Thomas Bronack, CBCP

Presentation Topics

- Vulnerability Management
- SBOMs
- CSF 2.0 Structure and Usage
- Continuous Threat Exploitation Management (CTEM)
- 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

Topics include:

- Vulnerability Management
- Continuous Threat Exploitation Management (CTEM), and Cloud Native Application Program Platform (CNAPP),
- Recovery Management

Contact Information:

- bronackt@gmail.com
- bronackt@dcag.com
- Website: www.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 E**nterprise 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.

The Software Supply Chain is at risk, as demonstrated by recent events and world turmoil, 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 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.

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

Thomas Bronack, CBCP
bronackt@DCAG.com
(917) 673-6992

Agenda

Thomas Bronack
Email: bronackt@dcag.com
Phone: (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.

3. **Vulnerability Management** must be considered to address this issue, along with the implementation of an SBOM tool to provide vulnerability-free applications for the production environment (legal requirement). **New Laws and Regulations** comply, and some require an **SBOM**.

4. **Business Continuity Management** must be enhanced to support Service Level Agreements and a company's ability to continue to supply services and products.

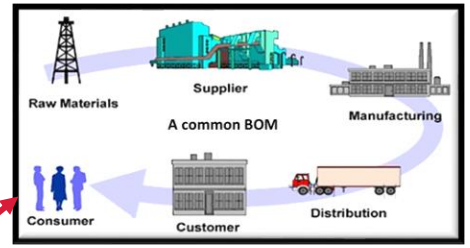
5. **The ability to develop** an idea to a concept that can be engineered, developed, and deployed to production as **vulnerability-free** must be defined and supported via "**Whole of Nation**" and "**Secure by Design**" guidelines provided by **DHS/CISA** for best performance and security.

Protecting Organizations is more difficult than ever

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

Suppliers
Vendors
Transport
Manufacturing

A World in Turmoil can choke supplies



Supply Issues cause delays in building and delivering goods, and increased costs

Builder Concerns
World Concerns
Delivery Concerns

Customers
Organization
Supply Chain

Technical Problems
Secure by Design
Cyber Crimes

Marketing
Sales
Delivery

Services
Engineering
Products
Development
Applications
Operations

Inventory
Supply Chain
Compliance
Delivery

Idea
Engineer Solution
Develop Solution
Verify & Validate
Deploy & Continuity
Audit & Compliance
Deliver
Support & Maintain

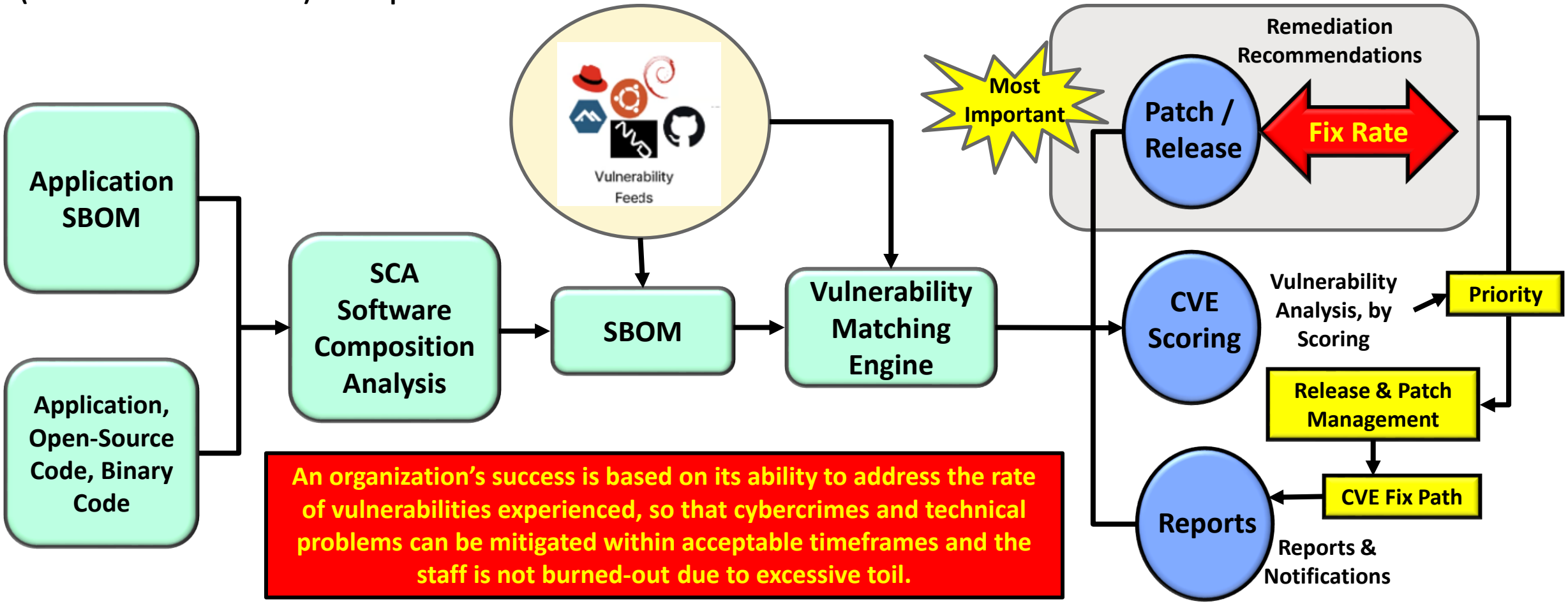
Product Engineering and Development Life Cycle

Identifying and Reporting Vulnerabilities

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

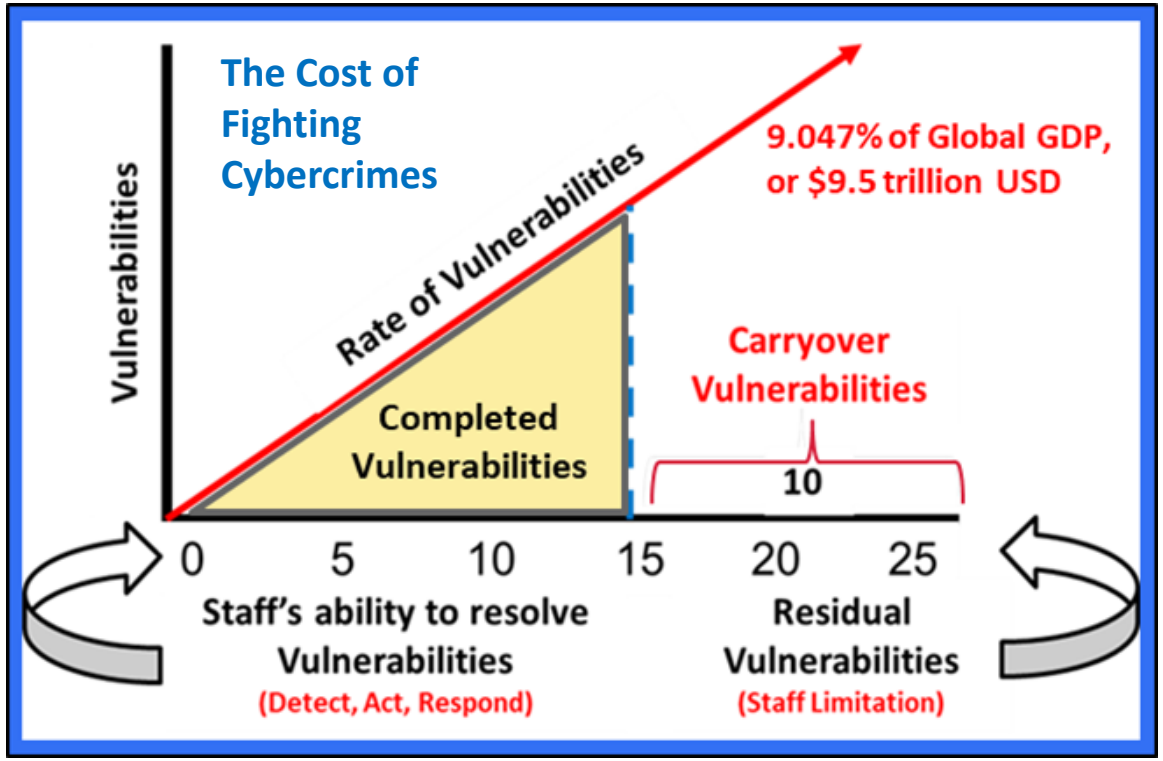
Vulnerabilities are identified within Applications, or existing Application SBOMs (Software Bill of Material) and reported.

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

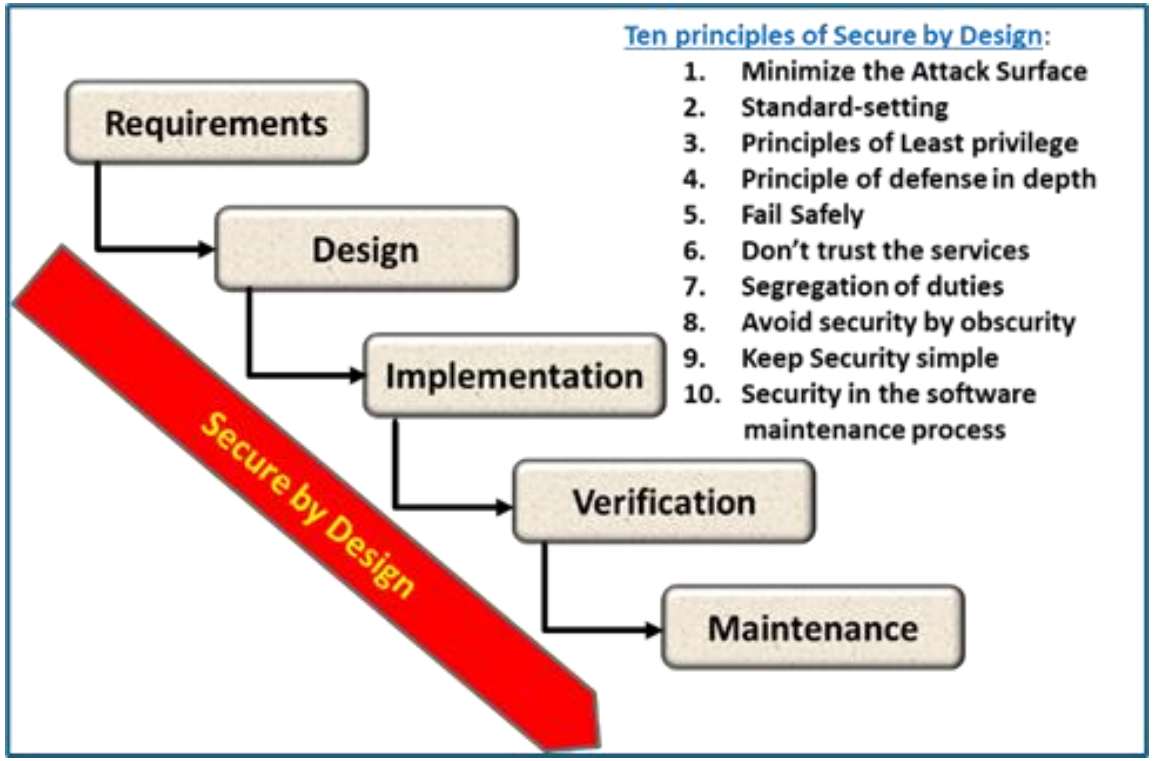


An organization's success is based on its ability to address the rate of vulnerabilities experienced, so that cybercrimes and technical problems can be mitigated within acceptable timeframes and the staff is not burned-out due to excessive toil.

Fighting Vulnerabilities and Secure by Design



The **cost of fighting cybercrimes** and technology threats is estimated at $9.5 Trillion and 9.04 % of Global GDP. Improving the vulnerability fix rate will greatly reduce costs and improve business service continuity and resilience.



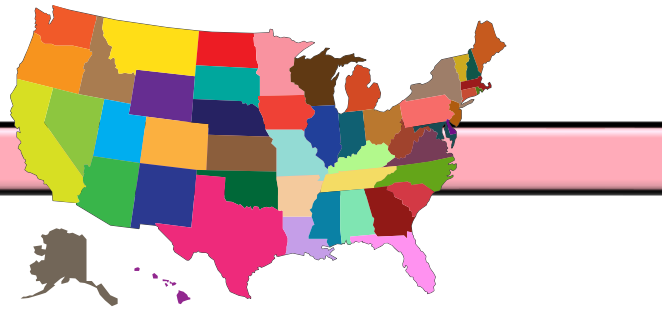
The government has developed a "**Whole of Nation**" approach to combat these costs through the "**Secure by Design**" methodology developed by DHS/CISA to safeguard Government, Business, Infrastructure, and Utilities from cybercrimes and technology threats.

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.

Business Resilience Definition and Plan of Action

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

Business resilience refers to an organization's ability to adapt, recover, and thrive in the face of disruptions or unexpected changes that could impact its operations, people, assets, brand, or reputation. It positions organizations to prepare for anything that might come their way[1].

Here's a plan on how to achieve business resilience within a major organization:

1.Risk Assessment and Identification:
1. Conduct a comprehensive risk assessment to identify potential threats and vulnerabilities. Consider both internal (e.g., supply chain disruptions, cyber attacks) and external (e.g., natural disasters, economic downturns) risks.
2. Engage stakeholders from various departments to ensure a holistic view of risks.

2.Business Continuity Planning:
1. Develop a robust business continuity plan (BCP) that outlines procedures for maintaining essential functions during disruptions.
2. Define roles, responsibilities, and communication channels during crises.
3. Regularly review and update the BCP to align with changing circumstances.

3.Diversify Supply Chains:
1. Relying on a single supplier or geographic region can be risky. Diversify suppliers and build redundancy.
2. Establish alternative sourcing options to mitigate supply chain disruptions.

4.Invest in IT Infrastructure and Security:
1. Strengthen IT systems and cybersecurity protocols.
2. Implement data backup and recovery mechanisms.
3. Train employees on security best practices.

5. Establish Strategic Direction and select supportive tools
1. Recovery Management Tool
2. Awareness and training

6.Employee Safety and Well-being:
1. Prioritize employee safety during disruptions.
2. Establish protocols for tracking remote and onsite workers' health and availability.
3. Provide mental health support and resources.

7.Scenario Testing and Drills:
1. Regularly conduct scenario-based testing and drills to validate the effectiveness of your resilience strategies.
2. Simulate disruptions and evaluate the organization's response.

8.Agility and Adaptability:
1. Foster an organizational culture that embraces change and agility.
2. Encourage cross-functional collaboration and innovation.
3. Be prepared to pivot swiftly when necessary.

9.Communication and Stakeholder Engagement:
1. Maintain transparent communication with employees, customers, suppliers, and other stakeholders.
2. Establish crisis communication protocols.
3. Address concerns promptly and proactively.

10.Learn from Past Disruptions:
1. Analyze previous disruptions and learn from them.
2. Identify areas for improvement and implement corrective actions.

11.Leadership Commitment:
1. Ensure that senior leadership actively supports and champions business resilience initiatives.
2. Allocate resources and budget for resilience planning and implementation.

Remember that business resilience is an ongoing process. Regularly assess, adapt, and refine your strategies to stay prepared for the unexpected[123]. 🌟

Getting started with facts and defined direction

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

Know your company:

1. Most Important Applications & Services (**Family Jewels**).
2. 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, and ITSM, ITOM.
4. Define Audit Universe implement legal & auditing functions.
5. Define Ideation, Brainstorming, Collaboration, to Concept cycle.
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 to the appropriate authorities (i.e., SEC Rule 2023-139)

Know your Environment:

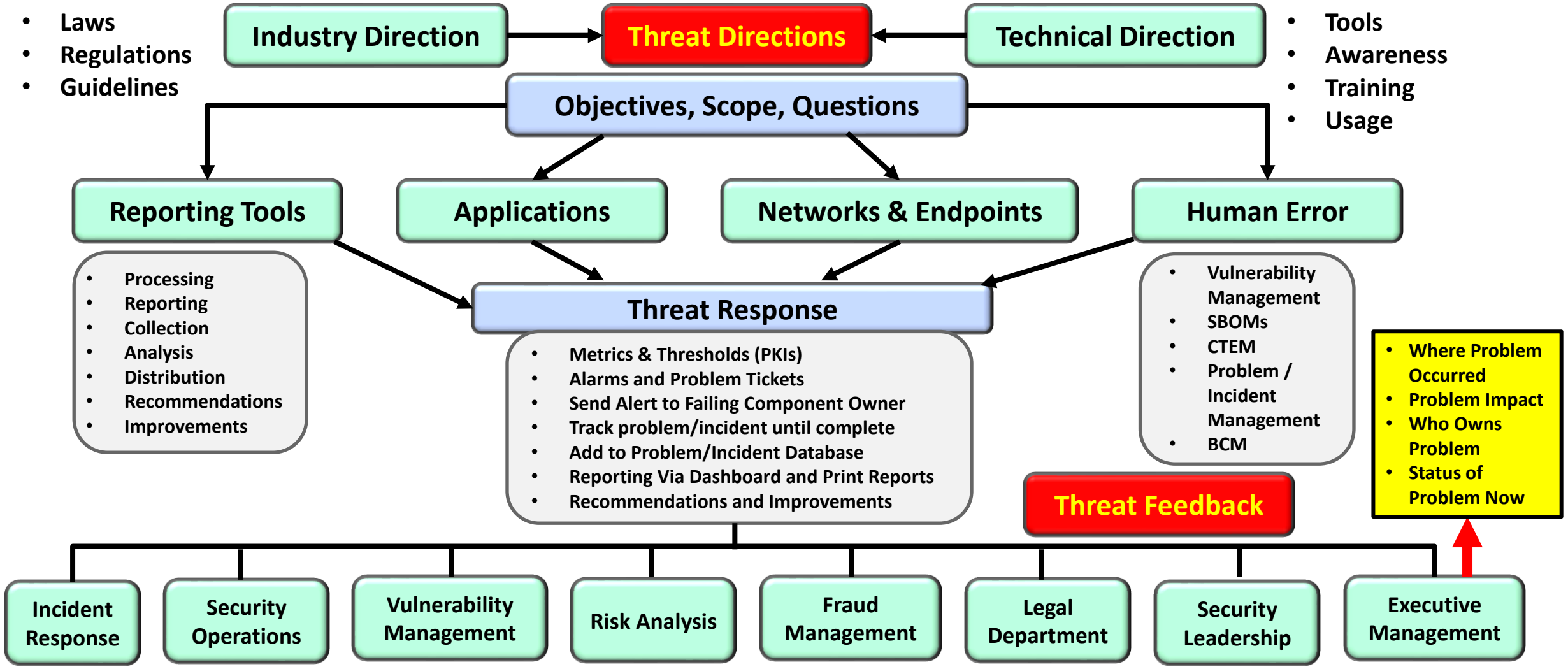
1. Physical and Data Security (Data Sensitivity & Data Flow).
2. Architecture and engineering process.
3. Asset Inventory and Configuration Management.
4. Identify and Access Management.
5. GRC based compliance and attestation, CIA based cybersecurity and elimination of viruses and malware.
6. Development 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.

Set you 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.

Addressing Threats

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



Know and Control your Environment

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

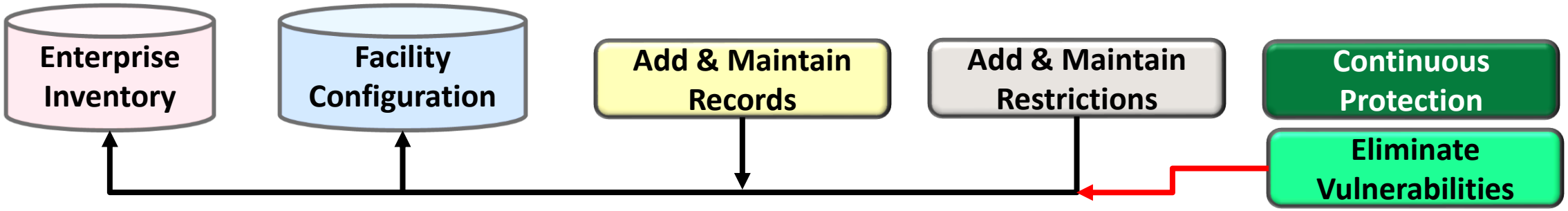
- **HW**AM
- **SW**AM
- **Tech**nology Management
- **Release** Management
- **Patch** Management
- **End-of-life**

- Facilities, or Locations
- Configuration of equipment
- Services and Applications
- COOP
- Location Recovery

- **Acquisition** - Order through Delivery
- **Install** and Test
- **Turnover** to User
- **Redeploy** as needed
- **Terminate** within laws and regulations

- **Components** via SBOM RBOM, or AIBOM
- **Identify Countries** parts origin
- Adhere to Laws and **country restrictions**
- Identify Vulnerabilities
- License Management

- **Identify** Vulnerabilities prior to production
- **Apply** Patches and Update Releases
- **Validate** mitigations
- **Vulnerability-free** production
- **CTEM** after Production



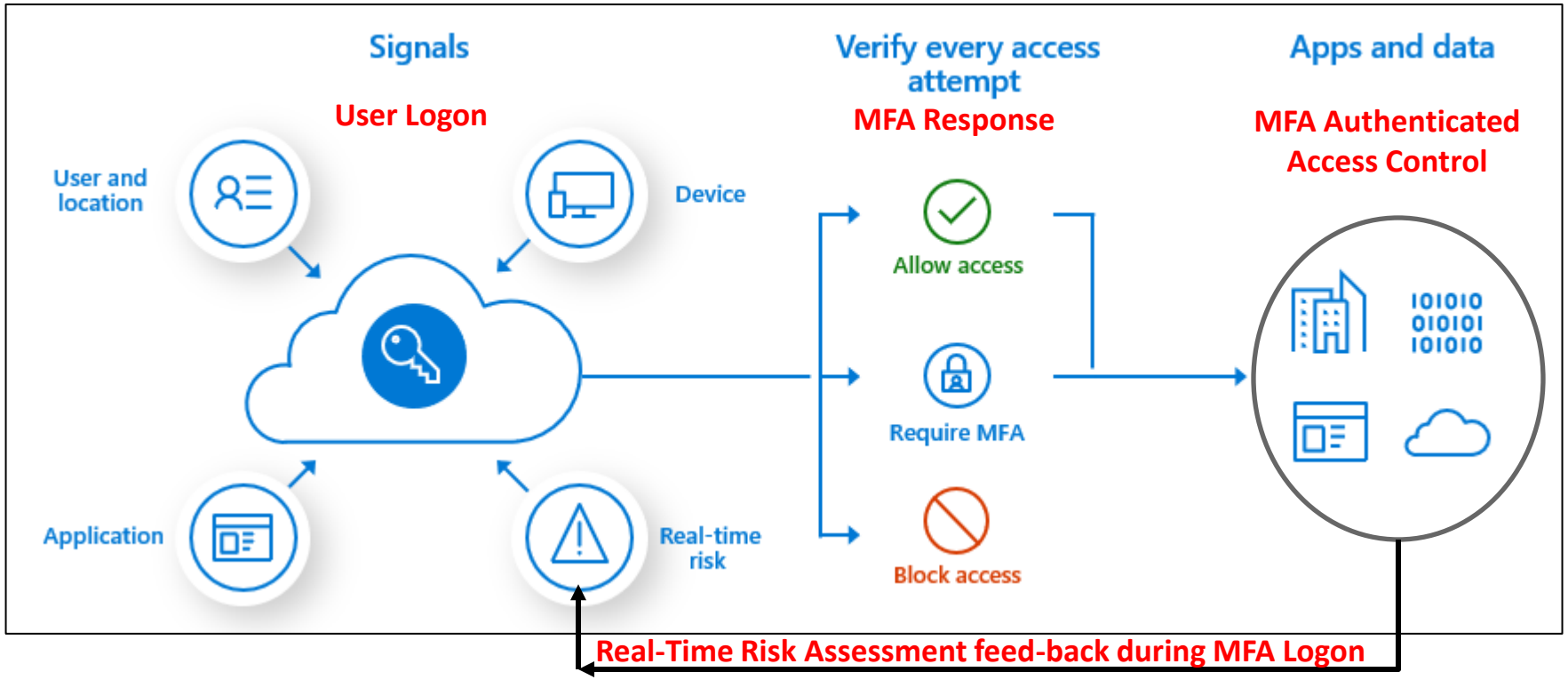
Requiring a Safer Login Process with MFA

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

MFA – Multi-Factor Authentication

MFA Process example:

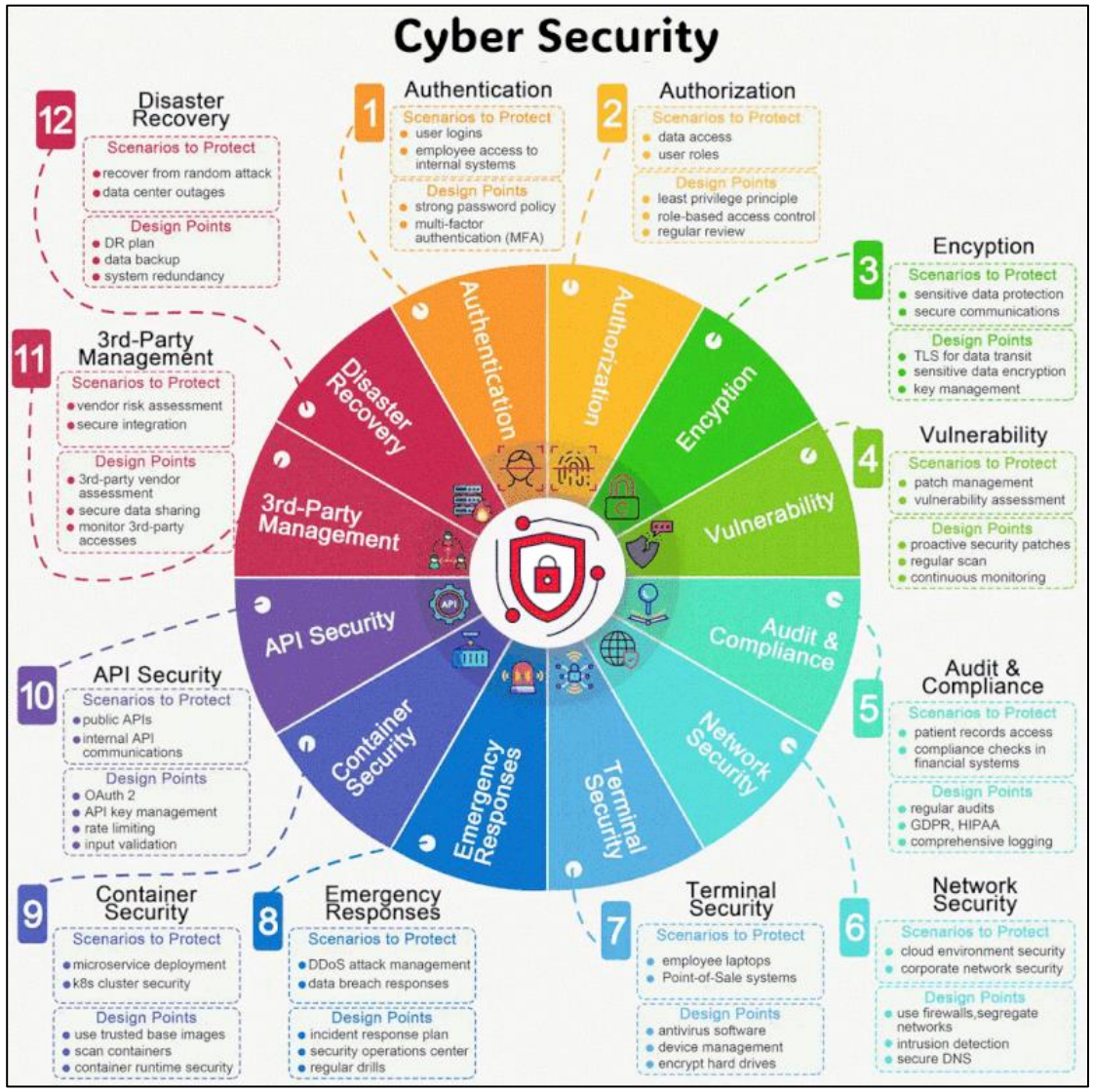
- User Logs On
- MFA requests Phone # verification
- MFA sends Code to Phone
- User enters code for verification
- MFA authorizes or rejects access based on matching code and component (i.e., phone, or IP address).



The recommended way to enable and use Microsoft Entra multifactor authentication is with Conditional Access policies. Conditional Access lets you create and define policies that react to sign-in events and that request additional actions before a user is granted access to an application or service.

Cyber Security and Continuity of Service

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



See Link for more detailed information.

Steps needed to protect enterprise and maintain business services:

1. **Authentication** - Identity Management,
2. **Authorization** – IAM, RBAC, ABAC, MFA, ZTA,
3. **Encryption** – Hashing, Key Management,
4. **Vulnerability** – CVE, CVSS, KVE, EPSS, SBOM, RBOM, AIBOM, Patches, New Release Management
5. **Audit & Compliance** - eliminate risk through controls
6. Network Security, Audit universe, Cross-Walks, Audit Scripts, Artefacts, Reports, Improved Controls,
7. **Terminal Security**, IP Addresses, VPN
8. **Emergency Response**, COOP,
9. **Container Security** – Kubernetes, Dockers, etc.
10. **API Security** – and Open-Source Modules
11. **3rd-Party Security**, Supply Chain Management
12. **Disaster Recovery**, Business Continuity, Personnel Safety and Violence Prevention.

Vulnerability Management definition and process

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

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:

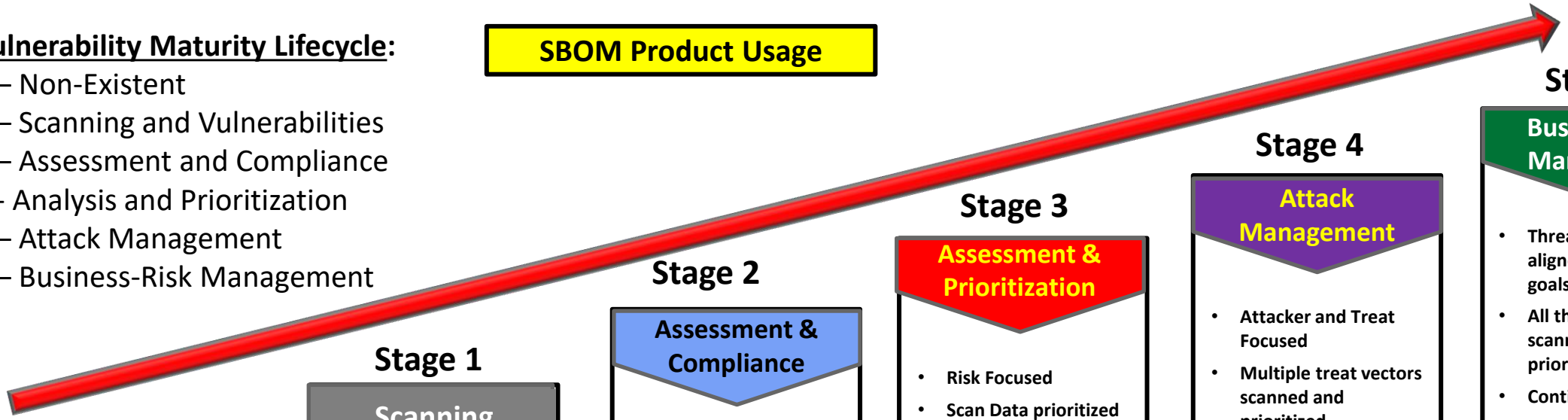
- **Plan** how to use Vulnerability Management
- **Discover** where your vulnerabilities exist
  - Vulnerability-Free Production Applications
  - Continuous Scanning for new Vulnerabilities impacting production applications via Continuous Threat Exploitation Management (CTEM)
- **Scan** applications with SBOMs (Software Bill of Materials)
- **Report** vulnerabilities, their symptoms, and mitigations via patches and new releases
- **Deploy** patches and new releases to mitigate vulnerabilities

Vulnerability Management Maturity Lifecycle

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

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

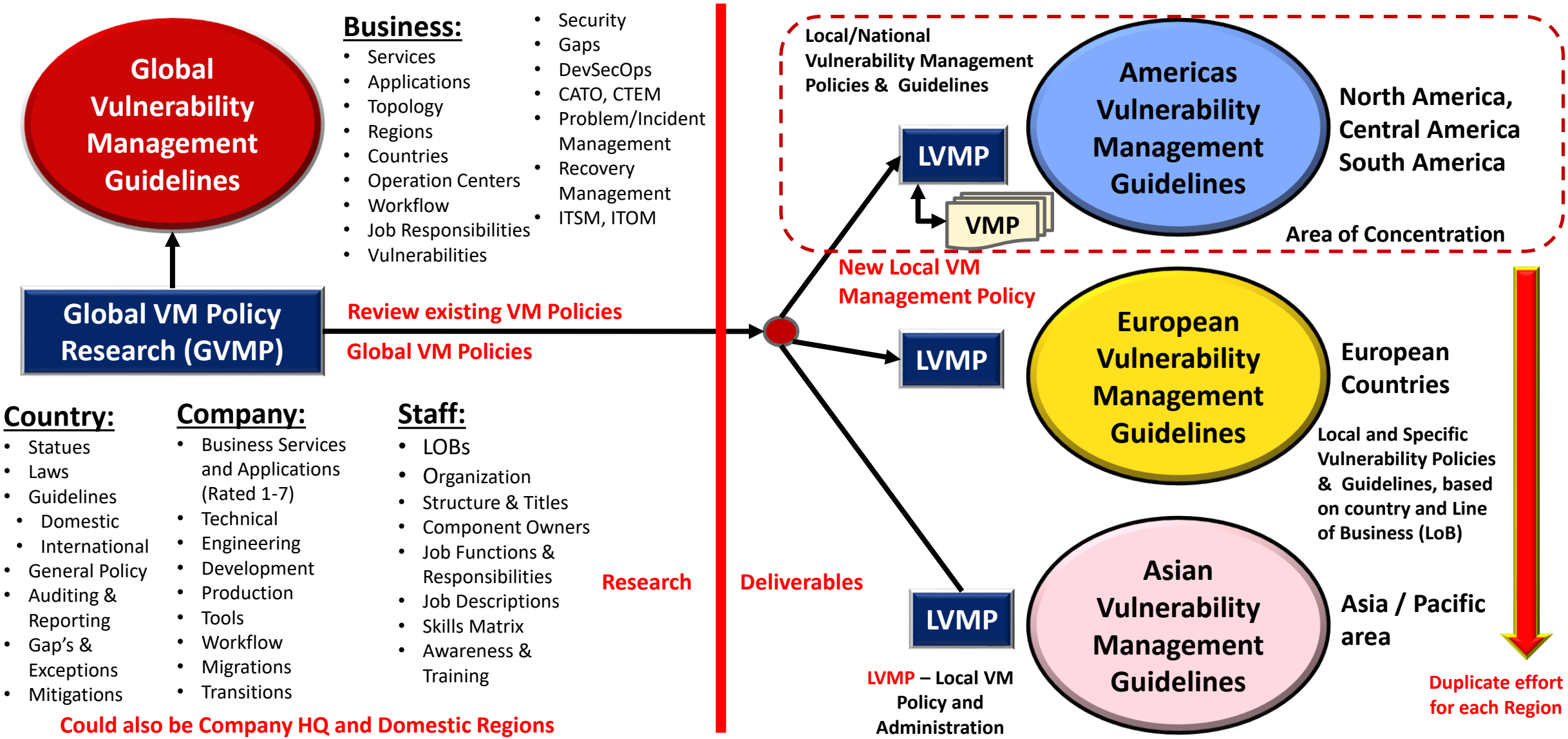
Integration

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

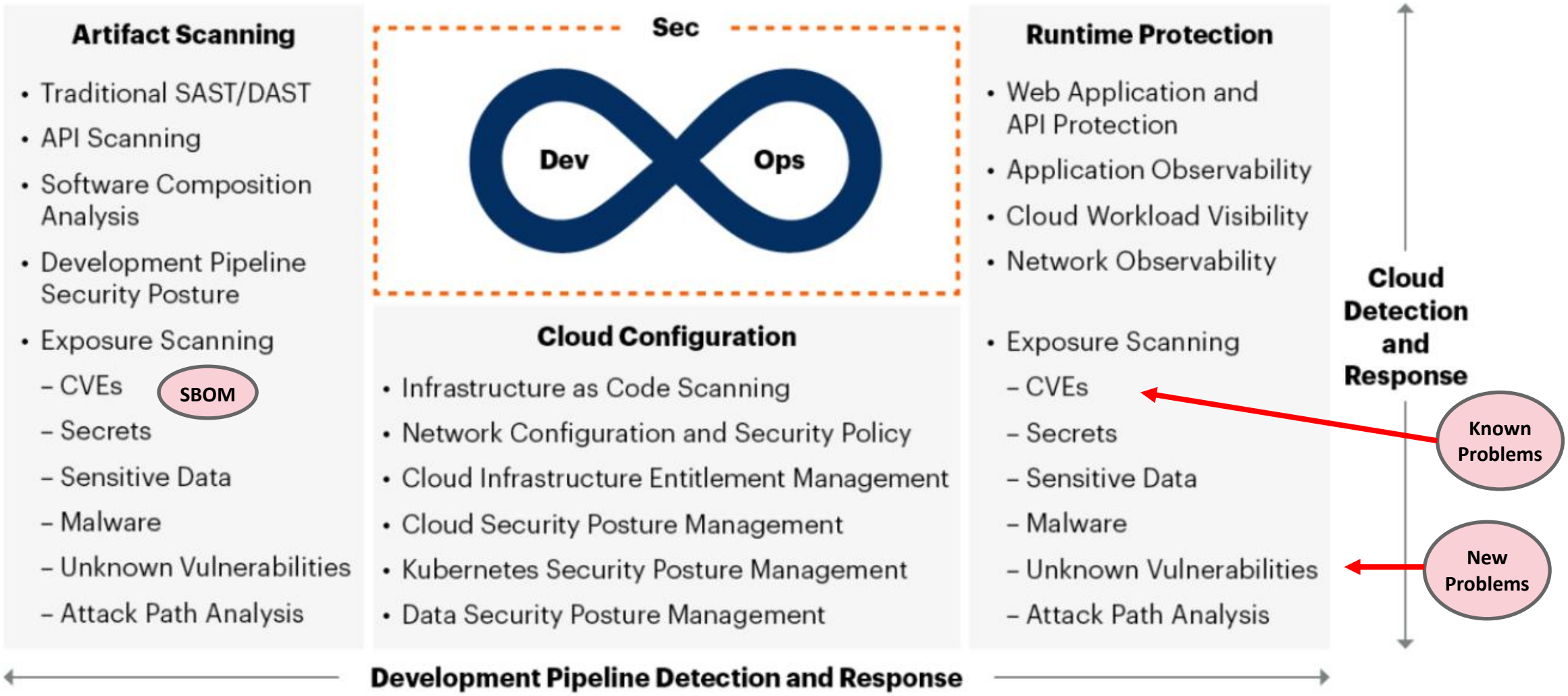
Global Vulnerability Management Policy generation

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



Cloud Native Application Protection Platform (CNAPP)

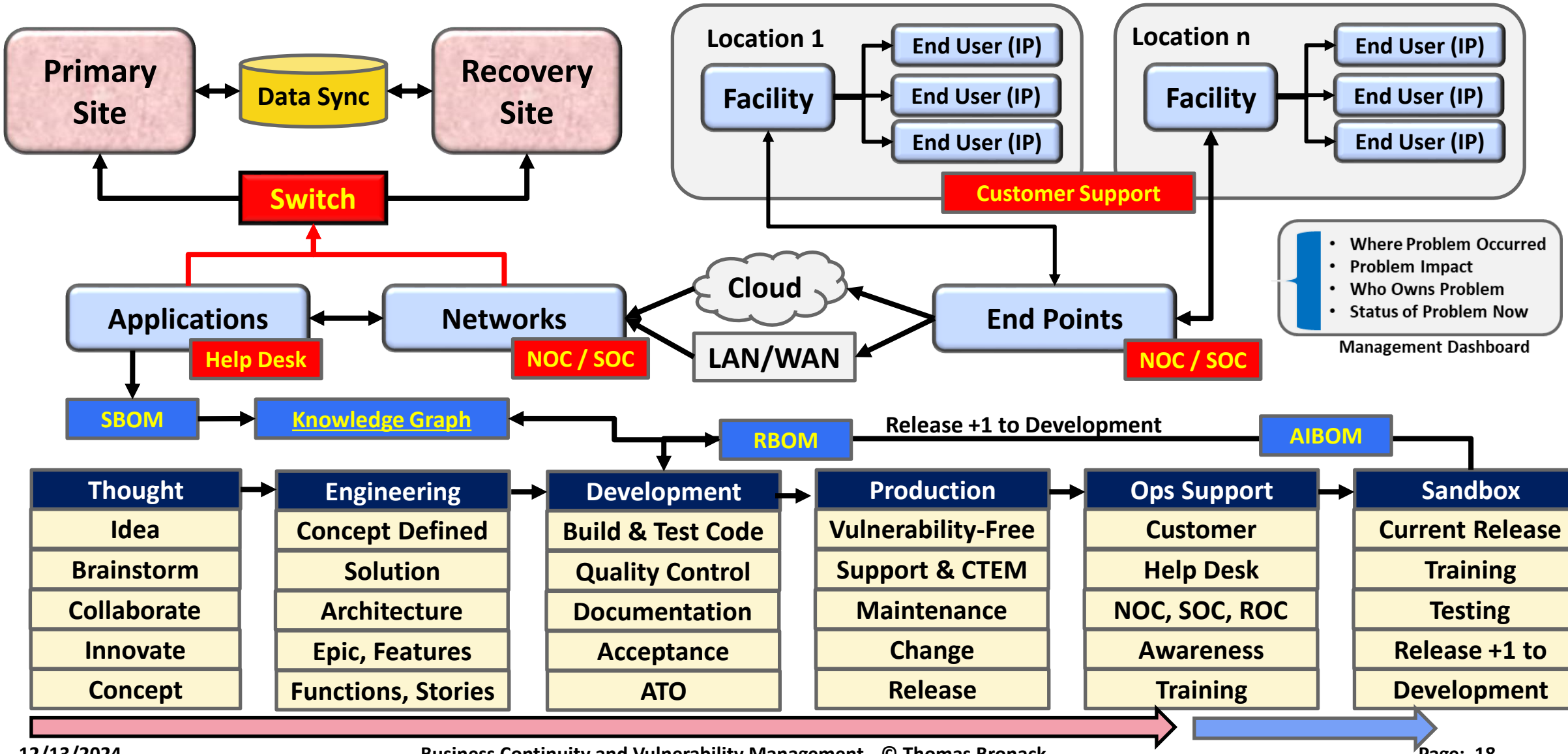
Thomas Bronack
Email: bronackt@dcag.com
Phone: (917) 673-6992



CVEs = common vulnerabilities and exposures

From Idea to Product, with Support and Recovery

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



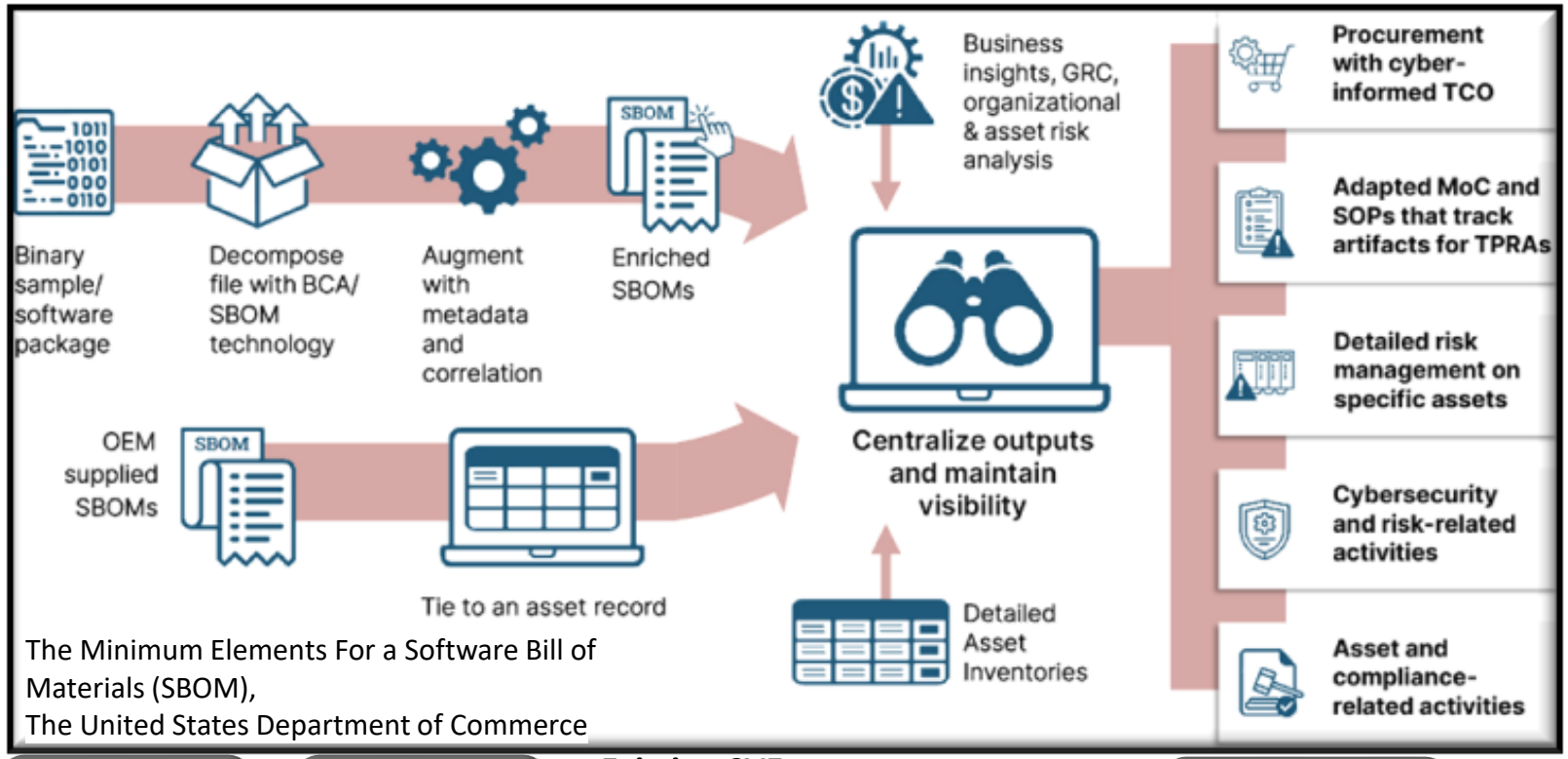
What is an SBOM and how does it work

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

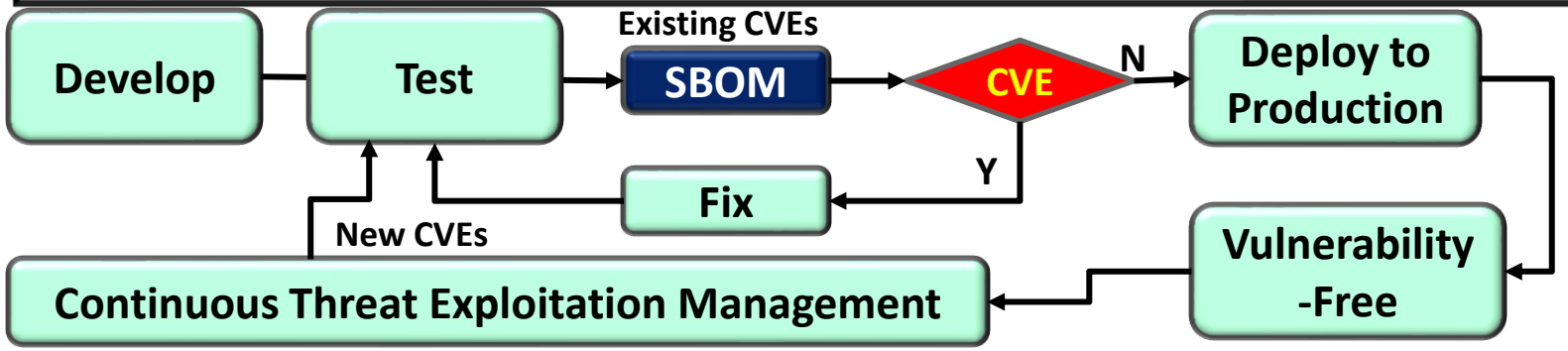
Software Bill of Materials (SBOMs) are used to validate program components used to create applications by scanning the application code and identifying program components (Open-Source Code, Vendor Code, and other Binary software products).

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.).

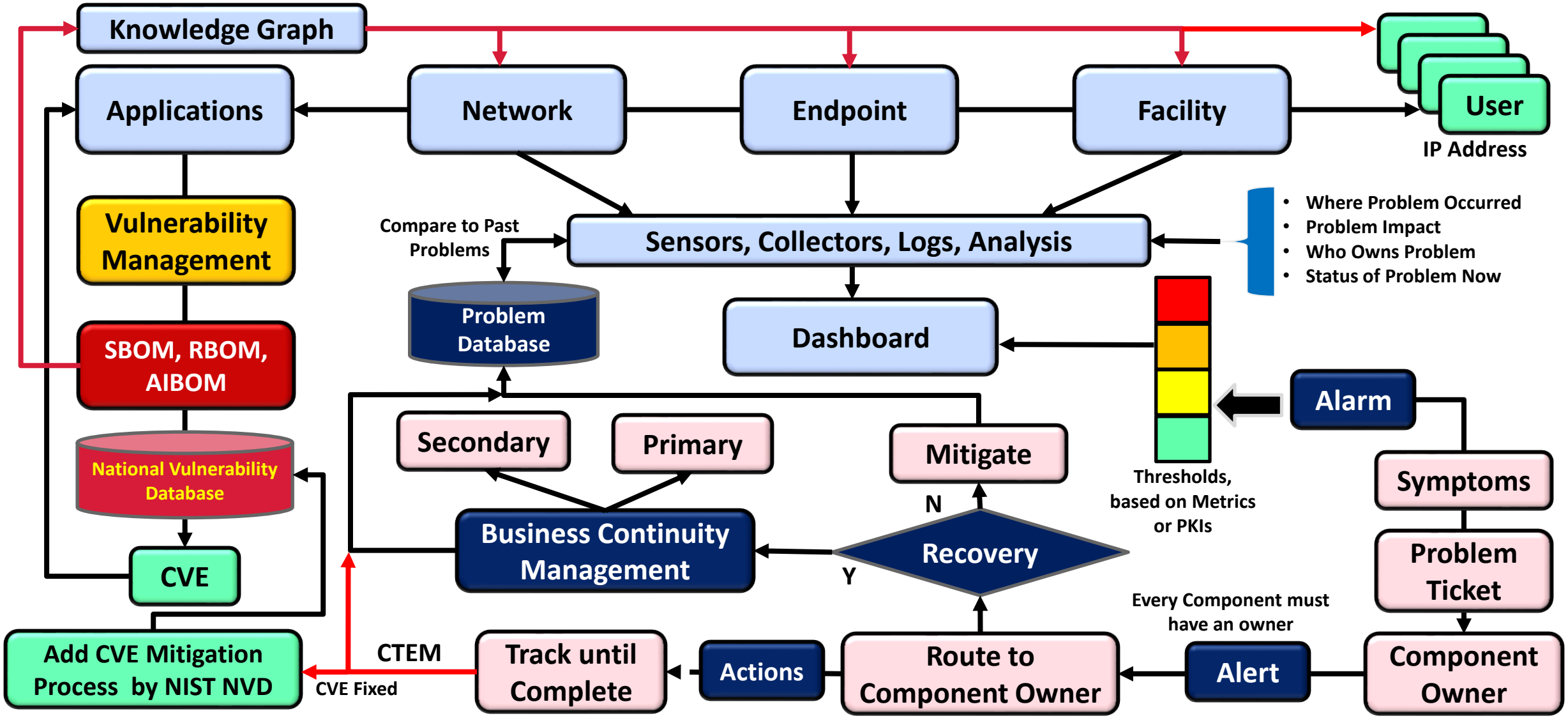


The Minimum Elements For a Software Bill of Materials (SBOM),
The United States Department of Commerce



Tracking Problems through a Dashboard

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

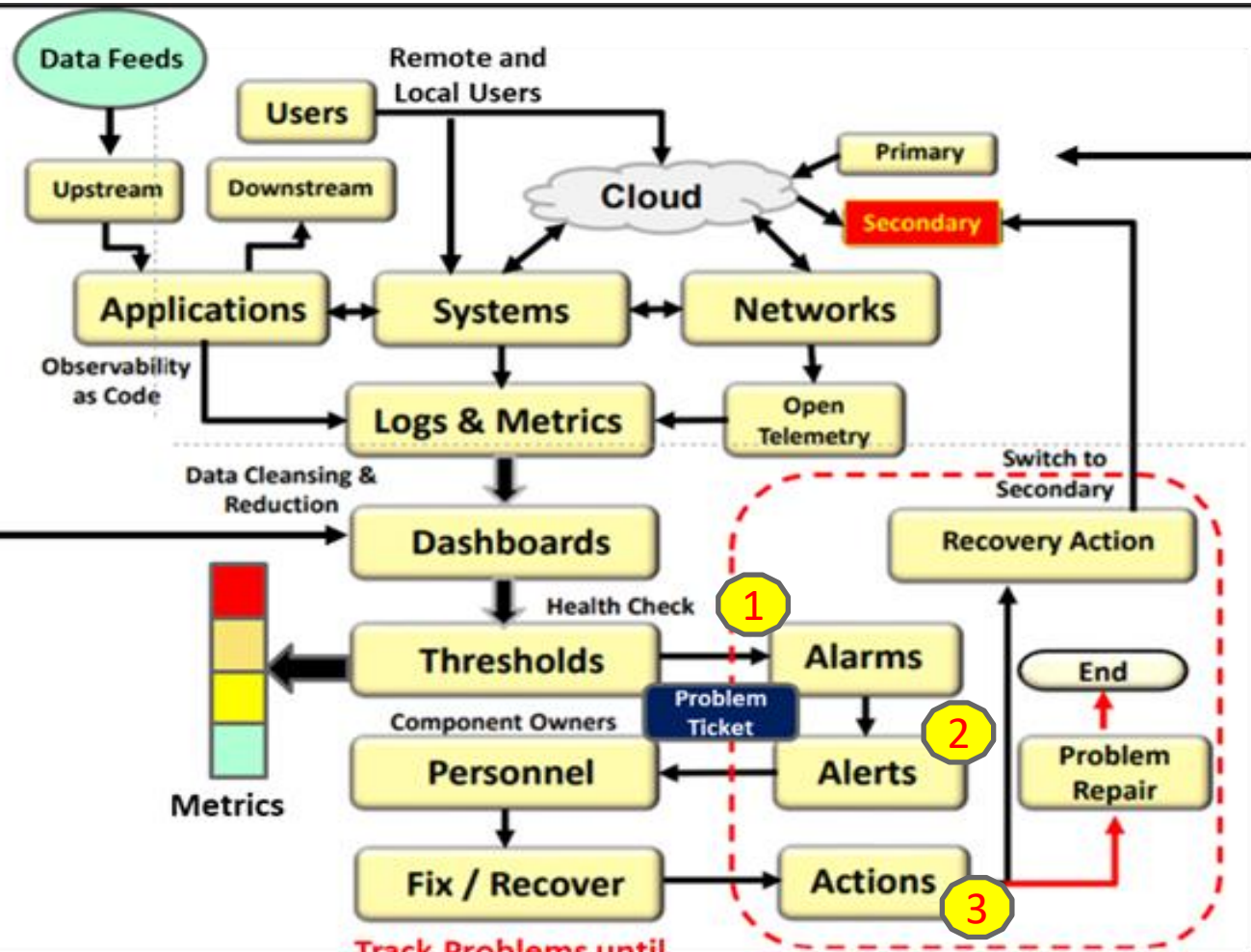


Problem / Incident recognition, reporting, and resolving

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

"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.

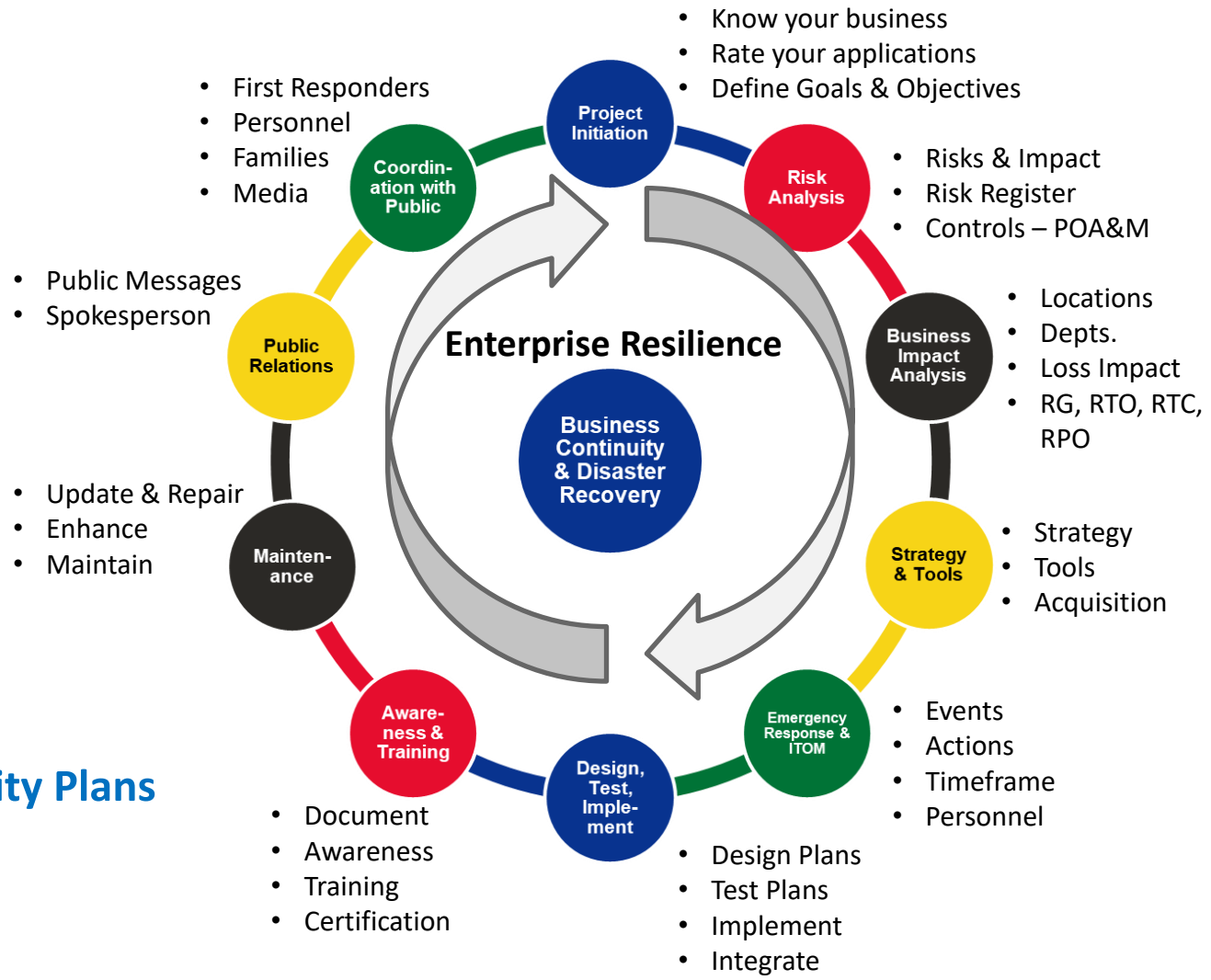
2. The Alarm and problem ticket are delivered to the component owner as an Alert (SMS text message, or email)

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

Ten Step Process to establish BCM/DR Practice

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

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

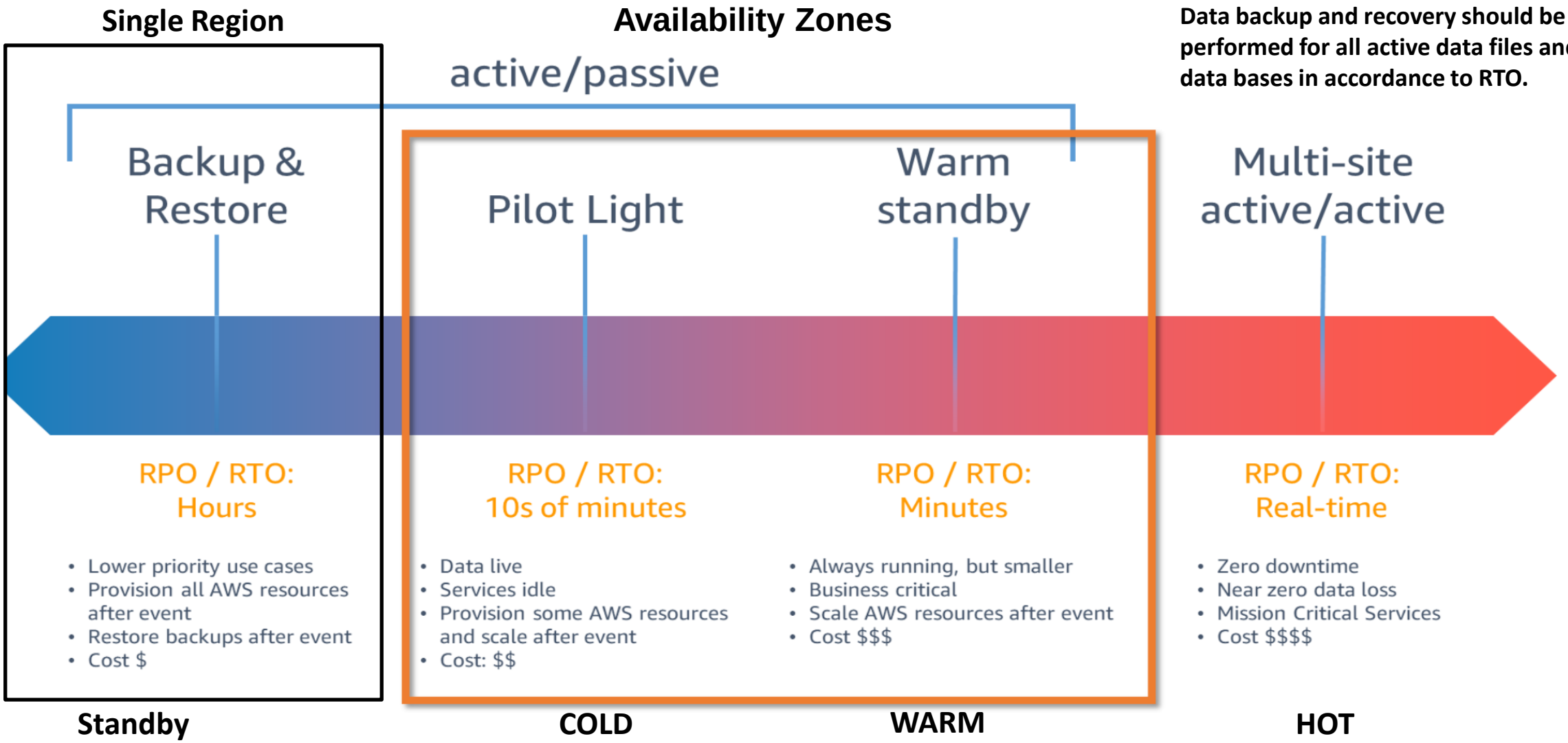


AWS DR Strategies

Link to AWS Disaster Recovery Strategies

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

Data backup and recovery should be performed for all active data files and data bases in accordance to RTO.



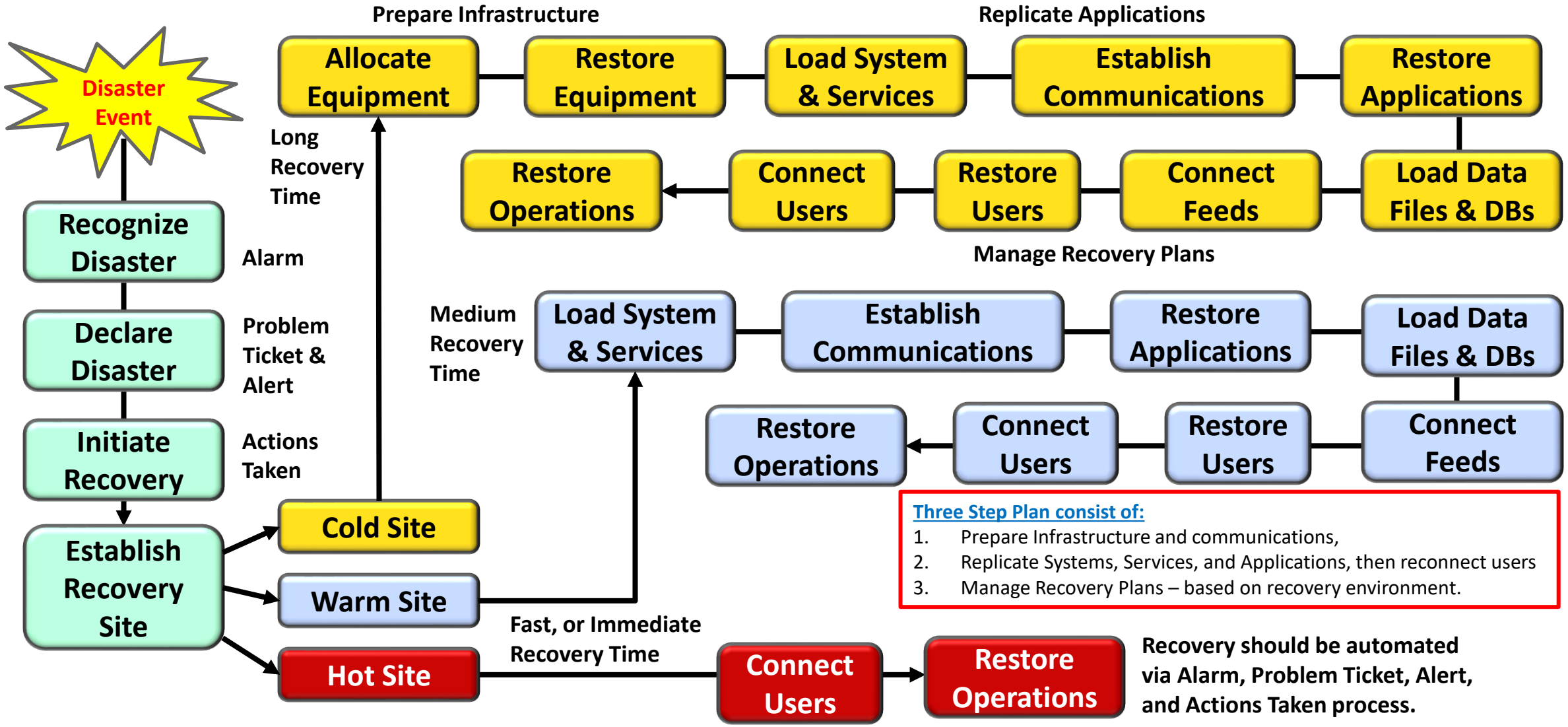
Resilience Patterns and Recovery Groups

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

Resiliency Patterns	Single Region	Multiple Regions		
	In-Region	Active Standby (Pilot 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**		

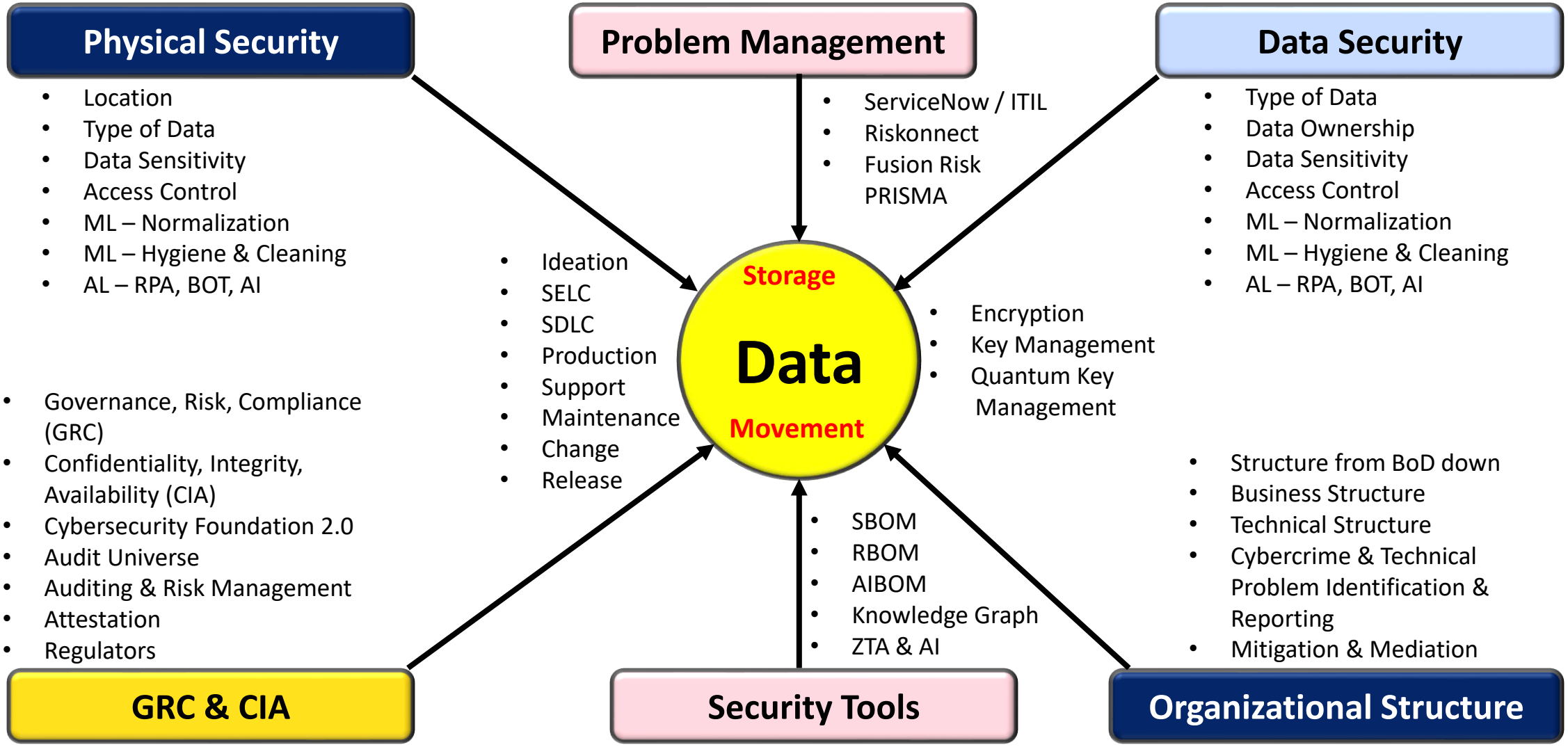
Sequence of Events to enact a Recovery Operation

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



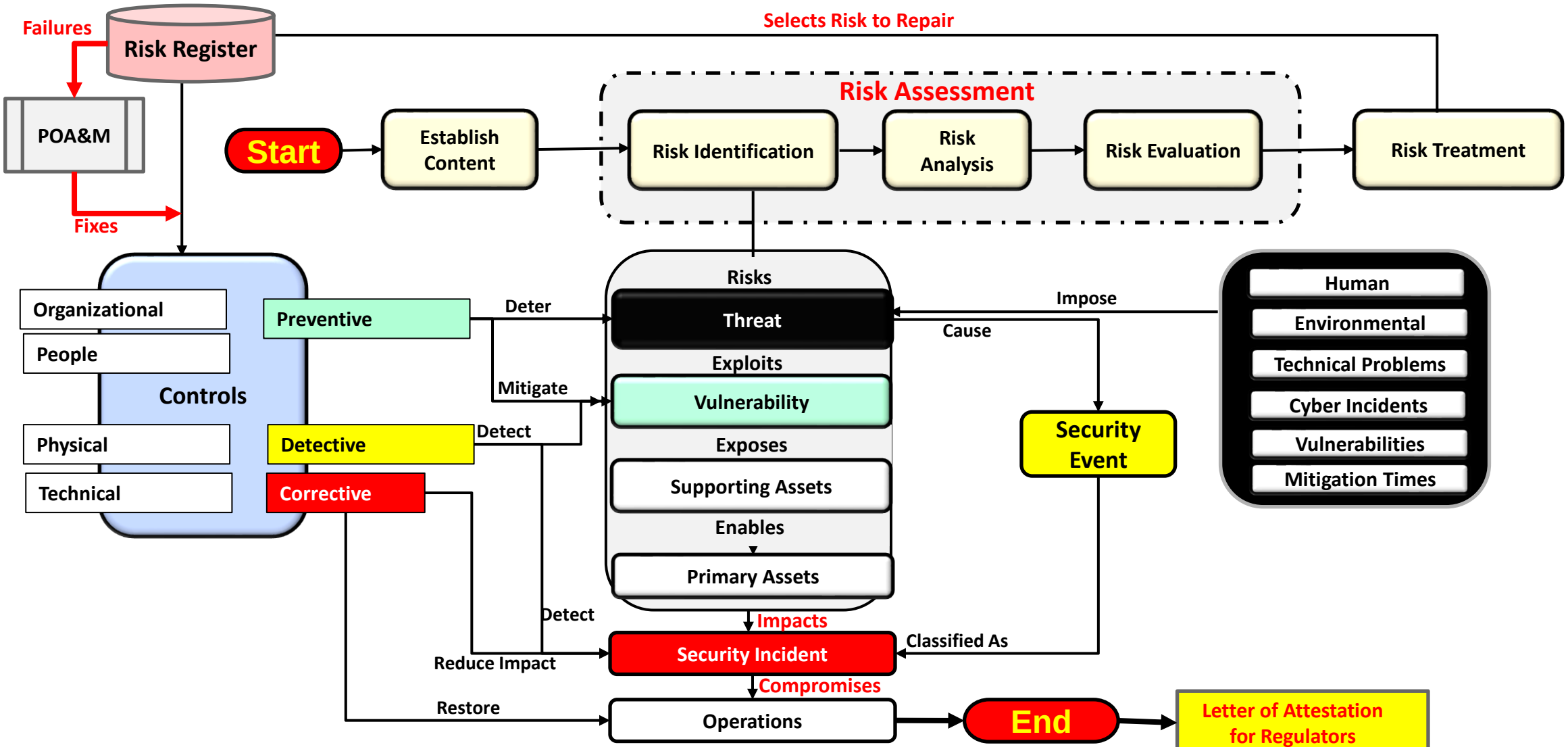
IT Security – Physical & Data

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



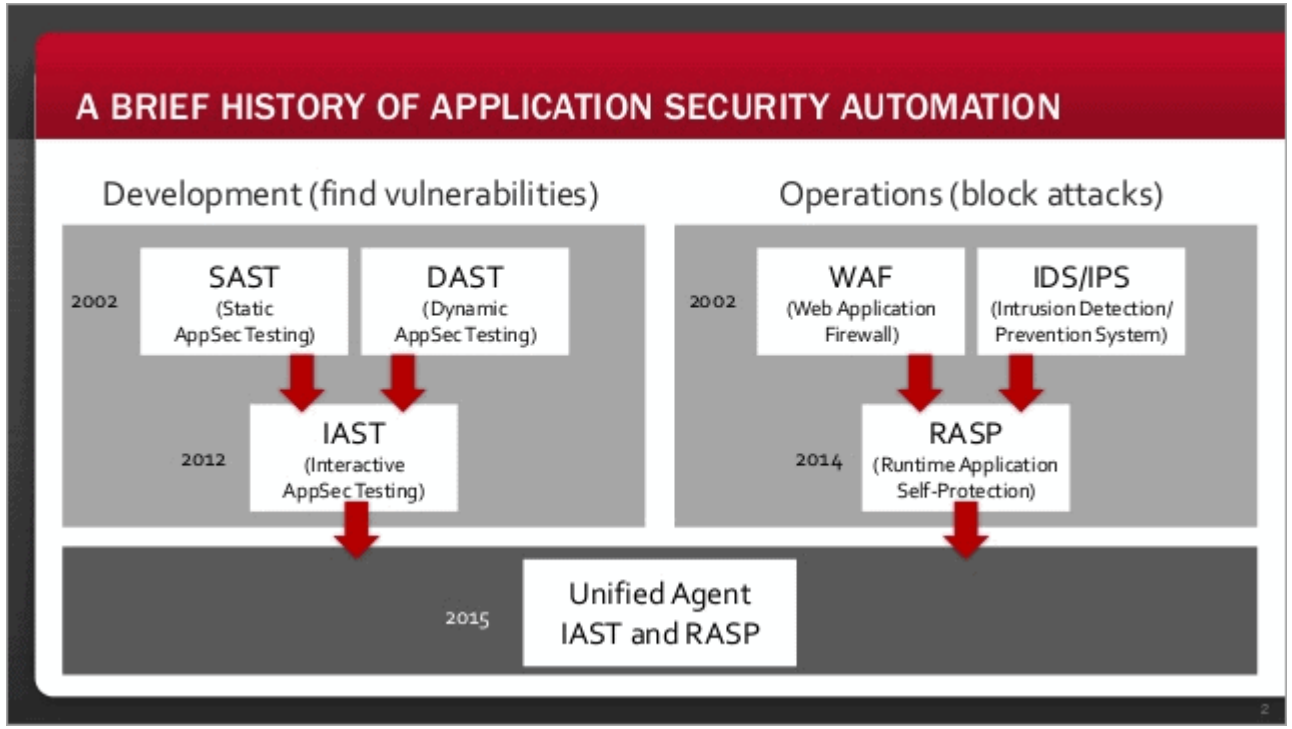
Risk Management with ISO 27000: 2022

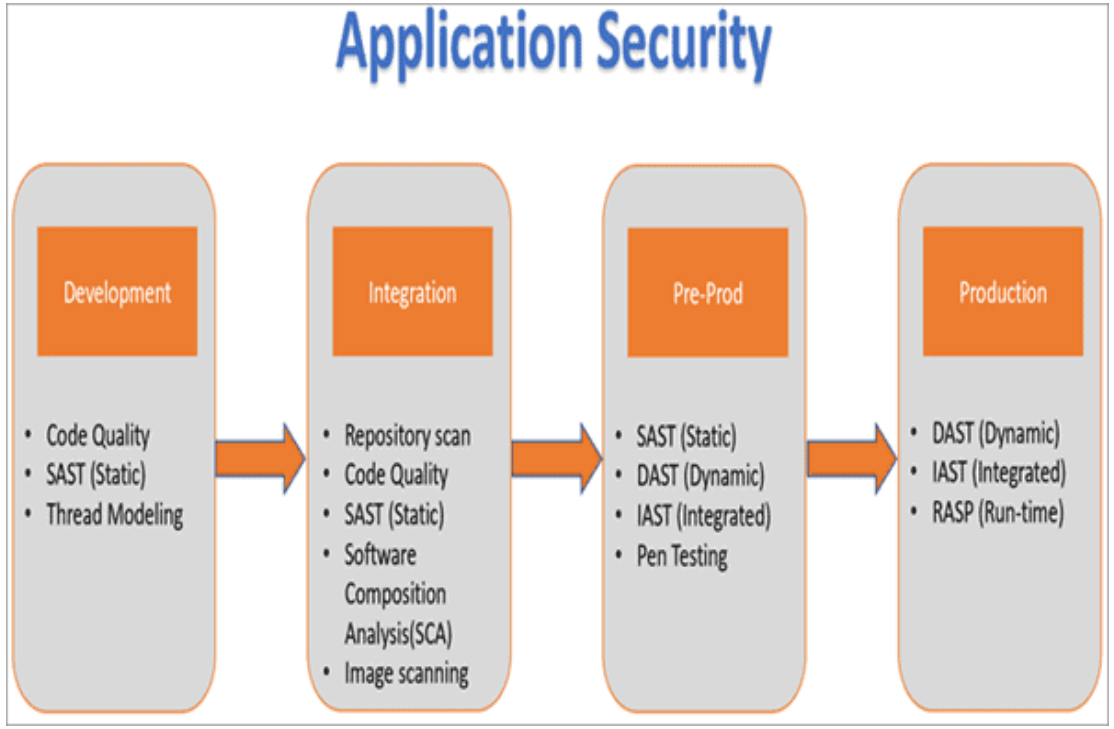
Thomas Bronack
Email: bronackt@dcag.com
Phone: (917) 673-6992



Application Security Testing – Dev/Sec/Ops

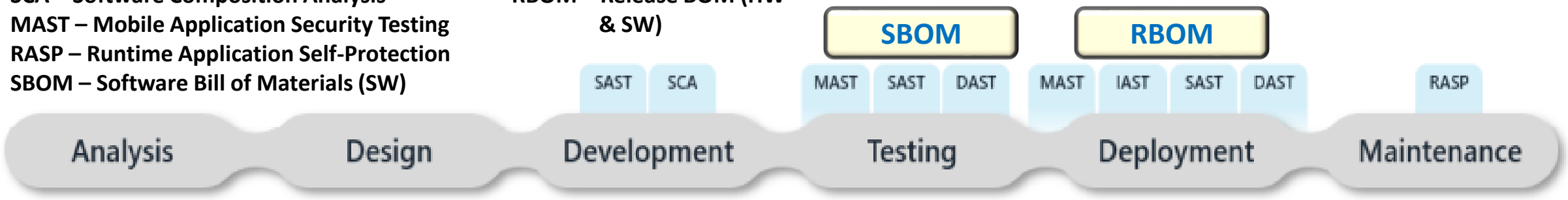
Thomas Bronack
bronackt@gmail.com
(917) 673-6992





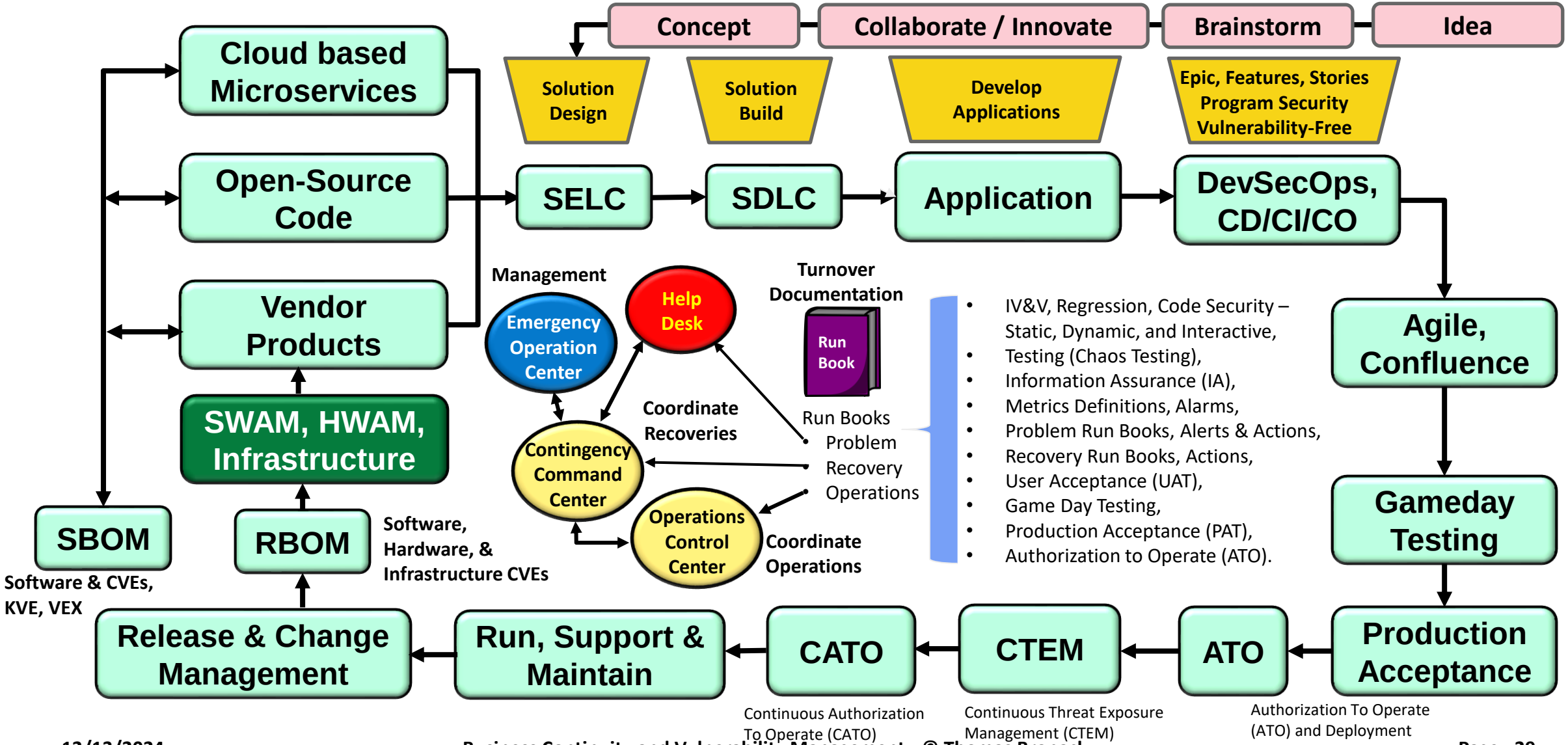
SCA – Software Composition Analysis
MAST – Mobile Application Security Testing
RASP – Runtime Application Self-Protection
SBOM – Software Bill of Materials (SW)

RBOM – Release BOM (HW & SW)



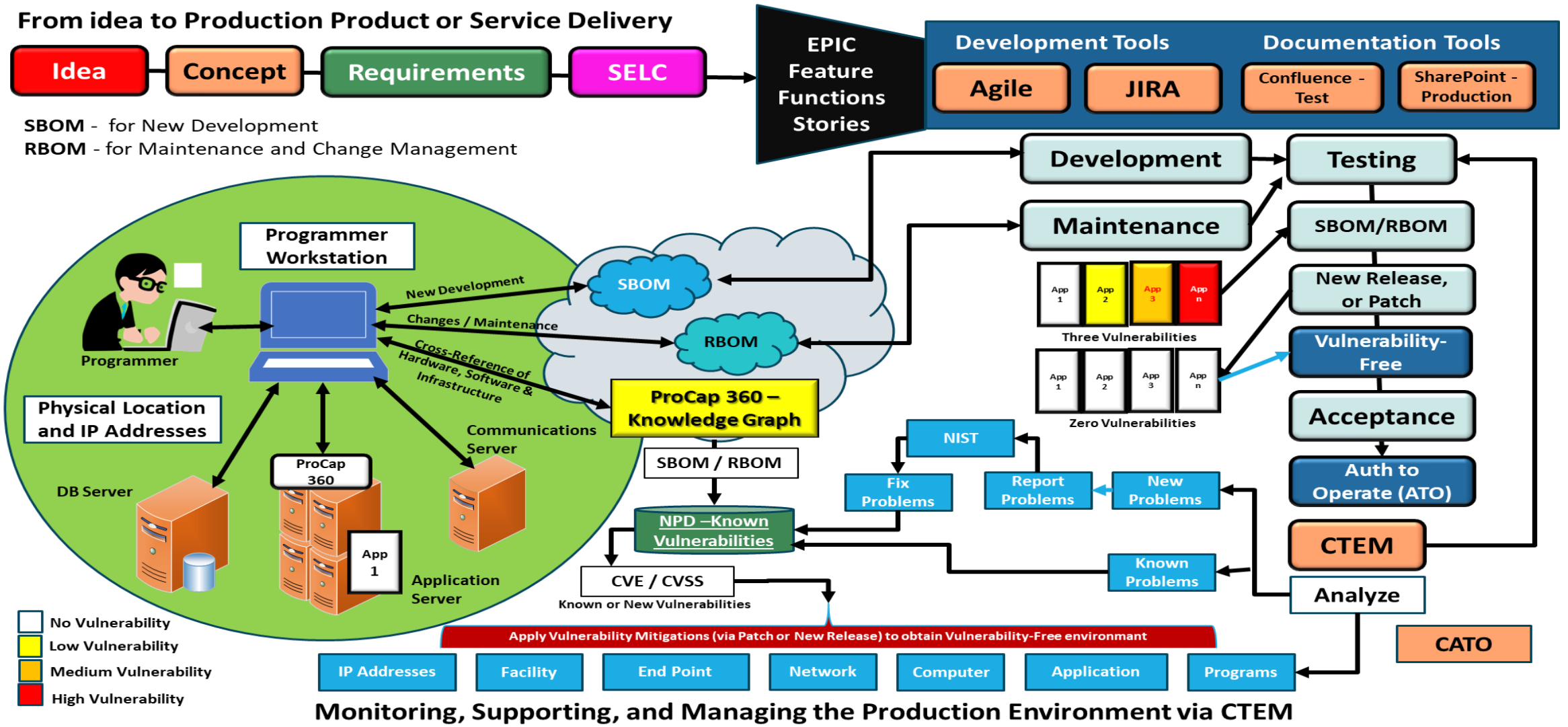
Application Construction and entry to Production

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



Providing an enhanced Customer Experience (CX)

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

The Customer Experience Pyramid is an empirical research based framework, which is quite useful in directing the organizations through their CX Transformation journey.

The CX Pyramid entails 2 core dimensions:

1. **Focus Areas** – the organizational spheres that must change to enable provision of amazing digital Customer Experiences.
2. **Strategic Building Blocks** – the strategies that define how this change can take place to deliver exceptional Customer Experiences.

Let's discuss the Focus Areas of the CX Pyramid first. The 4 Focus Areas crucial in a business to change in order to deliver top-quality digital Customer Experiences at scale are:

- A Technical Infrastructure to encourage cross-departmental operations and journey-focused Customer Experience Management.
- Leadership committed to a Customer-centric Strategy.
- A structure characterized by established networks for collaboration across teams, units, and silos.
- Establishing processes to nurture collaboration across functional groups to institute Customer-centered Design.

The CX Pyramid is instrumental in designing and delivering delightful Customer Experiences.

Project Overview

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

Introduce Concept:

- Needs Analysis
- Vulnerability Assessment
- Tools Review
- Metrics Defined
- Provide SOW Recommendation to Management
- Gain Management Approval
- Schedule Start and End Dates
- Contracts and Payment Schedule

Define Project and Scope:

- Risk Analysis
- Tools Review
- Tool Testing
- Vulnerability Management
- SBOM Usage
- RBOM Usage
- AIBOM Usage
- Business Continuity Management
- Verify Results
- Awareness and Training
- Continuous Threat Exploitation Management (CTEM)

Conduct Needs and Risk Analysis

- Define Weaknesses, Exceptions and Gaps
- Recommend Controls
- Recommend Improvements
- Define Benefits
- Develop Report and Presentation

Provide Report and Presentation

- Review Findings
- Projected Weaknesses
- Benefits to be obtained
- Enhanced security
- Savings
- Provide Plan of Action & Milestones (POA&M)
- Gain Management Approval

Conduct Project Activities:

- Initiate Project
- Assemble Team
- Prepare Team
- Assign Tasks
- Commence Work
- Provide Status
- Resolve Issues
- Complete Project
- Metrics Improved
- Costs vs Benefits
- Projected ROI
- Toil Reduction
- Financial Savings

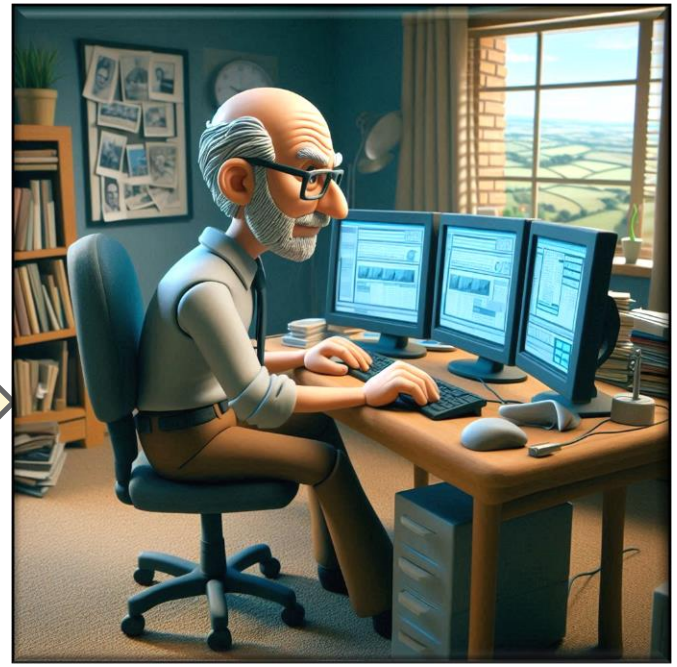
Reaching out to assist our clients

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

- Discuss
- Define
- Propose
- Achieve

Quality Service at a Reasonable Price

Helping Clients to achieve success



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