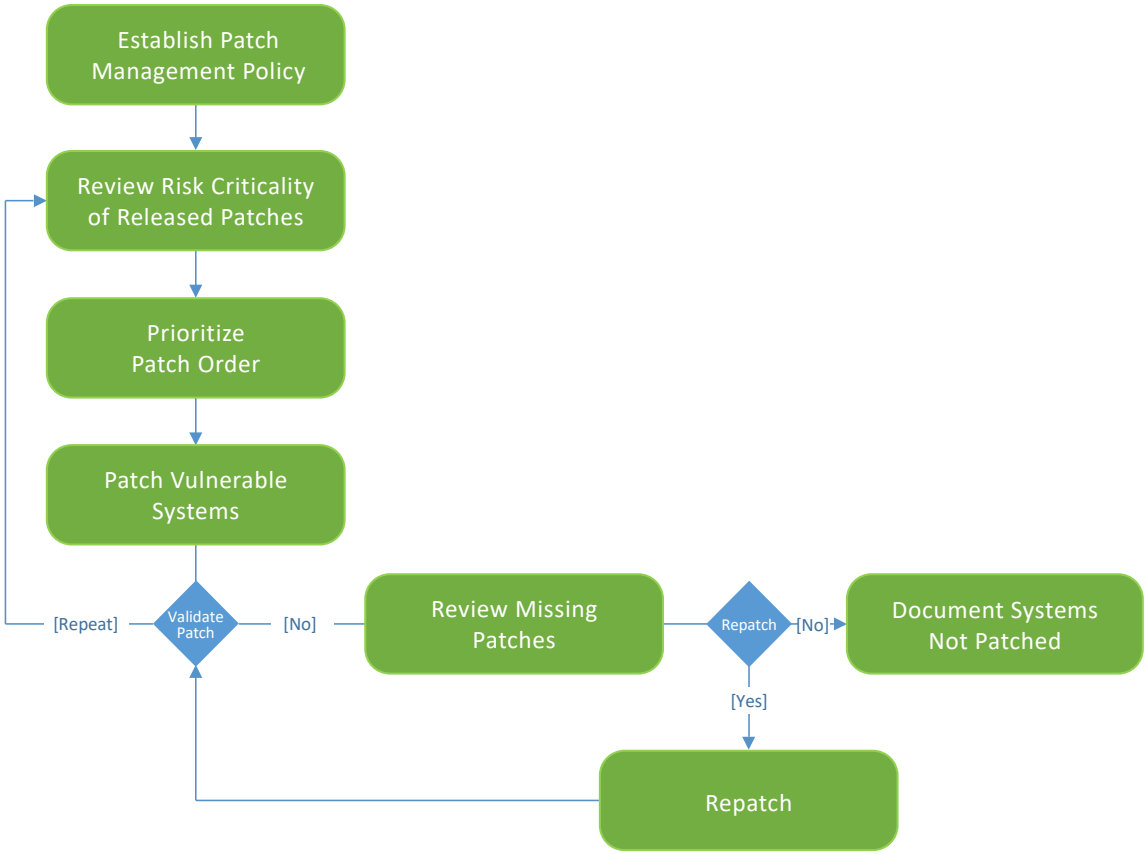
acceptance or exception to the patch management policy. All exceptions should to be reviewed at least bi-annually.

- ◊ Data provided: Documented Accepted Risks and associated applications and systems

Reference of common vulnerability management tools:

- ◊ InsightVM (Nexpose) by Rapid7 https://www.rapid7.com/products/insightvm/
- ◊ Qualys Vulnerability Management by Qualys https://www.qualys.com/apps/vulnerability-management/
- ◊ Tenable.sc by Tenable https://www.tenable.com/products/tenable-io

Patch Management Activity Diagram



USE CASE SPECIFICATION: SECURE SOFTWARE DEVELOPMENT & TESTING PRACTICES

Secure software development is a methodology for creating software that incorporates security into each development phase of the software development life cycle (SDLC). This is accomplished when secure coding standards are implemented during the development process at inception. Identifying and remediating application code vulnerabilities once an application has gone to production requires additional time, resources, cost, and risk exposure until remediation.

An industry best practice application security reference is the Open Web Application Security Project (OWASP)

- ◊ Open Web Application Security Project (OWASP) https://owasp.org/www-project-secure-coding-practices-quick-reference-guide/migrated_content.

Associated Actor	Relationship	Description
Cybersecurity Professional	Tests or Outsources	Cybersecurity professionals test applications for code level vulnerabilities. If the required skillset internally does not exist, they assist in outsourcing the test to a third-party application security vendor.
Development & Application Owner	Develops and Fixes	Development and Application owners fix vulnerabilities discovered in the code
Outsourced Application Security Penetration Testing Firm	Tests	Test for application code level vulnerabilities
Management	Reviews and Determines Risk Acceptance	Management reviews vulnerabilities in code and determines the appropriate level of risk acceptance for a given exposure.

FLOW OF EVENTS

Conduct Penetration Testing – When an application is developed by an organization it should be tested to ensure there are no code misconfigurations or vulnerabilities.

In the scenario of an internally developed application, cybersecurity professionals specializing in application security penetration testing should be enlisted. There are a several third-party tools that can be used to test application code for vulnerabilities. Select a tool that supports the coding language of the application.

◊ Data provided: Application Penetration Testing Report

Determine Risk & Exposure – Any vulnerabilities discovered during the testing process should be reviewed and the level of exposure determined. For example, if there is a vulnerability allowing a malicious user to take advantage of the application or system that would be determined as a high risk and high exposure to the agency or system.

◊ Data provided: List of vulnerabilities including associated risk

Remediate Vulnerable Code – Any vulnerability that is discovered should be reviewed by the development team and based on risk, prioritized for remediation.

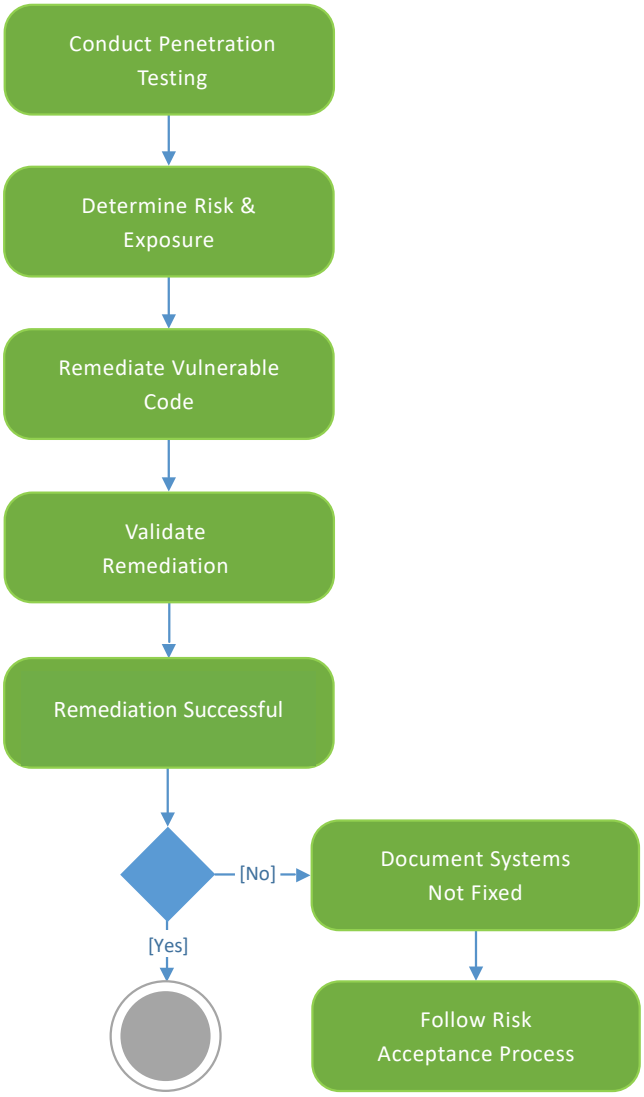
For example, if a vulnerability is determined to be High risk in terms of vulnerability exploitation and exposure, it should be fixed within a timeframe outlined by the agency's vulnerability management policy (mentioned above). Any vulnerability that is discovered that is critical in nature, should be fixed immediately. Based on the risk, an application code level vulnerability is just as risky as an operating system vulnerability. For example, if an attacker gains unauthorized access to an Justice and Public Safety application, application functionality and any data stored by the application may be affected. The integrity, confidentiality, and availability of the system has been compromised.

Validate Fix – Once the vulnerability has been remediated, it should be tested again and validated fixed properly by the application security professional or outsourced third-party cybersecurity organization. This is important, not only to make sure the flaw was appropriately fixed, but to also ensure no other vulnerabilities were introduced as part of the fix.

◊ Data provided: Application security report indicating remediation success

Repeat & Test New Applications – Code should be tested on a regular basis. New applications should be tested for application-level vulnerabilities before going live to production. In addition, any major code update or application release for an existing application should also trigger an application security test.

Secure Software Development & Testing Practices Activity Diagram



USE CASE SPECIFICATION: THREAT MODELING EXERCISES

Threat modeling is an exercise that is performed with the objective of identifying potential threats and attack vectors for a given system or application. Threat modeling is an important process to perform to ensure that existing controls in place to protect data and systems are designed correctly, but also to identify any new areas or vectors that are exposed or unprotected.

In Justice and Public Safety mission terms, given the complexity of interconnected systems and processes between systems and processes, performing threat modeling is important due to the unique threat model for the Justice and Public Safety industry.

There are several different frameworks that can be used to identify and perform threat modeling exercises. A few include common ones are the OWASP Top 10, and the MITRE Common Weaknesses Enumeration (CWE) and the MITRE ATTACK frameworks. Using a threat model framework helps ensure anticipated, and more importantly potentially, unanticipated outcomes and risks are identified.

MITRE Common Weaknesses Enumeration (CWE) Top 25 is a listing of the top 25 most common and commonly exploited vulnerabilities for a system. Understanding this list is a good way to gain an understanding of the most common threat vectors and weaknesses within systems and to work with the appropriate IT and development teams to test and identify weaknesses and vulnerabilities are identified and remediated.

- ♢ MITRE reference
  https://attack.mitre.org/

Open Web Application Security Project (OWASP) Top Ten is a list of the top 10 web application vulnerabilities that exist in web applications. Understand the top common vulnerabilities coded in web applications, to ensure those vulnerabilities do not exist within web applications. Malicious actors, when looking to gain unauthorized access to a system or network often attempt to exploit these to gain an initial foothold on the application and/or underlying system.

- ♢ OWASP Top 10 reference
  https://owasp.org/www-project-top-ten/

MITRE ATTACK Framework is federally funded and developed by the US government. The benefit of this framework is that it is comprised of 14 stages linked to the lifecycle of a cyber-attack. Each of the 14 stages are broken down into how an attacker could go about gaining access to a system or network. By understanding each stage, emulation of how an attacker thinks helps the exercise of threat modeling be as thorough as possible in identifying potential weaknesses of an application or system. To properly protect a system, fundamentally understanding potential weaknesses and exposures is necessary.

DREAD is a common way to properly risk rank identified threats. Understanding Damage Potential, Reproducibility, Exploitability, Affected Users and Discoverability can help determine true risk of a system or application, guiding where to focus any remediation or mitigation efforts for proper protection.

◊ DREAD reference
https://owasp.org/www-community/Threat_Modeling_Process#subjective-model-dread

There are a few other threat modeling frameworks that can be followed in addition to what is mentioned above. There is no one size fits all framework or silver bullet. What is important is to understand the system or application business purpose and choose the most suitable framework appropriate. In a similar manner, when designing a cybersecurity program to align to a cyber framework, aligning to a threat modeling framework is just as valuable.

Associated Actor	Relationship	Description
Cybersecurity Professional	Conducts	Cybersecurity professionals conduct threat modeling to identify threat actors and/or scenarios. Outsourced third-party cybersecurity professionals may be needed in lieu of internal resources
Web & Application Developer	Assists and Fixes	Web and application developers assist in threat modeling discussions and remediate findings if there are code changes needed to protect the application
IT Network Engineer & System Owner	Assists and Fixes	IT Network Engineers and System owners assist in threat modeling exercise and remediate findings if network or system level changes are needed
Business Professional	Participates	Business professionals participate in threat modeling exercises to educate them on potential threat vectors
Management	Reviews and Determines Risk Acceptance	Business professionals participate in threat modeling exercises to educate them on potential threat vectors

FLOW OF EVENTS

Understand the Purpose of the Application or System – Cybersecurity professionals meet with business owners of applications and systems. The purpose of the meeting is to determine the criticality and risk of systems in each area or function.

◊ Data provided: List of applications including associated business risk

Pick a Threat Modeling Framework – Cybersecurity professionals review different threat modeling frameworks and pick one that is most suitable to the system or application selected for threat modeling.

◊ Data provided: Threat Modeling Framework

Create a Detailed Application or System Overview – Create a detailed application overview. Start with the most business-critical application and have a discussion around what the application specifically does, what systems it is connected to and where it sits from a network perspective, i.e., internal or internet facing.

Decompose the Application or System – Decompose the application and identify what is expected from the application or system to function as designed.

◊ Data provided: Documented Application Overview and Business Function

Identify Potential Threats – Identify potential threats or ways that the application can be misused or misconfigured to gain unauthorized access to the system, application, or data.

Risk Rank Identified Threats – Use a risk ranking methodology such as DREAD and perform a threat ranking process to properly risk rank identified threats. Prioritize threats based on risk to ensure proper attention is placed on the highest risk to the protection of the system, application, and data.

◊ Data provided: Documented list of potential threats by risk

Identify Potential Vulnerabilities – Identify potential vulnerabilities associated identified threats.

◊ Data provided: Documented list of known vulnerabilities

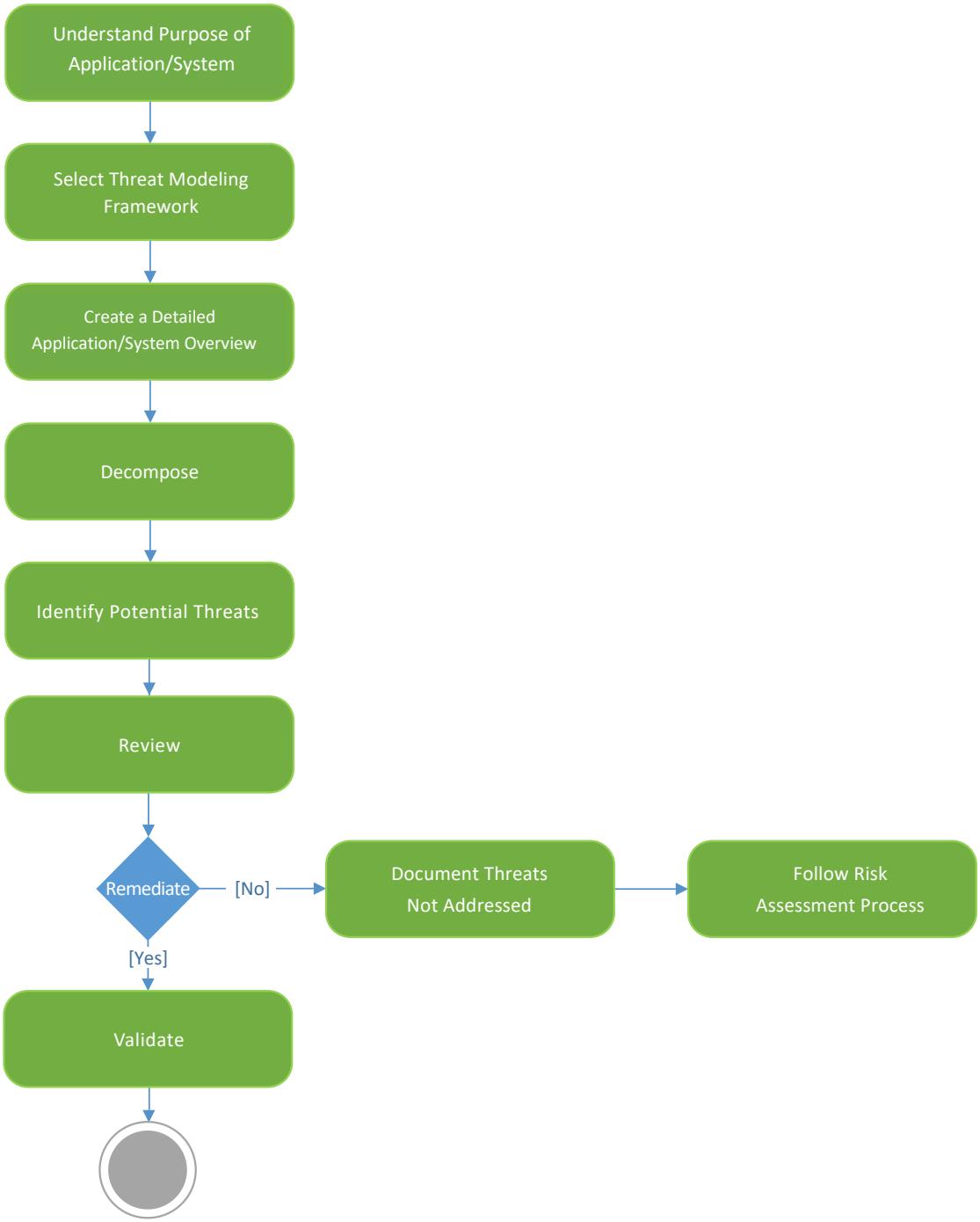
Review for Identified Potential Threats – Review the application or system for identified potential threats. This can be accomplished by conducing vulnerability scanning or penetration testing.

Remediate – Remediate areas of exposure and vulnerabilities, including implementing mitigating controls to threats from a network perspective.

◊ Data provided: Documentation validating remediation or mitigating controls

Repeat – Repeat exercise at least annually or as the application or system is updated.

Threat Modeling Exercise Activity Diagram



APPENDIX A: PEOPLE—SECURITY AWARENESS & TRAINING

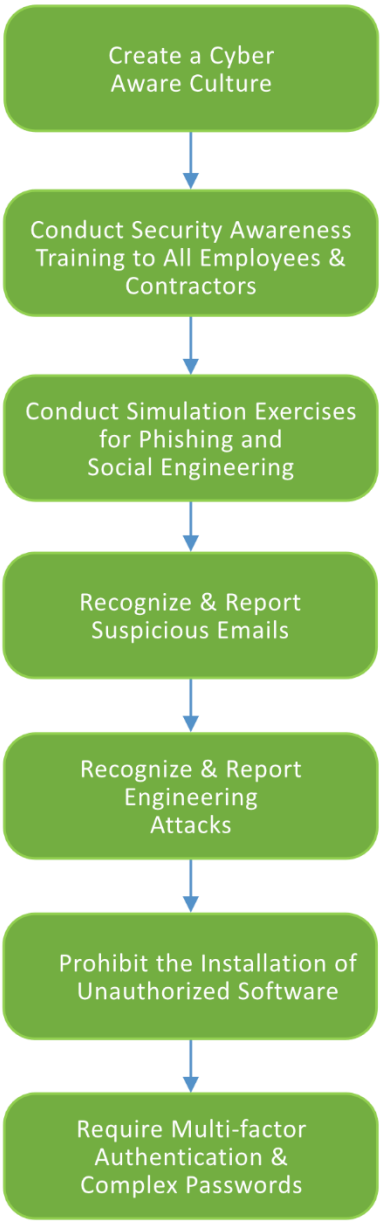
Having good cyber hygiene is not only based on technological controls but on establishing a security-focused mindset. People are just as important as technological controls and safeguards from a risk perspective. People are the first line of defense and ensuring the user base has been trained on cybersecurity concepts can mitigate some of the most dangerous threats faced by any agency or system.

People are one of the main gatekeepers of keeping systems and data protected. Having an informed workforce directly impacts how people behave that have access to a system. Fundamentally understanding that their actions can lead to a direct compromise of the integrity, availability, or confidentiality of a system is the key to a successful security awareness program.

Some fundamentals that employees should be trained on from a cybersecurity perspective include but are not limited to:

1. Create a cyber security awareness culture emphasizing that security is everyone's responsibility within the agency.
2. Establish an Acceptable Use Policy and Data handling procedures outlining what is acceptable as it pertains to the use of data and access to systems and networks.
3. Create a policy that requires complex passwords and multi factor authentication. Passwords should change at least every 90-180 days or in accordance with any regulatory or compliance requirements.
4. Unauthorized software should be prohibited from being installed on agency assets as they can contain malicious code and quickly lead to unauthorized access.
5. Recognizing emails with suspicious links or unknown senders can be used to gain unauthorized access to systems and networks. In addition, knowing where to report suspicious emails if they are received is also very important. Execute a phishing awareness simulation campaign and develop a mechanism to test employees on phishing awareness and adjust training accordingly.
6. Understand and recognize social engineering attacks, how it works and how it might be used as it pertains to the agency.

Cyber Security Awareness & Training Activity Diagram



APPENDIX B: INCIDENT MANAGEMENT & RESPONSE

Having an incident management and response plan is necessary to detect and defend a company or agency. The sections outlined in this chapter each play a vital role in incident recovery and the resumption of business function. It is impossible to detect a cyber incident if there are not proper logging and monitoring controls in place. Additionally, having a clear understanding of the system and application inventory during an incident can quickly identify what and where an incident may be occurring and provide the necessary information to contain an active incident.

Following strict patch and vulnerability management processes and procedures will protect against common vulnerability advisories used to penetrate a system. Training agency and company personnel on what to look for in suspicious-looking emails and links is often the first line of defense in securing an agency or company. Understanding and identifying what are the threats and who are the threat actors enables the identification of control weaknesses and focus on what needs to be invested in to strengthen the agency.

Being prepared for how the agency or company can be breached is one part of incident and threat management, the other part is how to respond when it is or has happened. Oftentimes, what is written in a standard operating procedure when in crisis may not always be followed. During an active incident, when alerts are going off and investigations are ongoing, it can be hard to exactly follow standard procedures. Therefore, the most critical thing that can be done in preparation of an incident is to have Incident Table Top exercises. These exercises can be done as a conclusion to a threat modeling exercise, or as a stand-alone activity. The goal is to pick a threat scenario, such as an agency worker who mistakenly clicks on a malicious link in their email and gets infected with a virus or malware. Once the scenario is set, stepping through a set of questions on what needs to happen from a technical perspective along with who in the agency or company needs to be notified will result in a plan should this occur. On paper, this might seem easy to think about, if this then that type of mentality is often misguided as people generally do not know how to or even respond as planned during an emergency. Therefore, it is imperative that several high-threat scenarios are broken down and walked through so that when there is an emergency, a cohesive plan that has been worked on and socialized to the people in in position to respond can.

Responding to incidents is not all about technological controls and remediations. What incident response outside firm is called to help and when should they be called? How management is informed, and when does the Legal department get involved? When do the authorities get called, do customer or consumer contracts require notification? What is the response to a press inquiry?

There are several good industry references for creating an incident response plan and conducting tabletop exercises.

- ♢ NIST ITL Bulletin, Guide for Cybersecurity Incident Recovery https://csrc.nist.gov/CSRC/media/Publications/Shared/documents/itl-bulletin/itlbul2017-02.pdf
- ♢ CRR Supplemental Resource Guide Incident Management

https://www.cisa.gov/sites/default/files/publications/CRR_Resource_Guide-IM_0.pdf

◊ Crowdstrike Cybersecurity Incident (IR) Plan & Process
https://www.crowdstrike.com/cybersecurity-101/incident-response/#:~:text=An%20incident%20response%20plan%20is,of%20its%20incident%20response%20program.&text=the%20organization's%20approach%20to%20incident,responsibilities%20for%20completing%20IR%20activities

APPENDIX C: REFERENCES & RESOURCES

Common Cybersecurity Frameworks & Standards

- National Institute of Standards and Technology (NIST) https://www.nist.gov/cyberframework/cybersecurity-framework-faqs-framework-components
- Information Standardization Organization (ISO) ISO 2001/IEC 27001 https://www.nist.gov/cyberframework/cybersecurity-framework-faqs-framework-components

Common software security specific frameworks

- OPEN SAMM https://www.opensamm.org/
- OWASP https://owasp.org/

Common Regulatory and Industry Requirements

- Payment Card Industry (PCI) https://www.pcisecuritystandards.org/document_library?document=pci_dss
- California Consumer Protection Act (CCPA) https://oag.ca.gov/privacy/ccpa
- Gramm Leach Bliley Act (GLBA) https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act
- Sarbanes Oxley (SOX) https://www.congress.gov/bill/107th-congress/house-bill/3763
- Health Insurance and Portability Accountability Act https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html
- Criminal Justice Information Services (CJIS) https://www.fbi.gov/services/cjis#:~:text=The%20FBI's%20Criminal%20Justice%20Information,partners%2C%20and%20the%20general%20public
- Federal Information Security Management Act of 2014 (FISMA) https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf
- Federal Risk and Authorization Management Program (FedRAMP) https://www.fedramp.gov/