Implementing Vulnerability Management tools Guidelines and Procedures, SBOMs, Continuous Threat Exploitation Management (CTEM) and enhanced Business Continuity Management

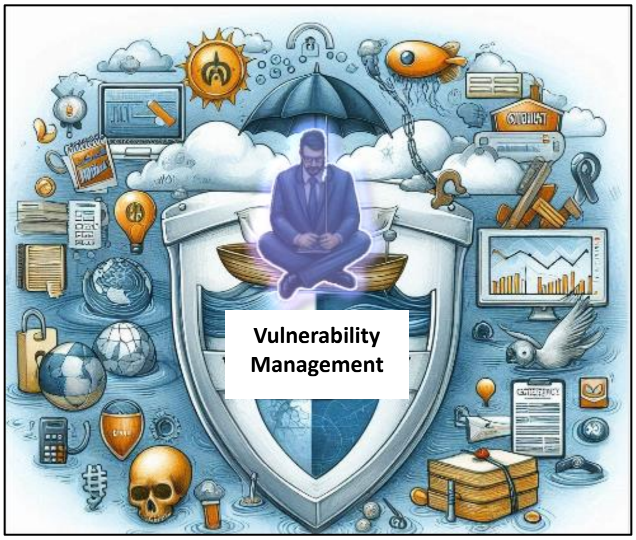


Figure 1: Achieve peace through a protected organization!

Contents include:

Continuous monitoring is essential for maintaining a secure and efficient IT environment. Here are the key reasons why it is important:

1. **Vulnerability-Free:** CVEs resolved prior to entering the production environment for new and changed applications and services.
2. **Early Detection of Threats**: Continuous monitoring helps in identifying potential security threats and vulnerabilities in real-time, allowing for immediate action before they can be exploited.
3. **Compliance**: Many industries have regulatory requirements that mandate continuous monitoring to ensure that systems and data are protected according to specific standards.
4. **Improved Incident / Problem Response**: By constantly monitoring systems, organizations can quickly detect and respond to incidents / Problems, minimizing the impact on operations.
5. **Enhanced Visibility**: Continuous monitoring provides a comprehensive view of the IT environment, making it easier to track changes, identify anomalies, and ensure that all systems are functioning as expected.
6. **Initiative-taking Risk Management**: It allows organizations to proactively manage risks by identifying and addressing vulnerabilities before attackers can exploit them.
7. **Cost Efficiency**: Early detection and mitigation of issues can save organizations significant costs associated with data breaches, downtime, and recovery efforts.
8. **Business Continuity**: Continuous monitoring supports business continuity by ensuring that systems are always up and running, reducing the risk of unexpected outages and disruptions.

Contents

Tabe of Figures

Introduction.

In this paper, I will discuss how SBOMs (Software Bill of Materials) and Vulnerability Management will help your organization safeguard against cybercrimes and technical problems. It also describes how to control the Software Supply Chain and achieve a vulnerability-free and compliant environment.

The problem

Critical infrastructure (Assets, Inventory and Configuration Management) comprises the physical and virtual resources and systems so vital to the Nation that their incapacity or destruction would have a debilitating impact on national security, national economic security, or national public health or safety. It is diverse and complex, and includes distributed networks, varied organizational structures, operating models, interdependent systems, and governance constructs[1].

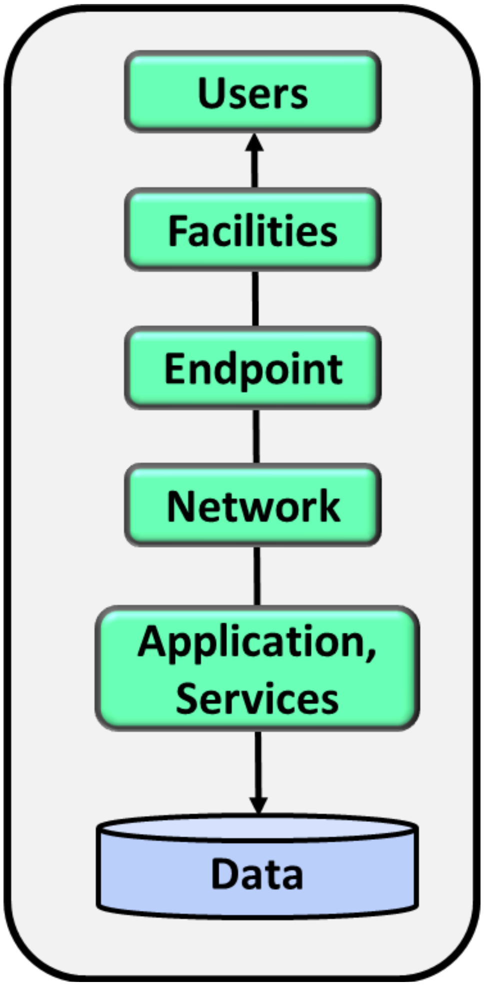


Figure 2: Logical and Physical protection must be applied to secure operations.

A rapid **Rise in vulnerabilities** is the largest threat to enterprises due to increased attacks by Nation-States (i.e., China, Russia, Iran, Korea, etc.) and Hackers, with costs rising every year. It is the new battleground faced by the United States and other countries depending on technology to survive and flourish. Imagine a world without electronics and their impact on our civilization.

The **rate of Vulnerabilities surpasses** the ability of most companies to fix them, leading to undue toil on staff, burnout and turnover. This rate is expected to rise and an automated approach to identifying and responding to detected vulnerabilities must be devised and deployed.

Vulnerability Management must be considered to understand the Software Supply Chain and avoid injecting known vulnerabilities into your systems and applications. The implementation of an SBOM tool can aid in providing vulnerability-free applications for the production environment (legal requirement).

SBOM tools also provide gateways to control application movement from engineering, through development, testing, quality control, and production acceptance to ensure the application, service, or product is vulnerability-free (Application Factory concept, with gateways based on Cybersecurity Score). These tools can also provide facilities to **support requirements definitions** (Requirements Transparency Matrix), assignment of work,

[1] National Security Memorandum on Critical Infrastructure Security and Resilience | The White House

capturing documentation and final products, and assisting in the control of an application's development and **support throughout its lifecycle**.

New Laws and Regulations have been devised and must be complied with by an **SBOM**.

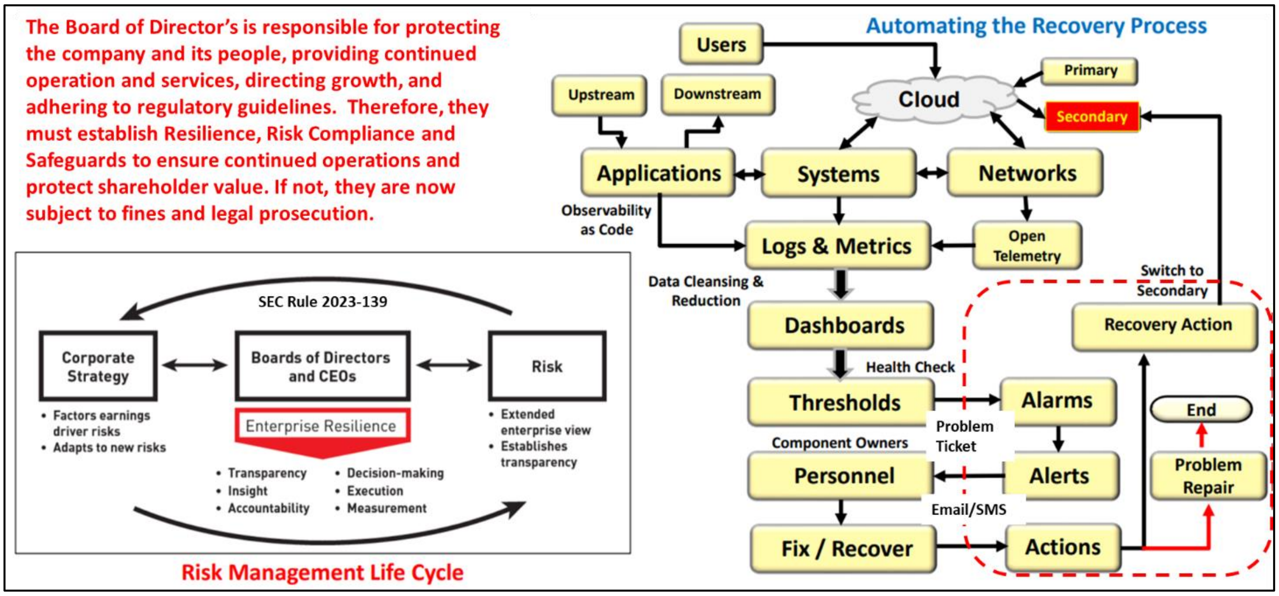
Business Continuity Management must be enhanced to support Service Level Agreements and a company's ability to continue to supply services and products in the event of another CrowdStrike type of occurrence.

Component owners must be identified and assigned to all assets they support for incident / problem management to quickly designate problems to their owner (component owner) and track problems through escalations and work stations until completed, documented, and stored in the company incident / problem management database.

The ability to develop an idea to a concept that can be engineered, developed, and deployed to production as **vulnerability-free** must be defined and supported via "**Whole of Nation**" and "**Secure by Design**" guidelines for best performance and security.

A **Vulnerability Risk Management Guidelines and Procedures Manual/Interactive Tool** must be developed and distributed throughout the organization to achieve awareness, and the feedback needed to quickly identify and respond to detected vulnerabilities in all their forms.

The Board of Directors concerns



The Board of Director's is responsible for protecting the company and its people, providing continued operation and services, directing growth, and adhering to regulatory guidelines. Therefore, they must establish Resilience, Risk Compliance and Safeguards to ensure continued operations and protect shareholder value. If not, they are now subject to fines and legal prosecution.

Figure 3: The Board of Directors Concerns and the new SEC Rule 2023-139

Protecting Shareholders and Investor's is the Board of Directors responsibility and failure to do so is now subject to penalties and fines associated SEC Rule 2023-139, dictating their responsibility to report breaches of material subsequence to the SEC via 'K' forms.

What is a CVE and how are they detected and reported.

Every month, the National Institute of Standards and Technology (NIST) adds over 2,000 new security vulnerabilities to the National Vulnerability Database. Security teams do not need to track all these vulnerabilities, but they do need a way to identify and resolve the ones that pose a potential threat to their systems. That's what the vulnerability management lifecycle is for.

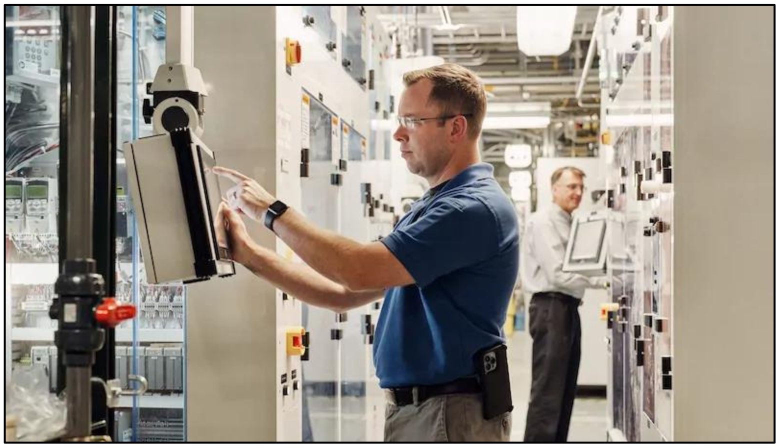


Figure 4: NIST reports over 2,000 vulnerabilities each month.

The vulnerability management lifecycle is a continuous process for discovering, prioritizing and addressing vulnerabilities in a company's IT assets.

A typical round of the lifecycle has five stages:

1. Asset inventory and vulnerability assessment.
2. Vulnerability prioritization.
3. Vulnerability resolution.
4. Verification and monitoring.
5. Reporting and improvement.

The vulnerability management lifecycle allows organizations to improve security posture by taking a more strategic approach to vulnerability management. Instead of reacting to new vulnerabilities as they appear, security teams actively hunt for flaws in their systems. Organizations can identify the most critical vulnerabilities and put protections in place before threat actor's strike.

Why does the vulnerability management lifecycle matter?

A vulnerability is any security weakness in the structure, function or implementation of a network or asset that hackers can exploit to harm a company.

Vulnerabilities can arise from fundamental flaws in an asset's construction. Such was the case with the infamous Log4J vulnerability, where coding errors in a popular Java library allowed hackers to remotely run malware on victims' computers. Other vulnerabilities are caused by human error, like a misconfigured cloud storage bucket that exposes sensitive data to the public internet. (these problem types are protected against in the "Secure by Design" Pledge).

Every vulnerability is a risk for organizations. According to IBM's X-Force Threat Intelligence Index, vulnerability exploitation is the second most common cyberattack vector. X-Force also found that the number of new vulnerabilities increases every year, with 23,964 recorded in 2022 alone.

Hackers have a growing stockpile of vulnerabilities at their disposal. In response, enterprises have made vulnerability management a key component of their cyber risk management strategies. The vulnerability management lifecycle offers a formal model for effective vulnerability management programs in an ever-changing cyberthreat landscape. By adopting the lifecycle, organizations can see the following benefits:

Proactive vulnerability discovery and resolution: Businesses often do not know about their vulnerabilities until hackers have exploited them. The vulnerability management lifecycle is built around continuous monitoring so security teams can find vulnerabilities before adversaries do.

Strategic resource allocation: Tens of thousands of new vulnerabilities are discovered yearly, but only a few are relevant to an organization. The vulnerability management lifecycle helps enterprises pinpoint the most critical vulnerabilities in their networks and prioritize the biggest risks for remediation.

A more consistent vulnerability management process: The vulnerability management lifecycle gives security teams a repeatable process to follow, from vulnerability discovery to remediation and beyond. A more consistent process produces more consistent results, and it enables companies to automate key workflows like asset inventory, vulnerability assessment and patch management.

The stages the Vulnerability Management Life Cycle are:

0. **Planning and Paperwork** – Resources, tools, guidelines and procedures, paperwork, etc.
1. **Asset discovery and vulnerability** – Inventory and catalog of hardware and software components, the organizations network, endpoints, and facilities and users within facilities used to support applications, products, or services. After identifying assets, the security team assesses them for vulnerabilities. The team can use a combination of tools and methods, including automated vulnerability scanners, manual penetration testing and external threat intelligence from the cybersecurity community, or SBOMs.
2. **Vulnerability Prioritization** - The security team prioritizes the vulnerabilities they found in the assessment stage. Prioritization ensures that the team addresses the most critical vulnerabilities first. This stage also helps the team avoid pouring time and resources into low-risk vulnerabilities.
    a. **Critical Ratings -** from external sources like MITRE list of CVEs (Common Vulnerability Exposures) and CVSS (Common Vulnerability Scoring System).
    b. **Asset Criticality –** the assets relative importance, regardless of the CVSS.
    c. **Likelihood of Exploitation –** rating devised by security team.
    d. **False Positives –** reported CVEs that are false.
3. **Vulnerability resolution, including:**
    a. Remediation.
    b. Mitigation.
    c. Acceptance.
4. **Verification and Monitoring –** to ensure resolution of CVE is completed successfully.
5. **Reporting and improvements –** to ensure problem management practices are adhered to and that Lessons Learned are distributed to those who have a need to best understand the mitigation of a vulnerability.

CISA has also announced the **Vulnrichment** program to improve vulnerability reporting.

Improvements in how DHS/CISA addresses CVEs and CVSS are constantly improving, so attention should be placed on the agency’s advancements.

Fighting Cybercrime costs with Secure by Design

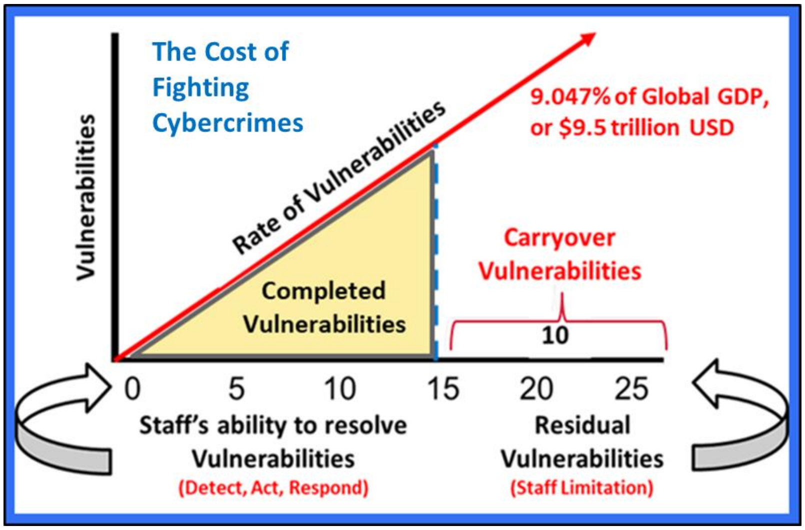


Figure 5: The cost of vulnerability defense today.

The current costs associated with combating cybercrimes and technology threats in the United States in 2024 is estimated at $9.5 Trillion dollars, which is 9.047% of the GDP, and projected to rise. This astonishing cost must be addressed so the funds can be put to better use by society. Because of this cost, the US Government has developed a "Whole of Nation" approach, where government, businesses, utility companies, and infrastructure firms all contribute to combating the problem through a "Secure by Design" approach to ensure vulnerability-free applications are introduced to the production environment and that all components from vendors live up to these same standards. The DHS/CISA has released a Pledge where companies can agree to the Secure by Design directive (like a "Seal of Approval" for product developers).

The DHS/CISA (Department of Homeland Security/Cybercrime and Infrastructure Security Agency), in response to new Executive Orders, Laws, Regulations, and Statures (some requiring SBOMs) has developed their guidelines to validate the Software Supply Chain and ensure that only vulnerability-free software products are introduced to the production environments of Information Technology (IT) organizations.

The United States is amid a generational investment in the Nation's infrastructure. This investment, and the emergence of innovative technologies, presents an opportunity to build for the future. In the 21st century, the United States will rely on new sources of energy, modes of transportation, and an increasingly interconnected and interdependent economy. This modernization effort will ensure critical infrastructure provides a strong and innovative economy, protects American families, and enhances our collective resilience to disasters before they happen — creating a resilient Nation for generations to come. A collective approach must be made to achieve this goal!

The United States also faces an era of strategic competition with nation-state actors who target American critical infrastructure and tolerate or enable malicious actions conducted by non-state actors (hackers). Adversaries target our critical infrastructure using licit and illicit means. In the event of crisis or conflict, the Nation's adversaries will also likely increase their efforts to compromise critical infrastructure to undermine the will of the American public and jeopardize the projection of United States military power. The growing impact of climate change, including changes to the frequency and intensity of natural hazards, as well as scarcities; supply chain shocks; and the potential for instability, conflict, or mass displacement places further strain on the assets and systems that Americans depend upon to live and do business.

Artificial Intelligence has given rise to new security detection and response conditions through Deep Fakes and newly devised persistent malware and virus attacks. Like SBOMs, **AIBOMs** must be devised to detect the presence of AI threats to aid in their elimination prior to entry into the production environment.

Actions must be taken to protect our society and internal structures, but first we must develop a Plan of Action with Milestones (POA&M) to define our goals and pathway to follow.

Whole of Nation and Secure by Design

The government has been addressing the problems associated with Cybercrimes and Technology issues for years. DHS launched a **Continuous Diagnostics and Mitigation (CDM)** project years ago. The goal of this project was to detect and score all cybercrimes and technical problems within the entire US Government and its affiliates. A dashboard system was devised, and Agencies utilized an approved set of tools to detect hardware and software problems. Initially all Hardware Assets (HWAM) were detected, then the Software Assets (SWAM) residing on the hardware were identified, finally a cross-reference of software was established by release level to define which modules had to be updated against vulnerabilities. Locational information was added to the findings so that it was possible to develop an Inventory and Configuration profile for the US Government. Software analysis of a specific asset (i.e., Microsoft Windows) was performed and the reports and displays generated showed a wide range of release levels for components presently residing on hardware assets. Those software assets below an approved release level were scheduled for update. Unfortunately, a government is hard to coordinate in a manner that stays ahead, or even abreast, of problems related to release levels and patch requirements, making the project goals difficult to achieve. Obviously, an automated approach needed to be added to the solution!

This consideration was adopted by DHS/CISA within its Secure by Design approach and the advent of Machine Learning, Artificial Intelligence, and now Generative AI has made it conceivable to automate solutions when vulnerabilities are detected, but they are still after the event has occurred and a mitigation added to the National Vulnerability database (NVD). Another roadblock!

Fortunately, new tools and concepts are constantly being devised to assist in identifying and proactively mitigating cybercrimes and technology threats as they occur. These tools recognize a problem and take pre-programmed actions to define the issue, seek advice online about the issue, and quarantine or rectify the issue in real-time. The process is currently underway and not fully developed or available in its present form. So, we still must take corrective actions on our own until the new tools have matured enough to be introduced into the IT environment.

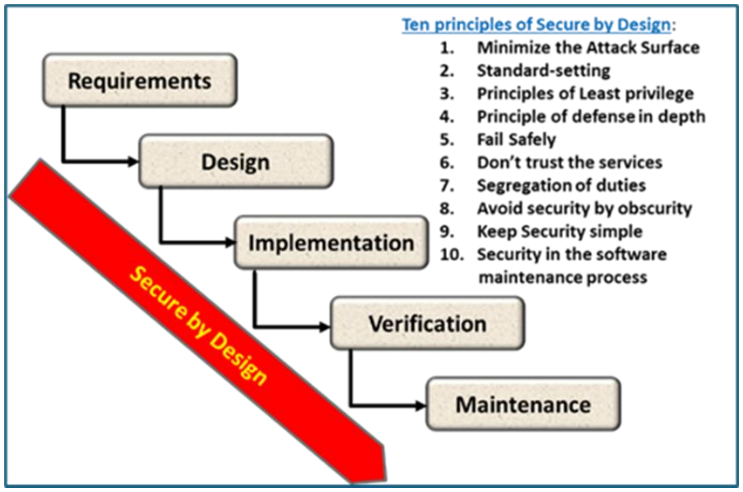

Requirements
Design
Implementation
Verification
Maintenance
Secure by Design
Ten principles of Secure by Design:
1. Minimize the Attack Surface
2. Standard-setting
3. Principles of Least privilege
4. Principle of defense in depth
5. Fail Safely
6. Don't trust the services
7. Segregation of duties
8. Avoid security by obscurity
9. Keep Security simple
10. Security in the software maintenance process

Figure 6: Secure by Design principles and phases.

The Secure by Design approach is a five step process, with ten principles, that helps a firm understand how to perform a **Requirements Definition** (i.e., idea, brainstorm, collaborate, innovate, and conceptualize), **design** (solution definition through the Systems Engineering Life Cycle), **Implement** (Systems Development Life Cycle), **Verification** (via Testing, Quality Control, Acceptance, and Deployment after receiving an Authorization to Operate), **Maintenance** (Support for Incidents, Technical Problems, Enhancements, Patches, and New Releases).

These principles will be further analyzed to identify improvements and safeguards that better protect our government and organizations against the ever-changing threats posed by Nation-States and Hackers.

New Laws and Regulations

Presently, implementing Applications and Services can include vulnerabilities and malware, which can cost your company lost revenue, damage your brand and reputation, result in fines and penalties, burden your staff and result in higher turnover levels.

A method must be implemented to catch vulnerabilities and malware prior to production acceptance.

New Laws have been mandated in the United States and Europe to address the problems, including:

- **Executive Order 14028** – Improving Nation’s Software Security Supply Chain and mandating SBOMs.
- **NSM-22**- National Security Memorandum on Critical Infrastructure Security and Resilience.
- **OMB M-22-18** and M-23-16 – Improving the Defense and Resilience of Government Networks.
- **SEC Rule 2023-139** – Disclosure of Material Cybersecurity breaches to protect shareholders.
- **FDA** – Control over medical device supply chain and cybersecurity problems (requires SBOMs).
- **CRA** – European Cyber Resilience Act – Hardware and Software Components cyber requirements.
- **DORA** – Digital Operational Resilience Act – Strengthen the financial sectors resilience.
- **GDPR** – EU Digital Rights of their Citizens.
- **Deploying AI Security Systems -** joint paper from CISA, NSA, and DOJ on employing AI Security.

Once the development process is upgraded and new Standards and Procedures created, an Awareness Program must be developed and the Staff Trained.

New Vulnerability Management guidelines and procedures must be integrated into the staff’s daily process for new and changed applications and services, with automated support whenever feasible.

Input from every part of your organization will help identify all types of vulnerabilities, some not yet defined, that must be addressed. Taking a “**Whole of Enterprise**” approach to Vulnerability Management will result in your enterprise benefitting from the entire staff’s input and improve your staff’s ability to understand, detect, and recommend mitigations to vulnerabilities.

Managing Vulnerabilities to protect the Enterprise.

What are Vulnerabilities and how do they impact your organization:

1. A **vulnerability** is a recognized error condition that has been reported and defined as a Common Vulnerabilities Exposure (CVE) in the National Vulnerability Database (NVD), with description and resolution in the form of a patch or new release, along with component owner identification for Software Supply Chain management.
2. Companies apply **Patches or New Releases** to mitigate the problem. Mostly done manually, so there is a need to automate this process.
3. **Speed to resolve CVE's is too slow**, allowing Nation-States and Hackers to comprise additional attacks after reading the public vulnerability information.
4. **Companies resolve** new releases in months, and patches in weeks, while **hackers and Nation-States devise** new attacks in minutes to hours. (i.e., CrowdStrike secondary hacks started almost immediately.)

After the **CrowdStrike incident**, it was discovered that new attackers were using the information provided by CrowdStrike to devise **new attack vectors** for additional exploits against unsuspecting companies.

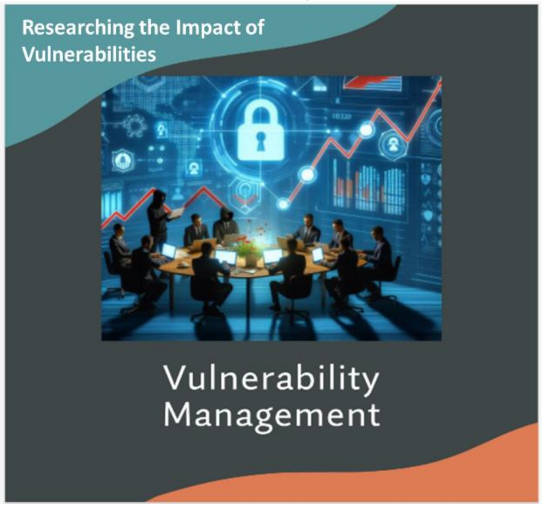


Figure 7: Managing vulnerabilities to protect the enterprise.

These attacks, combined with the initial attack, **prolonged outages**, overworked the staff, and caused loss revenue, tarnished reputations, and loss of business. Insurance companies will experience losses due to this problem and the future cost of insuring against repeat events will be greater.

Another problem that arose because of the CrowdStrike issue was a company's ability to recover operations within acceptable Service Level Agreements (SLAs). This increased costs to IT organizations also resulted in a new round of discussion on how best to protect the enterprise. Fines related to failed SLA goals were also received by companies whose clients were impacted by the outage, with lawsuits to follow.

As companies had to wait for a mitigation by CrowdStrike before they could even start their systems (thumb drive to start system and accept download of corrected CrowdStrike system), others could not correct data streams for a restart (Old Master, combined with Forward Recovery of changed data to create a New Master).

Companies may not have had an available relocation site because they were too slow to declare a disaster and there was not enough space to support them at the managed services providers (MSP) site. In short, there were a host of problems that were not even conceived of within a recovery operation. We must make better preparations in the future!

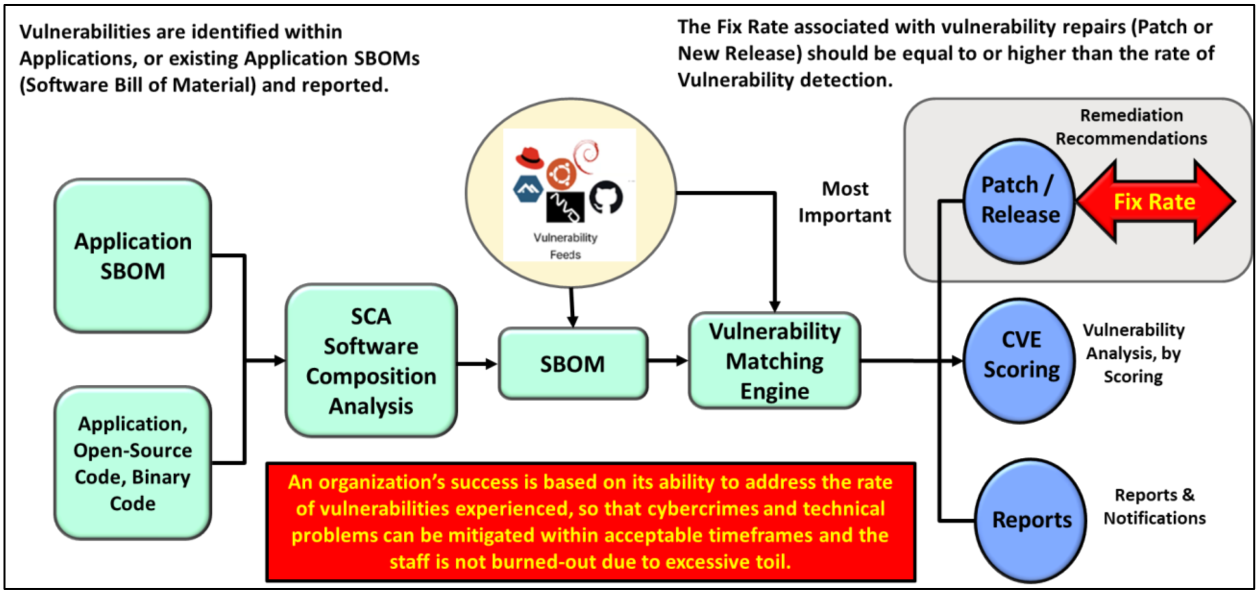
What is the major problem faced by organizations?

The increasing rate of cybercrimes and vulnerabilities is overwhelming most companies, along with the lack of trained staff and their being overburden with too many tools for a person to master to respond to cybercrimes and vulnerabilities. The costs keep going up, but management wants the same, and more, work done for less money. It is achievable, but a capital investment must be made to receive operations cost reductions and service improvements that far exceed the initial investment in new tools and staff training.

SBOMs are a start, but not the complete answer to our problem. Knowing you have a hundred vulnerabilities will not always allow you to determine which vulnerability to fix first, or how many components in your environment are impacted by a vulnerability.

Organizations need SBOMs and Vulnerability Management today because:

1. **Transparency and Security**: SBOMs offer a clear view of software components and highlight resolved security vulnerabilities contained in CVEs.
2. **Compliance with Regulations:** They help adhere to cybersecurity norms and industry best practices to provide vulnerability-free entry to production.
3. **Effective Vulnerability Management**: SBOMs facilitate quick identification and correction of known software vulnerabilities.



Vulnerabilities are identified within Applications, or existing Application SBOMs (Software Bill of Material) and reported.

The Fix Rate associated with vulnerability repairs (Patch or New Release) should be equal to or higher than the rate of Vulnerability detection.

An organization's success is based on its ability to address the rate of vulnerabilities experienced, so that cybercrimes and technical problems can be mitigated within acceptable timeframes and the staff is not burned-out due to excessive toil.

Application SBOM
Application, Open-Source Code, Binary Code
SCA Software Composition Analysis
Vulnerability Feeds
SBOM
Most Important
Vulnerability Matching Engine
Remediation Recommendations
Patch / Release
Fix Rate
CVE Scoring
Vulnerability Analysis, by Scoring
Reports
Reports & Notifications

Figure 8: Identifying and Reporting Vulnerabilities

The largest problem faced in today's IT Environments is the ability to generate a "**Fix Rate**" for vulnerabilities equal to or greater than the number of vulnerabilities experienced in a day. If you cannot fix vulnerabilities at a rate equal to the rate experienced, then you will have existing vulnerabilities left over at the end of the day and it will be an even greater exposure to your enterprise. Features must be built into SBOM products to assist you in this effort. For example, a **Knowledge Graph** will provide an overall picture of your environment and allow for quicker identification of the impact of a vulnerability across multiple components, while **vulnerability scoring** will provide guidelines for fixing the vulnerabilities with the greatest impact.

A **knowledge graph** can significantly enhance the process of identifying assets associated with a vulnerability by providing a structured and interconnected representation of data. Here is how it works:

1. **Data Integration:** Knowledge graphs integrate data from various sources, such as vulnerability databases, asset inventories, and network configurations. This creates a comprehensive view of the relationships between vulnerabilities and assets.
2. **Entity Relationships:** By mapping entities (e.g., software components, hardware devices, vulnerabilities) and their relationships, a knowledge graph can show how a specific vulnerability is connected to different assets. For example, it can link a vulnerability in a software library to all the applications that use that library.
3. **Contextual Insights:** Knowledge graphs provide contextual information about each entity. This includes details like the severity of the vulnerability, the criticality of the affected asset, and the potential impact on the organization. This helps prioritize remediation efforts.
4. **Automated Reasoning:** Advanced knowledge graphs use automated reasoning to infer new relationships and insights. For instance, if a new vulnerability is discovered in a software component, the knowledge graph can automatically identify all assets that might be affected based on their dependencies.
5. **Visualization:** Knowledge graphs offer visual representations of complex relationships, making it easier for security teams to understand the scope and impact of vulnerabilities. This visualization can highlight critical paths and dependencies that might not be obvious from raw data.
6. **Querying and Analysis:** Security teams can query the knowledge graph to find specific information, such as all assets affected by a particular vulnerability, or all vulnerabilities present in a specific asset. This makes it easier to conduct thorough analyses and generate reports.

For example, a knowledge graph constructed from the National Vulnerability Database (NVD) can combine named entity recognition (NER), relation extraction (RE), and entity prediction to map vulnerabilities to affected products, vendors, and other relevant entities. This integrated approach helps in quickly identifying and addressing vulnerabilities across the entire software supply chain and assists in locating vendors committing violations.

Reporting problems within the IT Environment

The flow of creating applications and providing vulnerability-free applications into the production environment, while supporting error notification and recovery, is an issue faced by every organization.

Idea to Concept - Starting with an idea, or business suggestion, executives will develop the concept (brainstorm, collaborate, innovate, and develop the concept) to a level where it can be presented to the engineering department. **Engineers will develop potential solutions** (architecture, assets, components, programs, systems, vendor products, etc.) that can bring the concept to market and then provide the development department with the solution specifications (i.e., Epic, Features, Stories, etc.).

Once **development receives the solution specifications**, they will conduct a business analysis, technical analysis, Buy vs Build decision, and a Go / No-Go decision. Once approved, the development department will build and test code (Statis, Dynamic, Interactive), test the application (functions, security, etc.), provide acceptance validation (Program, System, Interactive, Game Day, Acceptance), and conduct Authorization To Operate (ensure vulnerability-free status, provide Support and Maintenance, provide Change and Release Management). Once the application is in production, supportive services must be provided to Users (Customer Support), Cloud and Network operations (NOC, SOC), and applications (Help Desk).

Network and security controls are provided by the NOC (Network Operations Center), SOC (Security Operations Center), while the Help Desk provides application support, and Customer Support centers in distributed facilities support customers. End-to-end communications is provided from the application, through the network and cloud, to endpoints where facilities and end users are located.

An inventory would provide a complete listing of all hardware, software, and infrastructure components and vendor contracts and supportive personnel, while configurations provide specific lists of components at facilities and distributed locations.

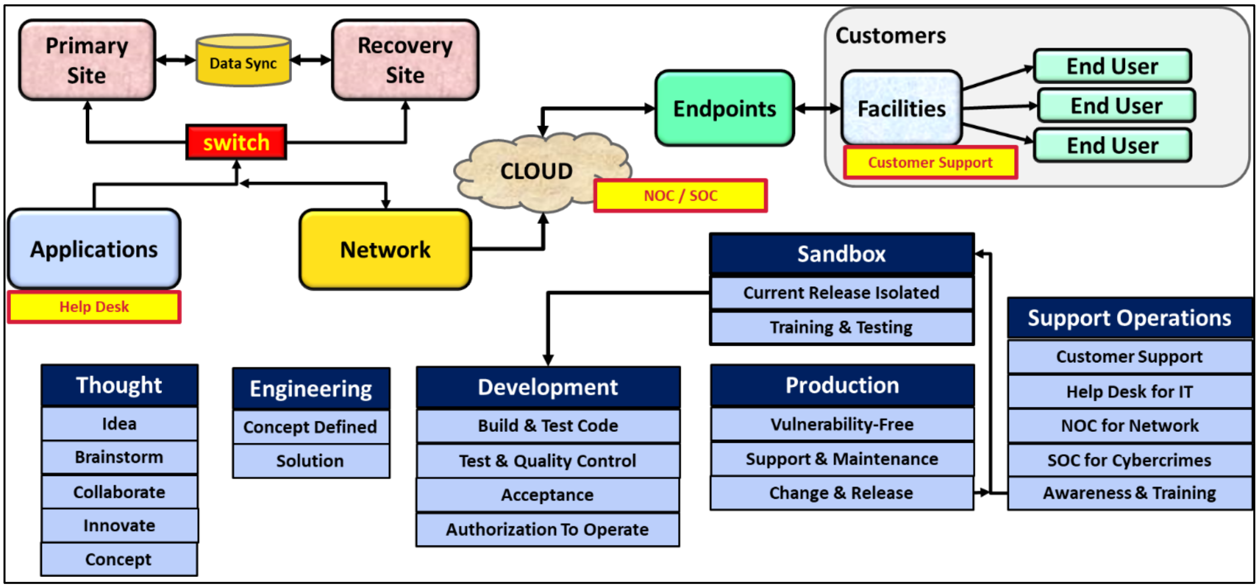


Figure 9: Enterprise Design through Support

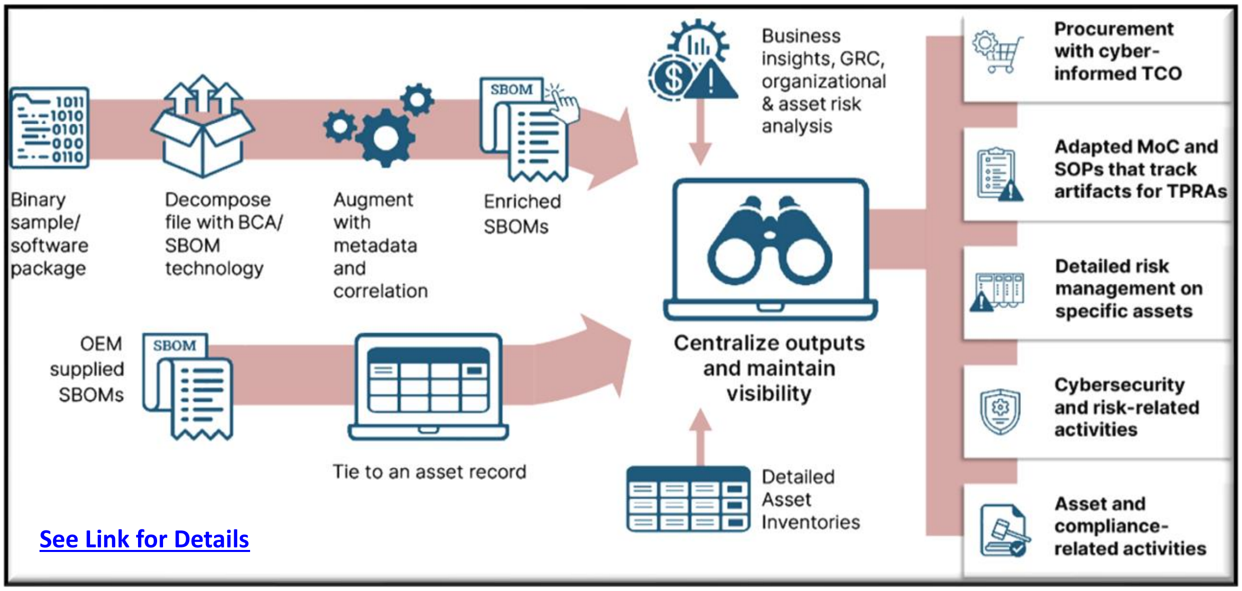
Recovery operations are supported by synchronized data based on Recovery Time Objectives (RTO) and the ability to switch from the primary to recovery system within an acceptable time defined in a Service Level Agreement (SLA Recovery Time Demands).

Vulnerability-free applications ensure that known CVE (Common Vulnerability Exploit) are not present within applications destined for the production environment and is a critical component within the Secure by Design guidelines, but they only represent known mitigations that reside in the National Vulnerability Database (NVD). **Active problems** are not yet mitigated and have not been reported to the NVD, so they cannot be recognized and could still be included within production applications (i.e., the CrowdStrike issue was an original issue and not reported to the NVD until CrowdStrike mitigated and documented the problem and its solution). **Relying on CVE mitigations alone** is not enough to provide complete protection for applications, so for full protection real-time detection and mitigation must also be implemented!

To best protect your environment you should examine the use of a Continuous Threat Exploitation Management (CTEM) tool to identify new problems and issue warnings that can be acted on to protect your environment during active production.

CrowdStrike is now facing multiple lawsuits from users who are accusing them of defrauding their investors and the investors of other companies. This case will be a baseline for other lawsuits associated with not rigorously testing changes made to products before they are released and will serve as a severe lesson to other companies. It proves the need for rigorous testing of changes before they become active in a production environment.

Protecting the company through SBOMs



1011
1010
0101
000
0110
Binary sample/ software package
Decompose file with BCA/ SBOM technology
Augment with metadata and correlation
SBOM
Enriched SBOMs
Business insights, GRC, organizational & asset risk analysis
Centralize outputs and maintain visibility
OEM supplied SBOMs
SBOM
Tie to an asset record
Detailed Asset Inventories
Procurement with cyber-informed TCO
Adapted MoC and SOPs that track artifacts for TPRAs
Detailed risk management on specific assets
Cybersecurity and risk-related activities
Asset and compliance-related activities
See Link for Details

Figure 10 Protecting applications against vulnerabilities with SBOMs.

Software Bill of Materials – are lists of software components that are included in an application. Sometimes programs are embedded within other programs (like assemblies used to build cars) and these tiers may be multiple layers in depth. Each program will be checked to see if a vulnerability (CVE – Common Vulnerability Exploitation) is associated with the program / component. A Public Vulnerability Databases (National Vulnerability Database – NVD) is maintained by DHS, but there are other databases containing CVE's and their explanation (i.e., Identifier, description, and mitigation as a patch or a new release), so it is important to know of **these databases** and include them in your vulnerability searches.

Using SBOMs to combat vulnerabilities has allowed the application test team to identify and mitigate program problems before they enter the production environment, thereby adhering to laws and improving the reliability of production operations. Combining vulnerability management with code testing programs (static, dynamic, interactive, and runtime) will further safeguard your organization and can be used to accelerate the movement to a DevSecOps environment.

The use of a Software Bill of Materials (SBOM) is essential for defending against active vulnerabilities in the software supply chain, and mandatory for complying with new laws and regulations. An SBOM provides information about the programs that make up an application, like parts in an assembly.

Like recalls associated with cars, SBOMs can warn companies of potential vulnerabilities in currently used or planned to be used programs that comprise an application, which is especially important when assembling cloud-based SaaS applications.

Software Bill of Materials (SBOMs) are used to validate program components used to create applications by scanning the application code and identifying program components (Open-Source Code, Vendor Code, and other Binary software products), even when they are embedded levels below the surface.

It then searches public vulnerability data bases to determine if active vulnerabilities are associated with the program product and any recommending changes that should be made prior to the product being introduced to the production environment (Patches, New Releases, etc.).

Integrating SBOMs within the testing environment will reduce your exposures to vulnerabilities and malware, so It is highly recommended and, in cases, mandatory to adhere to laws (FDA, EO 14028, etc.)!

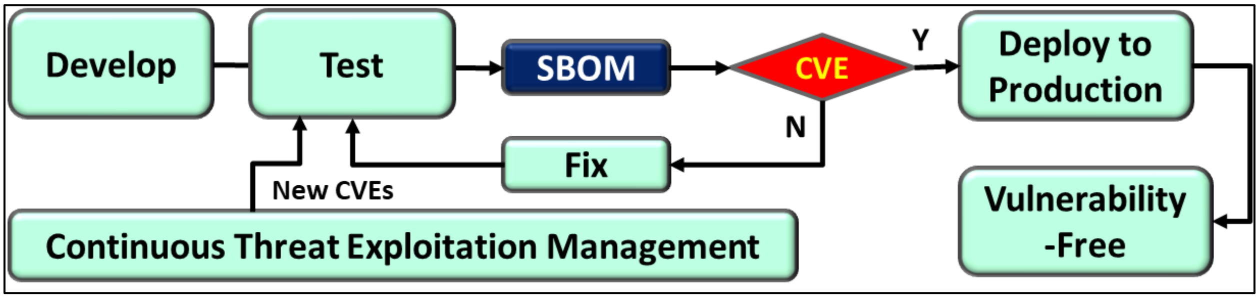


Figure 11: Where SBOMs fit within the software life cycle.

The above picture shows where SBOMS can help companies detect vulnerabilities in developing and deploying active code. The use of an SBOM will help assure you have eliminated known vulnerabilities, but you still must be concerned about unreported violations and malware (known as Zero Day vulnerabilities). Ethical hackers will report any potential vulnerabilities, but those hackers that are less than ethical can discover a vulnerability and keep it a secret until they release the exploit, thereby the name Zero Day vulnerability.

Analyzing the impact of Vulnerabilities

How do you know your company can react to a vulnerability attack and what would the impact be should such an attack occur?

Hackers use malware and viruses to obtain intellectual information, trade secrets, and other information from employees and company management that they can sell to bidders. Once discovered, the virus or malware is mitigated by the component owner and added to the National Vulnerability Database so that SBOMs can detect them and report the vulnerability to company personnel.

To determine the impact that vulnerabilities may have on your company, you must perform an investigation to define your present position and determine the future state you want to achieve. This process must include present direct costs (CAPEX, OPEX), exposures, weaknesses, and the potential losses to your company through Indirect Costs associated with reputation, and legal exposures.

Vulnerability Impact and defining Mitigation Actions

Direct Costs:

1. Intellectual Property
2. Financial Loses (CAPEX / OPEX)
3. Regulatory Fines
4. Incident investigation and recovery costs
5. Customer compensation (Failed SLAs)
6. Insurance costs

Indirect Costs:

1. Tarnished Customer Trust
2. Loss of Goodwill
3. Loss of prospective customers
4. Risk of legal action
5. Downtime and decreased productivity

How to protect the business?

1. Security Awareness & Vulnerability Management
2. Patch and Release Management
3. Password Management
4. Principle of Least Privilege (Secure by Design)
5. Advanced tools (i.e., SBOMs, etc.)

Figure 12: Analyzing the impact of vulnerabilities.

The end goal of this investigation must be a direction plan to determine how best to protect your company. This plan must include Security Awareness and Vulnerability Management to address patch and release management, password management to isolate procedures to only those personnel authorized to take these actions, the principle of Least Privileged should be used when considering access controls. Finally, advanced tools should be examined to determine which tools are best suited to safeguarding the company and its assets.

Using Vulnerability Management Tools and SBOMs

Determining the company's exposure to vulnerabilities and their impact on business continuity management.

1. **Present Cost** of vulnerabilities are defined, and a **benchmark** (CAPEX/OPEX) created.
2. **Workflow** associated with identifying and mitigation vulnerabilities (actions, tools, & time limit).
3. **Define weaknesses and gaps** in the process.
4. **Devise how to overcome gaps and weaknesses** to optimize vulnerability management workflow to an acceptable level that supports Service Level Agreements.
5. **Provide report to management** and request funding to resolve gaps and weaknesses, including:
   a. **Requirements Definition.**
   b. **Analysis of Alternatives (AoA)** for SBOM and Vulnerability Management Vendors.
   c. **Forward RFP to Vendors**, collect responses, analyze and select best of bread and most compatible to organization.

d. **Purchase product,** provide awareness and training, implement and deploy, integrate within functional activities, and

e. **Develop post-implementation benchmark** and compare to original benchmark to define savings or additional costs.

Determining the Return On Investment (ROI) and benefits received will require a comprehensive benchmark of Key Performance Indicators (KPIs) prior to and after the vulnerability management tool selection and included in the Analysis of Alternatives (AoA) performed when selecting tools.

Comparing Prior KPIs / Post KPIs = ROI or performing a Cost vs Benefits analysis when evaluating new products can be used to justify the purchase of a product.

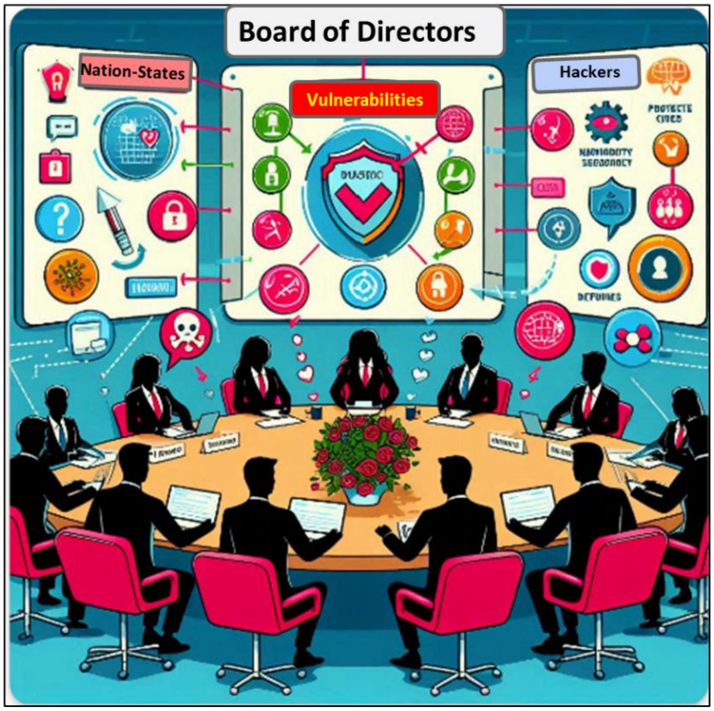


Figure 13: SBOMs help the Board of Directors protect shareholders and investors.

Vulnerability Management Maturity Lifecycle

When an organization determines it must examine and potentially include Vulnerability Management within their enterprise, they should consider the steps contained within the Vulnerability Management Maturity Lifecycle.

These steps are illustrated below, and your company should organize your study to first determine where you are in the maturity lifecycle and then plot the actions you want to take to achieve the level of maturity you deem best for your enterprise.

When developing your vulnerability management approach, you should consider the use of SBOMs to detect known vulnerabilities and tools that can be used to detect active vulnerabilities that may not have been mitigated and reported in the national Vulnerability Database.

Prior to becoming a CPE, a failure goes through a life cycle until mitigated and reported to the NVD. Some vulnerabilities are provided to the VEX (Vulnerability Exploitability Exchange) for further explanation while others are included in a KVE (Known Exploited Vulnerability Catalog) like those CVEs associated with a Microsoft Exchange Server, or other critical component.

The use of Continuous Threat Exploitation Management

Continuous Threat Exploitation Management (CTEM) tools should also be included in your research to determine how best to uncover and protect against active malware and viruses.

Finally, Guidelines and Procedures must be developed to provide awareness training to your staff and management on what vulnerabilities are, how to detect them, and how to best protect against their injection into the product supply chain for both new developments and changes made to current products. Not Taking these actions may result in your company being exposed to potential losses in reputation and business (use CrowdStrike as an example and if that does not scare you, nothing will).

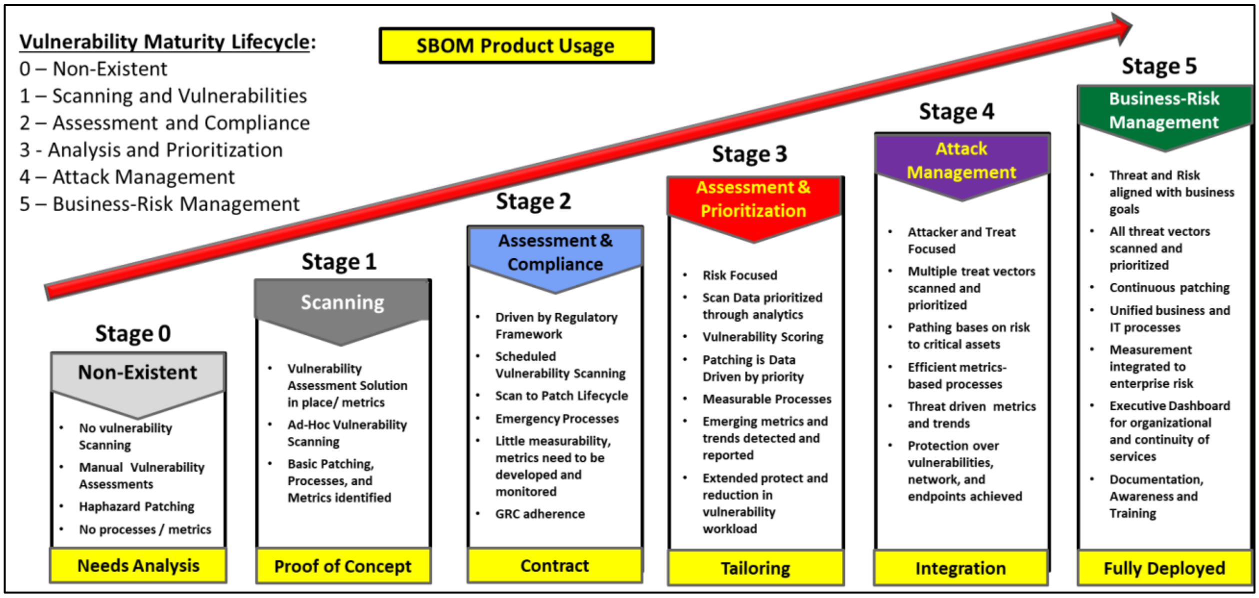

Vulnerability Maturity Lifecycle:
0 – Non-Existent
1 – Scanning and Vulnerabilities
2 – Assessment and Compliance
3 - Analysis and Prioritization
4 – Attack Management
5 – Business-Risk Management
SBOM Product Usage
Stage 0
Non-Existent
No vulnerability Scanning
Manual Vulnerability Assessments
Haphazard Patching
No processes / metrics
Needs Analysis
Stage 1
Scanning
Vulnerability Assessment Solution in place/ metrics
Ad-Hoc Vulnerability Scanning
Basic Patching, Processes, and Metrics identified
Proof of Concept
Stage 2
Assessment & Compliance
Driven by Regulatory Framework
Scheduled Vulnerability Scanning
Scan to Patch Lifecycle
Emergency Processes
Little measurability, metrics need to be developed and monitored
GRC adherence
Contract
Stage 3
Assessment & Prioritization
Risk Focused
Scan Data prioritized through analytics
Vulnerability Scoring
Patching is Data Driven by priority
Measurable Processes
Emerging metrics and trends detected and reported
Extended protect and reduction in vulnerability workload
Tailoring
Stage 4
Attack Management
Attacker and Treat Focused
Multiple treat vectors scanned and prioritized
Pathing bases on risk to critical assets
Efficient metrics-based processes
Threat driven metrics and trends
Protection over vulnerabilities, network, and endpoints achieved
Integration
Stage 5
Business-Risk Management
Threat and Risk aligned with business goals
All threat vectors scanned and prioritized
Continuous patching
Unified business and IT processes
Measurement integrated to enterprise risk
Executive Dashboard for organizational and continuity of services
Documentation, Awareness and Training
Fully Deployed

Figure 14: Vulnerability Management stages of Maturity.

Vulnerability Management Guidelines and Procedures generation

Once you have determined where you company is in the Vulnerability Management Life Cycle your next step would be to determine how best to protect your environment through vulnerability management tools and define the maturity lifecycle best suited to your enterprise. It is essential to define guidelines and procedures for management and staff so they can contribute to detecting and resolving vulnerabilities going forward. In enterprises that cover the world, guidelines and procedures may differ due to local laws and available tools. When this occurs, it will be necessary to develop various releases of your vulnerability management guidelines and procedures manual. Of course maintaining these manuals will be a concern for you as well, so utilizing automated tools to support your manual should be researched.

Even with a vulnerability management program in place, you can still experience problems that can impact your ability to continuously provide business operations to your customers and staff. For this reason, you must continue your Business Continuity Management efforts.

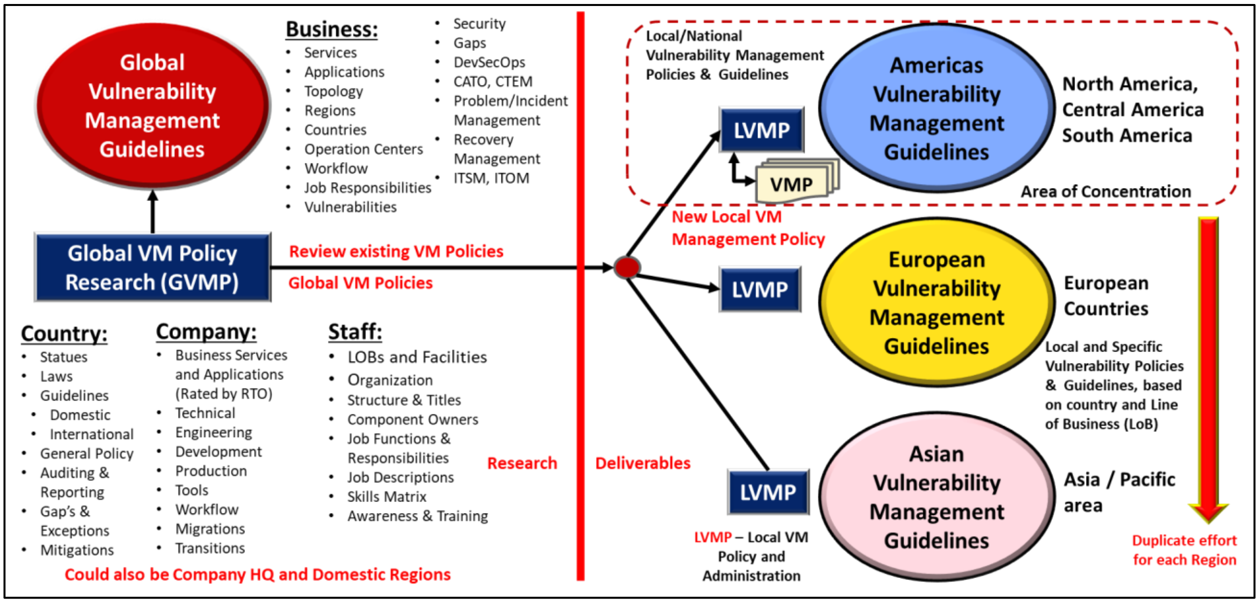

Global Vulnerability Management Guidelines
Business:
Services
Applications
Topology
Regions
Countries
Operation Centers
Workflow
Job Responsibilities
Vulnerabilities
Security
Gaps
DevSecOps
CATO, CTEM
Problem/Incident Management
Recovery Management
ITSM, ITOM
Global VM Policy Research (GVMP)
Review existing VM Policies
Global VM Policies
Country:
Statues
Laws
Guidelines
Domestic
International
General Policy
Auditing & Reporting
Gap's & Exceptions
Mitigations
Company:
Business Services and Applications (Rated by RTO)
Technical
Engineering
Development
Production
Tools
Workflow
Migrations
Transitions
Staff:
LOBs and Facilities
Organization
Structure & Titles
Component Owners
Job Functions & Responsibilities
Job Descriptions
Skills Matrix
Awareness & Training
Research
Deliverables
Could also be Company HQ and Domestic Regions
Local/National Vulnerability Management Policies & Guidelines
LVMP
VMP
New Local VM Management Policy
Americas Vulnerability Management Guidelines
North America, Central America South America
Area of Concentration
LVMP
European Vulnerability Management Guidelines
European Countries
Local and Specific Vulnerability Policies & Guidelines, based on country and Line of Business (LoB)
LVMP
Asian Vulnerability Management Guidelines
Asia / Pacific area
LVMP – Local VM Policy and Administration
Duplicate effort for each Region

Figure 15: Vulnerability Management Guidelines and Procedures generation.

Use the above picture as a guideline for your global vulnerability management development efforts.

The Ten step process of Business Continuity and Disaster Recovery Management

1. **Project Initiation and Management** – Gain management approval, backing, and long-term funding. Designate resources and define their responsibilities.
2. **Risk Evaluation and Controls Improvement** – define the Audit Universe (domestic and international laws and regulations that must be adhered to), conduct a Risk Analysis, identify gaps, exceptions, and weaknesses, then define controls needed to overcome risks – including insurance needs.
3. **Business Impact Analysis (BIA)** – define each function / facility/ department within a Line of Business and determine what would happen if they suffered a disaster event (i.e., loss of IT operations, facility loss, crisis impacting their people or location like a tornado or flood, etc.). For each of the potential disaster events, determine what actions must be taken and define these actions within a recovery plan. Provide awareness and training to management and staff, select tools, if necessary, develop strategy, build plan, and conduct exercises to orientate the teams and achieve a safe and efficient recovery should a disaster event occur.
4. **Developing Business Continuity Strategies** – Strategies are different for recovering IT Applications (Disaster Recovery), or Business Locations (Business Recovery), or an Active Shooter (Personnel Safety and Violence Prevention). Because of these differences, it is necessary to develop a comprehensive strategy (Business Continuity Management) that covers all recovery disciplines and needs. Purchasing an automated tool may be a solution that should be included in developing your recovery strategy.
5. **Emergency Response and Operations Restoration** (Backup, Vaulting, Restoration) – Make sure your data is backed up and available to use for recovery operation. Backup and recovery times

(i.e., Recovery Time Objective (RTO), and Recovery Point Objective (RPO) and Recovery Time Capability (RTC) which is the time you can presently recover data in) will dictate the amount of time needed to recover the impacted function of service.

6. **Designing and Implementing** Business Continuity Plans.
7. **Awareness and Training** must be provided to company personnel.
8. **Maintaining** and Exercising Business Continuity Plans
9. **Public Relations** and Crisis Communications
10. **Coordinating with Public Authorities** like First Responders, industry experts, and regulators must be maintained.

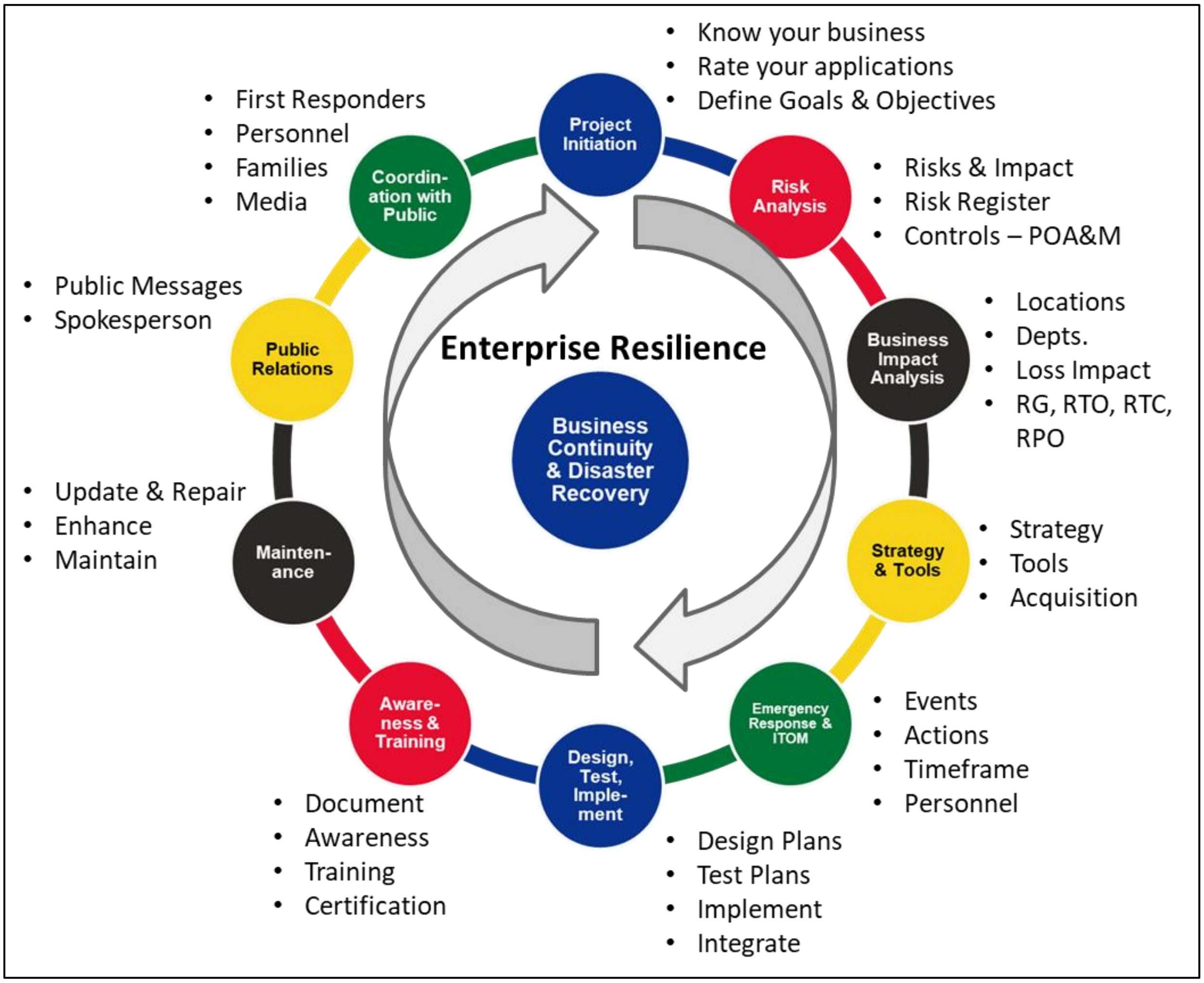


Figure 16: The ten step process to establish the Business Continuity and Disaster Recovery process.

Having a Business Continuity Organization capable of managing the full range of disaster events that can impact an organization's ability to continue providing acceptable services to its clients is essential to an organization's success. Combining BCM with Vulnerability Management will provide a means to proactively protect the organization against vulnerabilities, while ensuring the organization's success going forward. Integrating these guidelines and procedures within everyday activities should be a goal of your preparedness!

AWS DR Strategies

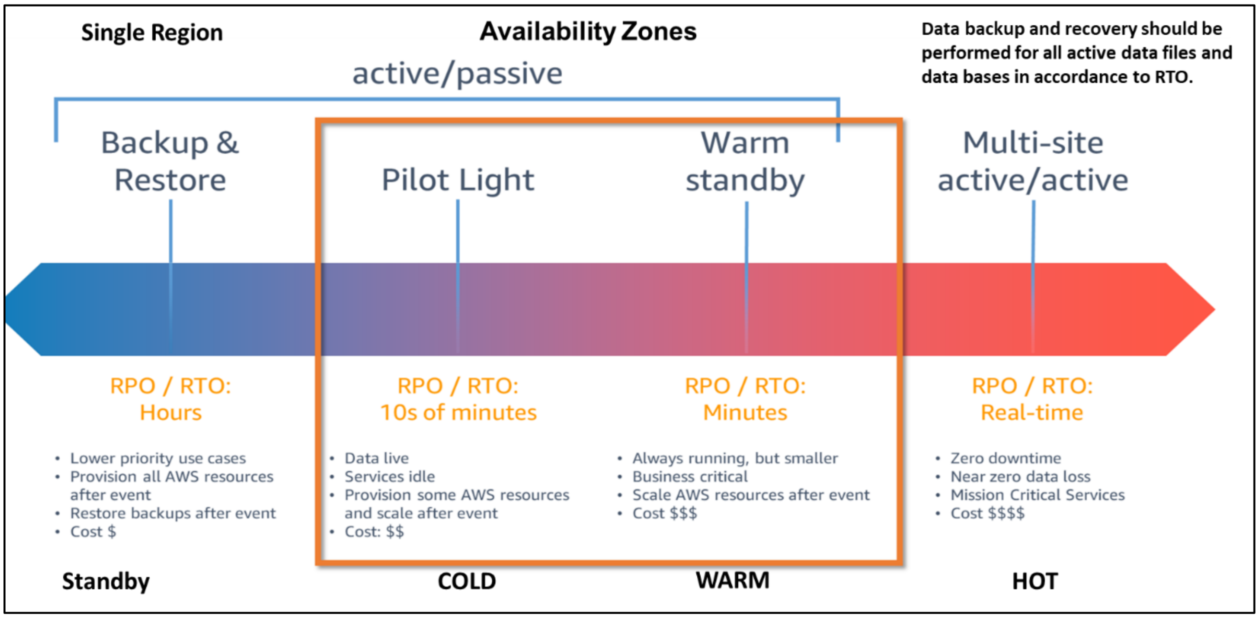
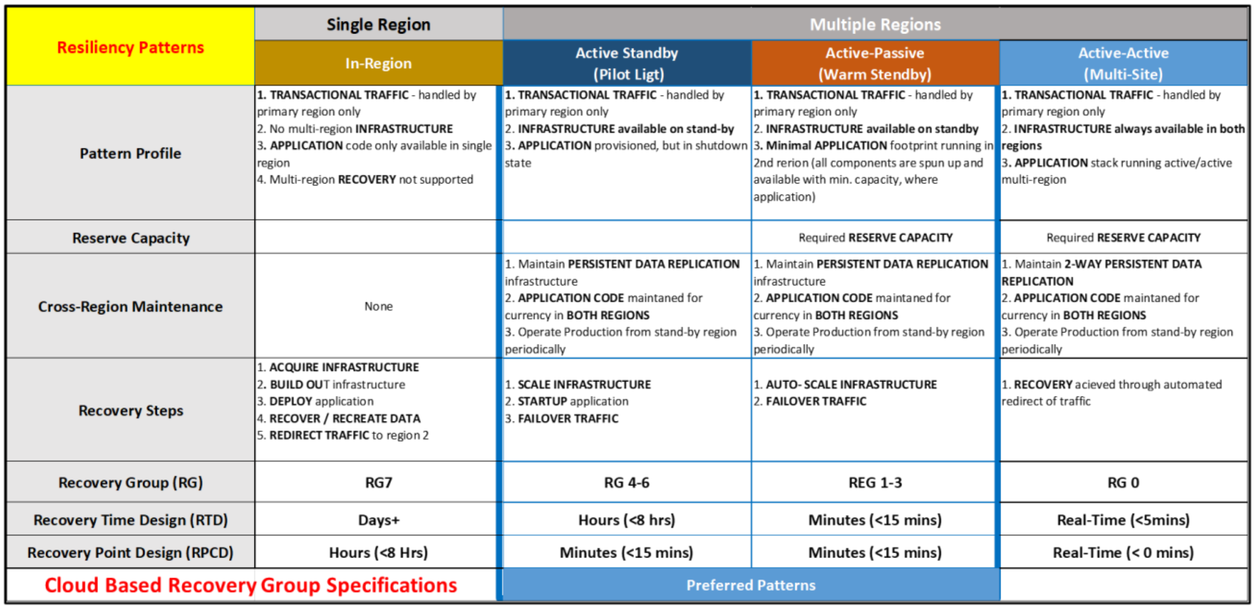

Single Region
Availability Zones
active/passive
Data backup and recovery should be performed for all active data files and data bases in accordance to RTO.
Backup & Restore
Pilot Light
Warm standby
Multi-site active/active
RPO / RTO: Hours
RPO / RTO: 10s of minutes
RPO / RTO: Minutes
RPO / RTO: Real-time
• Lower priority use cases
• Provision all AWS resources after event
• Restore backups after event
• Cost $
• Data live
• Services idle
• Provision some AWS resources and scale after event
• Cost: $$
• Always running, but smaller
• Business critical
• Scale AWS resources after event
• Cost $$$
• Zero downtime
• Near zero data loss
• Mission Critical Services
• Cost $$$$
Standby
COLD
WARM
HOT

Figure 17: AWS DR Strategies

Break your recovery options into categories based on application importance and Recovery Time Objectives, then choose the best strategy for each category.

Resilience Patterns and Recovery Groups

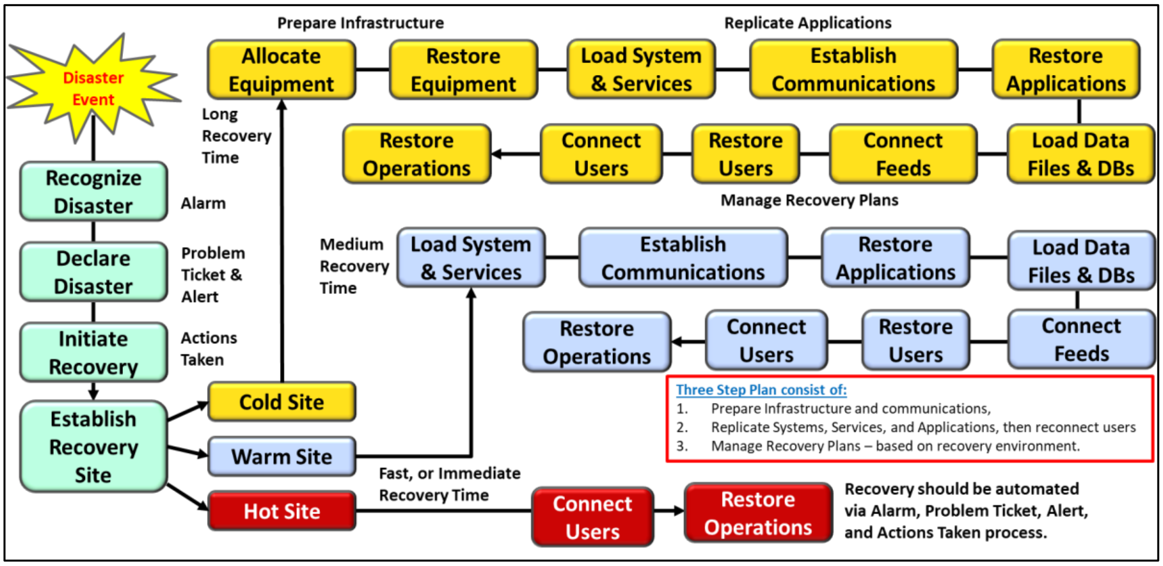


Resiliency Patterns	Single Region	Multiple Regions		
	In-Region	Active Standby (Pilot Ligt)	Active-Passive (Warm Stendby)	Active-Active (Multi-Site)
Pattern Profile	1. **TRANSACTIONAL TRAFFIC** - handled by primary region only 2. No multi-region **INFRASTRUCTURE** 3. **APPLICATION** code only available in single region 4. Multi-region **RECOVERY** not supported	1. **TRANSACTIONAL TRAFFIC** - handled by primary region only 2. **INFRASTRUCTURE available on stand-by** 3. **APPLICATION** provisioned, but in shutdown state	1. **TRANSACTIONAL TRAFFIC** - handled by primary region only 2. **INFRASTRUCTURE available on standby** 3. **Minimal APPLICATION** footprint running in 2nd rerion (all components are spun up and available with min. capacity, where application)	1. **TRANSACTIONAL TRAFFIC** - handled by primary region only 2. **INFRASTRUCTURE always available in both regions** 3. **APPLICATION** stack running active/active multi-region
Reserve Capacity			Required **RESERVE CAPACITY**	Required **RESERVE CAPACITY**
Cross-Region Maintenance	None	1. Maintain **PERSISTENT DATA REPLICATION** infrastructure 2. **APPLICATION CODE** maintaned for currency in **BOTH REGIONS** 3. Operate Production from stand-by region periodically	1. Maintain **PERSISTENT DATA REPLICATION** infrastructure 2. **APPLICATION CODE** maintaned for currency in **BOTH REGIONS** 3. Operate Production from stand-by region periodically	1. Maintain **2-WAY PERSISTENT DATA REPLICATION** 2. **APPLICATION CODE** maintaned for currency in **BOTH REGIONS** 3. Operate Production from stand-by region periodically
Recovery Steps	1. **ACQUIRE INFRASTRUCTURE** 2. **BUILD OUT** infrastructure 3. **DEPLOY** application 4. **RECOVER / RECREATE DATA** 5. **REDIRECT TRAFFIC** to region 2	1. **SCALE INFRASTRUCTURE** 2. **STARTUP** application 3. **FAILOVER TRAFFIC**	1. **AUTO- SCALE INFRASTRUCTURE** 2. **FAILOVER TRAFFIC**	1. **RECOVERY** acieved through automated redirect of traffic
Recovery Group (RG)	RG7	RG 4-6	REG 1-3	RG 0
Recovery Time Design (RTD)	Days+	Hours (<8 hrs)	Minutes (<15 mins)	Real-Time (<5mins)
Recovery Point Design (RPCD)	Hours (<8 Hrs)	Minutes (<15 mins)	Minutes (<15 mins)	Real-Time (< 0 mins)
Cloud Based Recovery Group Specifications		Preferred Patterns		

Figure 18: Define Recovery Groups and patterns.

Determine the resources and time requirements associated with your recovery needs and plot the recoveries into Recovery Groups.

Define the Sequence of events associated with each recovery strategy!



Three Step Plan consist of:

1. Prepare Infrastructure and communications,
2. Replicate Systems, Services, and Applications, then reconnect users
3. Manage Recovery Plans – based on recovery environment.

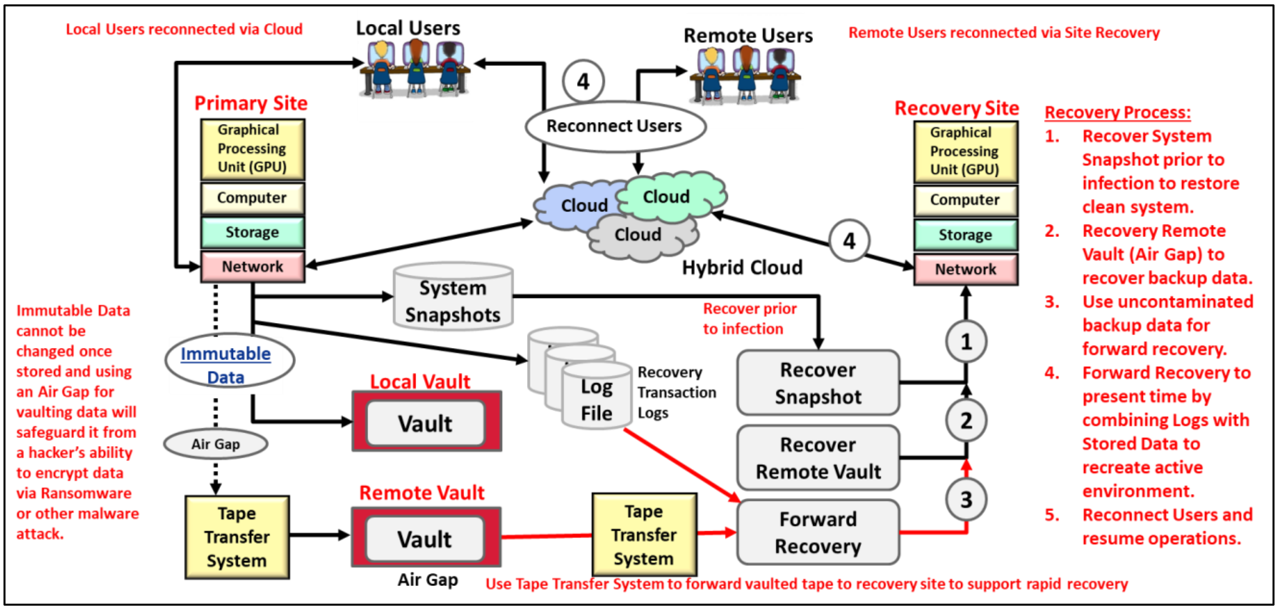
Figure 19: Define sequence of recovery operations for each Recovery Group

Separate application recovery into Cold, Warm, and Hot sites depending on their Recovery Time Objective (RTO).

The available recovery processes are defined above. Your company must choose the best recovery scenario for each of your products and services and then implement and continuously evaluate the recovery to guarantee the protections provided to your organization.

Patterns can be coded into the cloud system to enact recovery actions when needed. They simulate manually entered commands a support Infrastructure as Code (IoC) to build a recovery site, then move data and applications to the recovery site, reconnect users and continue operations. Their use should be included in your cloud applications.

Protect your company against Ransomware attacks!



Immutable Data cannot be changed once stored and using an Air Gap for vaulting data will safeguard it from a hacker's ability to encrypt data via Ransomware or other malware attack.

Recovery Process:

1. Recover System Snapshot prior to infection to restore clean system.
2. Recovery Remote Vault (Air Gap) to recover backup data.
3. Use uncontaminated backup data for forward recovery.
4. Forward Recovery to present time by combining Logs with Stored Data to recreate active environment.
5. Reconnect Users and resume operations.

Figure 20: Protect your company against Ransomware attacks!

Ransomware aims to take control over your data via encryption that can lock you out of your own data. To avoid the impact of ransomware, periodically backup data to a remote vault not connected to the system and save the data using an immutable method. The duration between backups to the off-site vault is your checkpoint to recovering from Ransomware. Additionally, as data is being transferred, a backup log should be maintained so that it can be combined with an original Master File to create a current copy of your data for restoration. System Snapshots are used to provide a recovery point in time that you can fallback to for restoring your system environment and aid in recovery from viruses, and malware attacks like Ransomware.

The sequence would be:

1. **Identify** that you have a Ransomware event and when it occurred.
2. **Restore** a System Snapshot taken prior to the Ransomware infection.
3. **Retrieve** a Master backup from the protected vault (air gap and immutable data).
4. **Combine** System Logs from the time of failure to present, if data has been validated as clean and not infected, to create current Master for system recovery and restart.
5. **Connect Users** to the recovered system!
6. **Continue production operations** from the recovery site or restored primary site.

Risk Management Guidelines

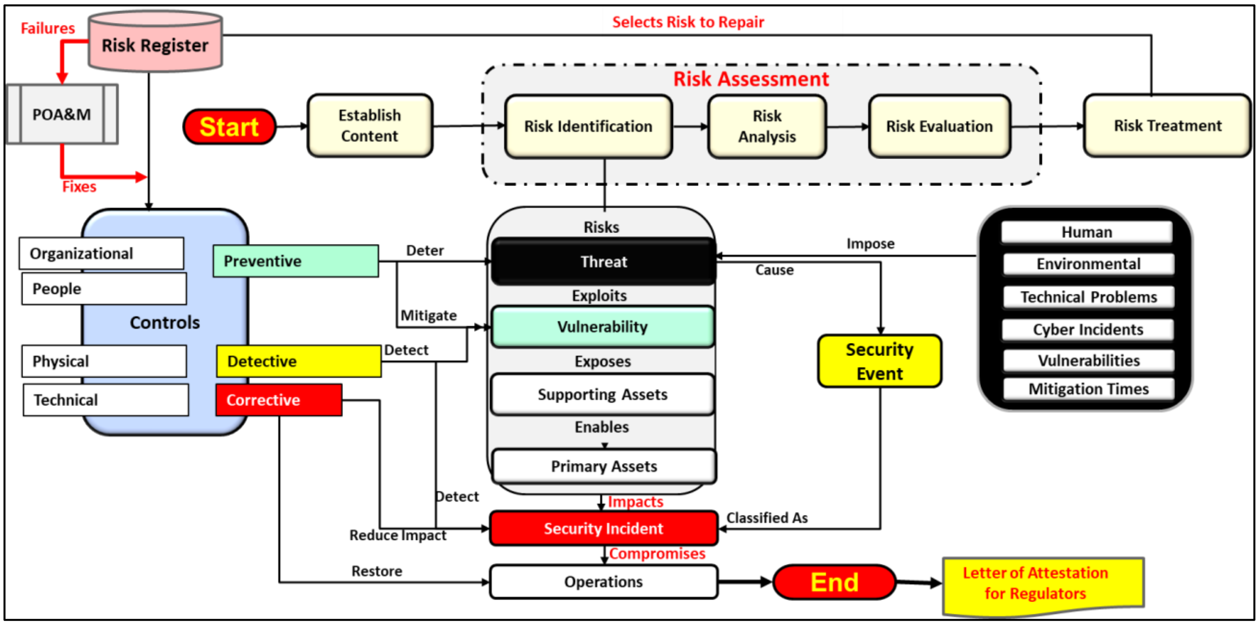


Figure 21: Risk Management Guidelines and Flow.

Follow the risk management guidelines to identify weaknesses, gaps and exceptions in compliance.

Define your application construction and production entry process!

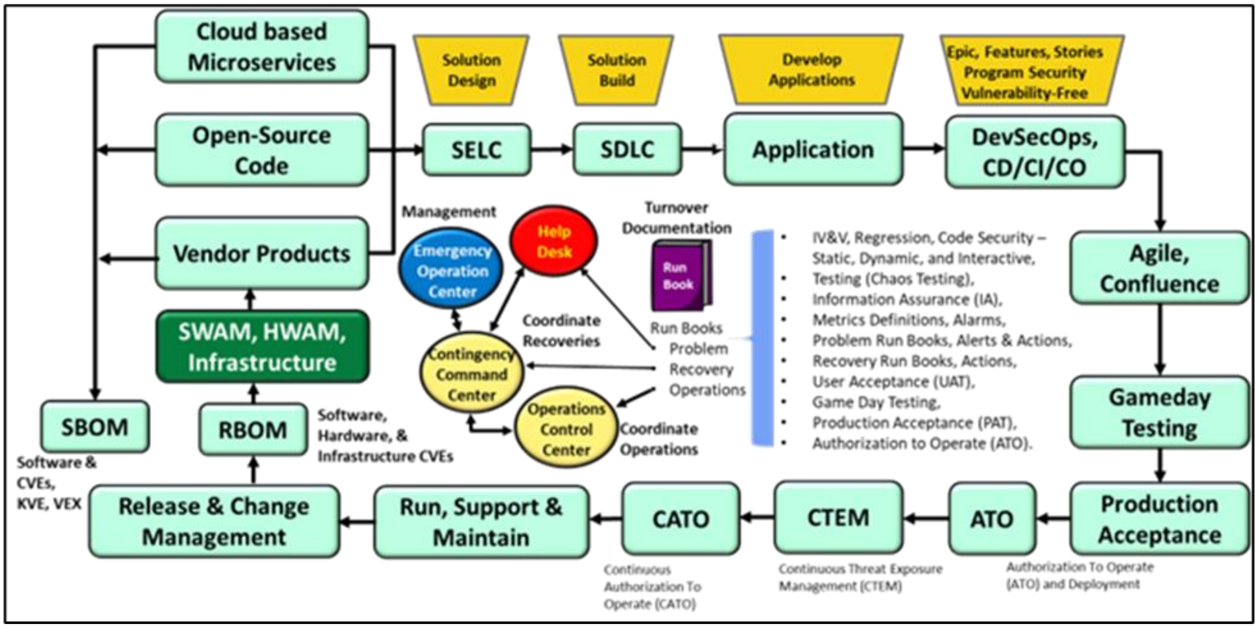

Cloud based Microservices
Open-Source Code
Vendor Products
SWAM, HWAM, Infrastructure
SBOM
RBOM
Software & CVEs, KVE, VEX
Software, Hardware, & Infrastructure CVEs
Release & Change Management
Solution Design
Solution Build
Develop Applications
Epic, Features, Stories Program Security Vulnerability-Free
SELC
SDLC
Application
DevSecOps, CD/CI/CO
Agile, Confluence
Gameday Testing
Production Acceptance
ATO
CTEM
CATO
Run, Support & Maintain
Management
Emergency Operation Center
Help Desk
Contingency Command Center
Operations Control Center
Coordinate Recoveries
Coordinate Operations
Turnover Documentation
Run Book
Run Books
Problem
Recovery
Operations
IV&V, Regression, Code Security – Static, Dynamic, and Interactive,
Testing (Chaos Testing),
Information Assurance (IA),
Metrics Definitions, Alarms,
Problem Run Books, Alerts & Actions,
Recovery Run Books, Actions,
User Acceptance (UAT),
Game Day Testing,
Production Acceptance (PAT),
Authorization to Operate (ATO).
Continuous Authorization To Operate (CATO)
Continuous Threat Exposure Management (CTEM)
Authorization To Operate (ATO) and Deployment

Figure 22: Define your application construction process for production entry!

Following this process will help you bring ideas to concepts, then solutions, which can be developed and evaluated for entry to the production environment. Create Run and Recovery books during the process.

Define your sequence for migrating applications to the cloud!

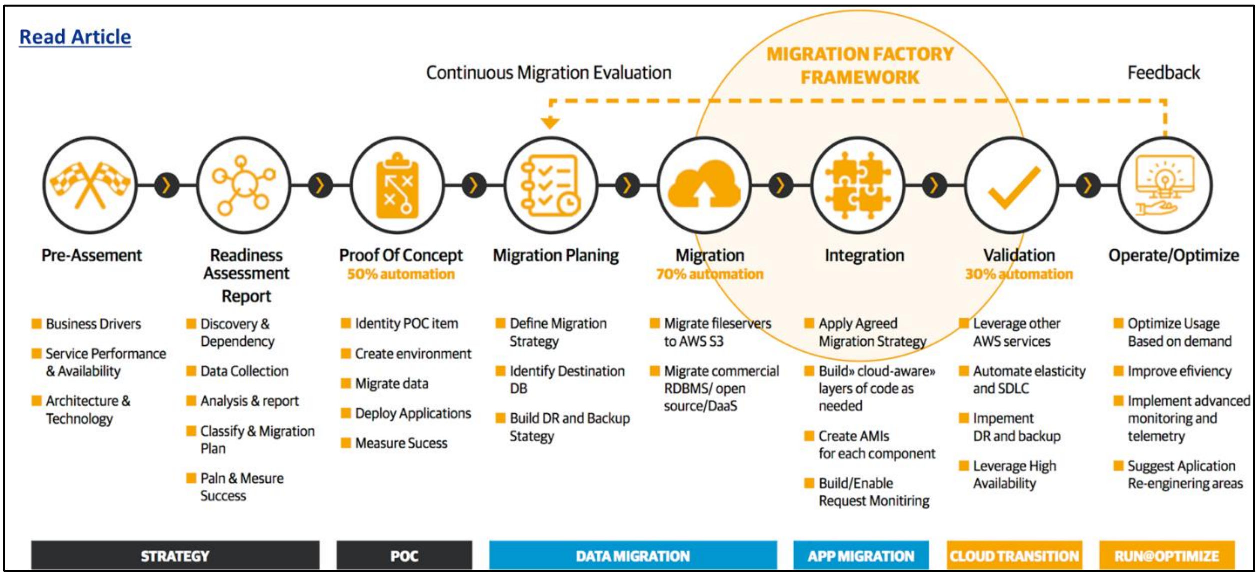

Read Article
Continuous Migration Evaluation
MIGRATION FACTORY FRAMEWORK
Feedback
Pre-Assement
Readiness Assessment Report
Proof Of Concept
50% automation
Migration Planing
Migration
70% automation
Integration
Validation
30% automation
Operate/Optimize
Business Drivers
Service Performance & Availability
Architecture & Technology
Discovery & Dependency
Data Collection
Analysis & report
Classify & Migration Plan
Paln & Mesure Success
Identity POC item
Create environment
Migrate data
Deploy Applications
Measure Sucess
Define Migration Strategy
Identify Destination DB
Build DR and Backup Stategy
Migrate fileservers to AWS S3
Migrate commercial RDBMS/ open source/DaaS
Apply Agreed Migration Strategy
Build» cloud-aware» layers of code as needed
Create AMIs for each component
Build/Enable Request Monitiring
Leverage other AWS services
Automate elasticity and SDLC
Impement DR and backup
Leverage High Availability
Optimize Usage Based on demand
Improve efiviency
Implement advanced monitoring and telemetry
Suggest Aplication Re-enginering areas
STRATEGY
POC
DATA MIGRATION
APP MIGRATION
CLOUD TRANSITION
RUN@OPTIMIZE

Figure 23: Define your sequence for migrating applications to the cloud!

General steps and considerations to be taken when migrating applications to the cloud.

Detailed steps for migrating applications to the cloud.

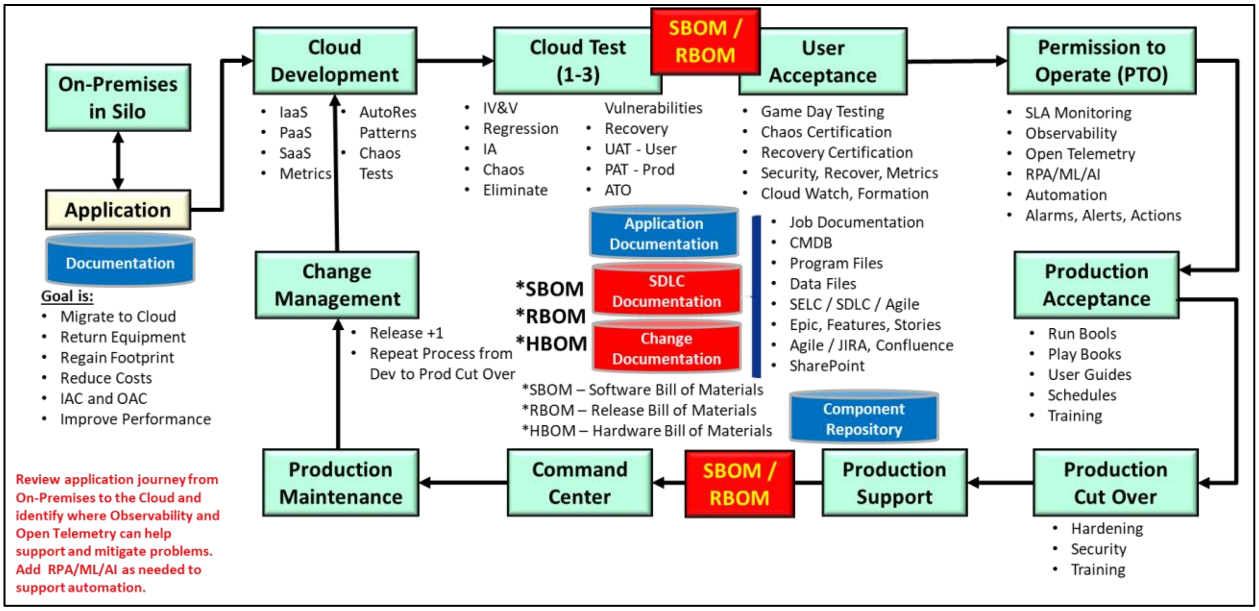


Figure 24: Detailed steps for migrating applications to the cloud.

Detailed steps to be taken when migrating applications to the cloud.

Application Security Testing – DevSecOps

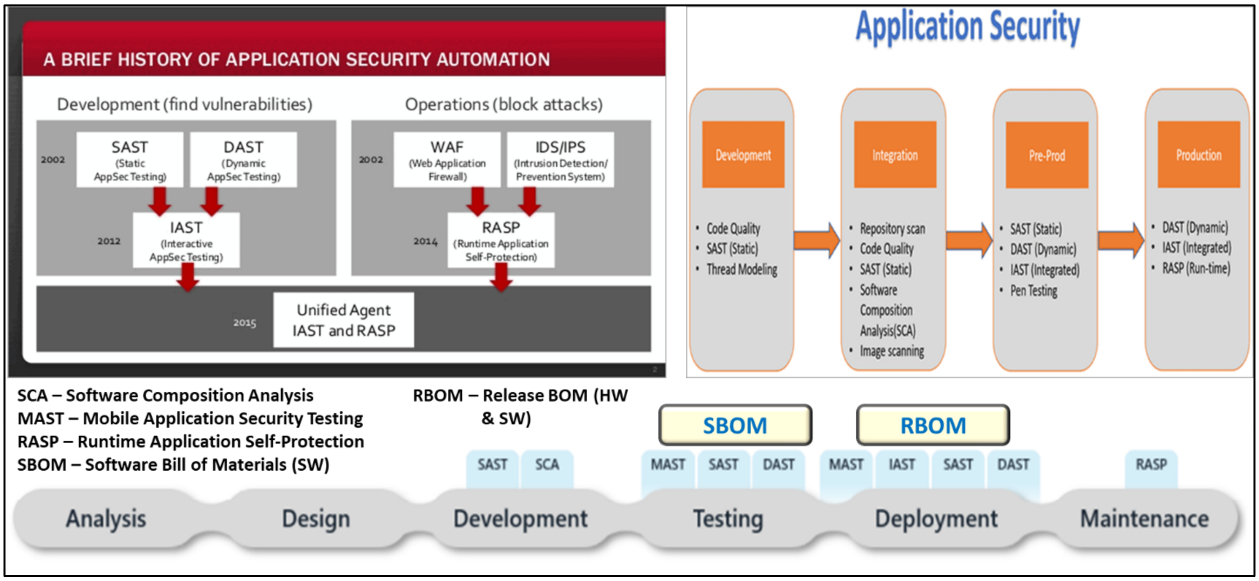

A BRIEF HISTORY OF APPLICATION SECURITY AUTOMATION
Development (find vulnerabilities)
Operations (block attacks)
2002
SAST (Static AppSec Testing)
DAST (Dynamic AppSec Testing)
2012
IAST (Interactive AppSec Testing)
2002
WAF (Web Application Firewall)
IDS/IPS (Intrusion Detection/ Prevention System)
2014
RASP (Runtime Application Self-Protection)
2015
Unified Agent IAST and RASP
Application Security
Development
• Code Quality
• SAST (Static)
• Thread Modeling
Integration
• Repository scan
• Code Quality
• SAST (Static)
• Software Composition Analysis(SCA)
• Image scanning
Pre-Prod
• SAST (Static)
• DAST (Dynamic)
• IAST (Integrated)
• Pen Testing
Production
• DAST (Dynamic)
• IAST (Integrated)
• RASP (Run-time)
SCA – Software Composition Analysis
MAST – Mobile Application Security Testing
RASP – Runtime Application Self-Protection
SBOM – Software Bill of Materials (SW)
RBOM – Release BOM (HW & SW)
SBOM
RBOM
SAST
SCA
MAST
SAST
DAST
MAST
IAST
SAST
DAST
RASP
Analysis
Design
Development
Testing
Deployment
Maintenance

Figure 25: Application Code Security Testing – DevSecOps

Procedures for ensuring application program code is assessed properly under suitable conditions.

Software Total Cost of Ownership

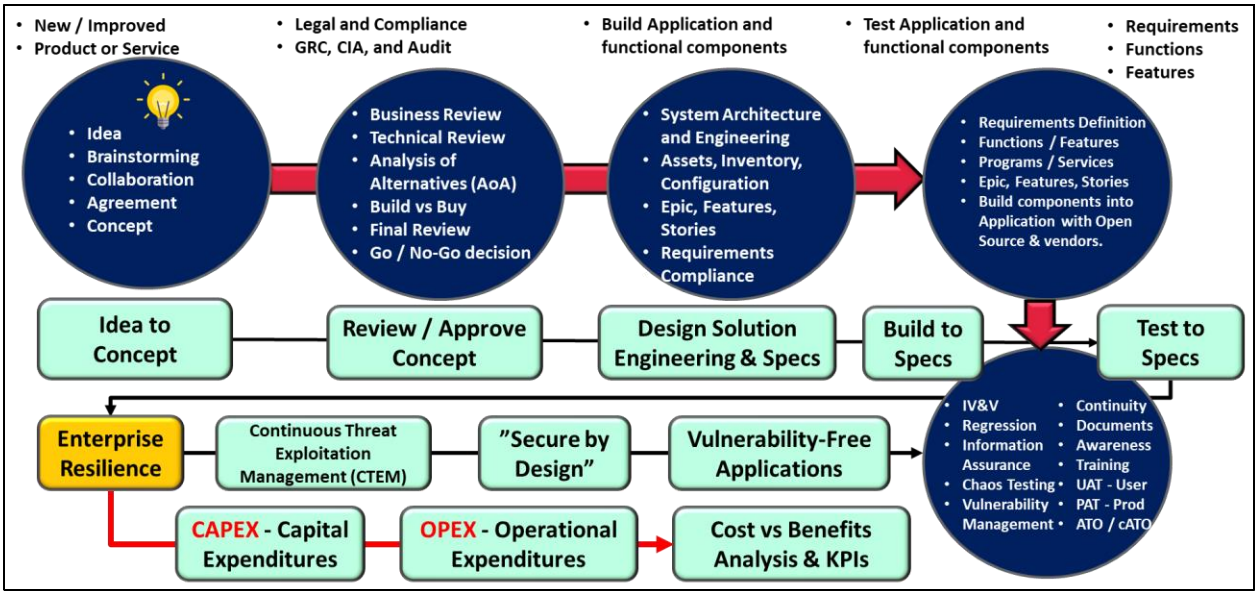
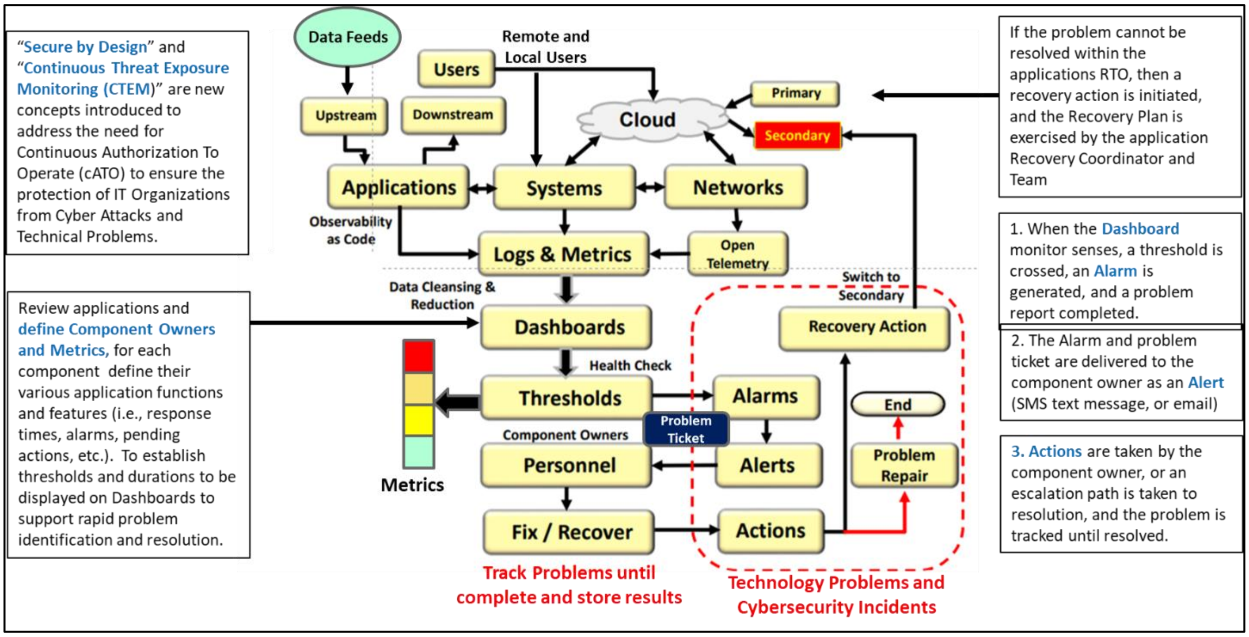

• New / Improved
• Product or Service
• Legal and Compliance
• GRC, CIA, and Audit
• Build Application and functional components
• Test Application and functional components
• Requirements
• Functions
• Features
• Idea
• Brainstorming
• Collaboration
• Agreement
• Concept
• Business Review
• Technical Review
• Analysis of Alternatives (AoA)
• Build vs Buy
• Final Review
• Go / No-Go decision
• System Architecture and Engineering
• Assets, Inventory, Configuration
• Epic, Features, Stories
• Requirements Compliance
• Requirements Definition
• Functions / Features
• Programs / Services
• Epic, Features, Stories
• Build components into Application with Open Source & vendors.
Idea to Concept
Review / Approve Concept
Design Solution Engineering & Specs
Build to Specs
Test to Specs
• IV&V
• Regression
• Information Assurance
• Chaos Testing
• Vulnerability Management
• Continuity Documents
• Awareness Training
• UAT - User
• PAT - Prod
• ATO / cATO
Enterprise Resilience
Continuous Threat Exploitation Management (CTEM)
"Secure by Design"
Vulnerability-Free Applications
CAPEX - Capital Expenditures
OPEX - Operational Expenditures
Cost vs Benefits Analysis & KPIs

Figure 26: Software Total Cost of Ownership

From idea through IT Production and support, the cost of applications should be calculated so that improvements can be made to enhance efficiency and lower costs.

Assigning problems to their component owner.

Another critical issue to be aware of is the need to identify every component owner (both internally and externally) so that problem reports can be responded to by the component owner. The sequence of events is:



"Secure by Design" and "Continuous Threat Exposure Monitoring (CTEM)" are new concepts introduced to address the need for Continuous Authorization To Operate (cATO) to ensure the protection of IT Organizations from Cyber Attacks and Technical Problems.

Review applications and define Component Owners and Metrics, for each component define their various application functions and features (i.e., response times, alarms, pending actions, etc.). To establish thresholds and durations to be displayed on Dashboards to support rapid problem identification and resolution.

If the problem cannot be resolved within the applications RTO, then a recovery action is initiated, and the Recovery Plan is exercised by the application Recovery Coordinator and Team

1. When the Dashboard monitor senses, a threshold is crossed, an Alarm is generated, and a problem report completed.

2. The Alarm and problem ticket are delivered to the component owner as an Alert (SMS text message, or email)

3. Actions are taken by the component owner, or an escalation path is taken to resolution, and the problem is tracked until resolved.

Figure 27: The Problem Management process and component owners!

- **Assign a metric** to a component and monitor activity against that component.
- **Establish Thresholds** and assign levels to the Threshold (Green, Yellow, Orange, Red) from good to bad.
- **Whenever a Threshold is crossed** for a predefined period, issue an alarm.
- **When the alarm is activated**, create a problem report and place the Alarm message into the body of the trouble ticket.
- **Route problem ticket to the component** owner as an alert.
- **The component owner takes actions** to mitigate the problem.
- **Escalations are performed to include experts in the mitigation process,** if necessary.
- **The problem ticket is tracked** from beginning to end by the problem management system.
- **A Problem Playbook** is followed to resolve the problem if one is available (SOAR), or Oasis' Collaborative Automated Course of Operations (CACAO).
- **If the problem requires a recovery,** then a Recovery Runbook is followed and a system recovery is completed (Cold, Warm, or Hot Recovery).
- **The results of the problem are stored in the Problem Database** and can be accessed by personnel who want to review other problems of a similar nature for reference, or if a match is found, for mitigation (a large percentage of problems are repeats, so following this search first method will reduce problem resolution time).

What If the component owner is not known.

If you do not know who owns a component, then you will be at a loss when it comes to assigning a problem ticket and simple problems may linger for prolonged times. So it is important to know who owns a failing component. Internally, this problem can be resolved by assigning a component owner, but externally it may be extremely difficult to locate the owner of a component, especially when the component is embedded within an assembly of components to construct a program. For this reason, an SBOM is essential to locate components and define their owner. If your vulnerability search does not produce the owner of a component, then you may choose not to use that program.

How do you detect, rate, and mitigate vulnerabilities?

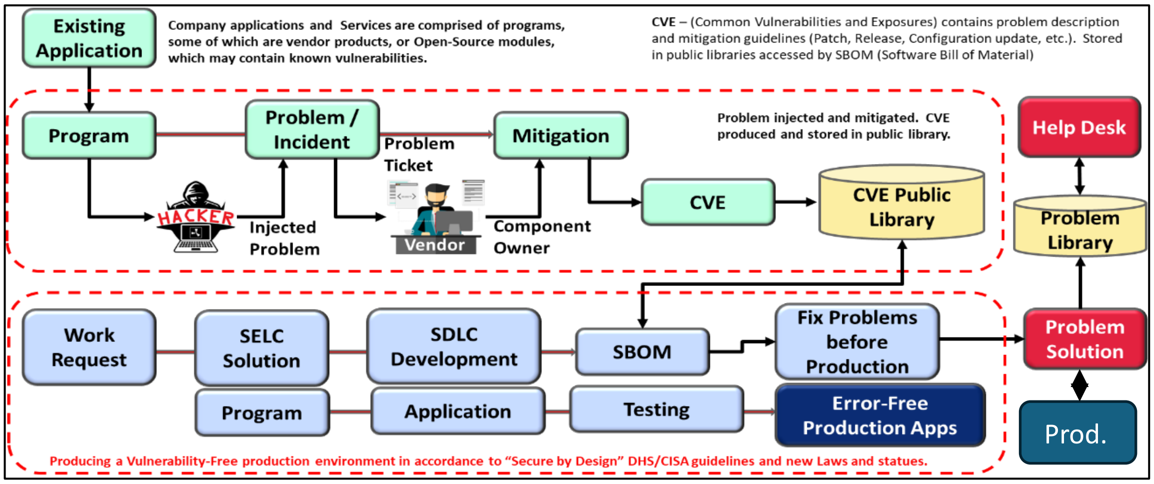

Existing Application
Company applications and Services are comprised of programs, some of which are vendor products, or Open-Source modules, which may contain known vulnerabilities.
CVE – (Common Vulnerabilities and Exposures) contains problem description and mitigation guidelines (Patch, Release, Configuration update, etc.). Stored in public libraries accessed by SBOM (Software Bill of Material)
Program
Problem / Incident
Problem Ticket
Mitigation
Problem injected and mitigated. CVE produced and stored in public library.
Help Desk
HACKER
Injected Problem
Vendor
Component Owner
CVE
CVE Public Library
Problem Library
Work Request
SELC Solution
SDLC Development
SBOM
Fix Problems before Production
Problem Solution
Program
Application
Testing
Error-Free Production Apps
Prod.
Producing a Vulnerability-Free production environment in accordance to "Secure by Design" DHS/CISA guidelines and new Laws and statues.

Figure 28: How vulnerabilities are researched and mitigated.

Whenever vulnerabilities are detected, they are analyzed and mitigated through a Root Cause Analysis (RCA) that provides a problem description, causes, and actions to be taken to resolve the problem or incident. These are named Common Vulnerability Enumerations (CVEs) and tracked from origination to resolution, then stored in a publicly addressable National Vulnerability Database (NVD). SBOMs examine the components contained within SaaS based and cloud applications to locate the programs composing cloud applications, vendor products, and services. The SBOM then examines the Public CVE Libraries to locate CVEs associated with the program so that technicians can repair any known vulnerabilities before production acceptance. This process will guarantee Vulnerability-Free production operations and adherence to new laws and regulations, along with reducing or eliminating cybercrime exposures.

When performing this process, an application security score may be determined, and thresholds used as gateways to govern the engineering, development, and maintenance process.

After storing mitigated problems within your in-house problem database, you should include a "Problem Solution" search first process to check and see if the problem is a repeat or new issue.

Providing you with a Helping Hand

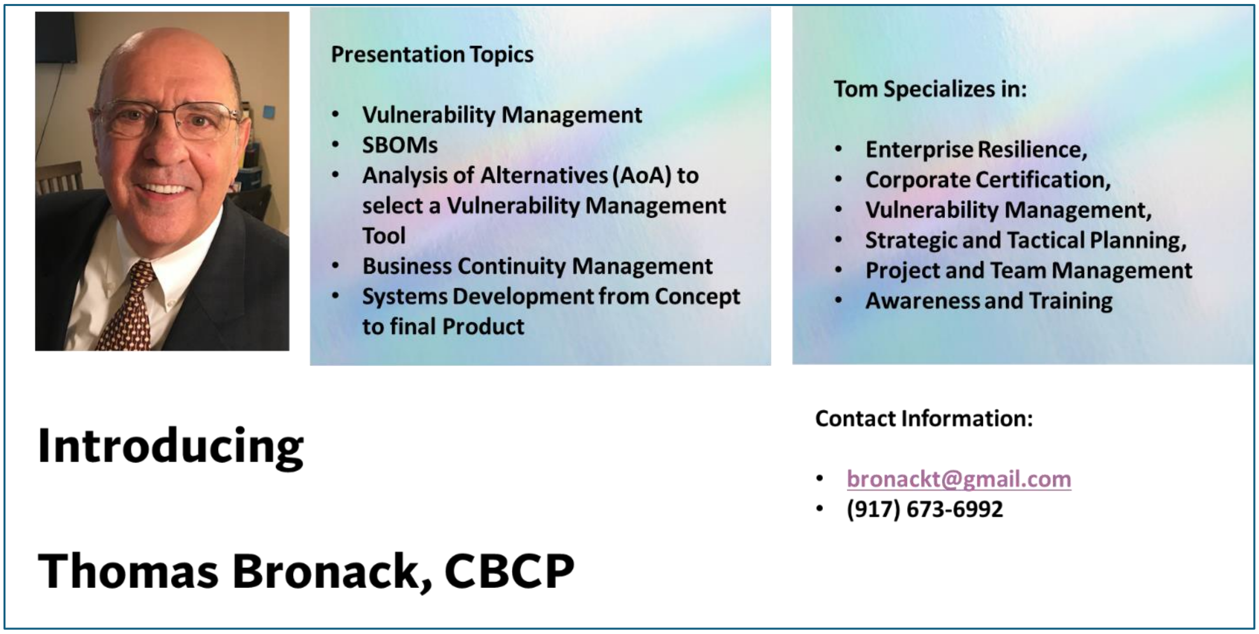
If you believe the information discussed in this paper will be helpful to your enterprise, or you were already thinking of initiating a project to include Vulnerability Management and its associated tools within your organization, then please contact us to discuss your needs and how we can help you establish a process to achieve your goals.

We look forward to being able to help you in your endeavors to produce a vulnerability-free production environment.

Contact:

Thomas Bronack, CBCP
President Data Center Assistance Group, LLC
Email: bronackt@gmail.com, or bronackt@dcag.com
Phone: (917) 673-6992

Figure 29: Our Helping Hands can assist you achieve your goals in an efficient and cost justified manner.



Presentation Topics

- Vulnerability Management
- SBOMs
- Analysis of Alternatives (AoA) to select a Vulnerability Management Tool
- Business Continuity Management
- Systems Development from Concept to final Product

Tom Specializes in:

- Enterprise Resilience,
- Corporate Certification,
- Vulnerability Management,
- Strategic and Tactical Planning,
- Project and Team Management
- Awareness and Training

Introducing

Thomas Bronack, CBCP

Contact Information:

- bronackt@gmail.com
- (917) 673-6992

A **senior level manager** with in-depth experience in **Enterprise Resilience and Corporate Certification** for large enterprises in disciplines like: Banking, Brokerage, Finance, Insurance, Pharmaceuticals, and Manufacturing which provided a solid understanding of the risks faced by companies and how best to safeguard a firm through workflow, compliance, and recovery.

The Software Supply Chain is at risk, as demonstrated by recent events, and this document is designed to help company management understand the needs associated with **protecting their organization's** ability to continuously provide services to customers within Service Level Agreements (SLAs), even when vulnerabilities may cause a catastrophic problem requiring recovery plan activation and a Vulnerability Management process in place.

I am presently pursuing an "**Whole of Nation**" approach to providing a "**Secure by Design**" production environment that complies with the **Secure by Design pledge** to produce vulnerability-free components and supplying data that the **Software Bill of Materials** (SBOM) needs to identify component owners for corrective action should an error condition be identified. This supports the software supply chain.

Mr. Bronack is the president of the Data Center Assistance Group, LLC and was previous president of the Data Center Assistance Group for over 35 years.