



Thomas Bronack, CBCP

Presentation Topics

- Vulnerability Management
- SBOMs to eliminate known problems
- CSF 2.0 Security Structure and Usage
- Continuous Threat Exploitation Management (CTEM) to identify new problems
- Systems Development from Concept to final Product
- Continuity of Services

Tom Specializes in:

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

Protecting your environment through Vulnerability Management, SBOMs CTEM, and Recovery Management.

Contact Information:

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

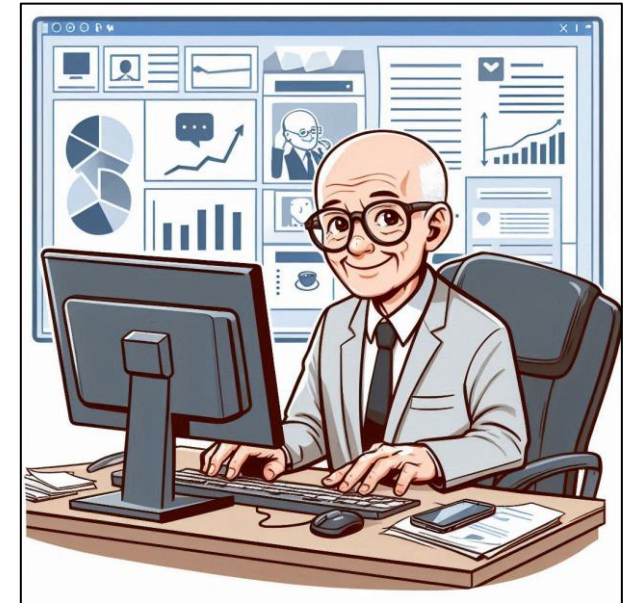
A word from Thomas Bronack

Thomas Bronack
Email: bronackt@dcag.com
Phone: (917) 673-6992

I am a **senior level manager** with in-depth experience in **Enterprise Resilience, Vulnerability Management, and Corporate Certification** for large enterprises in disciplines like: Banking, Brokerage, Finance, Insurance, Pharmaceuticals, Vendors, and Manufacturing which provided me with a solid understanding of the risks faced by companies and how best to safeguard a firm through workflow, compliance, and recovery using SBOMs (Software Bill of Materials) to eliminate known problems and CTEM (Continuous Threat Exploitation Management) to identify new problems needing mitigation.

The Software Supply Chain is at risk and companies are being hacked by Nation-States and bad actors, as demonstrated by recent events and world turmoil. 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 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, provides vulnerability-free production application turnover for ATO, and uses CTEM to detect new problems for resolution that supports CATO.



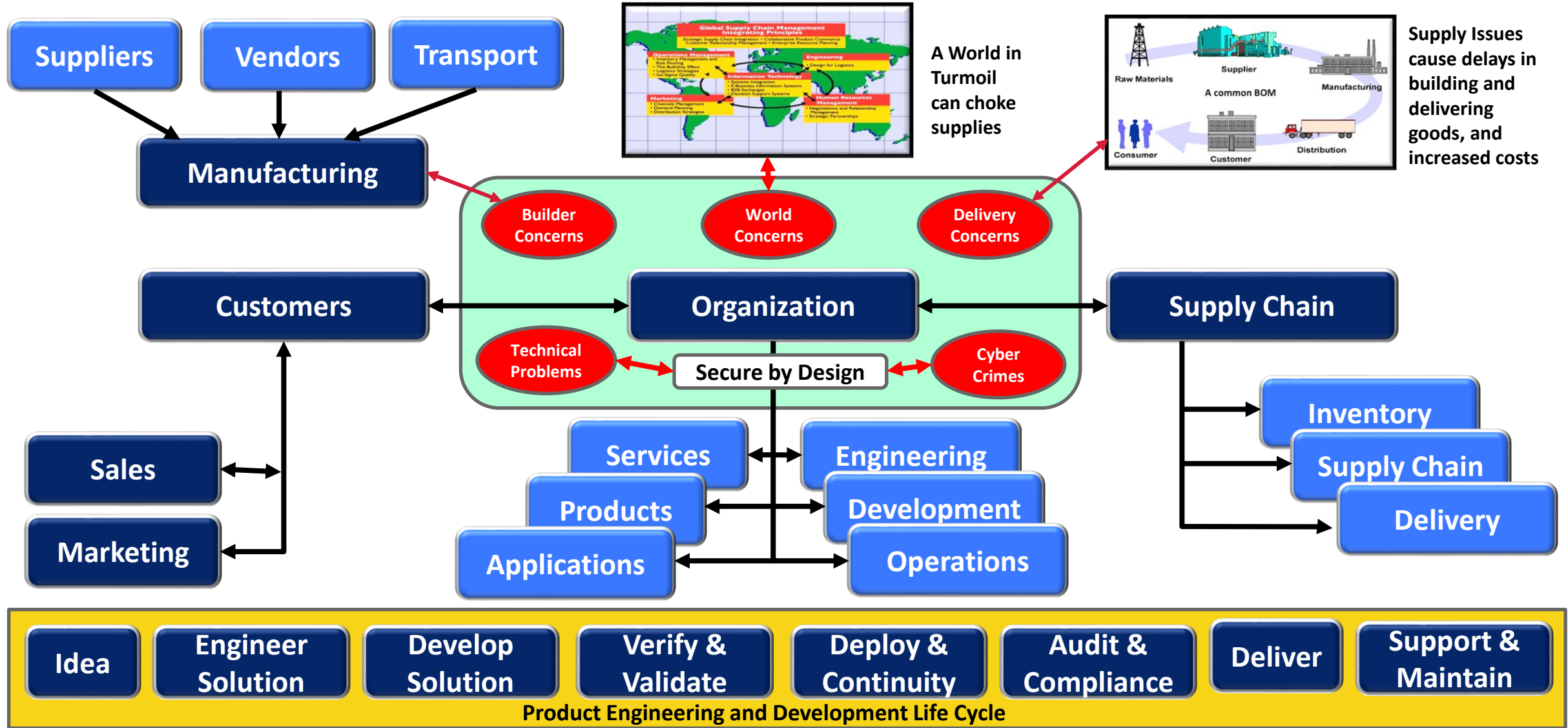
"A strong generalist with extensive IT industry experience, ready to help you".

Thomas Bronack,
bronackt@gmail.com or
bronackt@dcag.com
917-673-6992

1. **Rise in vulnerabilities** is 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.
2. The **rate of Vulnerabilities surpasses** the ability of most companies to fix them, leading to undue toil on staff, burnout and turnover. This issue must be addressed through automation and a tool upgrade.
3. **Develop a problem free** environment through Vulnerability Management:
 - a. **Eliminate known problems** via **SBOMs**,
 - b. **Identify New problems** through Continuous Threat Exploitation Management (**CTEM**),
 - c. **Develop and Publish** Standards and Guidelines, and
 - d. **Create a Resilience Operations Center (ROC)** to assist personnel identify and resolve potential Risks to the company.
- a. **Business Continuity Management** must be enhanced to support Service Level Agreements and a company's ability to continue to supply services and products, even if a disaster occurs
- b. **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.

Protecting Organization is more difficult than ever

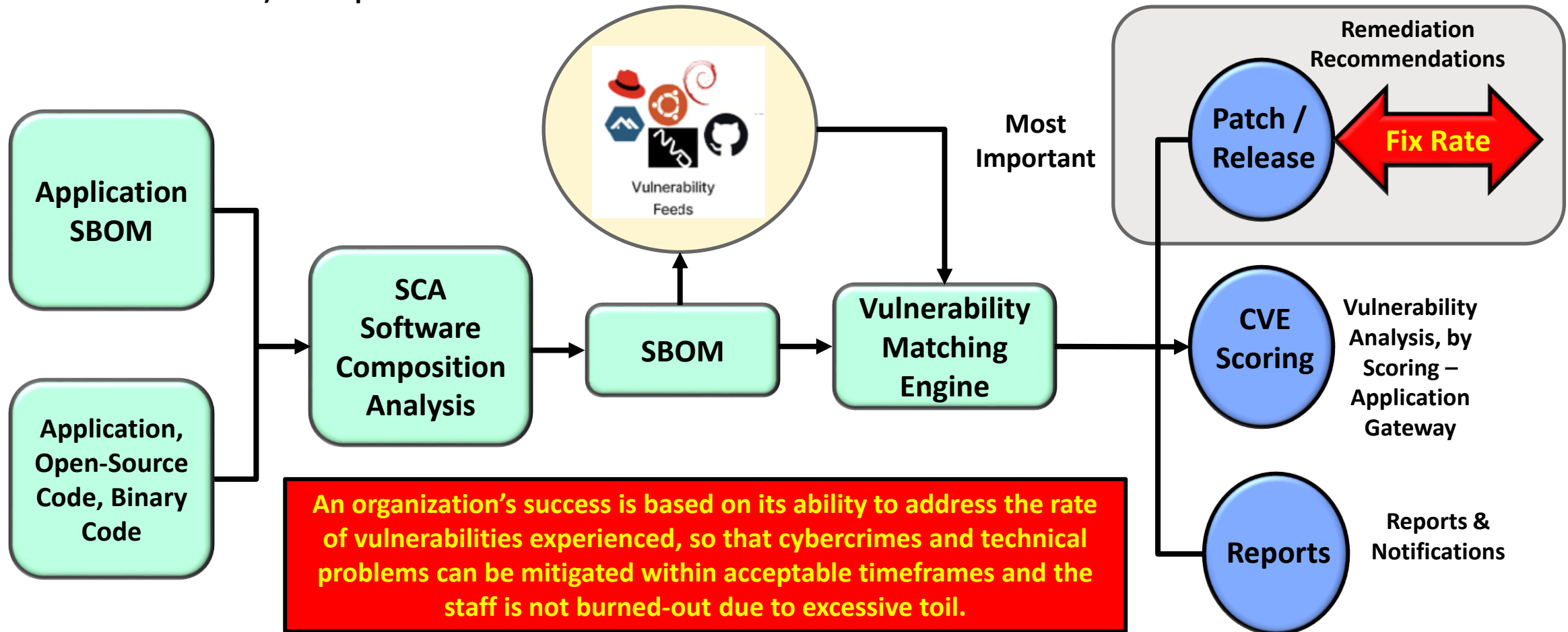
Thomas Bronack
 Email: bronackt@dcag.com
 Phone: (917) 673-6992



Identifying and Reporting Vulnerabilities

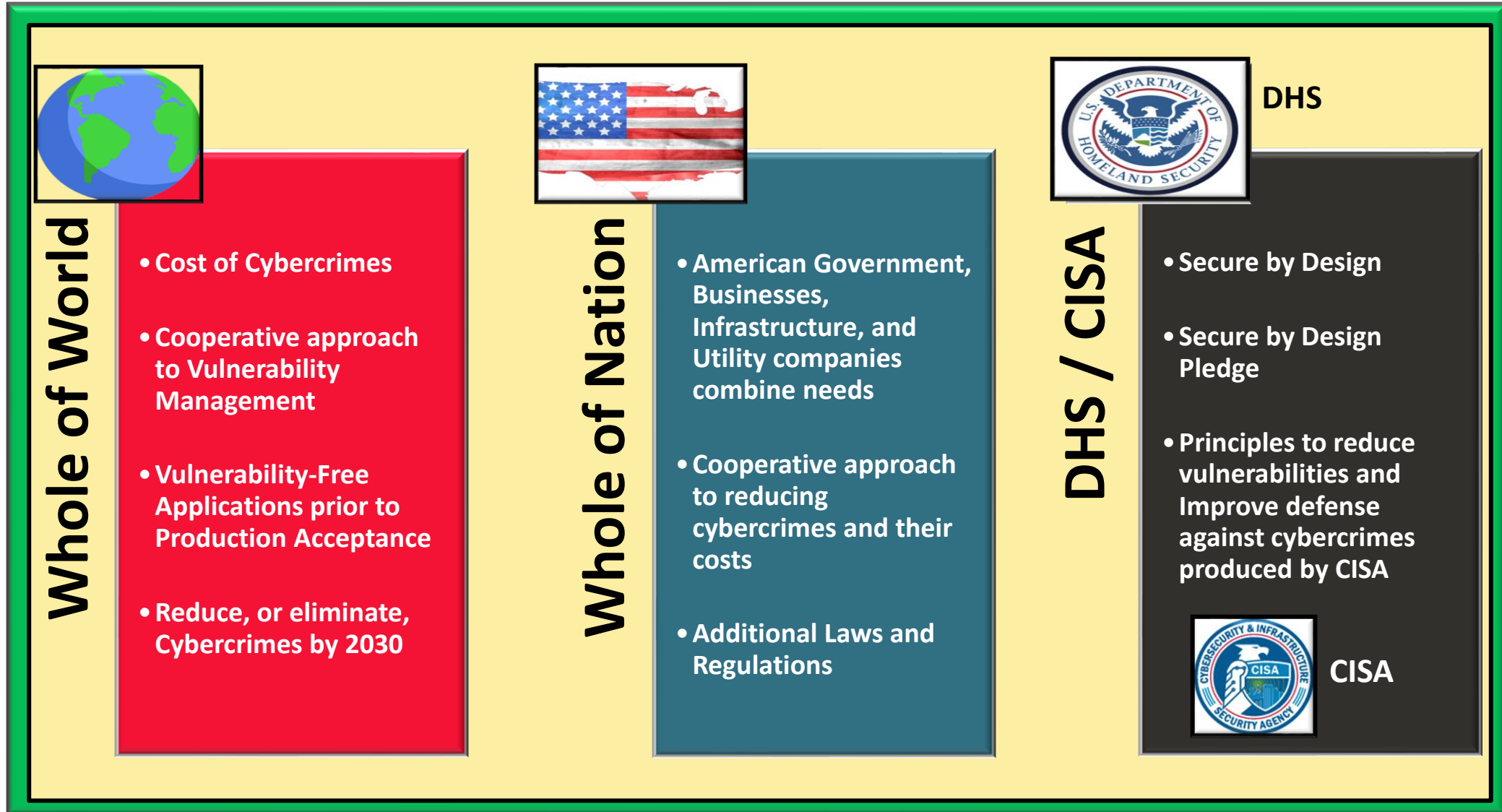
Existing Vulnerabilities are identified within Applications, or existing Application SBOMs (Software Bill of Material) and reported.

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.

Whole of World Approach



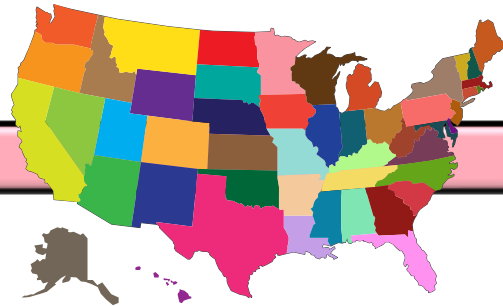
A Whole of World approach to Cybersecurity

Thomas Bronack
Email: bronackt@dcag.com
Phone: (917) 673-6992

Whole of World Approach



Whole of Nation Approach



Department of Homeland Security



Cybersecurity Infrastructure Security Agency



CISA
CYBER+INFRASTRUCTURE

2030 Most Significant Cyber Concerns:

1. Supply Chain Compromises
2. Advanced disinformation campaigns
3. Rise of Digital Surveillance
4. Human error and legacy systems
5. Targeted Attacks
6. Lack of analysis and controls
7. Rise of advanced hybrid attacks
8. Skill shortage
9. Cross-border ICT suppliers as a single-point-of-failure
10. Artificial Intelligence abuse

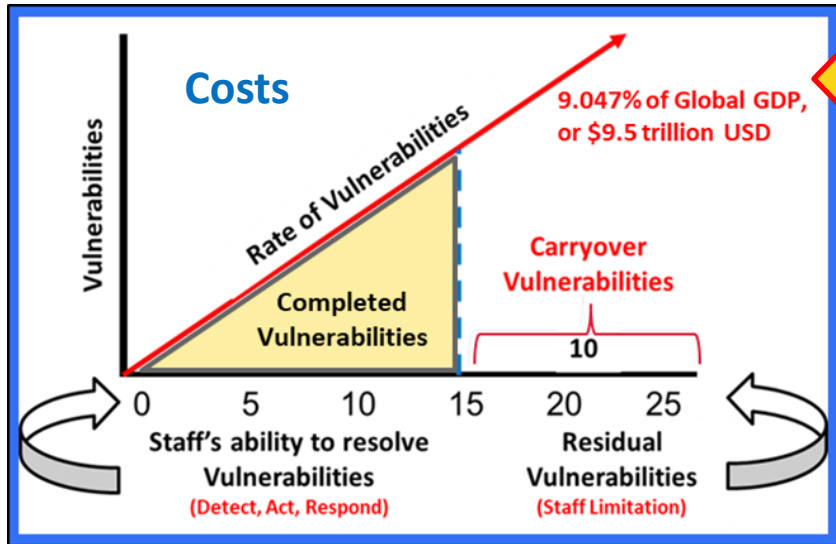
Vulnerability Management Process:

1. Detect Vulnerability (SBOM)
2. Assess the Risk (CVE)
3. Prioritize Remediation (CVSS, KVE, EPSS)
4. Confirm Remediation
5. Optimize through automation
6. Advance the use of BOMs for Software, Release Control, and Artificial Intelligence

DHS/CISA - Secure by Design principles:

1. Build security considerations into the [software requirements specification](#)
2. Address possible abuse cases (e.g., how users may misuse the software).
3. Create and enforce secure code guidelines.
4. Use appropriate security tools.
5. Conduct security audits at multiple [stages of the SDLC](#).
6. Conduct vulnerability testing that includes negative testing and penetration testing.
7. Incorporate security within deployment and maintenance processes.
8. Ensure reused software is from trusted sources and properly evaluated.
9. Provide feedback throughout the process on security effectiveness.
10. Educate developers and QA teams on [secure coding techniques](#).

Cost of Vulnerabilities, SBOMs, and CTEM



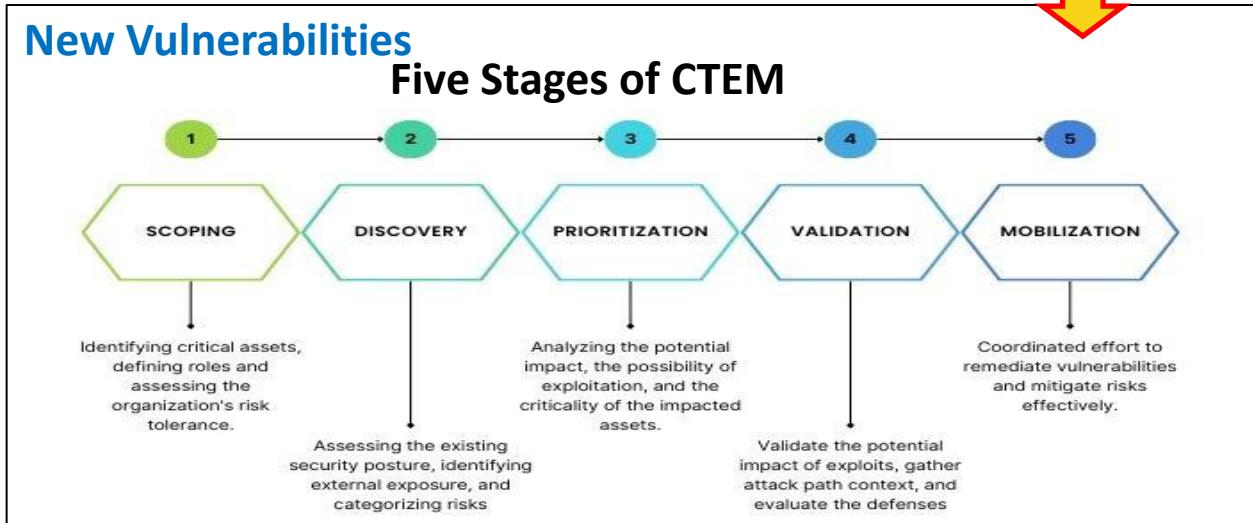
Costs of Vulnerabilities is Rising at a Rapid Rate

SBOMs can identify known problems to be fixed prior to production

CTEM identifies new problems when in Production



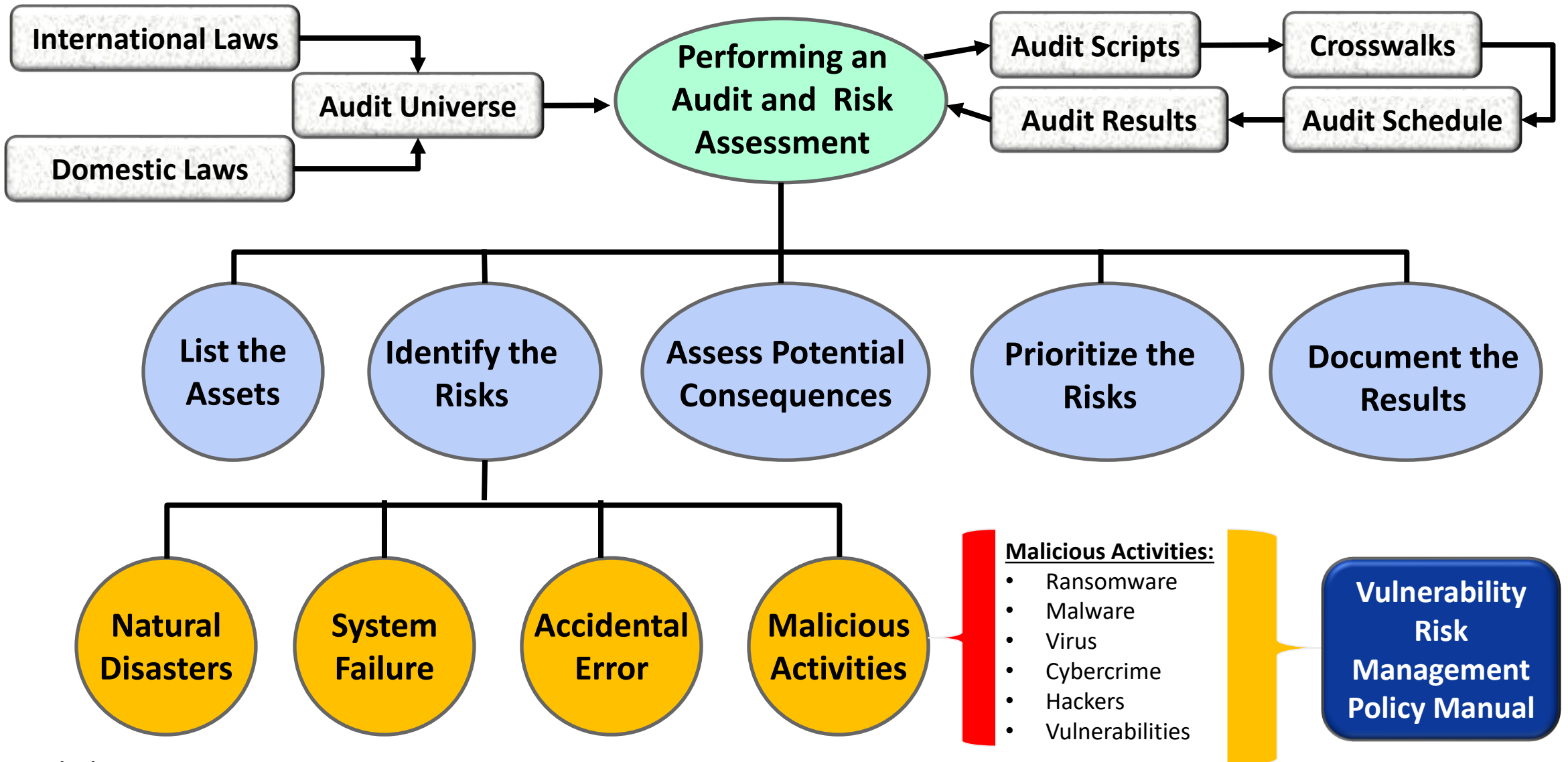
Combining disciplines will reduce vulnerabilities, costs, toil on personnel, and turnover.



Vulnerability Laws and Regulations requiring SBOMs

- Presently, implementing Applications and Services can include vulnerabilities and malware, which can cost your company in lost revenue, brand reputation, fines and penalties, burdening your staff and resulting in high levels of turnover. DHS/CISA has developed a [“Secure by Design”](#) approach to responding to these issues.
- 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
 - [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 ([ISO 14971:2019](#) Risk Management to Medical Devices)
 - [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 Procedures must be integrated into the staff’s daily process for new and changed applications and services, with automated support through RPAs whenever feasible.

Performing an Audit and Risk Assessment



Getting started with facts and a defined direction

Know your company:

1. Most Important Applications & Services (**Family Jewels**).
2. Risk Assessment and BIA to Define the damage caused if lost and maximum duration of survival without the application or service.
3. Define Requirements, Scope, Risk, Security, DevSecOps, Testing, Recovery, Acceptance, Deployment, ITSM, ITOM, and ITAM.
4. Define Audit Universe implement legal & auditing functions.
5. Define the Ideation, Brainstorming, Collaboration, Innovation, to Concept process.
6. Implement Systems Engineering Life Cycle (SELC) to respond to new ideas or business opportunities.
7. Implement Systems Development Life Cycle (SDLC) to deploy new products and services.
8. Define Company Organization to respond to cybersecurity and technology problems in a timely manner and to the appropriate authorities (i.e., [SEC Rule 2023-139](#))

Set your direction:

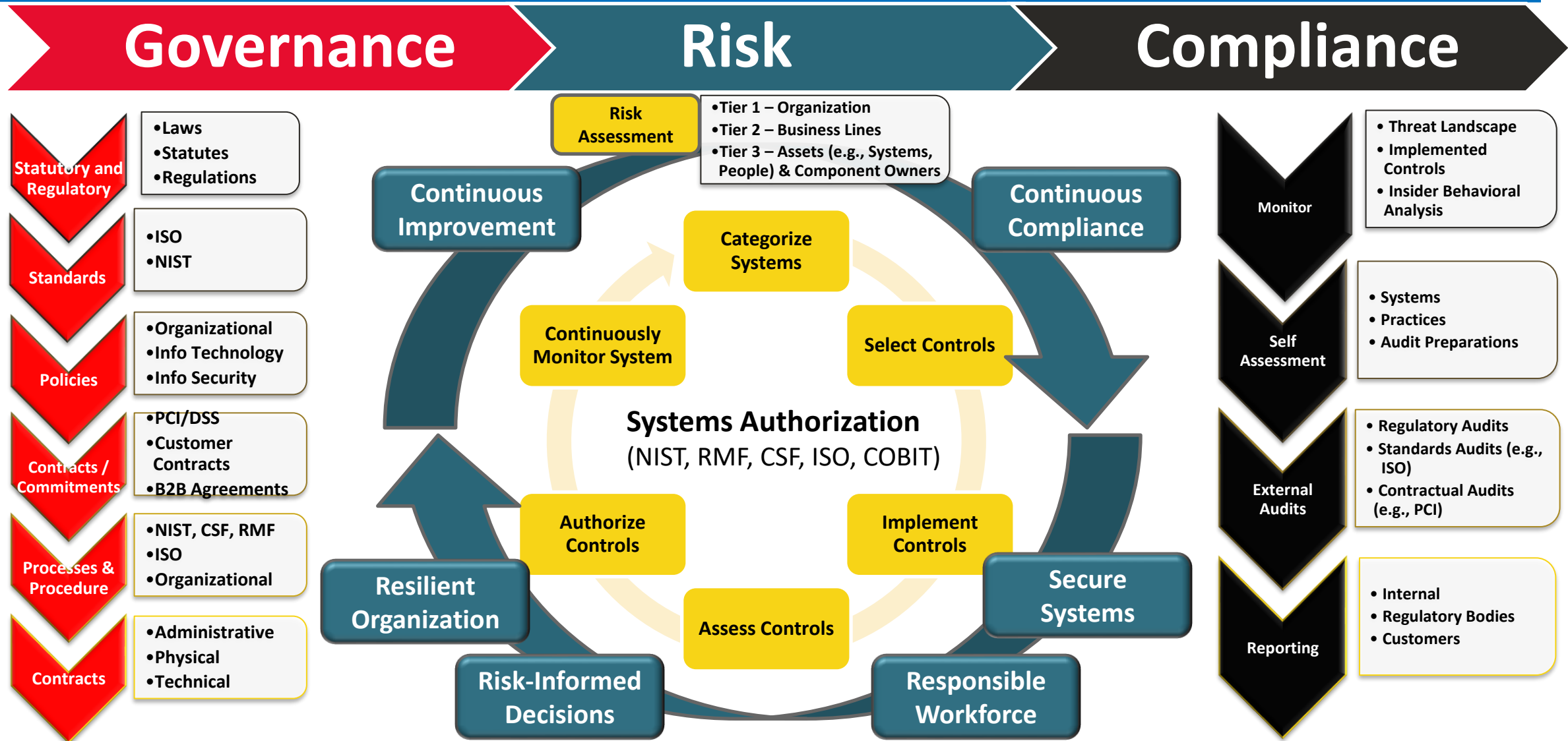
1. Most efficient, compliant, and secure production environment, capable of recovering from disaster events and providing continuous vulnerability-free products and services to customers. **Continuity of Succession / Delegation of Authority** must be included along with definition of duties.
2. Integrate guidelines, standard Operating Procedures, skill development, and awareness throughout the organization.

Know your Environment:

1. Physical and Data Security (Data Sensitivity & Data Flow).
2. Architecture and engineering process (i.e., TOGAF).
3. Asset Inventory and Configuration Management (ITAM).
4. Identity and Access Management (IAM - ZTA).
5. GRC based compliance and attestation, with CIA based cybersecurity and elimination of viruses and malware, and RMF based Risk Identification and Controls Development.
6. Development and implementation of DevSecOps.
7. Personnel Titles, Job Functions and Responsibilities, and the integration of sensitive and required services within their everyday work tasks.
8. Staff training and development.
9. Continuous Monitoring and Improvement, along with the adoption of new technologies and processes (i.e., SRE).
10. Deploying error-free products and services (see [EO 14028](#) and [OBM M-22-18](#)) and utilize the latest technologies to respond to encountered anomalies and verify compliance (i.e., CTEM).

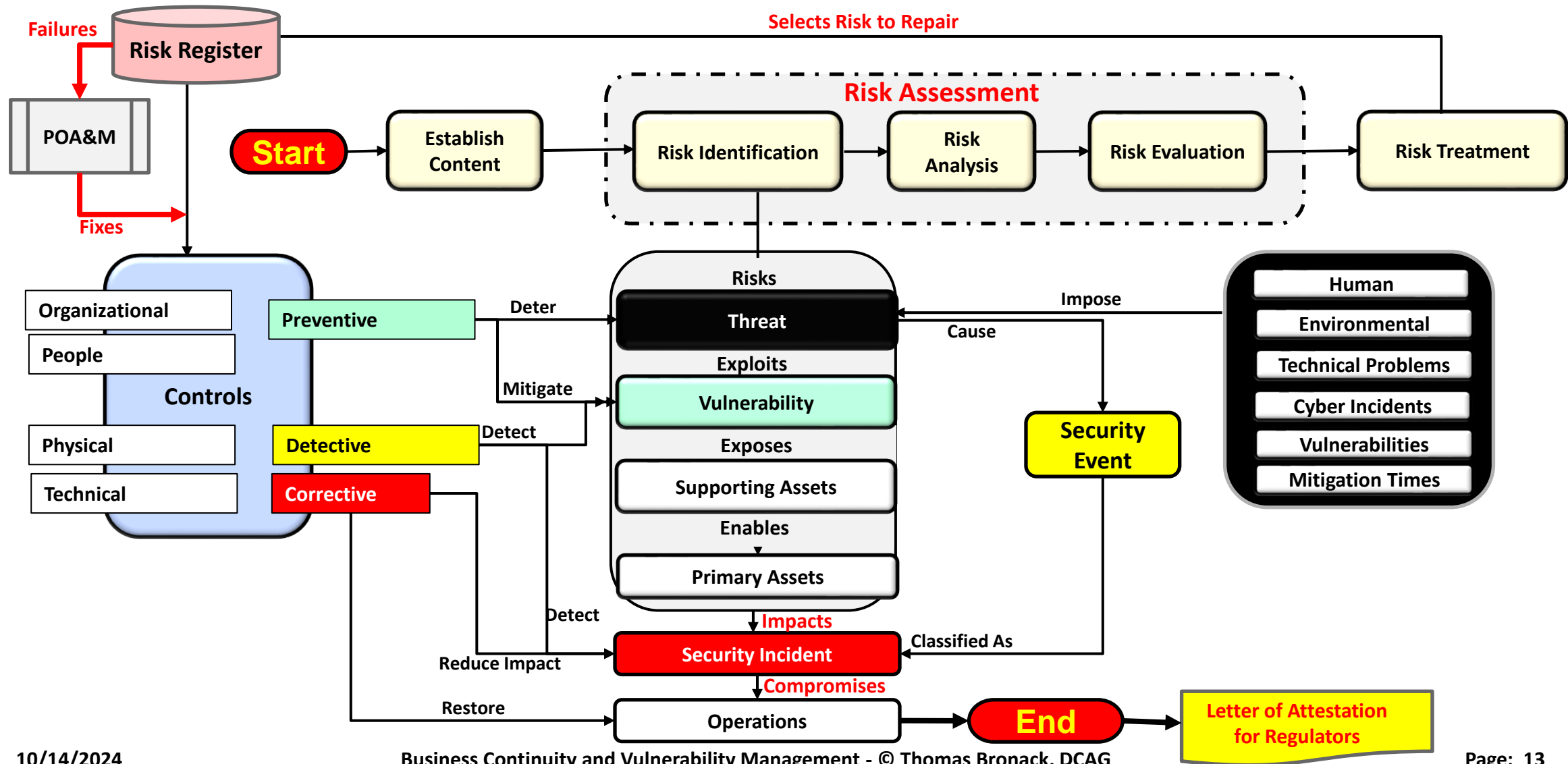
Ensuring Compliance via GRC and Risk Assessment

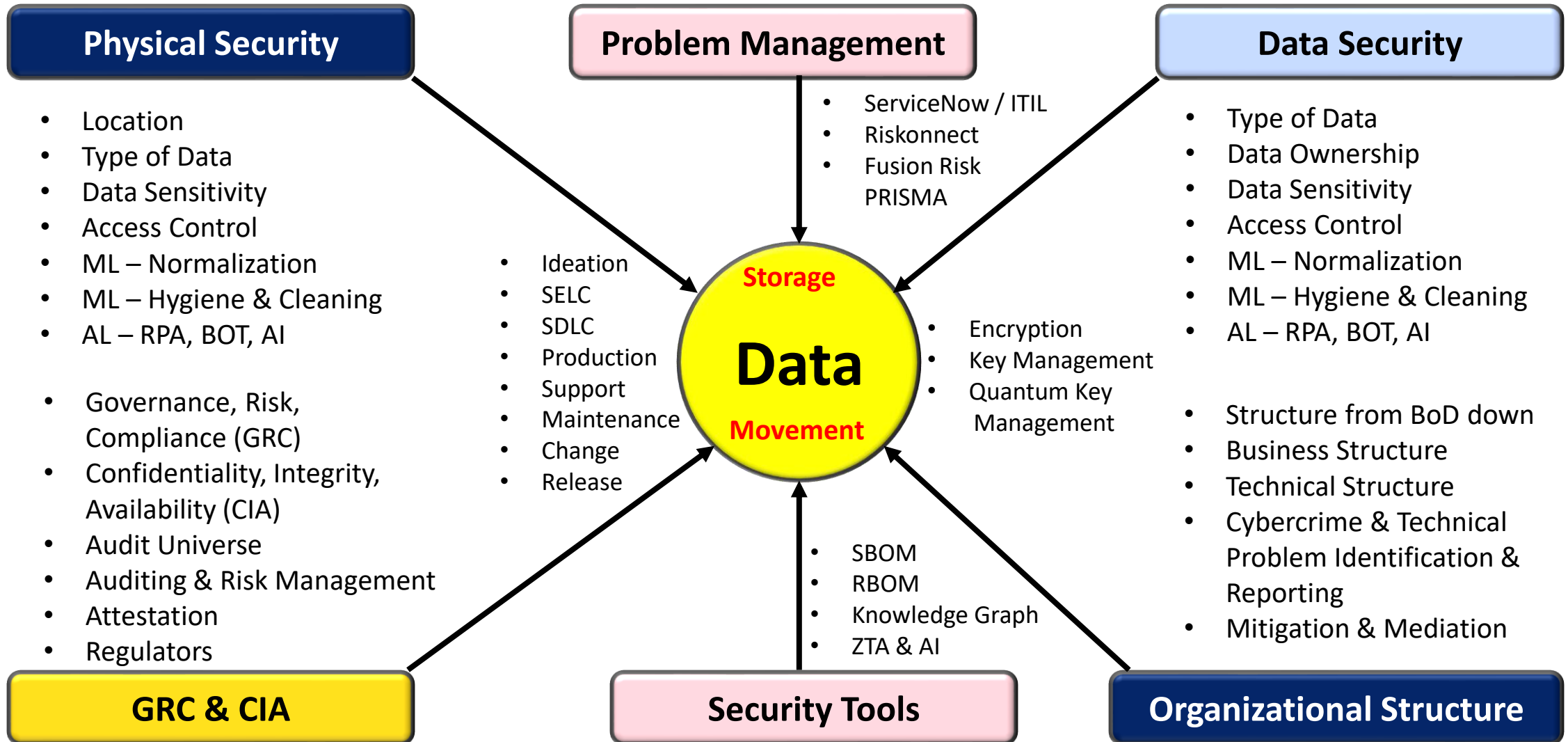
Thomas Bronack
 Email: bronackt@gmail.com
 Phone: (917) 673-6992



Risk Management with ISO 27000: 2022

Thomas Bronack
 Email: bronackt@dcag.com
 Phone: (917) 673-6992

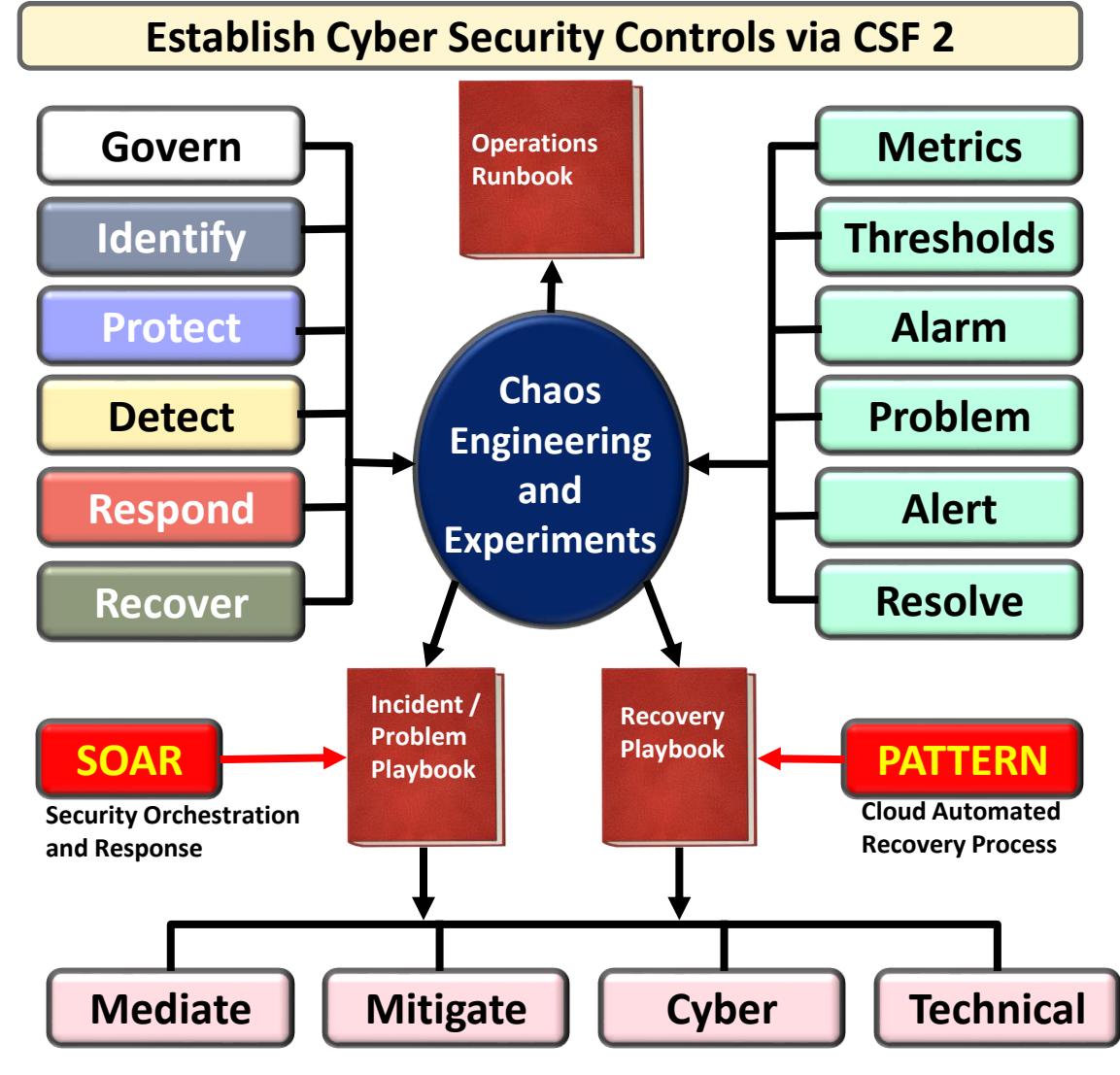




NIST CSF 2.0 Categories and Application

Thomas Bronack
 Email: bronackt@gmail.com
 Phone: (917) 673-6992

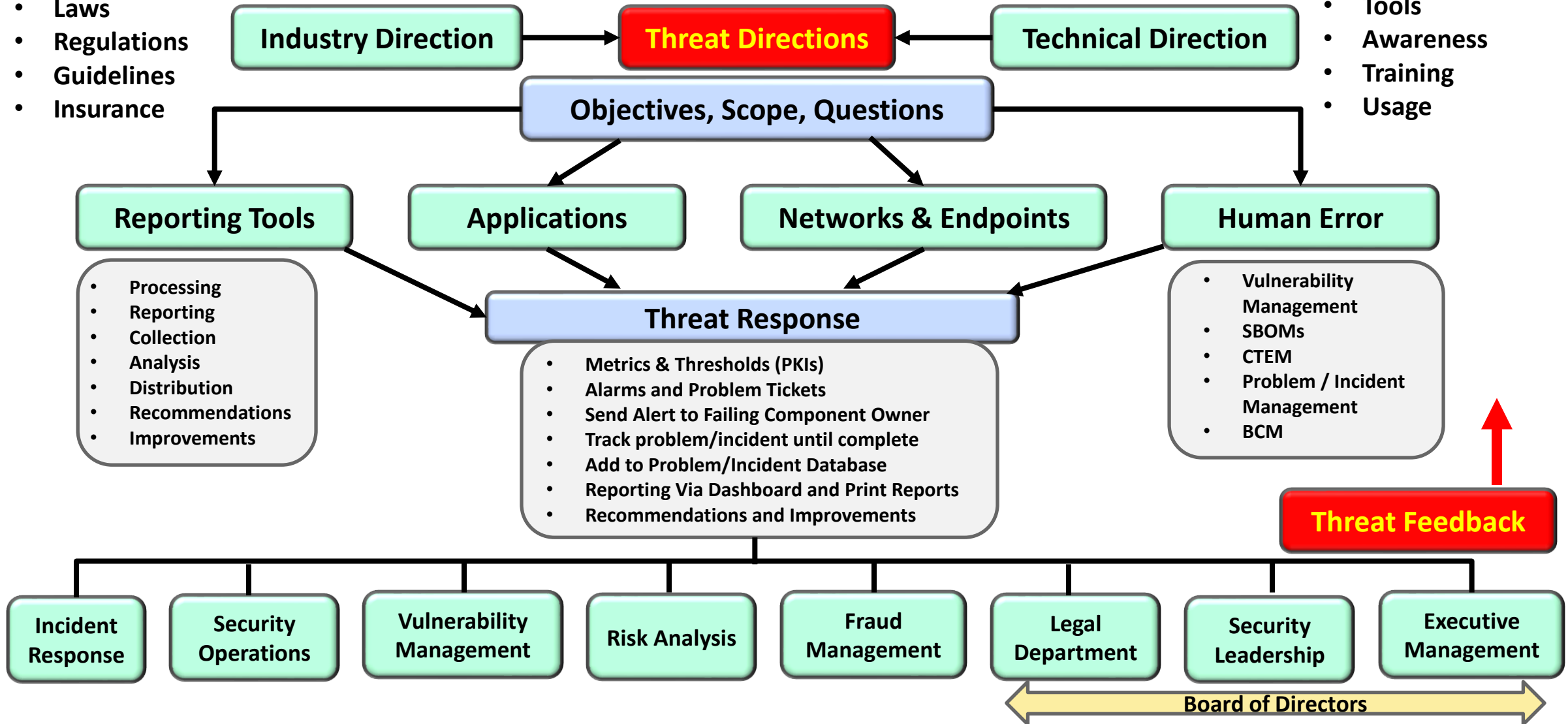
NIST Cybersecurity Framework 2.0		
CSF 2.0 Function	CSF 2.0 Category	CSF 2.0 Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles and Responsibilities	GV.RR
	Policies and Procedures	GV.PO
Identity (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Supply Chain Risk Management	ID.SC
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Adverse Event Analysis	DE.AE
	Continuous Monitoring	DE.CM
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO



Addressing Threats

- Laws
- Regulations
- Guidelines
- Insurance

- Tools
- Awareness
- Training
- Usage



Vulnerability Management definition and process

Vulnerability management is a **continuous, proactive, and often automated process** that keeps your computer systems, networks, and enterprise applications safe from cyberattacks and data breaches. As such, it is an important part of an overall security program.

Process:

- **Plan** how to use Vulnerability Management
- **Discover** where your vulnerabilities exist
 - Vulnerability-Free Production Application Programs
 - Continuous Scanning for new Vulnerabilities impacting production applications via Continuous Threat Exploitation Management (CTEM)
- **Scan** applications with **SBOMs** (Software Bill of Materials)
 - Use **CTEM** to scan production environment
- **Report** vulnerabilities, their symptoms, and mitigations via patches and new releases
- **Remediate** through patches and new releases to mitigate known vulnerabilities, or correcting new anomalies

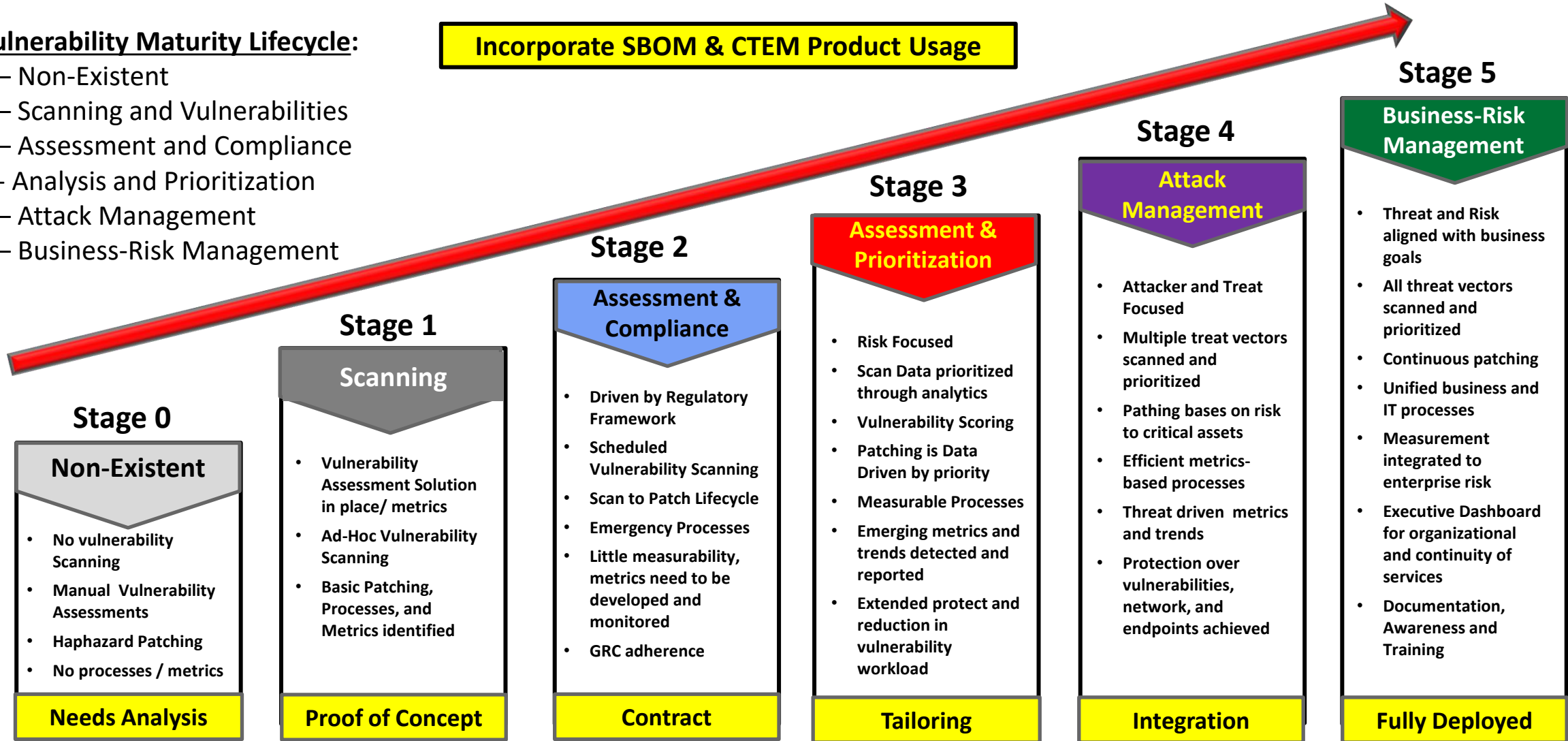


Vulnerability Management Maturity Lifecycle

Incorporate SBOM & CTEM Product Usage

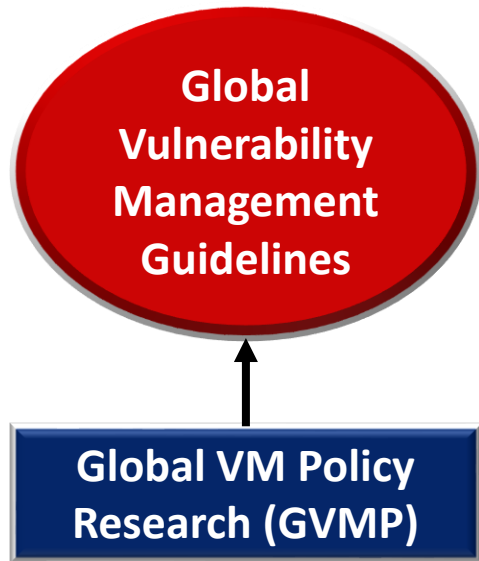
Vulnerability Maturity Lifecycle:

- 0 – Non-Existent
- 1 – Scanning and Vulnerabilities
- 2 – Assessment and Compliance
- 3 - Analysis and Prioritization
- 4 – Attack Management
- 5 – Business-Risk Management



Global Vulnerability Management Policy generation

Thomas Bronack
 Email: bronackt@dcag.com
 Phone: (917) 673-6992



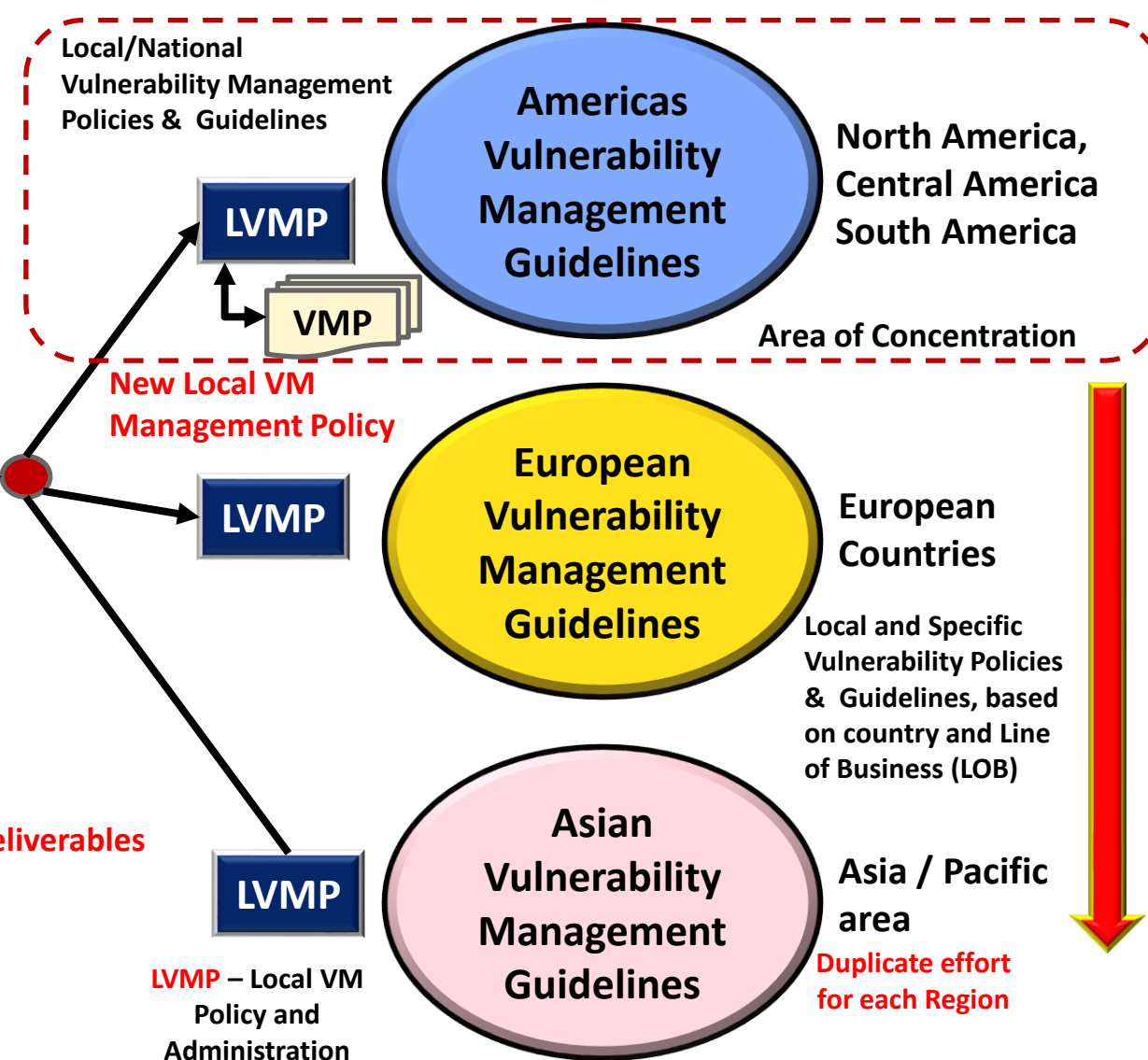
- Business:**
- Services
 - Applications
 - Topology
 - Regions
 - Countries
 - Operation Centers
 - Workflow
 - Job Responsibilities
 - Vulnerabilities
 - Security
 - Gaps
 - DevSecOps
 - CATO, CTEM
 - Problem/Incident Management
 - Recovery Management
 - ITAM, ITSM, ITOM

- Country:**
- Statues
 - Laws
 - Guidelines
 - Domestic
 - International
 - General Policy
 - Auditing & Reporting
 - Gap's & Exceptions
 - Mitigations
- Company:**
- Business Services and Applications (Rated 1-7)
 - Technical
 - Engineering
 - Development
 - Production
 - Tools
 - Workflow
 - Migrations
 - Transitions
- Staff:**
- LOBs
 - Organization
 - Structure & Titles
 - Component Owners
 - Job Functions & Responsibilities
 - Job Descriptions
 - Skills Matrix
 - Awareness & Training
- Could also be Company HQ and Domestic Regions**

Review existing VM Policies
Global VM Policies

Research

Deliverables



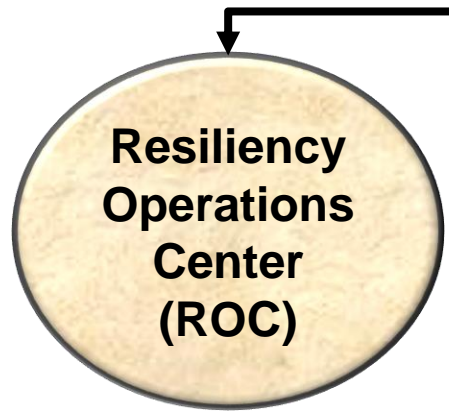
LVMP – Local VM Policy and Administration

Resiliency Operations Center (ROC)

Thomas Bronack
 Email: bronackt@dcag.com
 Phone: (917) 673-6992

ICT – Information and Communications Technology

Coordinating Resiliency throughout the organization



- Meet Departments,
- Understand needs,
- Vulnerability Management,
- Comply & Protect
- Define Recovery Actions
- Continuity of Business
- Document Action Plans and provide Awareness, Training & Exercise, Enactment.
- Optimize Workflow
- Continuous Improvement.



THE ICOR

THE INTERNATIONAL CONSORTIUM OF ORGANIZATIONAL RESILIENCE

(C) 2010-2016 ALL RIGHTS RESERVED

OWASP Vulnerability Management Cycles

Thomas Bronack
Email: bronackt@gmail.com
Phone: (917) 673-6992

Sequence:

1. Detection Cycle

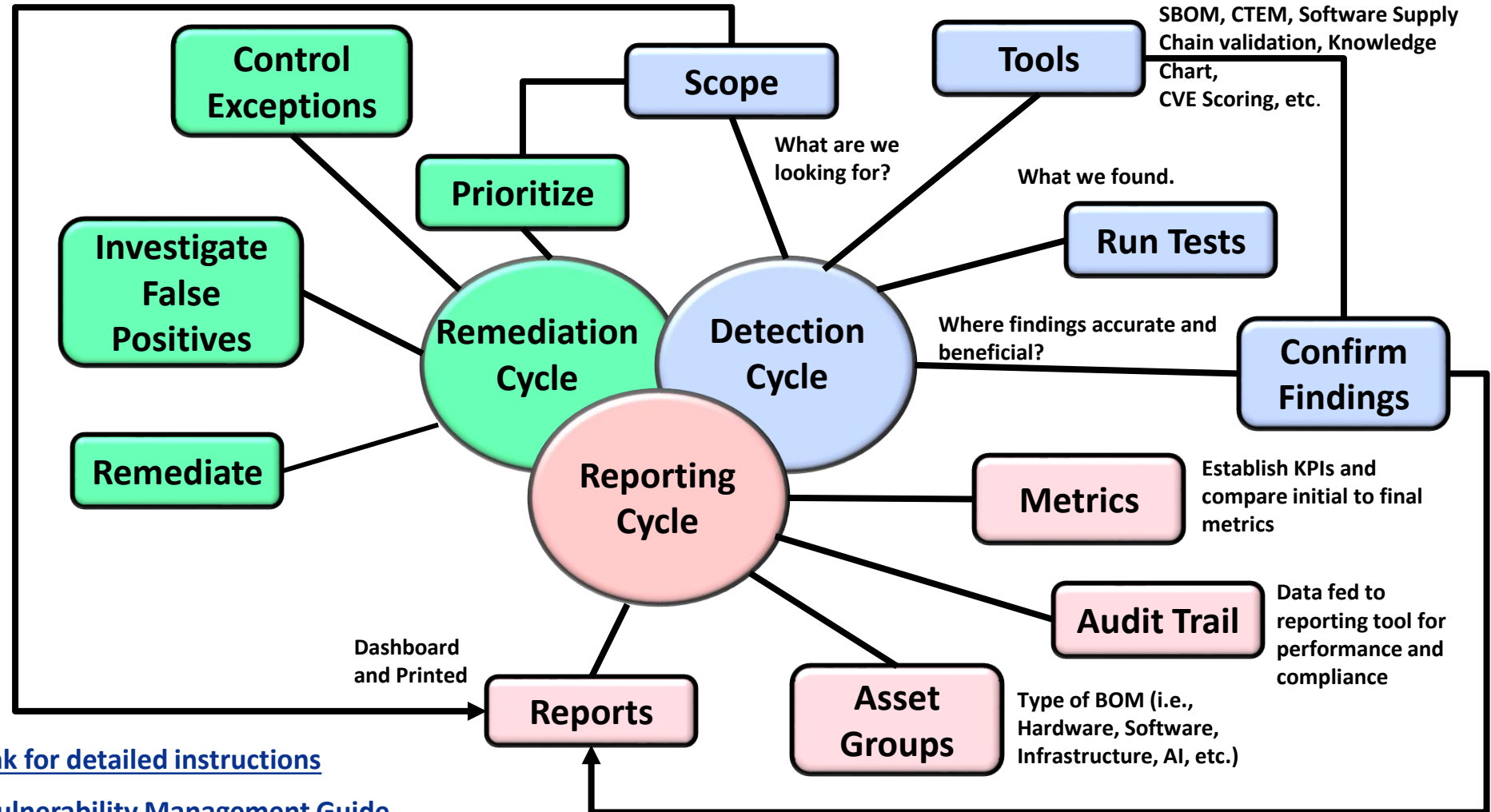
1. Define Scope
2. Select Tools
3. Run Tests
4. Confirm Findings

2. Reporting Cycle

1. Metrics
2. Audit Trail
3. Asset Groups

3. Remediation Cycle

1. Prioritize Scope
2. Define Controls and Exceptions
3. Investigate False Positives
4. Remediate



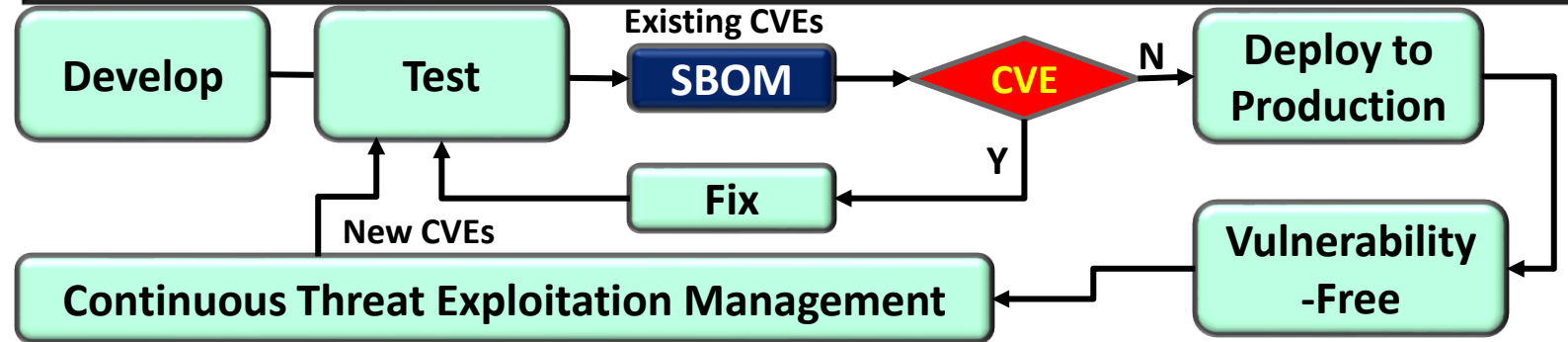
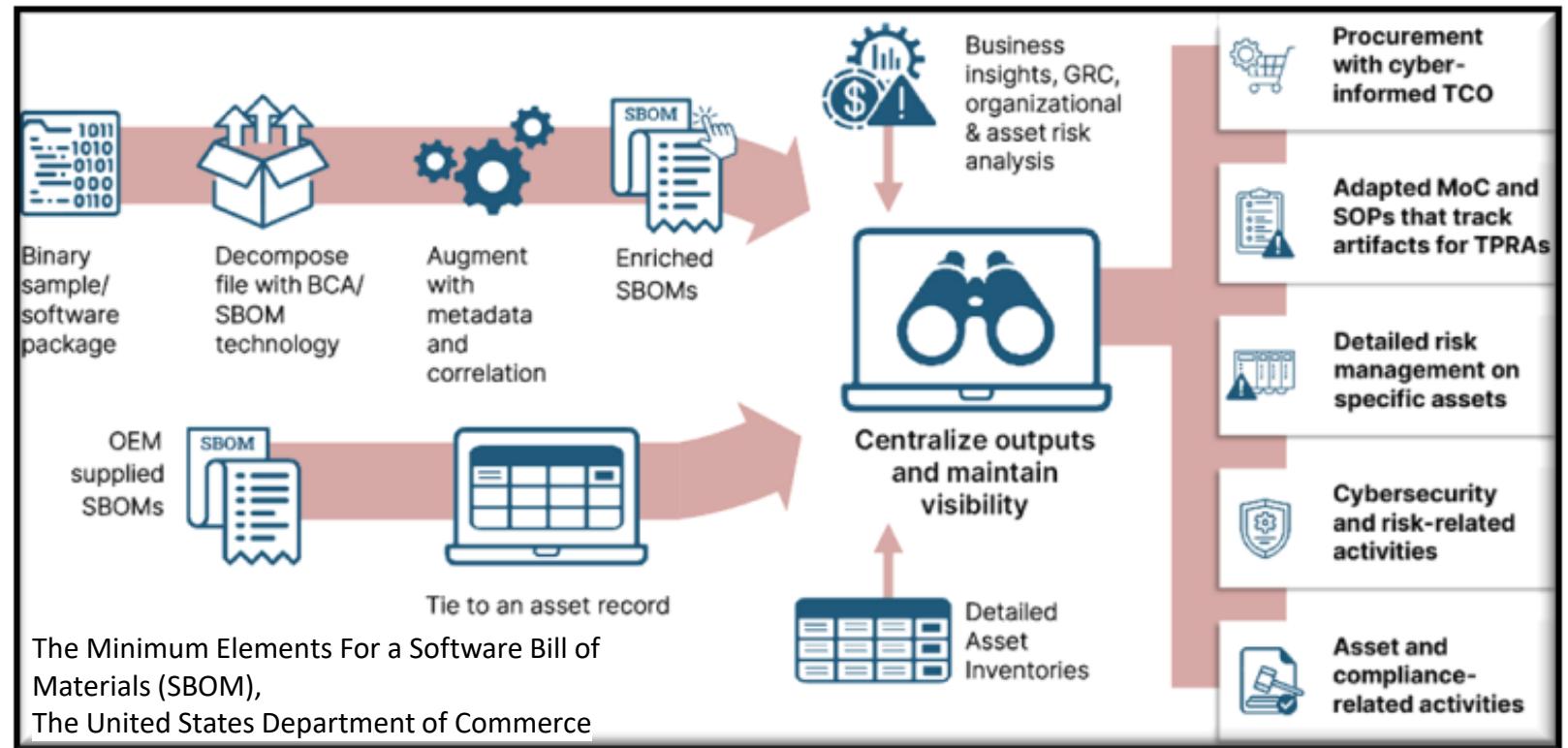
What is an SBOM and how does it work

Thomas Bronack
 Email: bronackt@dcag.com
 Phone: (917) 673-6992

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).

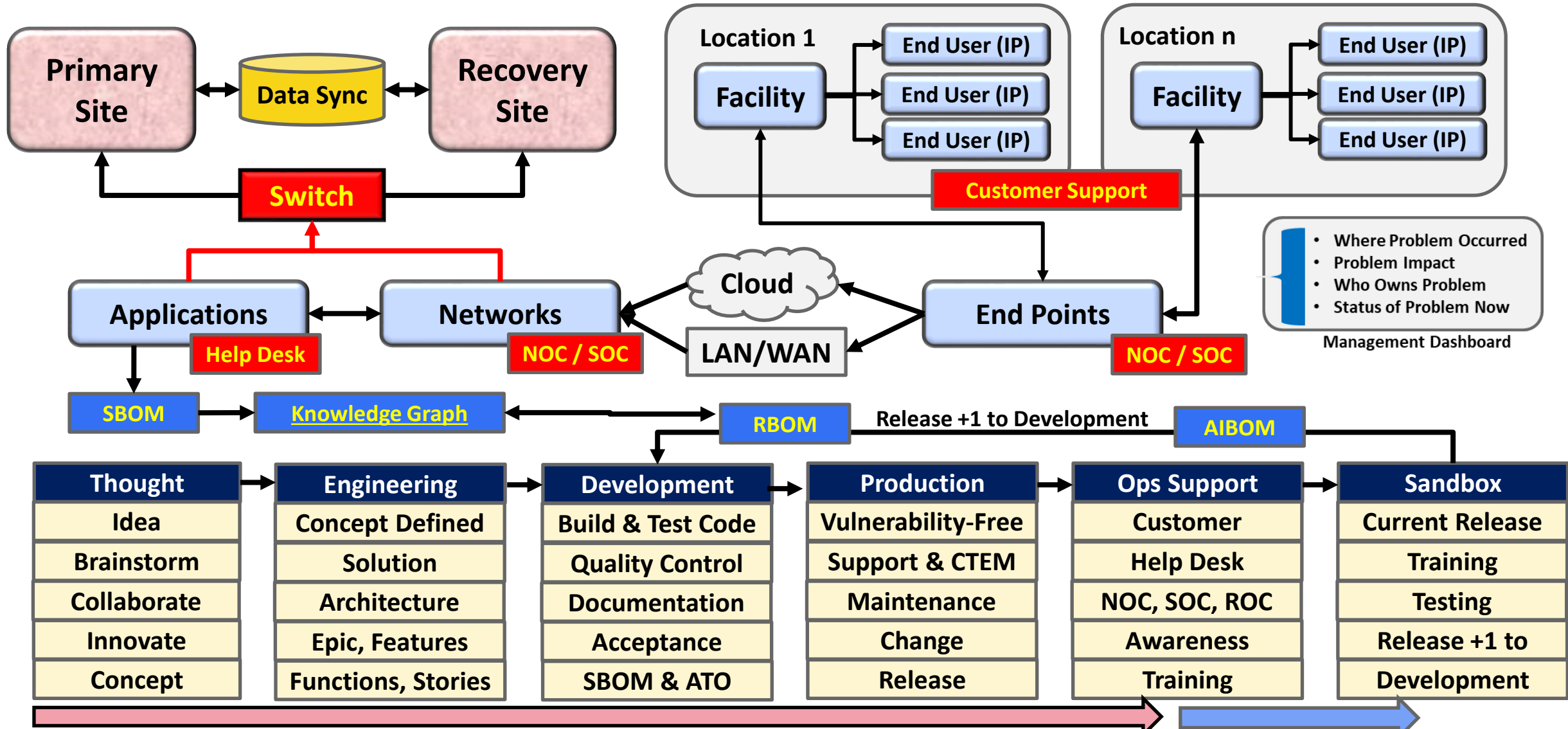
It then searches public vulnerability data bases to determine if active vulnerabilities are associated with the program product and any recommending changes that should be made prior to the product being introduced to the production environment (Patches, New Releases, etc.).

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



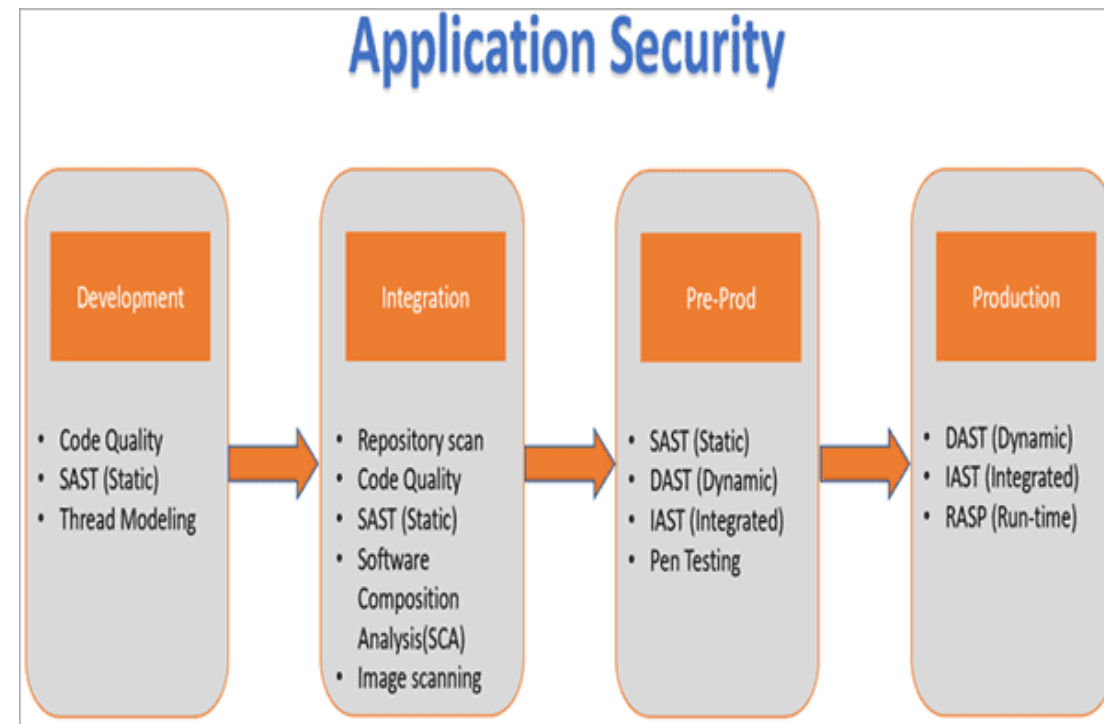
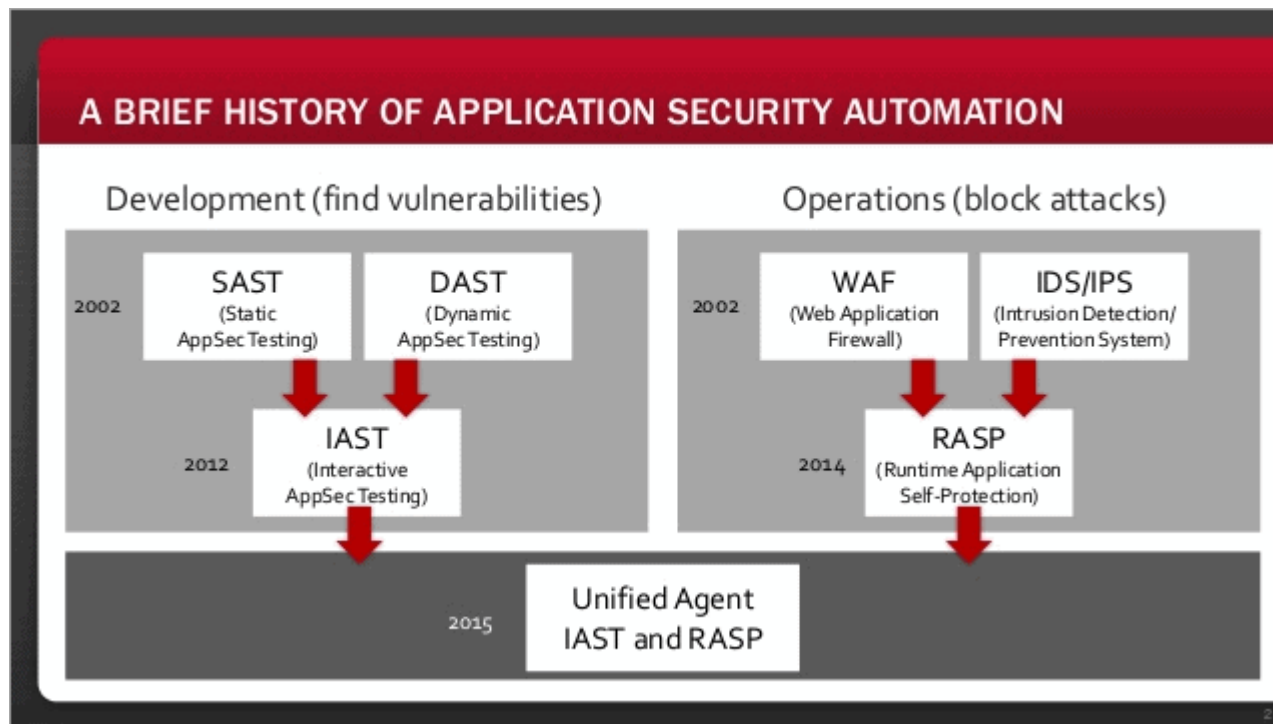
From Idea to Product, with Support and Recovery

Thomas Bronack
 Email: bronackt@dcag.com
 Phone: (917) 673-6992



Application Security Testing – Dev/Sec/Ops

Thomas Bronack
 Email: bronackt@dcag.com
 Phone: (917) 673-6992



SCA – Software Composition Analysis
 SAST – Static Application Software Testing
 IAST – Interactive App. Software Testing
 MAST – Mobile App. Security Testing
 RBOM – Release BOM (HW)

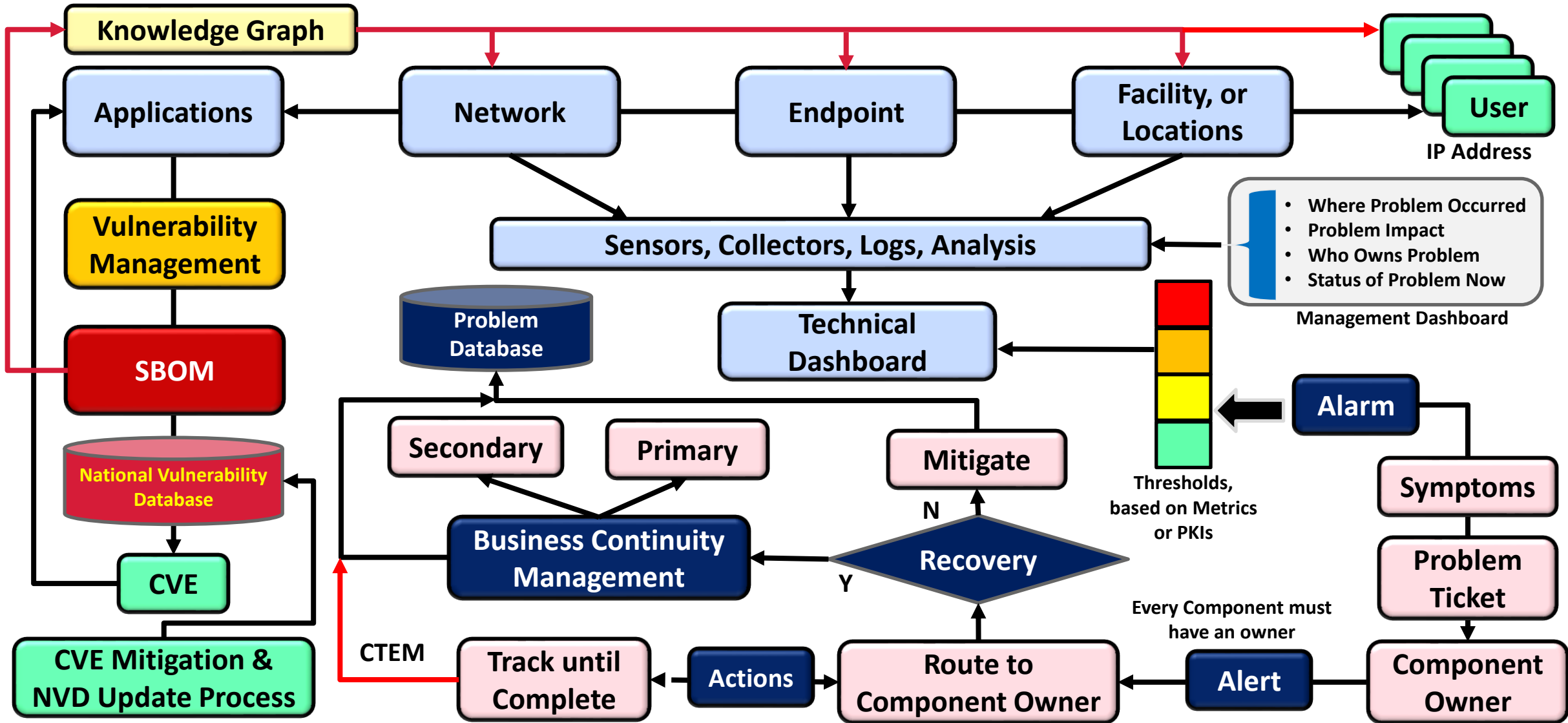
MAST – Mobile Application Security Testing
 RASP – Runtime Application Self-Protection
 AIBOM – ML and AI usage
 SBOM – Software Bill of Materials (SW)

SBOM, RBOM, AIBOM, et al



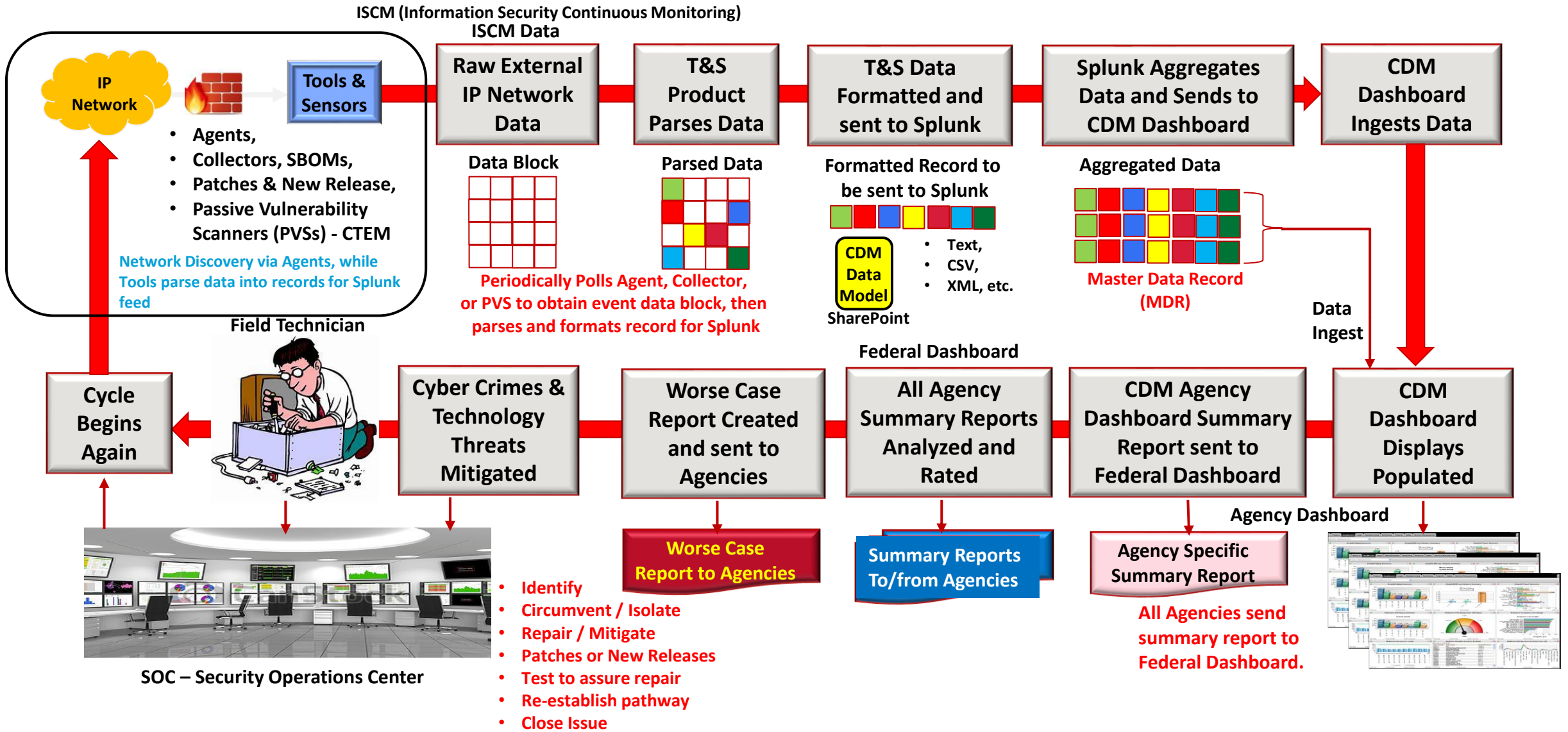
Tracking Problems through a Dashboard

Thomas Bronack
 Email: bronackt@dcag.com
 Phone: (917) 673-6992



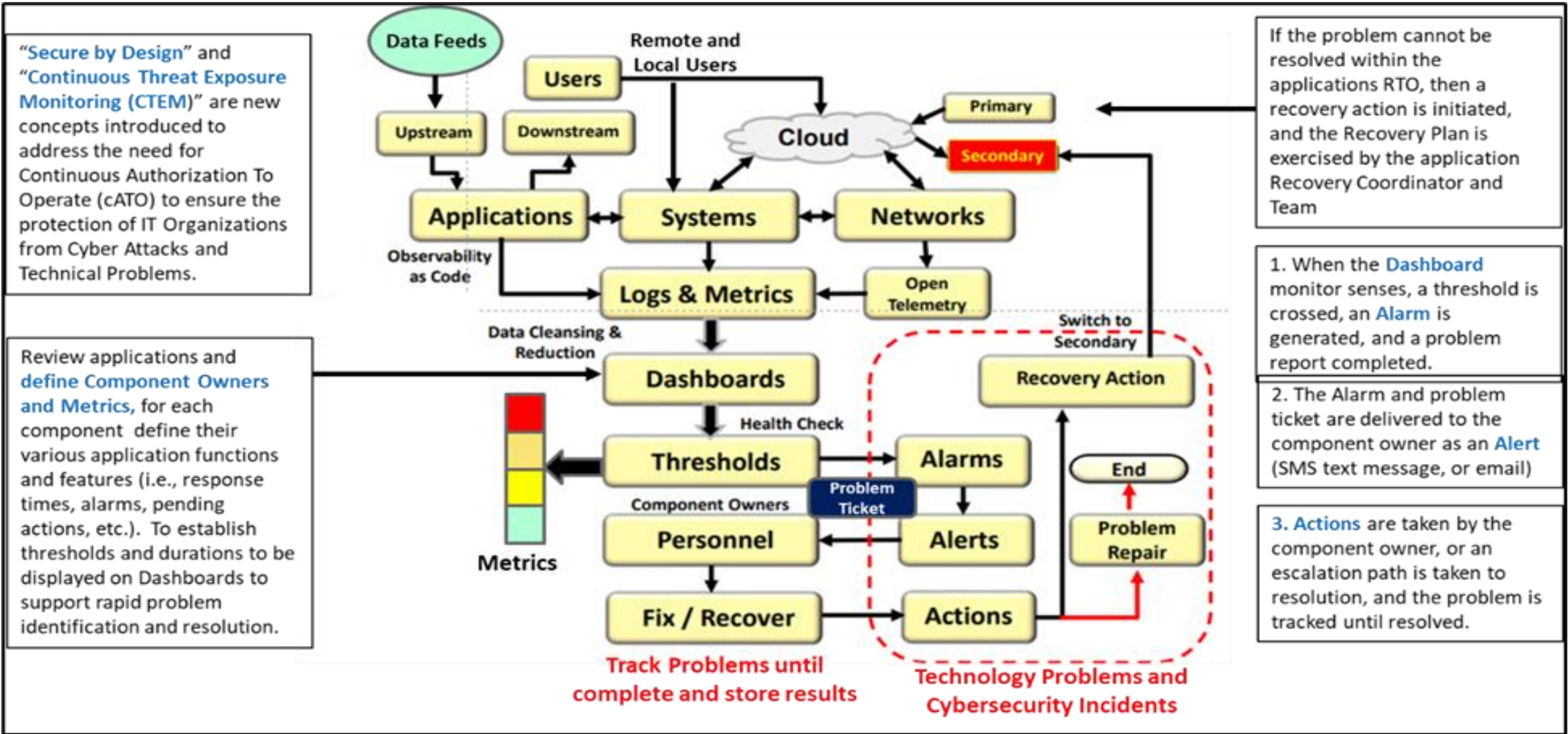
DHS Continuous Diagnostics and Mitigation (CDM) system for Cyber Crime mitigation

Thomas Bronack
 Email: bronackt@dcag.com
 Phone: (917) 673-6992



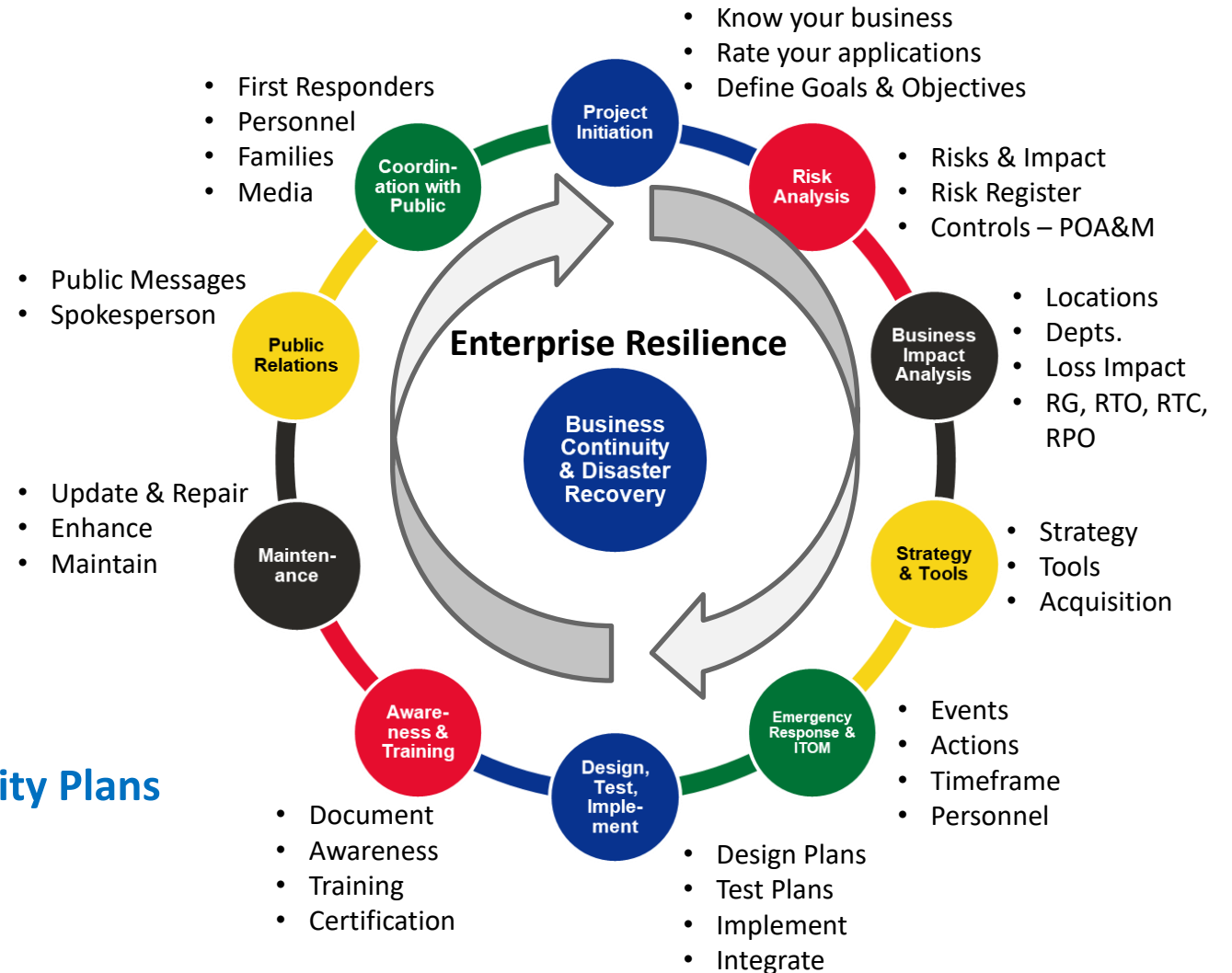
Problem / Incident Recognition, Reporting, and Resolving

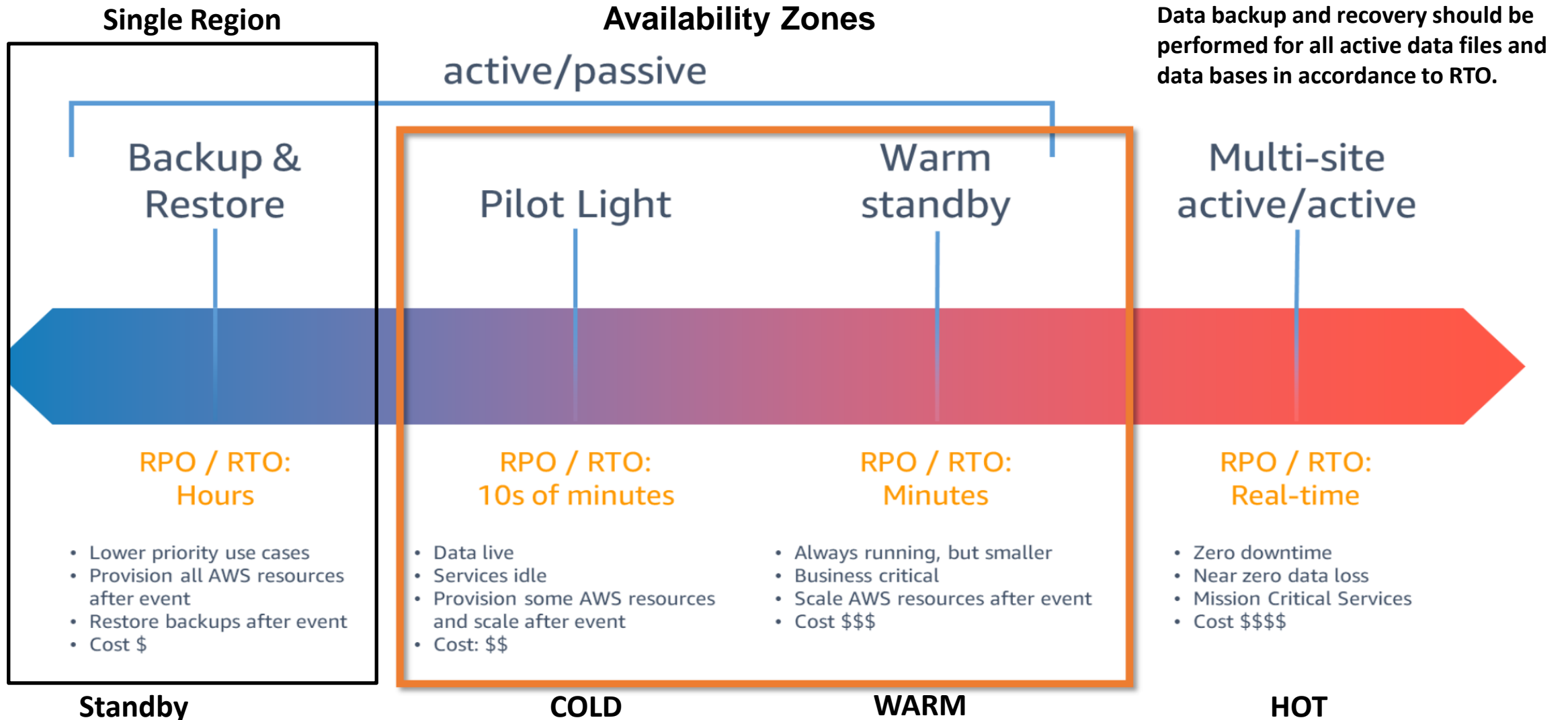
Thomas Bronack
 Email: bronackt@dcag.com
 Phone: (917) 673-6992



Ten Step Process to establish BCM/DR Practice

1. Project Initiation and Management
2. Risk Evaluation and Controls Improvement
3. Business Impact Analysis
4. Developing Business Continuity Strategies
5. Emergency Response and Operations
Restoration (Backup, Vaulting, Restoration)
6. Designing and Implementing Business
Continuity Plans
7. Awareness and Training
8. Maintaining and Exercising Business Continuity Plans
9. Public Relations and Crisis Communications
10. Coordinating with Public Authorities



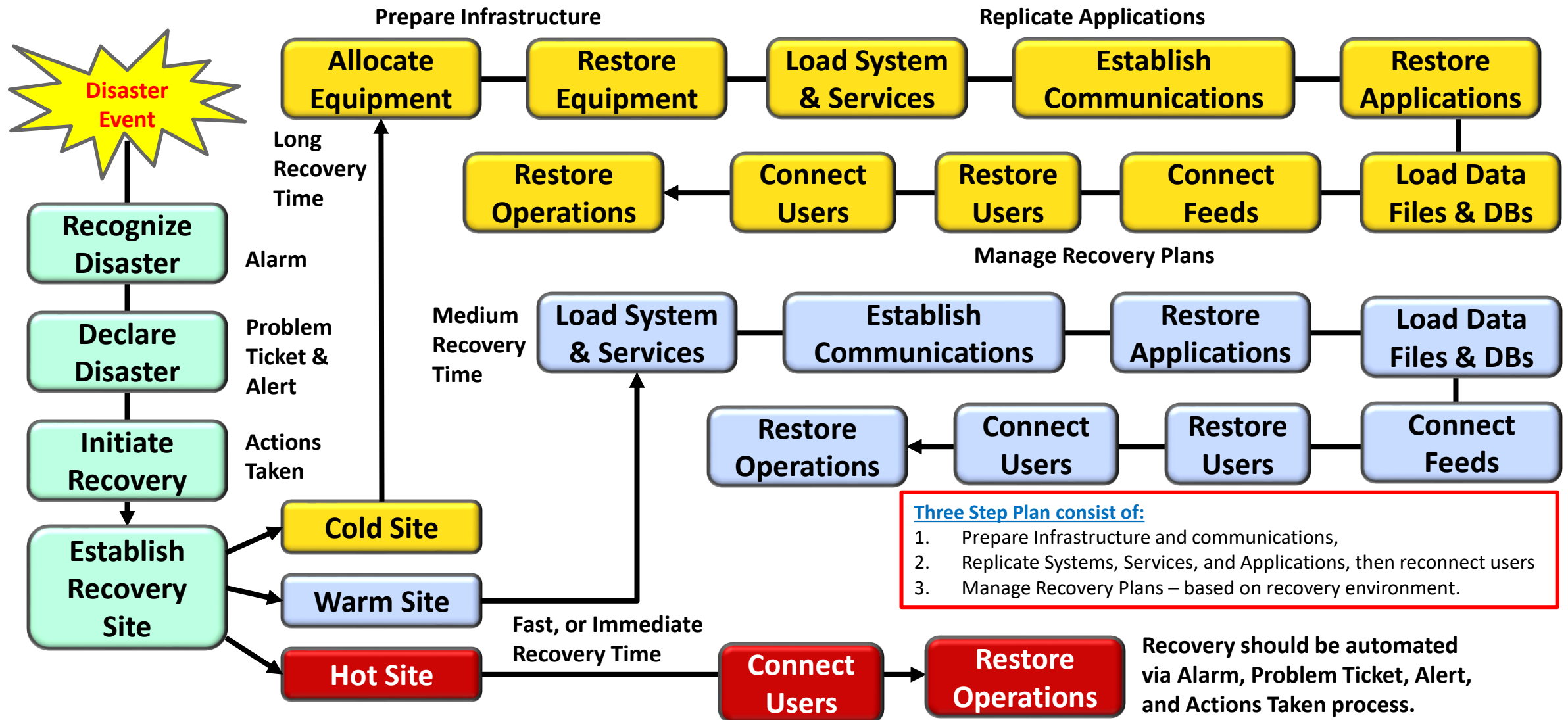


Resilience Patterns and Recovery Groups

Thomas Bronack
 Email: bronackt@dcag.com
 Phone: (917) 673-6992

Resiliency Patterns	Single Region	Multiple Regions		
	In-Region	Active Standby (Pilot Light)	Active-Passive (Warm Standby)	Active-Active (Multi-Site)
Pattern Profile	<ol style="list-style-type: none"> 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 	<ol style="list-style-type: none"> 1. TRANSACTIONAL TRAFFIC - handled by primary region only 2. INFRASTRUCTURE available on stand-by 3. APPLICATION provisioned, but in shutdown state 	<ol style="list-style-type: none"> 1. TRANSACTIONAL TRAFFIC - handled by primary region only 2. INFRASTRUCTURE available on standby 3. Minimal APPLICATION footprint running in 2nd region (all components are spun up and available with min. capacity, where application) 	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 1. Maintain PERSISTENT DATA REPLICATION infrastructure 2. APPLICATION CODE maintained for currency in BOTH REGIONS 3. Operate Production from stand-by region periodically 	<ol style="list-style-type: none"> 1. Maintain PERSISTENT DATA REPLICATION infrastructure 2. APPLICATION CODE maintained for currency in BOTH REGIONS 3. Operate Production from stand-by region periodically 	<ol style="list-style-type: none"> 1. Maintain 2-WAY PERSISTENT DATA REPLICATION 2. APPLICATION CODE maintained for currency in BOTH REGIONS 3. Operate Production from stand-by region periodically
Recovery Steps	<ol style="list-style-type: none"> 1. ACQUIRE INFRASTRUCTURE 2. BUILD OUT infrastructure 3. DEPLOY application 4. RECOVER / RECREATE DATA 5. REDIRECT TRAFFIC to region 2 	<ol style="list-style-type: none"> 1. SCALE INFRASTRUCTURE 2. STARTUP application 3. FAILOVER TRAFFIC 	<ol style="list-style-type: none"> 1. AUTO- SCALE INFRASTRUCTURE 2. FAILOVER TRAFFIC 	<ol style="list-style-type: none"> 1. RECOVERY achieved 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		

Sequence of Events to enact a Recovery Operation



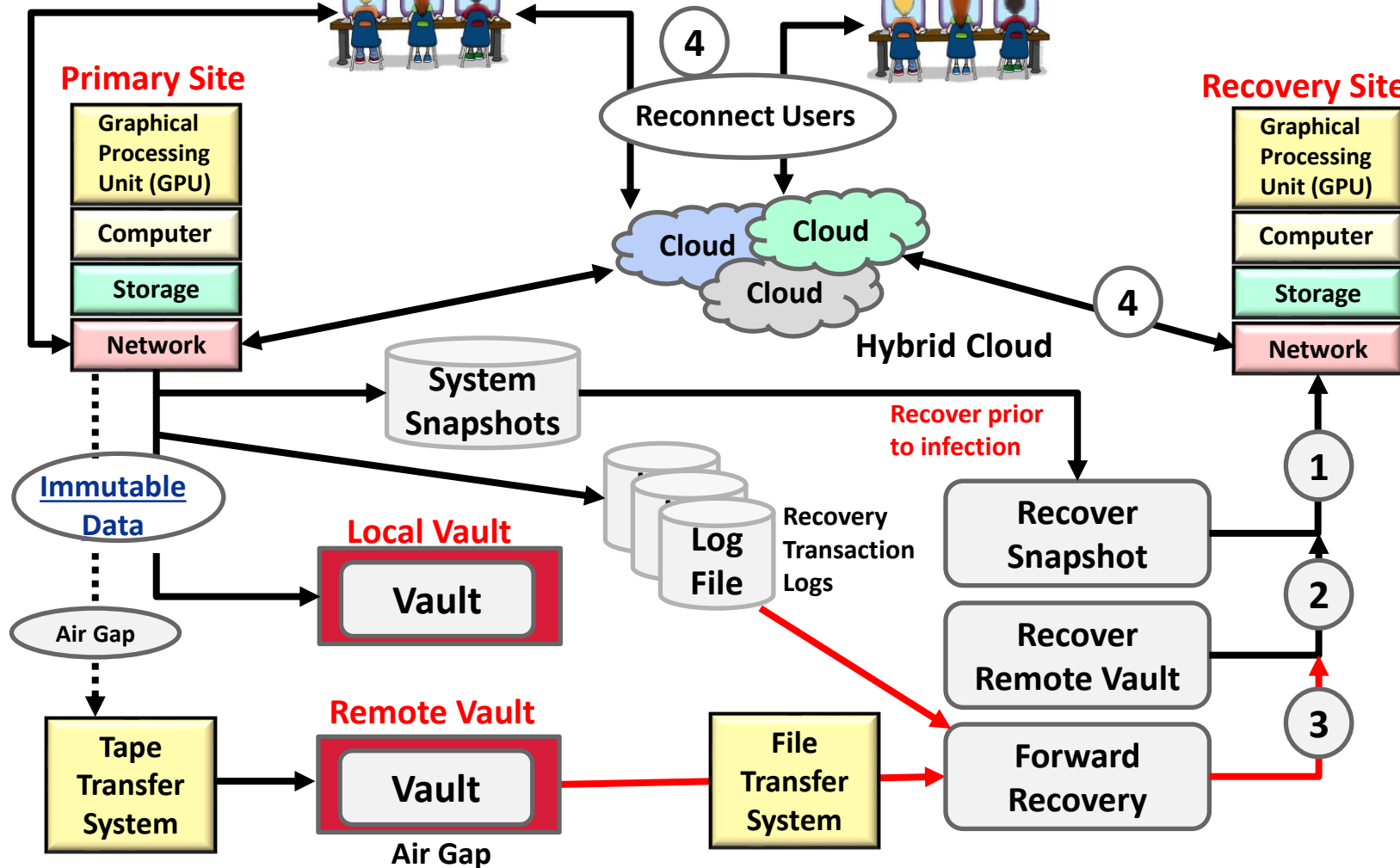
System Recovery – Even with Ransomware

Local Users reconnected via Cloud

Local Users

Remote Users

Remote Users reconnected via Site Recovery



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 system.
2. Recover Remote Vault (Air Gap) to recover backup data.
3. Forward Recovery to present time by combining Logs with Stored Data to recreate active environment.
4. Reconnect Users and resume operations.

Use Tape Transfer System to forward vaulted tape to recovery site to support rapid recovery

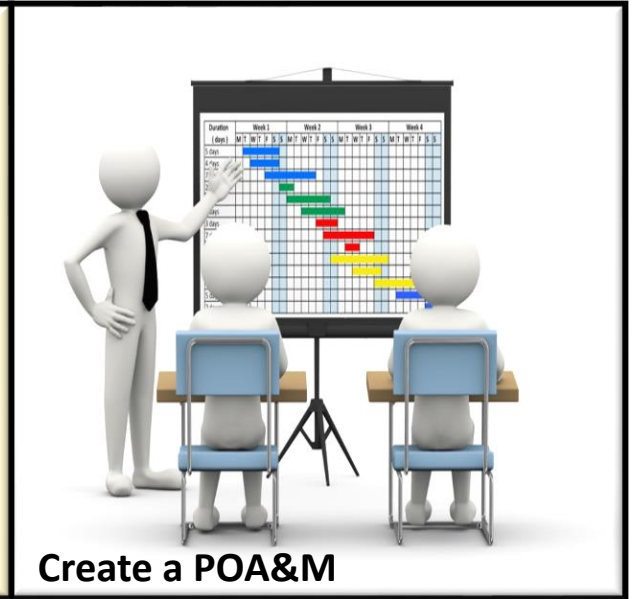
Design project to achieve goals within desired scope

Thomas Bronack
Email: bronackt@gmail.com
Phone: (917) 673-6992

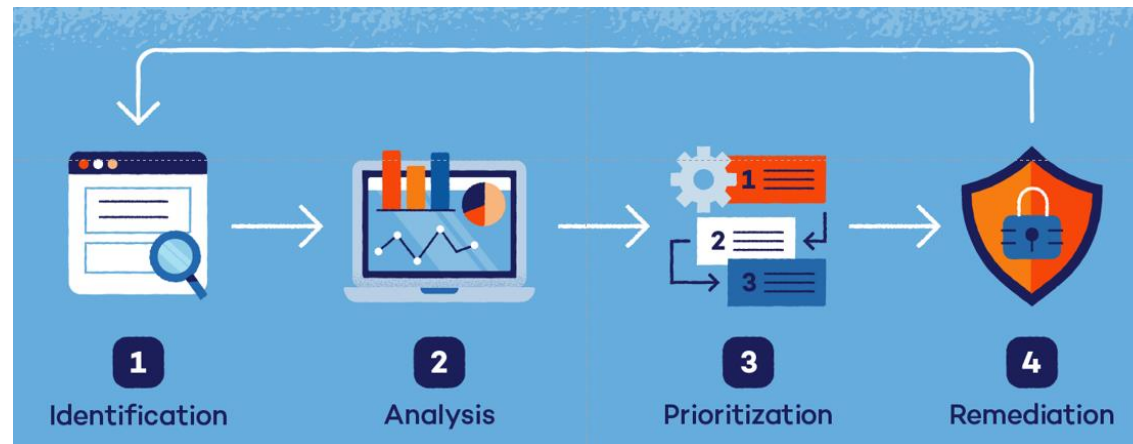


Project Goals:

1. Vulnerability Management Practice understood
2. Tool Assessment and Selection (AoA)
3. Workflow to determine how to use Vulnerability Management Tools
4. Vulnerability-Free Production Environment
5. Compliance to all required laws and regulations
6. Vulnerability Management Maturity Cycle
7. Continuous Threat Exploitation Management
8. Business Continuity Management
9. Awareness and Training.



1. Identify your needs and assess your weaknesses, exceptions, and gaps.
2. Define your goals and scope, then conduct an analysis of your environment and workflow.

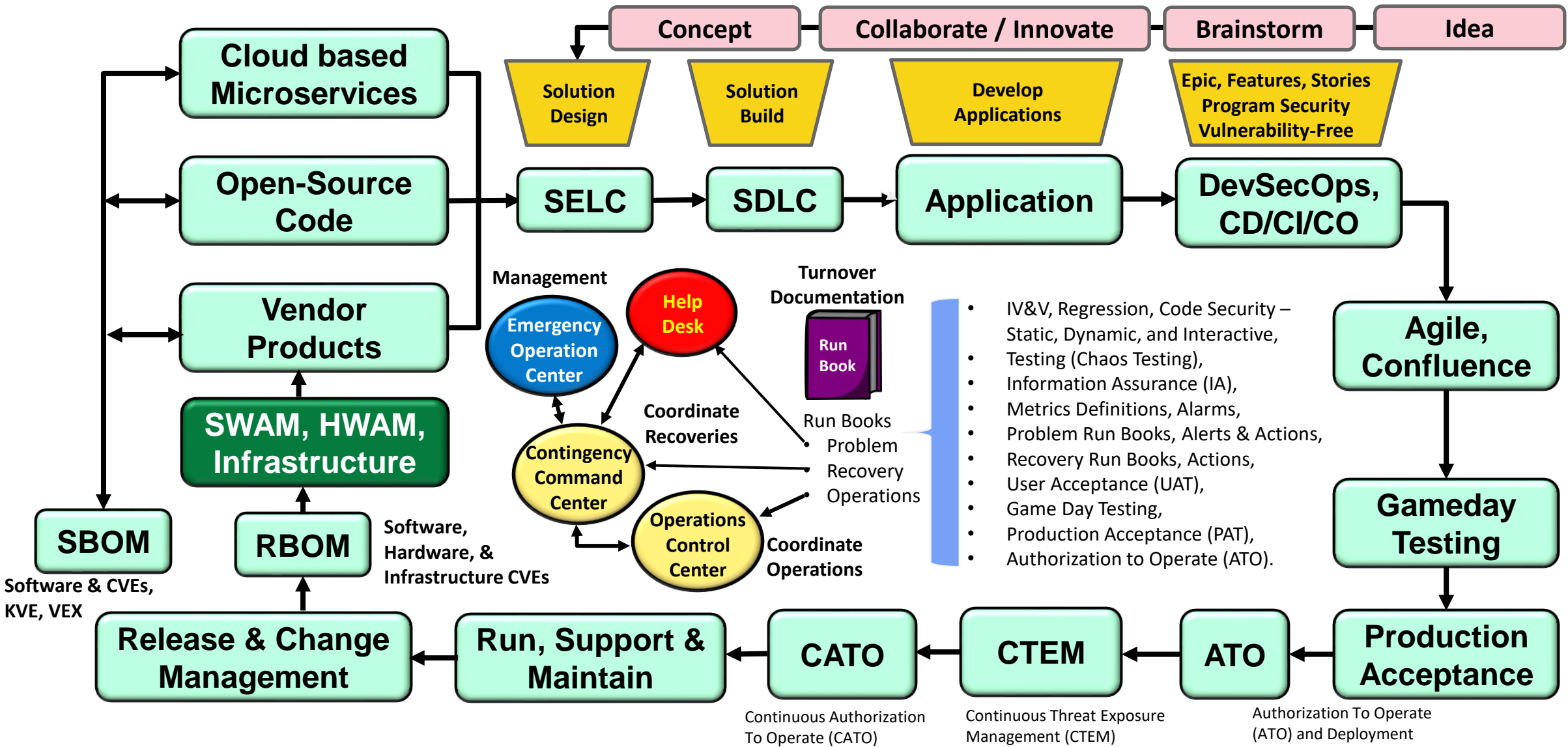


3. Prioritize located weaknesses and develop a Statement of Work (SOW) to resolve issues.
4. Devise a Remediation POA&M, gain approval, formulate team, and commence work.

Define project concept, actions, and deliverables within POA&M

Application Construction and entry to Production

Thomas Bronack
 Email: bronackt@dcag.com
 Phone: (917) 673-6992



Service deliver/support using Vulnerability Management

Thomas Bronack
 Email: bronackt@dcag.com
 Phone: (917) 673-6992

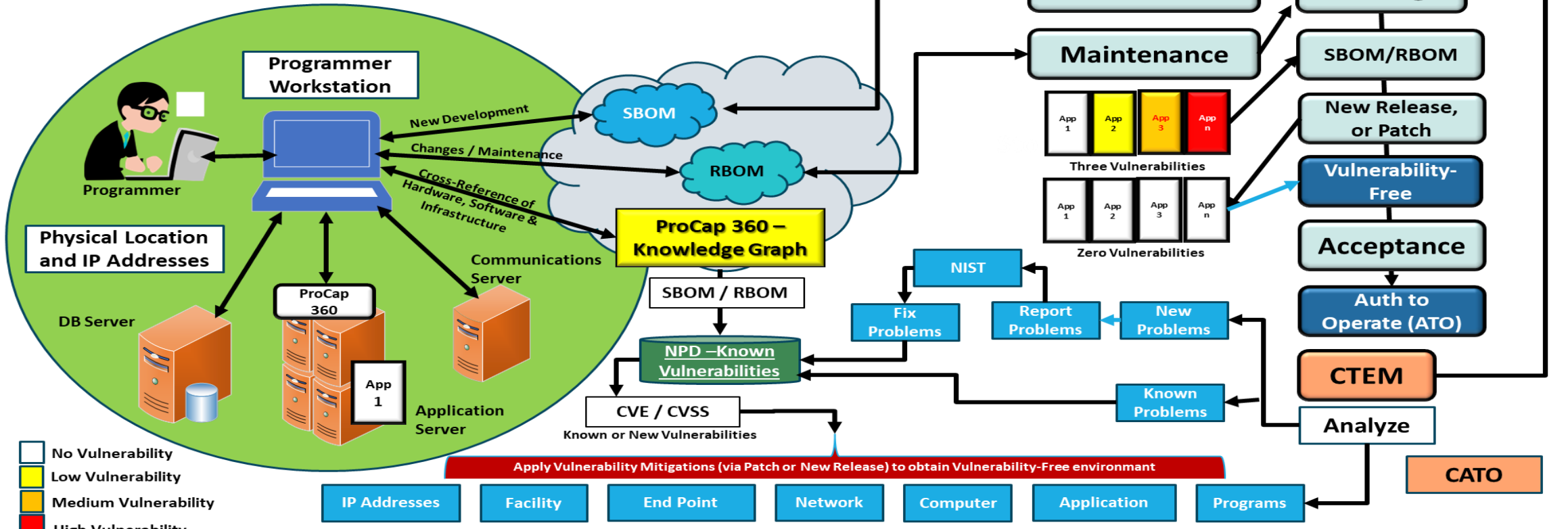
From idea to Production Product or Service Delivery



SBOM - for New Development
 RBOM - for Maintenance and Change Management



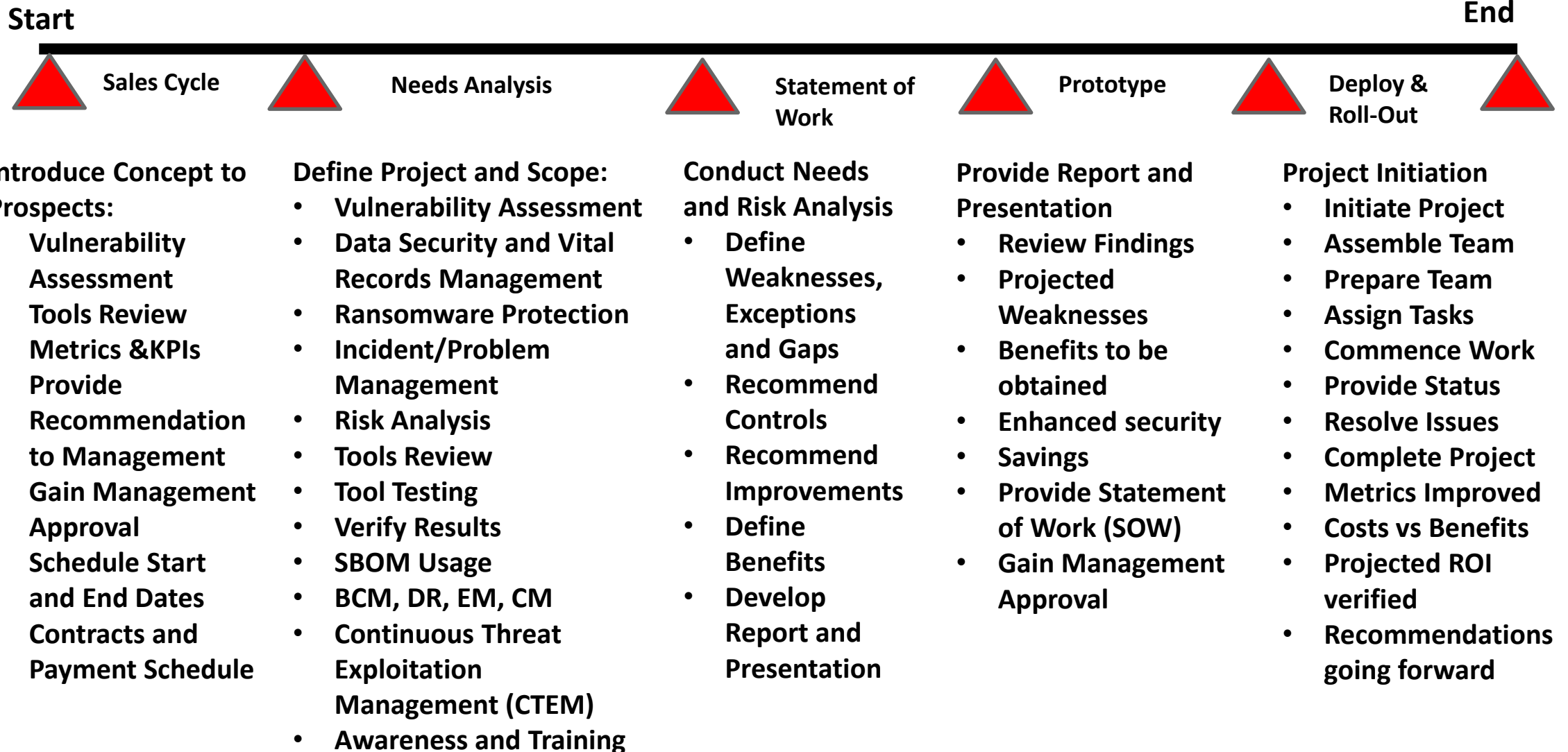
EPIC
 Feature
 Functions
 Stories



- No Vulnerability
- Low Vulnerability
- Medium Vulnerability
- High Vulnerability

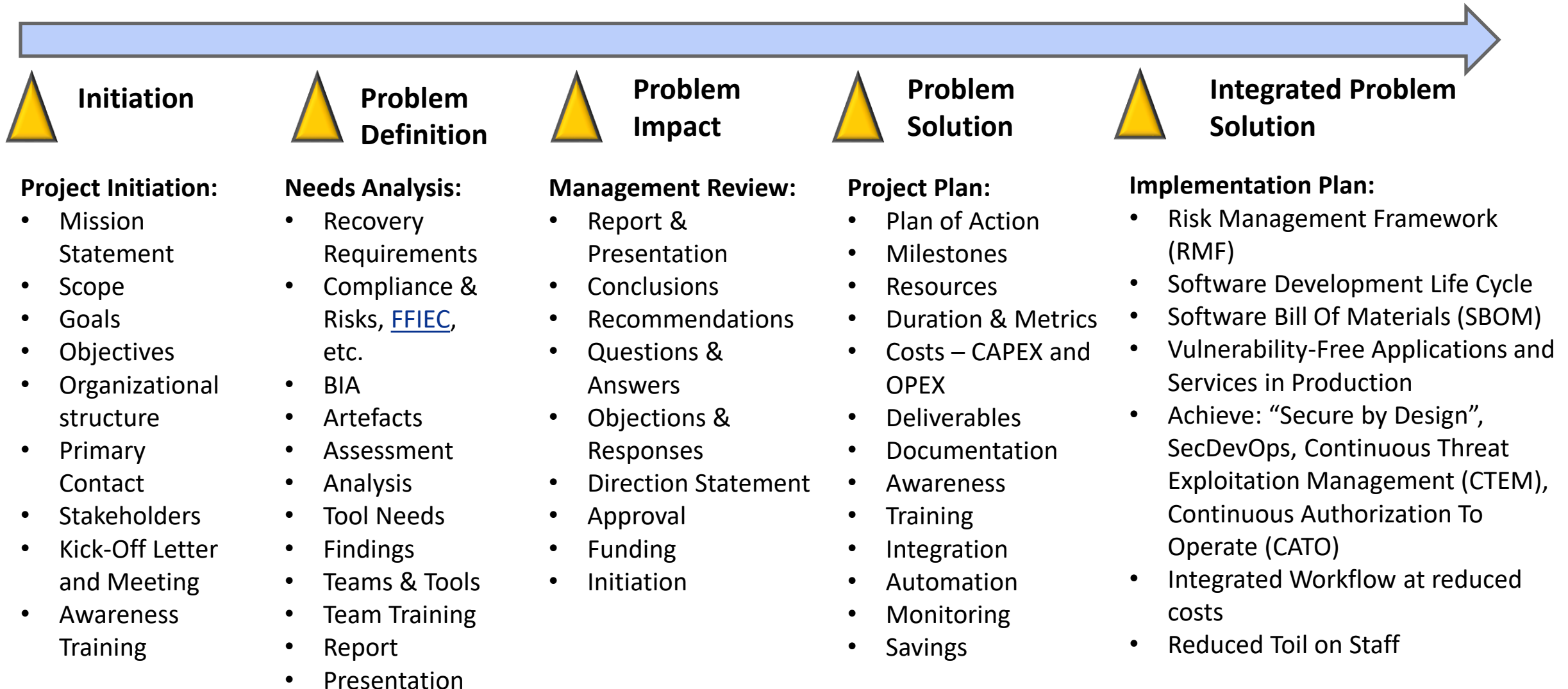
Monitoring, Supporting, and Managing the Production Environment via CTEM

Developing a detailed Project Plan



Process of Organizational Optimization

Thomas Bronack
Email: bronackt@gmail.com
Phone: (917) 673-6992

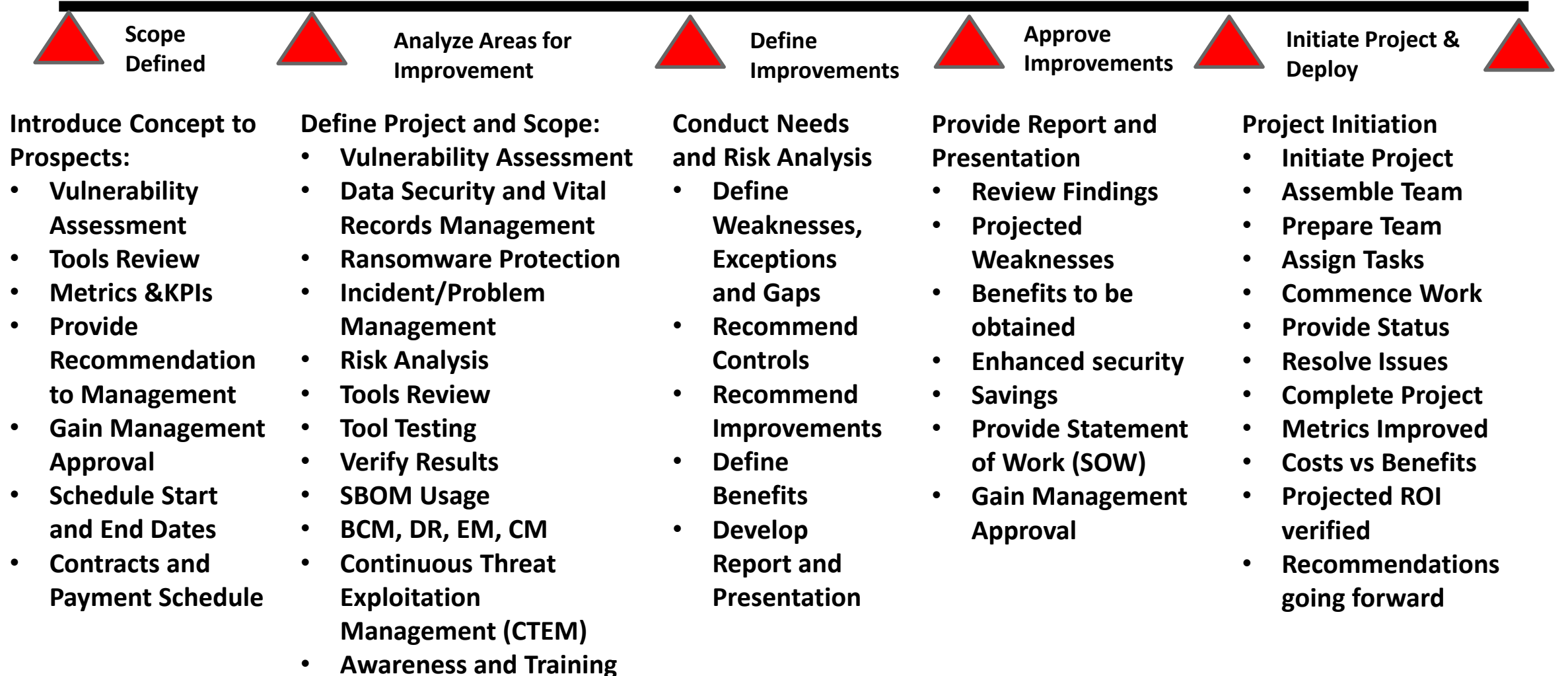


Designing a Project from Concept to Initiation

Thomas Bronack
 Email: bronackt@gmail.com
 Phone: (917) 673-6992

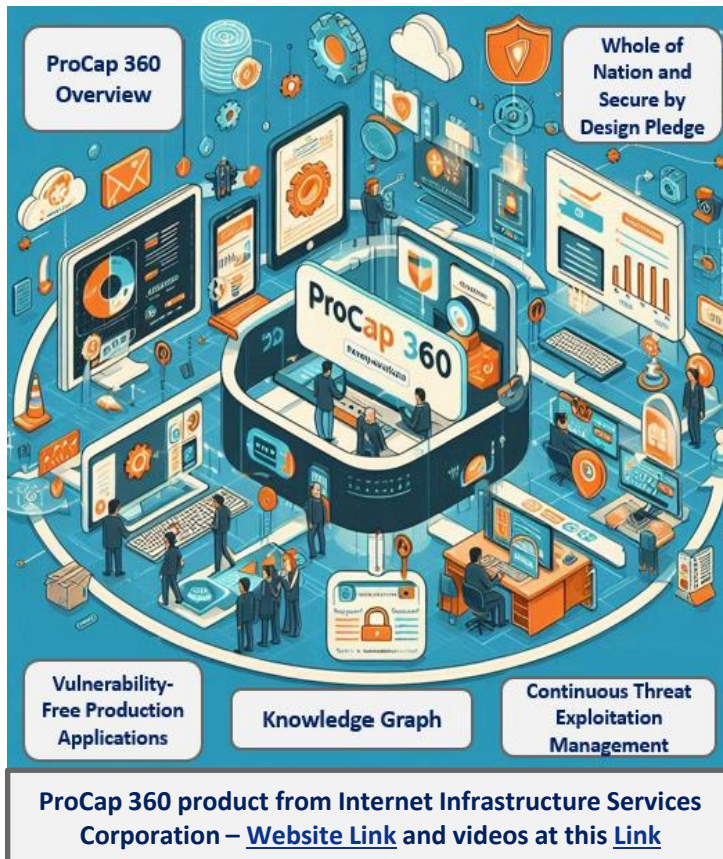
Start

End



Overview of ProCap 360™

Thomas Bronack
Email: bronackt@dcag.com
Phone: (917) 673-6992



Software applications are like digital bridges that connect us to the world. They enable us to communicate, collaborate, learn, work, and play. But just like physical bridges, they need to be designed, built, and operated with care and quality. Otherwise, they can collapse and cause harm.

That's why we need a solution that can automate the vulnerability management of the software development lifecycle. A solution that can scan, assess, prioritize, and remediate vulnerabilities in the software components and configurations across multiple cloud providers and regions. A solution that can provide a comprehensive and consistent view of the software pedigree, using the Application Software Bill of Materials (SBOM) as a blueprint. A solution that can integrate with the tools and platforms we use to develop, deploy, and operate our software applications. A solution that can comply with the industry standards and regulations that govern our software supply chain.

That solution is ProCap 360.

Installed currently in Azure, AWS and Google cloud providers, and optionally on premise, providing real-time component version, license and vulnerability scores for both SBOM and RBOM release components.

ProCap 360 is a cloud-based vulnerability management solution that leverages the power of [Knowledge Graph](#) technology, which provides visual analytics, application DevSecOps, and orchestration capabilities. ProCap 360 can integrate with popular tools and platforms, to streamline your vulnerability management visualization.

ProCap 360 is designed to complement your existing SIEM/SOAR scanning infrastructure. You can use ProCap 360 to perform policy assessments, authenticated code releases, and infrastructure build releases, and . ProCap 360 also supports dynamic, automated compliance reporting, for every non-production and production environment.

With ProCap 360, you can achieve a scalable and effective vulnerability management process for your multi-cloud applications. ProCap 360 helps you reduce your attack surface, improve your security posture, and protect your organization from potential threats and penalties.

ProCap 360 is available today for automating software lifecycle vulnerability management. It is the solution that we, the stakeholders of the digital world, need to support and adopt. It is the solution that will help us build stronger and more “secure by design” digital bridges than ever before.



Enterprise Resilience:

- Vulnerability Management
- Business Continuity Management
- Compliance Certification
- Resilience Operations Center (ROC), with Guidelines and Procedures, Awareness and Training.
- Relationship with ProCap 360™ to produce SBOMs, RBOMs, and AIBOMs, Knowledge Graph, Application Factory, Continuous Threat Exploitation Management (CTEM), and Compliance

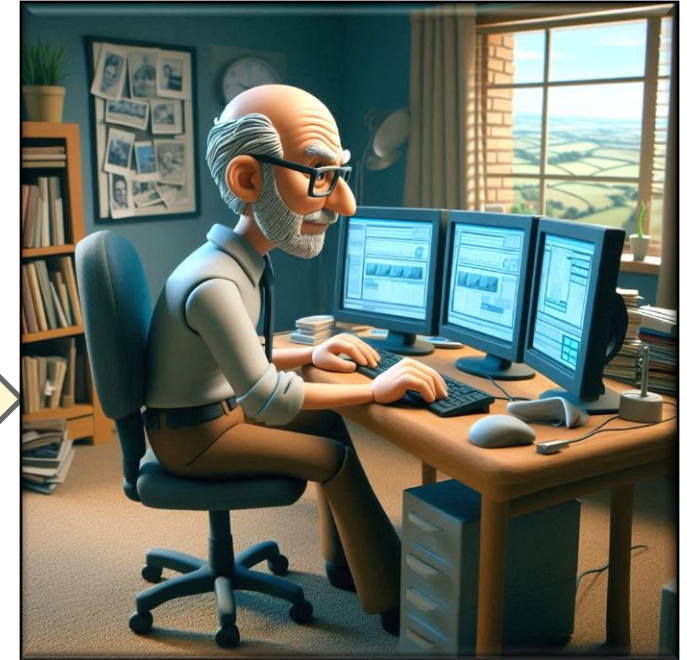
Reaching out to assist our clients

Thomas Bronack
Email: bronackt@dcag.com
Phone: (917) 673-6992



- Discuss
- Define
- Propose
- Achieve

Quality Service at
a Reasonable
Price



If you find the information included in this presentation of value and want to explore methods to improve the reliability of your enterprise and IT environment, please contact me to discuss your needs and request our assistance.

We look forward to our future relationship.

Thomas Bronack, CBCP
President
Data Center Assistance Group, LLC

bronackt@dcag.com
bronackt@gmail.com
917-673-6992