



Thomas Bronack, CBCP

### Presentation Topics

- Why Enterprise Resilience
- Knowing your Company and Compliance to Service Level Agreements
- Identifying and Controlling Risks
- Recovery Management
- Protecting the Company
- Reducing Problems and Costs
- Staff Awareness and Training

### Tom Specializes in:

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

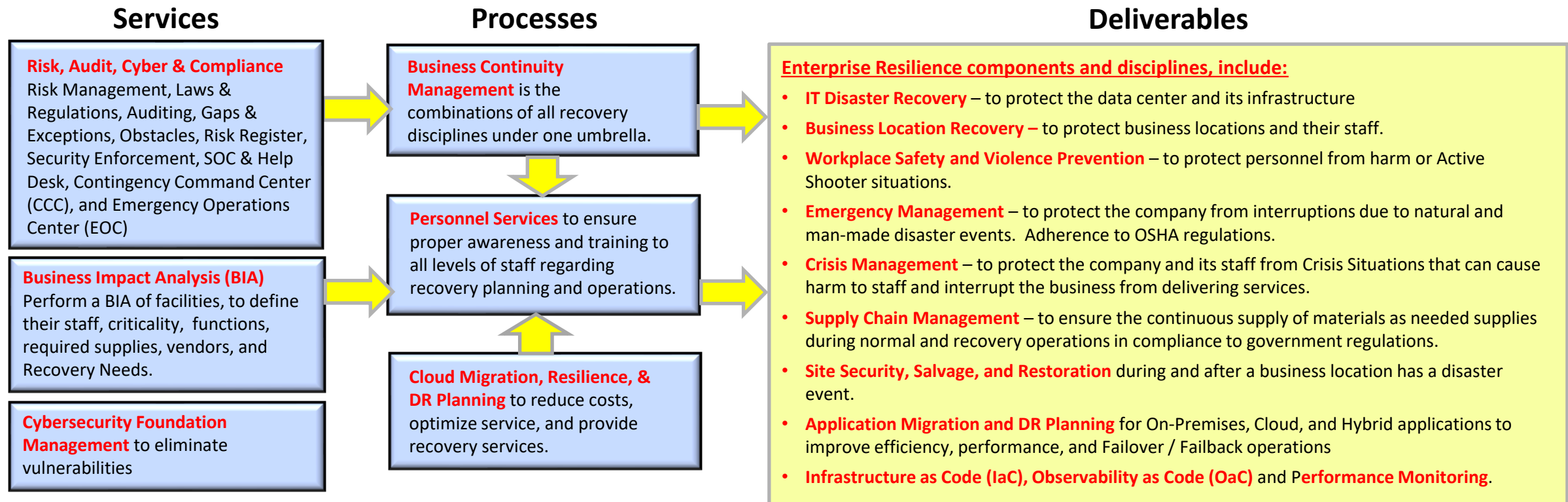
# Enterprise Resilience, Vulnerability Management, Corporate Certification and Recovery Management

### Contact Information:

- [bronackt@gmail.com](mailto:bronackt@gmail.com)
- [bronackt@dcag.com](mailto:bronackt@dcag.com)
- (917) 673-6992

# Overview of Process and Results

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



- Know the Mission, Organization, Functional Responsibilities, and Risk Appetite, Management and Controls.
- Define Threat Exploitations, Costs, and Methods to reduce vulnerabilities, technical threats and cybercrimes.
- Analyze environment, tools, personnel awareness and training, and methods for improving performance.
- Provide deliverables listed by coordinating program management to achieve goals and train staff.

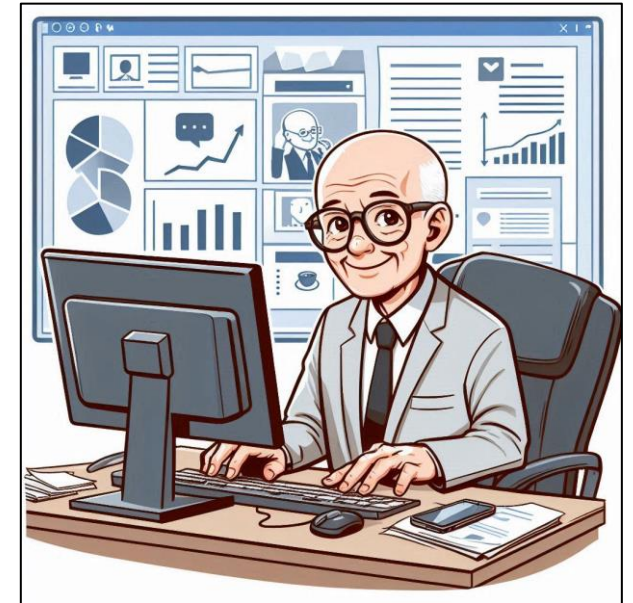
# A word from Thomas Bronack

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

I am a mid to 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, 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.

I provide analysis, evaluation, literature and presentation materials and seek consulting work or a permanent job. I develop and test recovery plans while training teams on strategic and tactical skills to help companies achieve an efficient, compliant, and vulnerability-free environment.

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](mailto:bronackt@dcag.com)  
(917) 673-6992

# What is Enterprise Resilience comprised of?

- Enterprise Resilience requires a Company Culture and Awareness
- Site Reliability Engineering (SRE)
- Metrics, Monitoring & Reporting
- Support & Improvement
- Automation



## Enterprise Resilience consists of:

- Enterprise Products & Services (**Company Jewels**),
- Critical Economic Services, Financial Health, and Visibility,
- Brand and Company Reputation,
- Legal, Audits, & Compliance (Audit Universe)
- Risk Management Foundation (RMF) & Business Impact Analysis (BIA),
- Recovery Groups, RTO, RPO, RTC, Certifications
- Business Continuity / Continuity of Operations/ Disaster Recovery, Emergency Management
- Crisis Management & Communications
- Critical Environments (Domain Management),
- Information Security (CSF),
- Human Resource Management (Personnel Safety & Violence Prevention – Active Shooter),
- Production Operations and Support (ITOM, ITSM),
- Incident & Problem Response,
- Organizational Behavior,
- Supply Chain Resilience,
- Migrating to the Cloud and hybrid Environments,
- Center of Excellence (COE) implementation.

# Business Continuity Management components

- **Preserve** the company Brand and Reputation, while protecting personnel.
- **Plan** for natural and man-made disaster events to reduce / eliminate outages.
- **Identify** and eliminate Risks and Business Flow Impacts to the company, its people, and resources.
- **Eliminate** Single-Point-Of-Failure.
- **Adhere** to regulatory and business requirements.
- **Ensure** continuity of business under catastrophic conditions – problems, incidents, and disaster events
- **Agree on** Recover Strategy and Select Tools
- **Integrate** production, testing, validation and continuous Improvement



**Include Emergency Management, Site Protection, Salvage, and Restoration for business locations**

# Process followed in performing Enterprise Resilience

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

## 1. Rating your company's sensitive applications

- a. **Revenue Generators** – Protecting Revenue Stream and Profits
- b. **Client Facing** (Dashboards, Websites, application extensions, etc.) – protecting Reputation & Brand
- c. **Supporting** company operations
- d. **Recovery** Time Objective ((RTO), Recovery Point Objective (RTO), Recovery Time Capability (RTC), and Recovery Group (service continuity, time to recover, time sensitive applications and services)

## 2. Locate weaknesses to be overcome

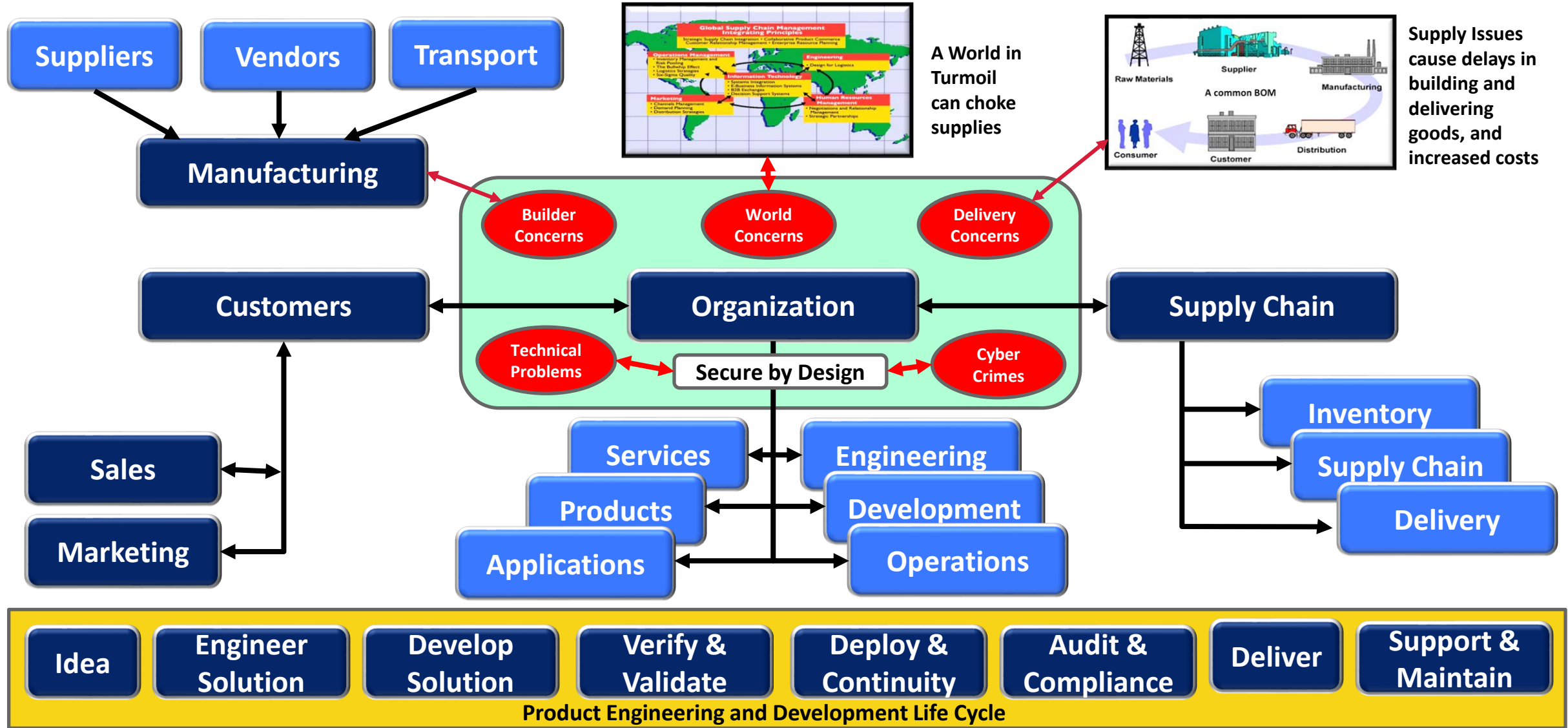
- a. **Analyze** exposures and how you can best protect the business going forward (Risk Assessment, BIA, Security (Physical / Data / CSF / CIA), Compliance (Laws, Regulations, Attestation, Auditing), Development (Systems Engineering Life Cycle – SELC), Operations (Systems Development Life Cycle – SDLC), Dev/Sec/Ops – Agile, Jira, Confluence, SharePoint), IT Operations (ServiceNow, ITIL), Standards & Procedures, Documentation, Awareness, Training, Career Pathing, Identity Management (IM, IAM, CIAM, RBAC, ABAC, MFA, ZTA).
- b. **Identify Gaps**, Exceptions, Obstacles and either Mitigate, or Mediate same. Implement required Controls over identified Risks(Place Risks in Risk Register and develop a POA&M to correct Risk)

## 3. Optimize Development, Test, Production, and Change Management Environments

- a. **Optimize auditing and** providing a Letter of Attestation to Regulators.
- b. **Ensure security** is optimized and in place with awareness and staff training provided as required.
- c. **Utilize Chaos Testing** to develop responses to encountered problems, prior to production acceptance. Ensure problem Runbooks are produced, and that problems triggers and recovery triggers are exercised correctly.
- d. **Implement** optimized Application Program Monitoring and Environment Observability System.
- e. **Monitor metrics** (PKIs, SLAs) to identify problems via thresholds that generate Alarms, Alerts, and Actions to be Taken.

# Protecting Organization is more difficult than ever

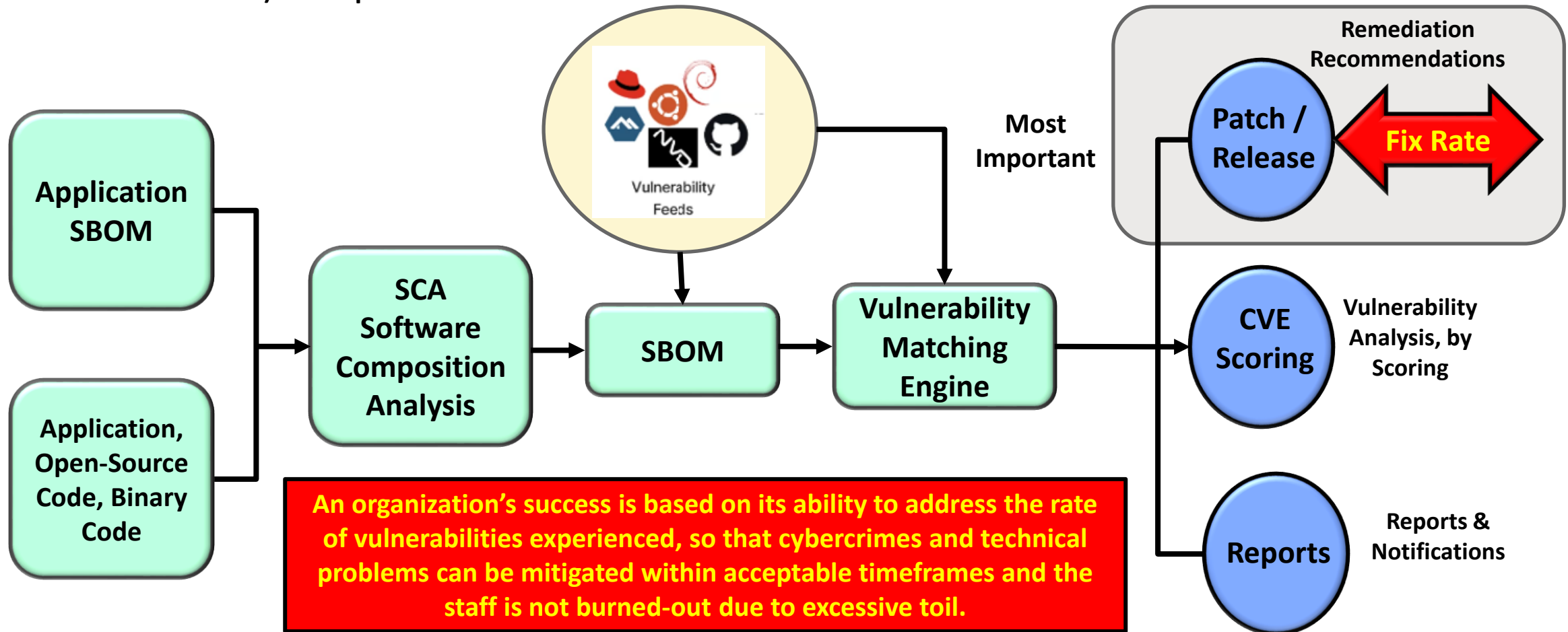
Thomas Bronack  
 Email: [bronackt@dcag.com](mailto:bronackt@dcag.com)  
 Phone: (917) 673-6992



# Identifying and Reporting Vulnerabilities

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

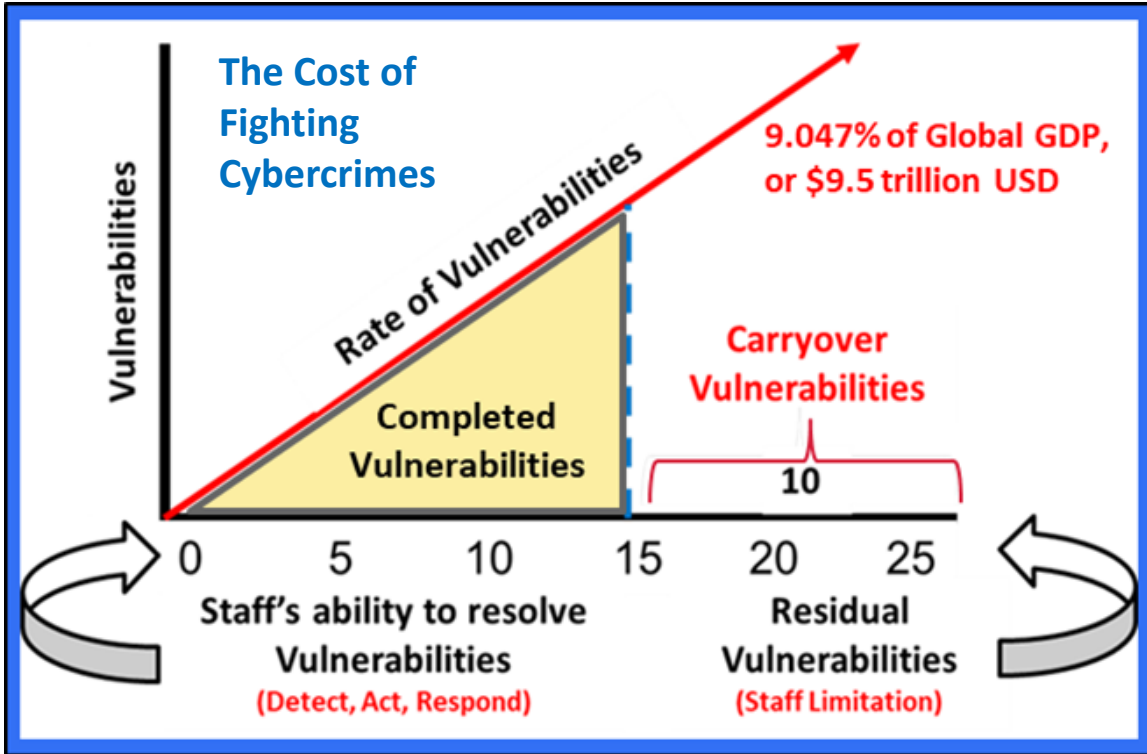
The Fix Rate associated with vulnerability repairs (Patch or New Release) should be equal to or higher than the rate of Vulnerability detection.



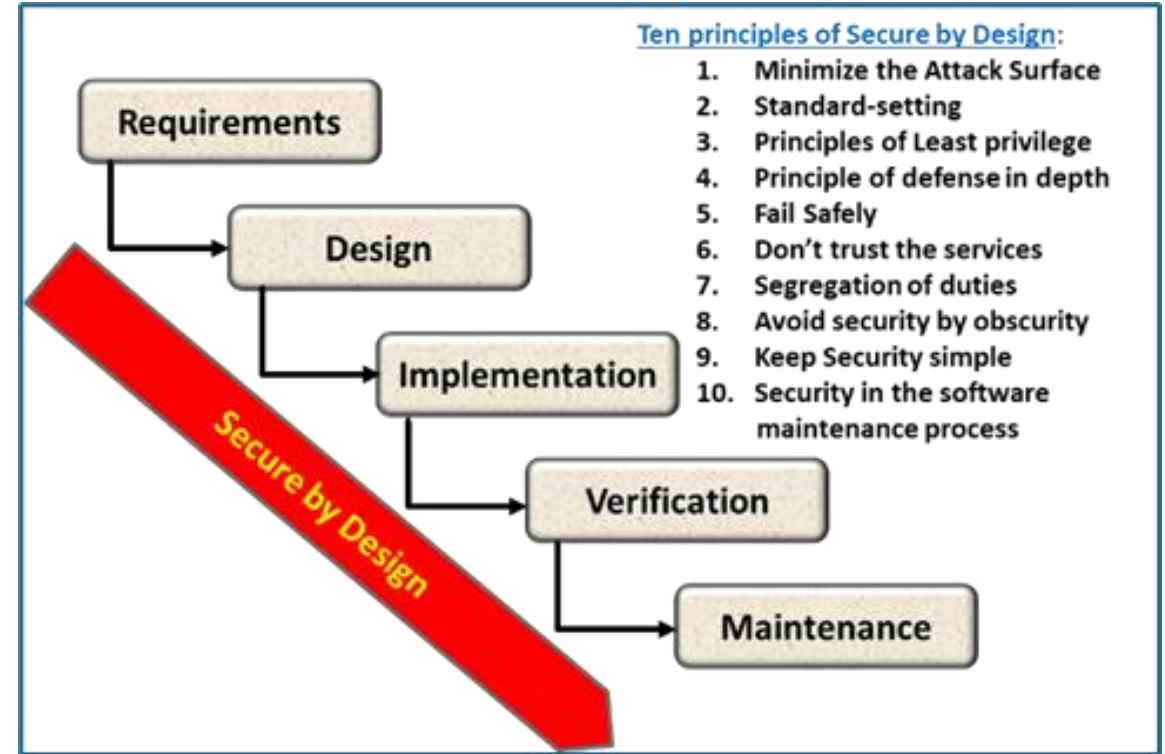


# Fighting Cybercrime Costs with Secure by Design

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



The **current cost of fighting cybercrimes** and technology threats is estimated at \$9.5 Trillion within the United States and 10.24 % 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 combating these costs through the “**Secure by Design**” methodology developed by DHS/CISA to safeguard Government, Business, Infrastructure, and Utilities .

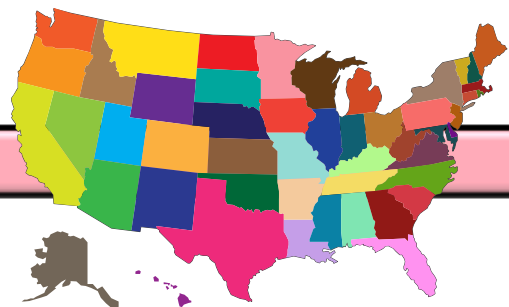
# A “Whole of World” approach to Cybersecurity

Thomas Bronack  
Email: [bronackt@dcag.com](mailto: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:

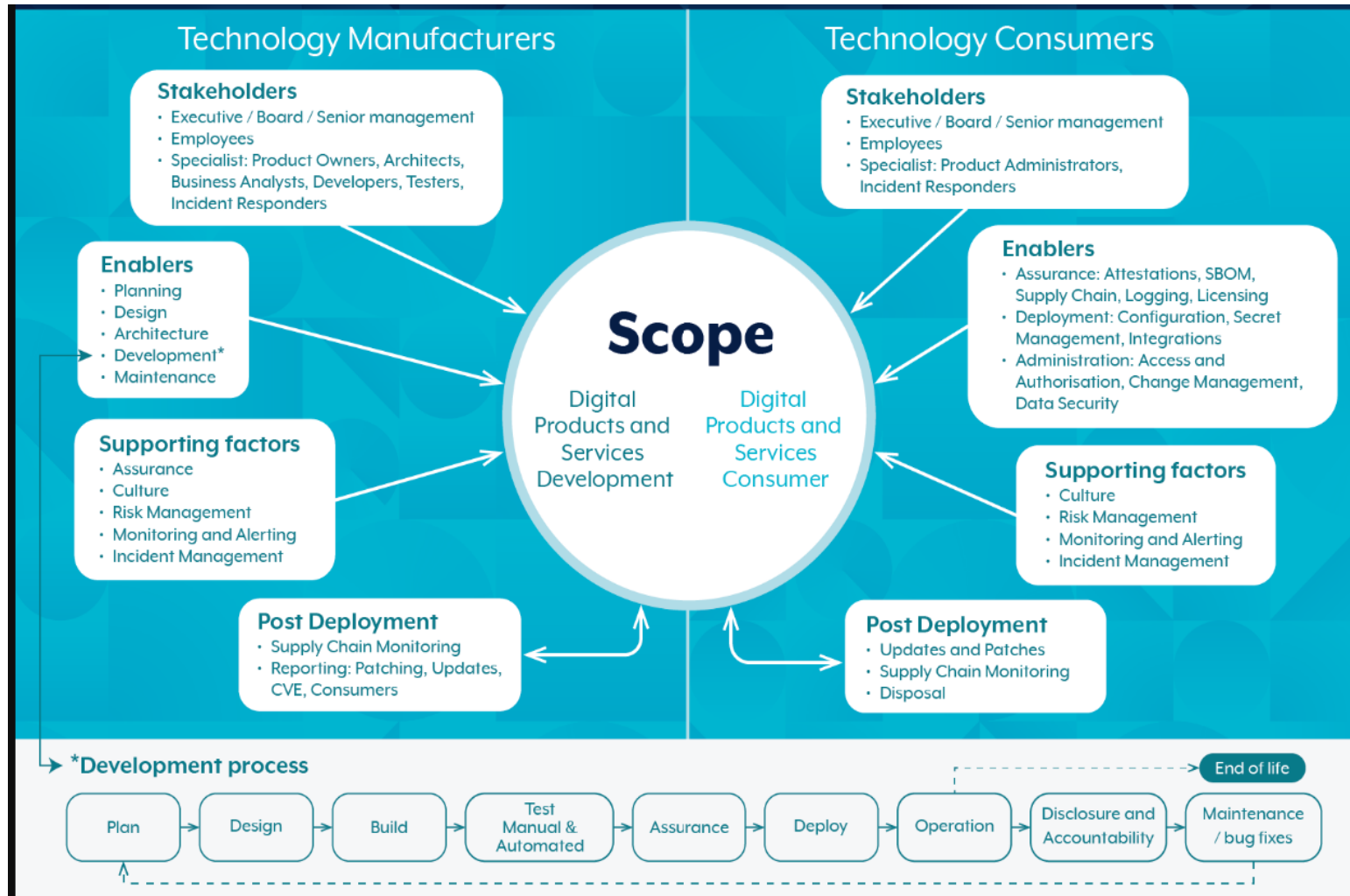
1. Detect Vulnerability (SBOM)
2. Assess the Risk (CVE)
3. Prioritize Remediation (CVSS, KVE, EPSS)
4. Confirm Remediation
5. Optimize through automation
6. Advance the use of BOMs for Software, Release Control, and Artificial Intelligence

### 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](#).

# Secure by Design – Process Overview

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



## What is Secure by Design:

The Cyber Defense Agency, CISA is charged with defending our nation against ever-evolving cyber threats and to understand, manage, and reduce risk to the cyber and physical infrastructure that Americans rely on every hour of every day. But, as we introduce more unsafe technology to our lives, this has become increasingly difficult.

As a nation, we have allowed a system where the cybersecurity burden is placed disproportionately on the shoulders of consumers and small organizations and away from the producers of the technology and those developing the products that increasingly run our digital lives. Americans need a new model to address the gaps in cybersecurity—a model where consumers can trust the safety and integrity of the technology that they use every day.

Every technology provider must take ownership at the executive level to ensure their products are secure by design.

## What it Means to Be Secure by Design

Products designed with Secure by Design principles prioritize the security of customers as a core business requirement, rather than merely treating it as a technical feature. During the design phase of a product’s development lifecycle, companies should implement Secure by Design principles to significantly decrease the number of exploitable flaws before introducing them to the market for widespread use or consumption. Out-of-the-box, products should be secure with additional security features such as multi-factor authentication (MFA), logging, and single sign-on (SSO) available at no extra cost.

- **Gramm Leach Bliley** – Safeguard Act (was Bank Holding Act);
- **HIPAA** – Healthcare regulations (including ePHI, HITECH, and Final Ombudsman Rule);
- **Sarbanes – Oxley Act** (sections 302, 404, and 409) on financial assessment and reporting by authorized “Signing Officer”;
- **EPA and Superfund** (how it applies to Dumping and Asset Management Disposal);
- **Supply Chain Management** “Laws and Guidelines” included in **ISO 24762** (SSAE 16 for Domestic compliance and SSAE 3402 for International Compliance, and NIST 800-34);
- **Supply Chain Management** “Technical Guidelines” described in **ISO 27031**;
- **Patriots Act** (Know Your Customer, Money Laundering, etc.);
- **Workplace Safety and Violence Prevention** via OSHA, OEM, DHS, and governmental regulations (State Workplace Guidelines and Building Requirements);
- **Income Tax and Financial Information protection** via **Office of the Comptroller of the Currency** (OCC) regulations (**Foreign Corrupt Practices Act**, **OCC-177** Contingency Recovery Plan, **OCC-187** Identifying Financial Records, **OCC-229** Access Controls, and **OCC-226** End User Computing).

These laws and regulations have been around for many years (Starting with OCC regulations and growing from there) and have served as the basis for Governance Regulations and Compliance (GRC). Additional industry compliance requirements like SEC, FFIEC and HITECH must be adhered to as well.

The CIA (Confidentiality, Integrity, Availability) deals with security and should be adhered to with the same aggressiveness as GRC.

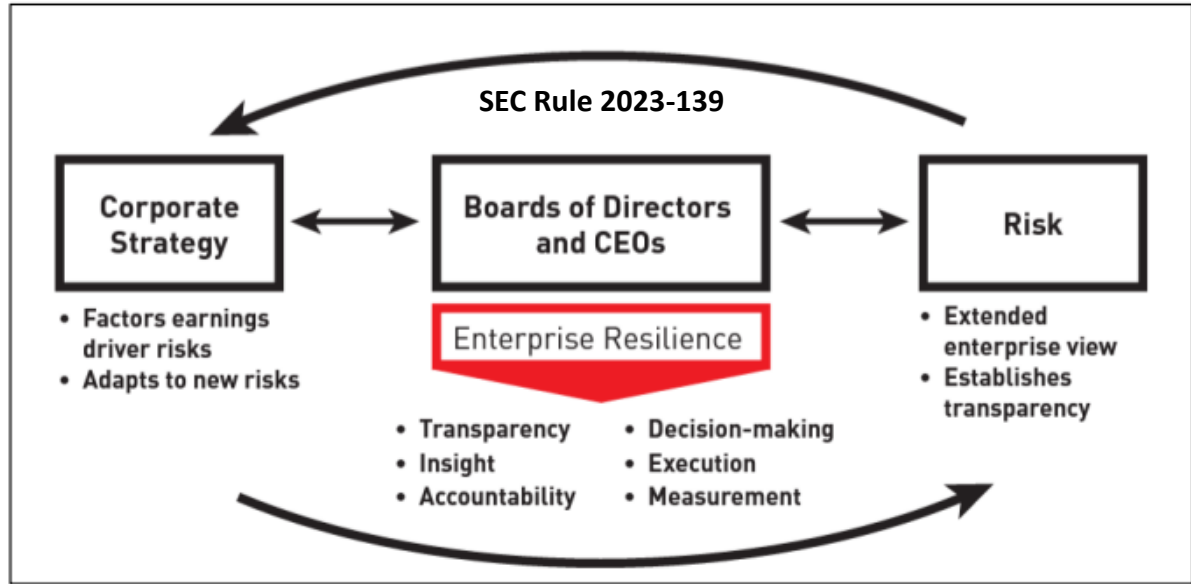
# New Laws and Regulations requiring SBOMs

- 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.
- 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
  - [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.

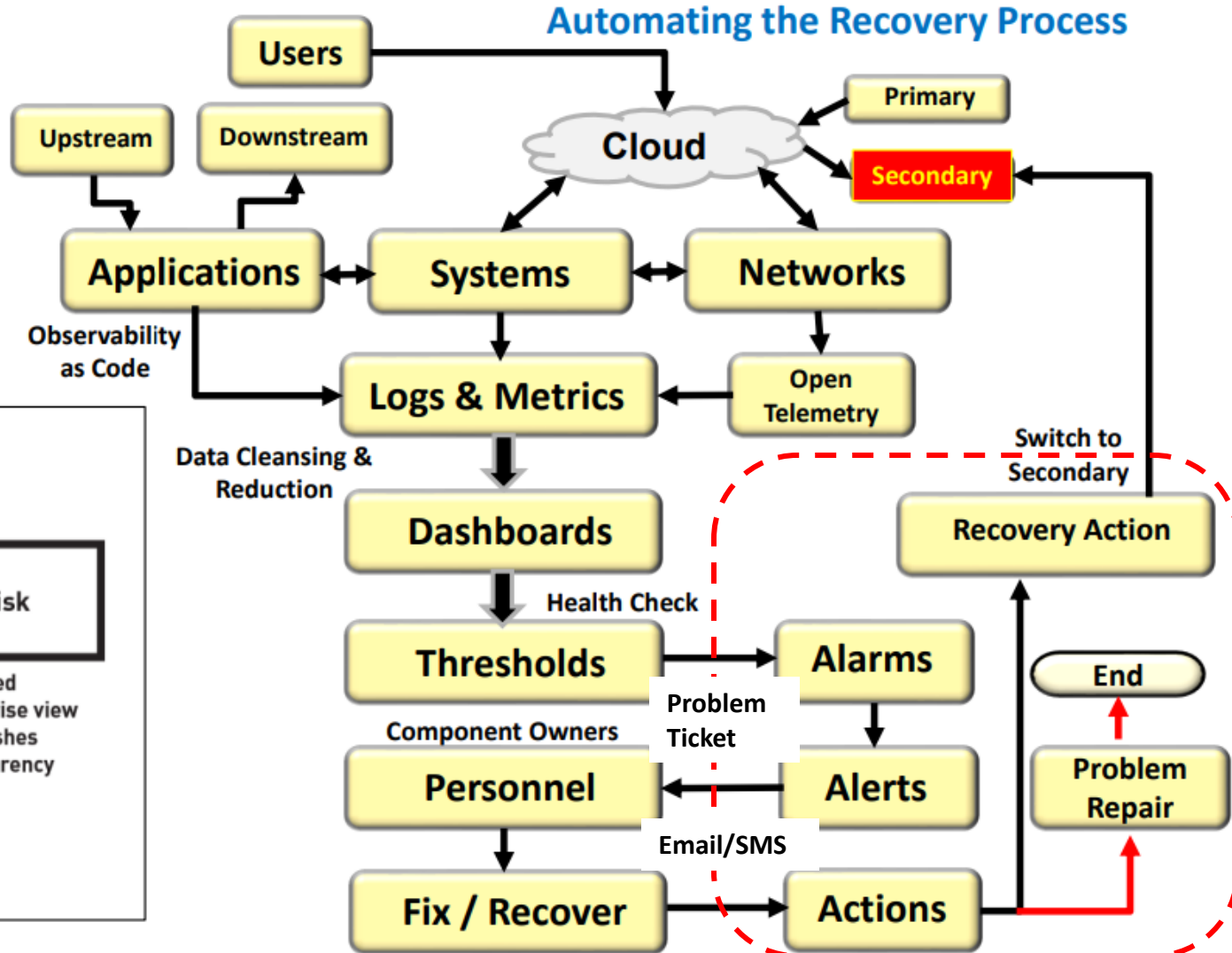
# Board of Directors concerns

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

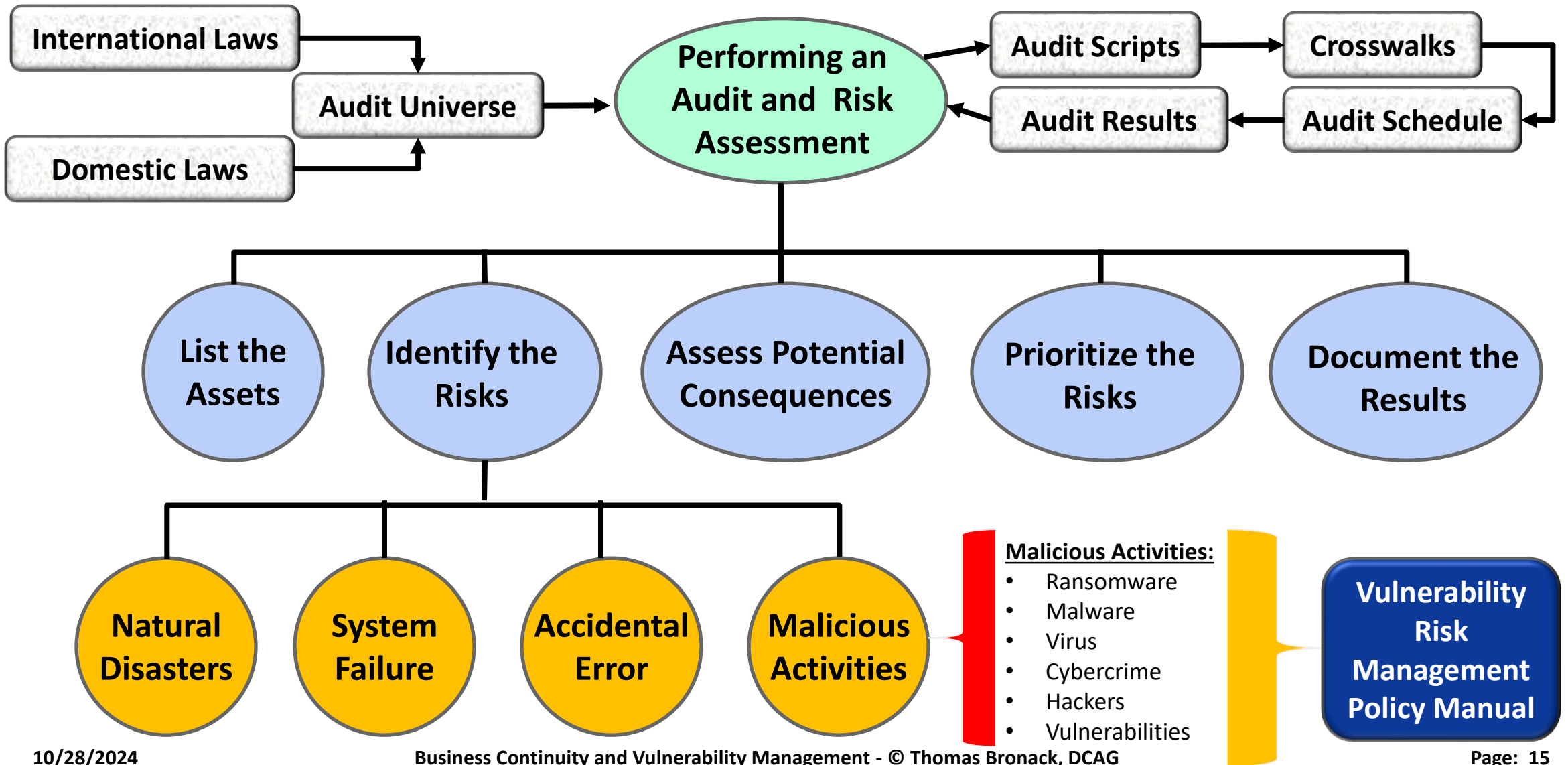
The Board of Director's is responsible for protecting the company and its people, providing continued operation and services, directing growth, and adhering to regulatory guidelines. Therefore, they must establish Resilience, Risk Compliance and Safeguards to ensure continued operations and protect shareholder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



**Risk Management Life Cycle**



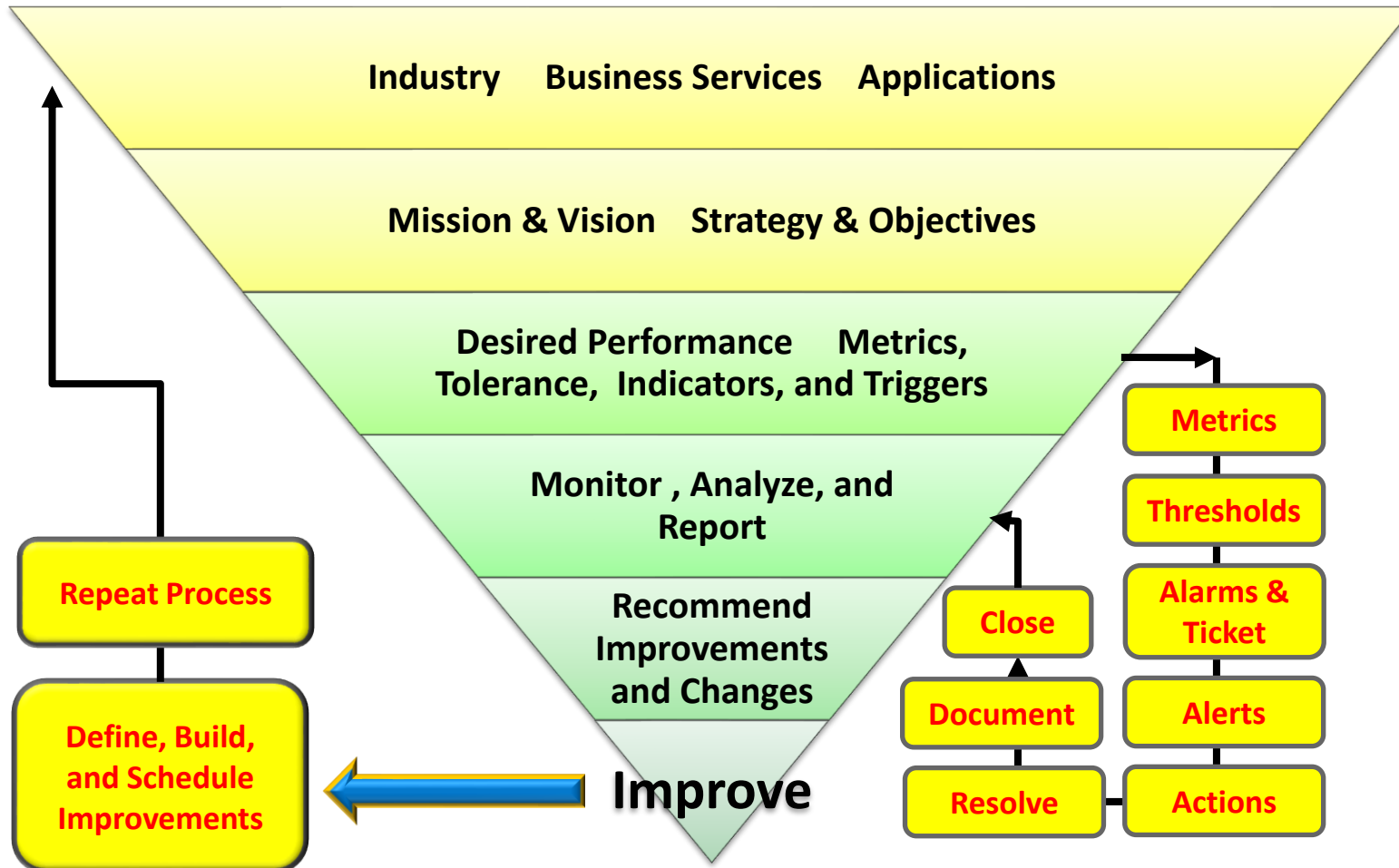
# Performing an Audit and Risk Assessment



# The Risk Evaluation Process Using COSO

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

## Defining the Risk Appetite using COSO



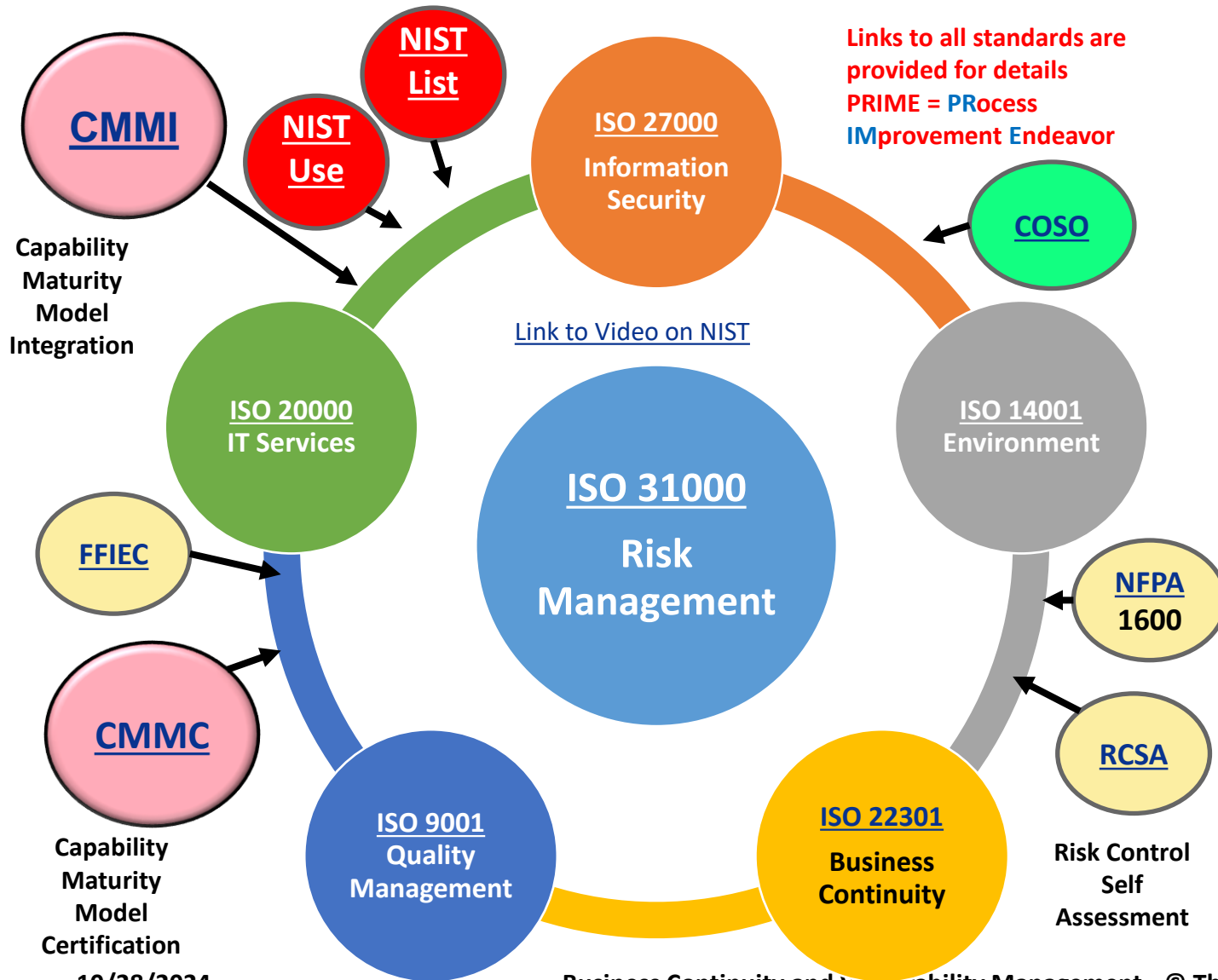
### COSO for Risk Appetite & Evaluation:

1. Review Business Mission and Vision
2. Consider Board and Management perspectives and appetites
3. Incorporates current strategic direction, risk profile, and culture.
4. Identifies and evaluates alternate strategies.
5. Chooses preferred strategy to enhance value.
6. Establishes Business Objectives.
7. Sets tolerance, define and measure metrics, indicators, and triggers.
8. Changing context of the business culture and competitive environment.
9. Monitors performance and revises appetite or strategy, as needed.



# The newest Integration Model – PRIME Approach

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



**Developing** a business optimization approach that combines these ISO Standards (**International**) and NIST Standards (**Domestic**) will achieve certification more quickly.

**Implementing** the standards separately will result in overlaps and inefficiencies.

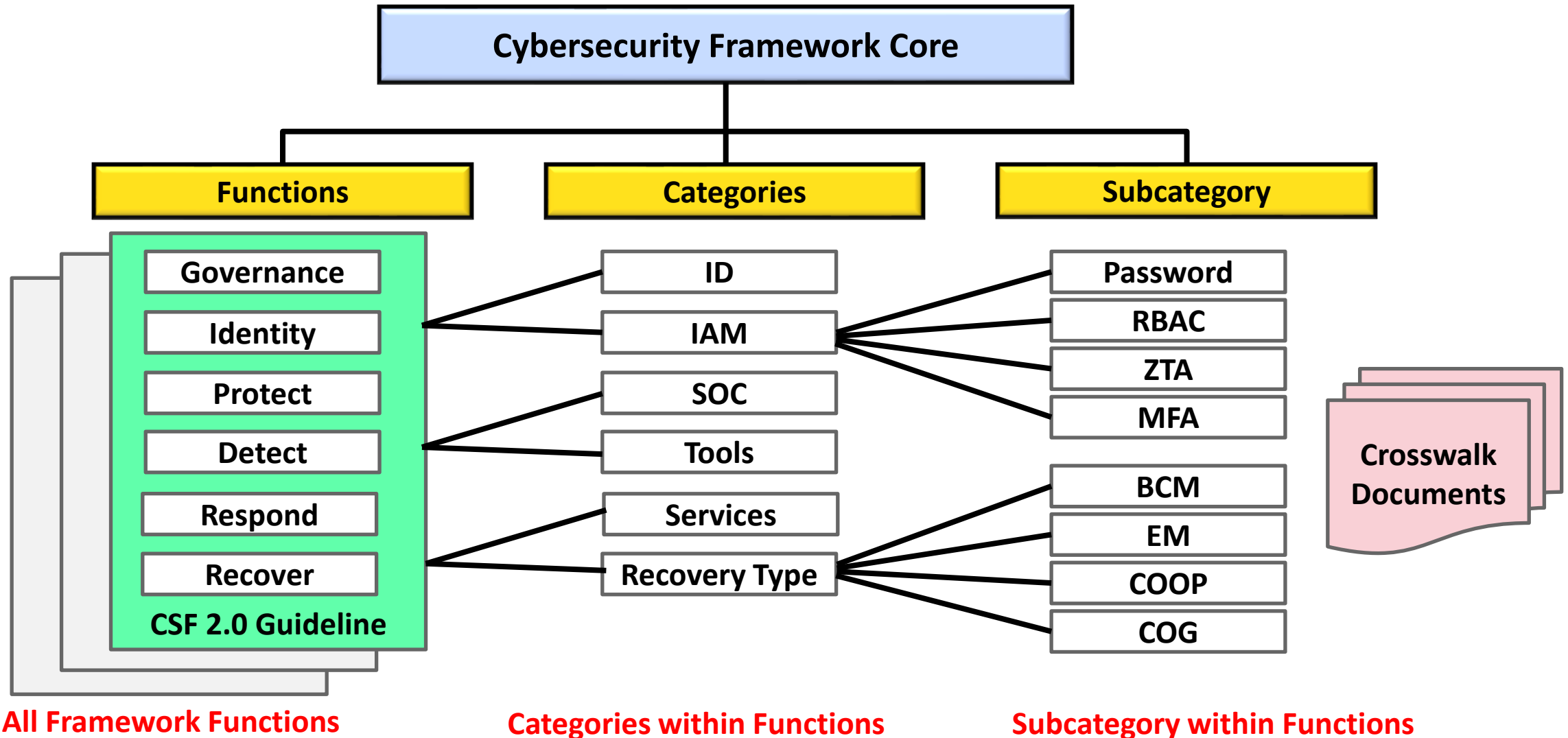
Start with **Risk Management** (31000) and ensure that **Information Security** (ISO 27000) is current and best suited to protect your **Data** and **Environmental facilities** (ISO 14001).

Then implement your **Business Continuity** (ISO 22301) Recovery Certification Process for Emergency, Crisis, Business, and IT Disaster Recovery Management.

**Integrate Quality Management** (ISO 9001) within your processes to ensure the products and services your company delivers will be of the highest quality and capable of protecting your brand and reputation.

Finally ensure your **IT Services** (ISO 20000) are of the highest quality possible and that all ISO standards are adhered to in compliance with existing laws and regulations, so that you never have to fear failing an audited.

# Creating a Crosswalk Audit Document



# Getting started with facts and a defined direction

## 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](#))

## 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.

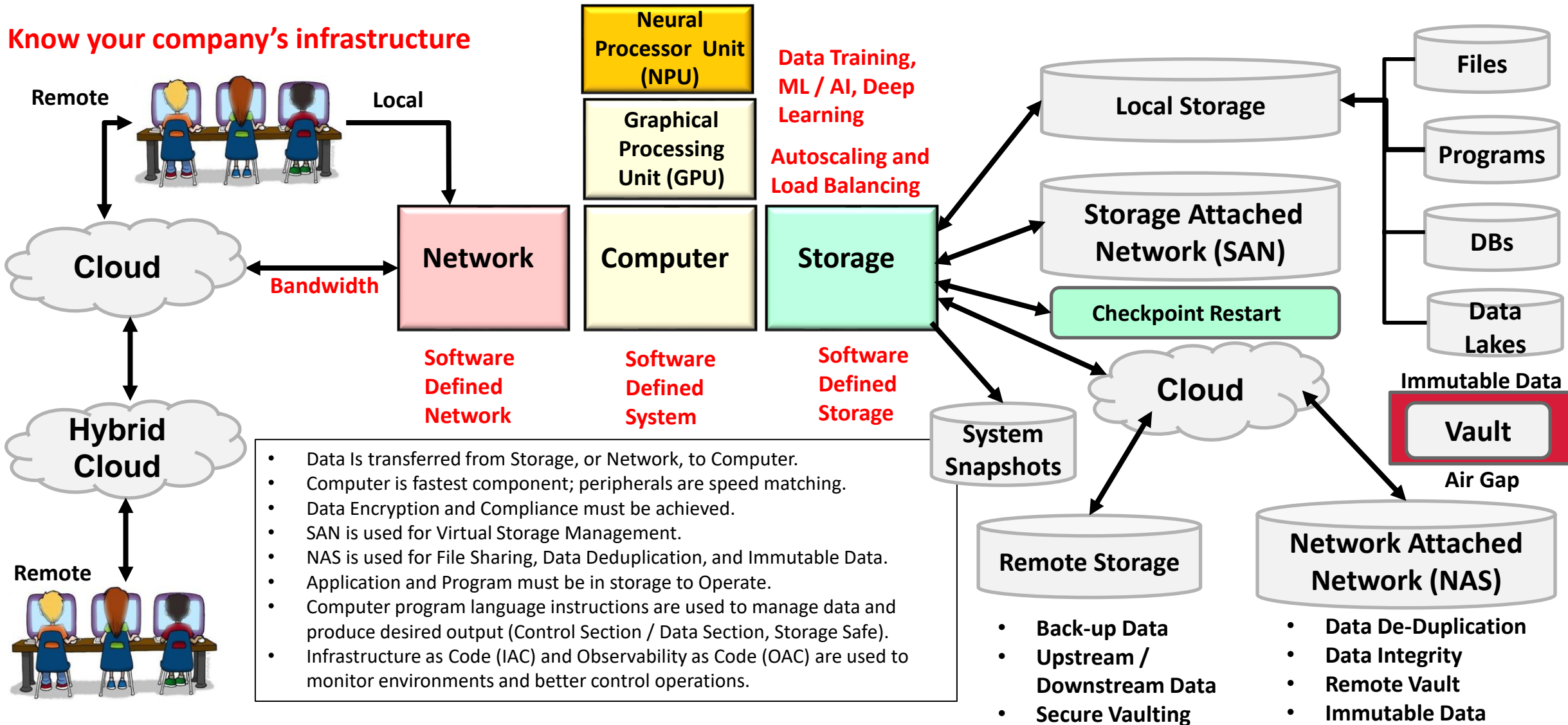
## Know your Environment:

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.

# Monitoring Operations and Controlling Resources

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

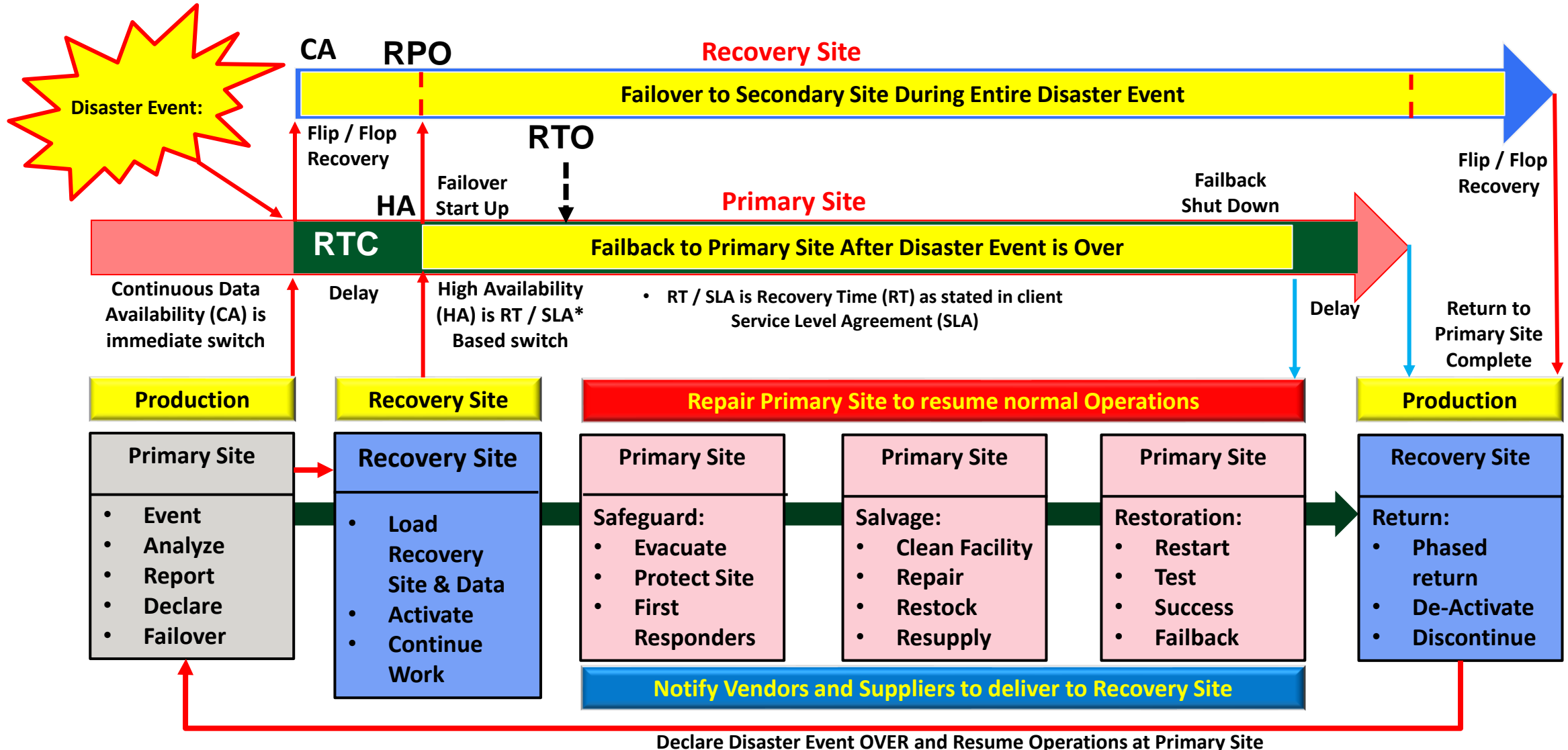
## Know your company's infrastructure



# The Disaster Event Life Cycle

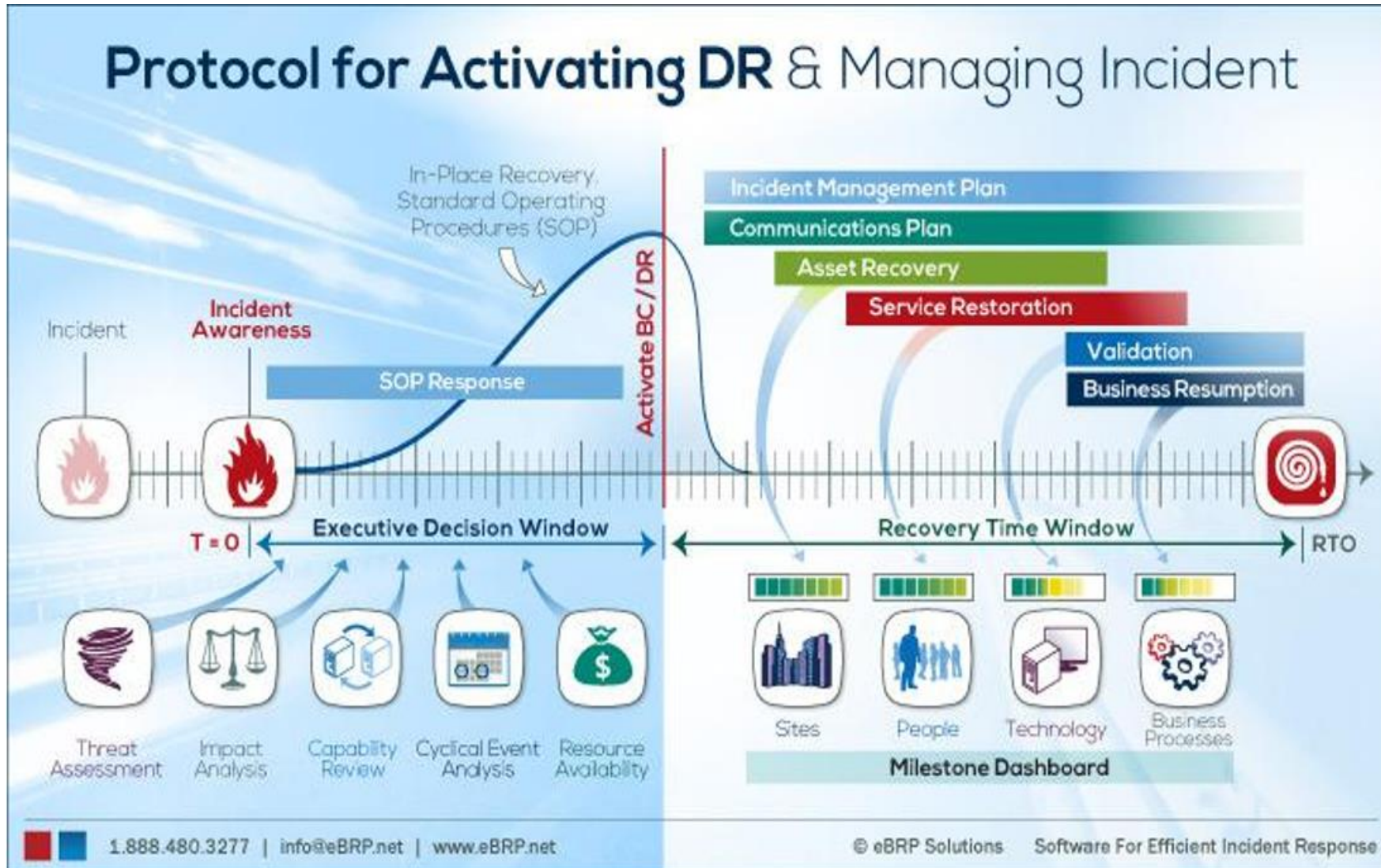
CA is Continuous Availability  
 HA is High Availability  
 RTO – Recovery Time Objective  
 RPO – Recovery Point Objective  
 RTC – Recovery Time Capability

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



# The Business Recovery Life Cycle

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

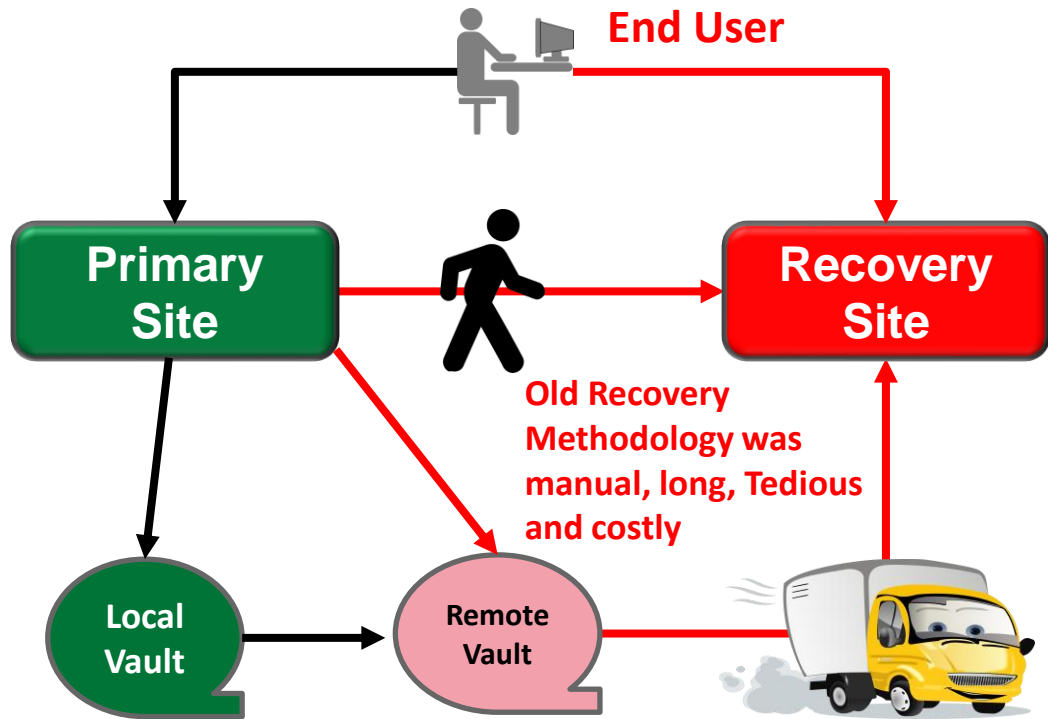


## DR Life Cycle:

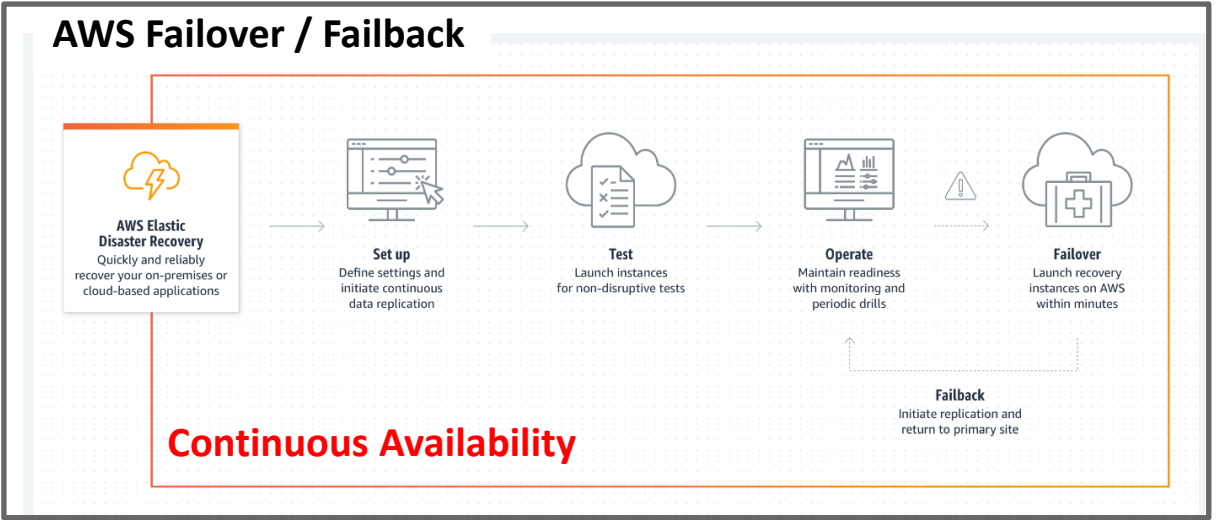
1. **Executive Decision Window**
  - a. Incident occurs
  - b. Incident awareness (RPO)
  - c. Threat Assessment
  - d. Impact Analysis
  - e. Capability Review
  - f. Cyclical Event Analysis
  - g. Resource Availability
  - h. SOP Response
  - i. Activate BC/DR Plan
2. **Recovery Time Window**
  - a. Incident Management
  - b. Communications
  - c. Asset Recovery
  - d. Service Restoration
  - e. Validation
  - f. Business Resumption (RTO)
3. **Milestones Dashboard**
  - a. Sites (Primary / Recovery)
  - b. People
  - c. Technology
  - d. Business Processes

# Evolution of Recovery Management

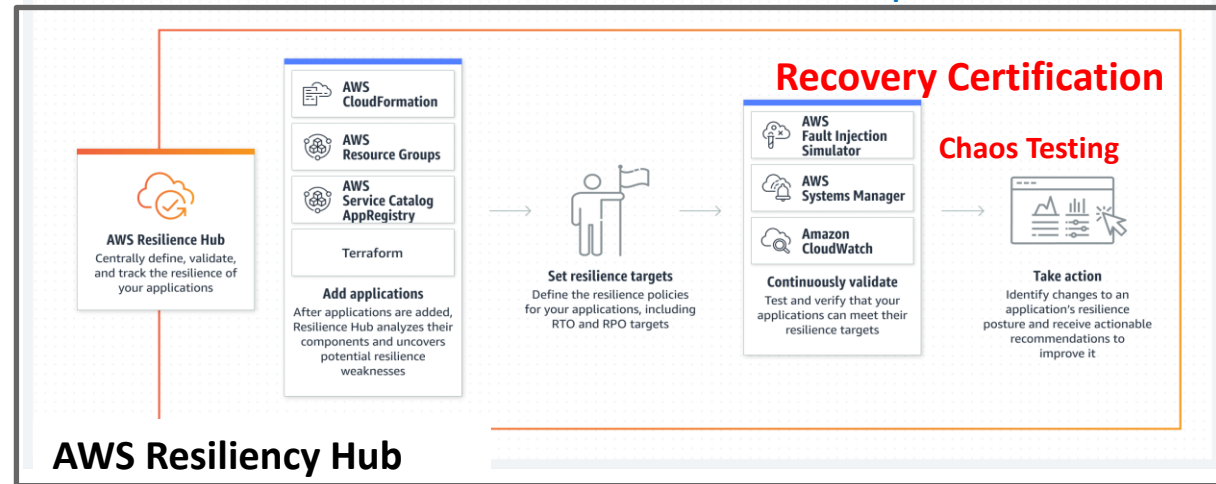
Thomas Bronack  
 Email: [bronackt@dcag.com](mailto:bronackt@dcag.com)  
 Phone: (917) 673-6992



1. Primary Site sends backups to local and remote vaults
2. Primary Site Fails
3. Disaster Declared (\$)
4. Tapes moved from vault to Recovery Site
5. People moved to recovery site
6. Configure Systems & Networks
7. Load Data & Applications
8. Initiation Recovery Operations
9. Connect Users
10. Initiate Production Operations
11. Reverse process when disaster event is over
12. Duration can be in days, but certainly hours



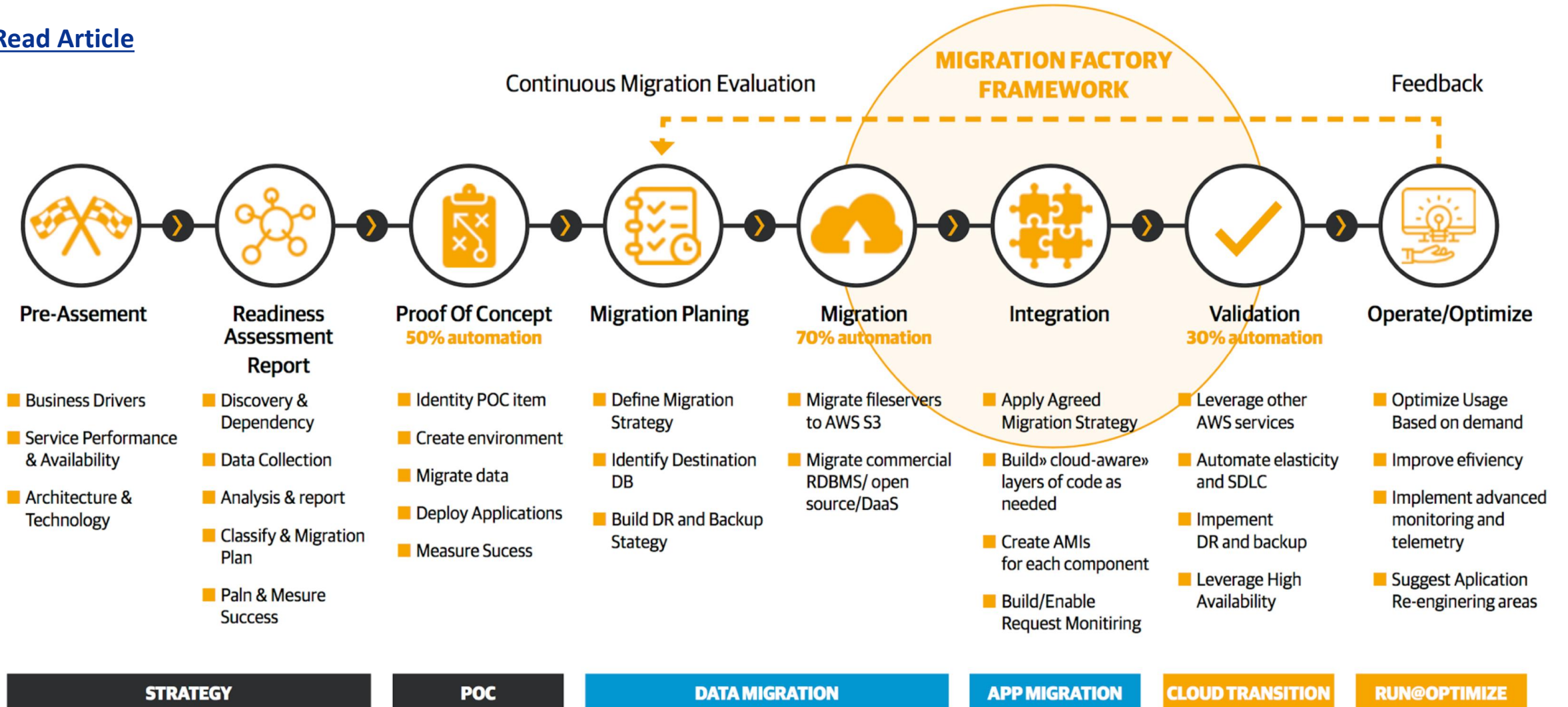
The new Recovery Methodology is quick & automated via Failover / Failback. CloudWatch performs Health Checks, and the Resiliency Hub allows for Failover / Failback and continuous validation without disruption



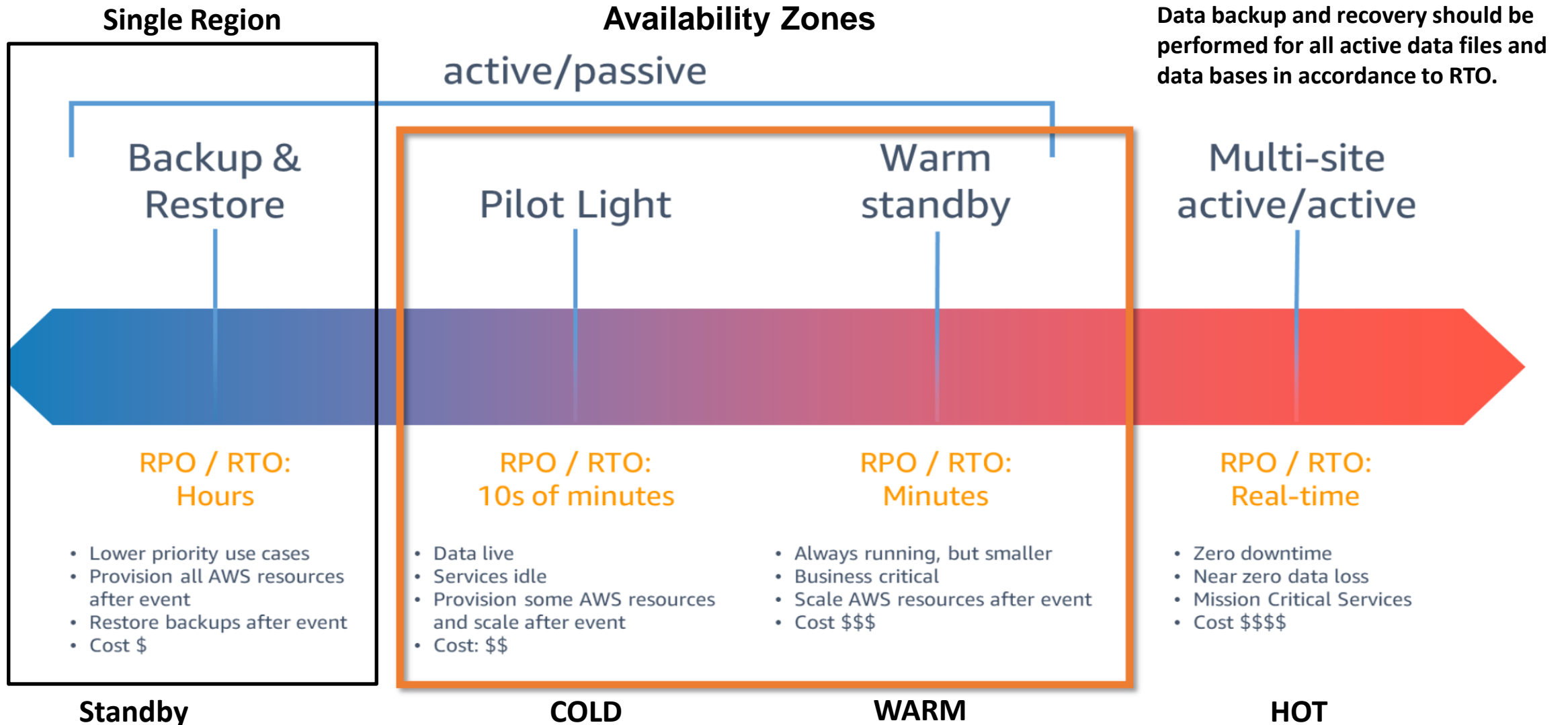
# Using AI Planning for Migrating Applications to AWS Cloud

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

[Read Article](#)







# Resilience Patterns and Recovery Groups

Thomas Bronack  
 Email: [bronackt@dcag.com](mailto: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"> <li>1. TRANSACTIONAL TRAFFIC - handled by primary region only</li> <li>2. No multi-region INFRASTRUCTURE</li> <li>3. APPLICATION code only available in single region</li> <li>4. Multi-region RECOVERY not supported</li> </ol>	<ol style="list-style-type: none"> <li>1. TRANSACTIONAL TRAFFIC - handled by primary region only</li> <li>2. INFRASTRUCTURE available on stand-by</li> <li>3. APPLICATION provisioned, but in shutdown state</li> </ol>	<ol style="list-style-type: none"> <li>1. TRANSACTIONAL TRAFFIC - handled by primary region only</li> <li>2. INFRASTRUCTURE available on standby</li> <li>3. Minimal APPLICATION footprint running in 2nd region (all components are spun up and available with min. capacity, where application)</li> </ol>	<ol style="list-style-type: none"> <li>1. TRANSACTIONAL TRAFFIC - handled by primary region only</li> <li>2. INFRASTRUCTURE always available in both regions</li> <li>3. APPLICATION stack running active/active multi-region</li> </ol>
Reserve Capacity			Required RESERVE CAPACITY	Required RESERVE CAPACITY
Cross-Region Maintenance	None	<ol style="list-style-type: none"> <li>1. Maintain PERSISTENT DATA REPLICATION infrastructure</li> <li>2. APPLICATION CODE maintained for currency in BOTH REGIONS</li> <li>3. Operate Production from stand-by region periodically</li> </ol>	<ol style="list-style-type: none"> <li>1. Maintain PERSISTENT DATA REPLICATION infrastructure</li> <li>2. APPLICATION CODE maintained for currency in BOTH REGIONS</li> <li>3. Operate Production from stand-by region periodically</li> </ol>	<ol style="list-style-type: none"> <li>1. Maintain 2-WAY PERSISTENT DATA REPLICATION</li> <li>2. APPLICATION CODE maintained for currency in BOTH REGIONS</li> <li>3. Operate Production from stand-by region periodically</li> </ol>
Recovery Steps	<ol style="list-style-type: none"> <li>1. ACQUIRE INFRASTRUCTURE</li> <li>2. BUILD OUT infrastructure</li> <li>3. DEPLOY application</li> <li>4. RECOVER / RECREATE DATA</li> <li>5. REDIRECT TRAFFIC to region 2</li> </ol>	<ol style="list-style-type: none"> <li>1. SCALE INFRASTRUCTURE</li> <li>2. STARTUP application</li> <li>3. FAILOVER TRAFFIC</li> </ol>	<ol style="list-style-type: none"> <li>1. AUTO- SCALE INFRASTRUCTURE</li> <li>2. FAILOVER TRAFFIC</li> </ol>	<ol style="list-style-type: none"> <li>1. RECOVERY achieved through automated redirect of traffic</li> </ol>
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)
<b>Cloud Based Recovery Group Specifications</b>		Preferred Patterns		

# Azure Environment and Recovery Management

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

## Extend on-premises into Azure

Business continuity & disaster recovery



Azure Site Recovery



Azure Backup



Storage Replica

Extend on-premises capacity

Storage



Azure File Sync



Storage Migration Service

Compute



Cloud witness



Create Azure VM

Networking



Azure Network Adapter



Azure Extended Network



Migrate to Cloud

Receive Cloud Services

## Centrally manage from Azure

Secure



Azure Security Center

Monitor



Azure Monitor

Update



Azure Update Management

Govern



Azure Arc for Servers



Azure Policy

Receive Cloud Services and / or perform recovery



Migrate on-premises applications to Cloud and receive SaaS Cloud services



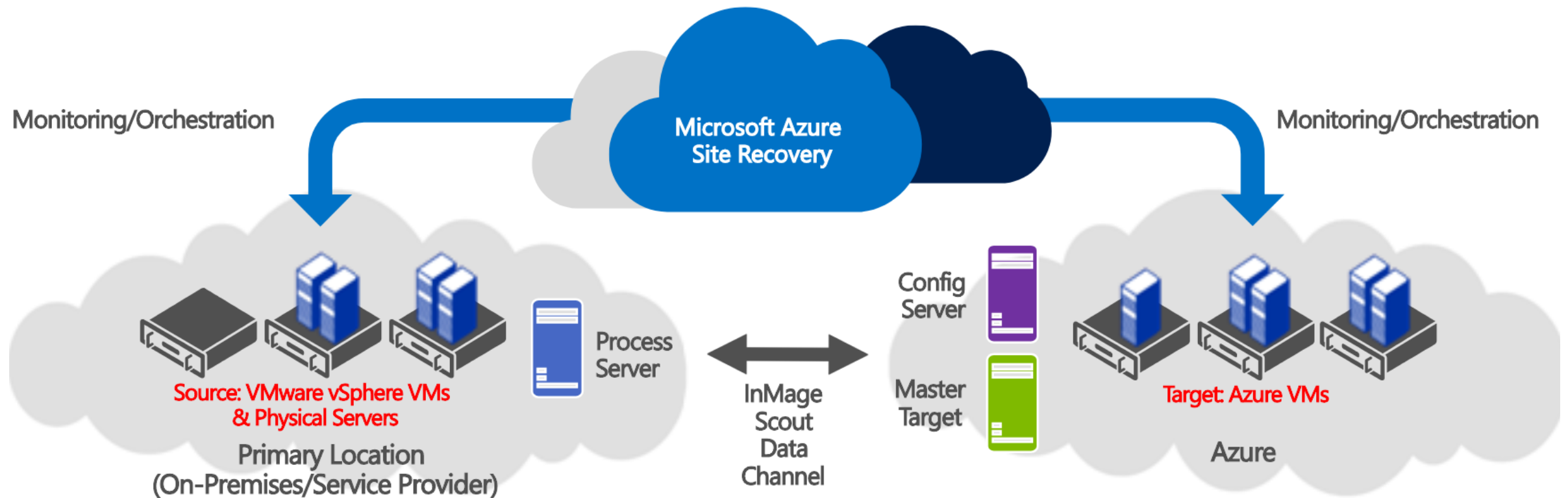
Backup / Recovery Managed Service Providers (MSP)



Microsoft Azure

# Azure Recovery Management Environment

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



**Process Server** – Used for Caching, Compression & Encryption

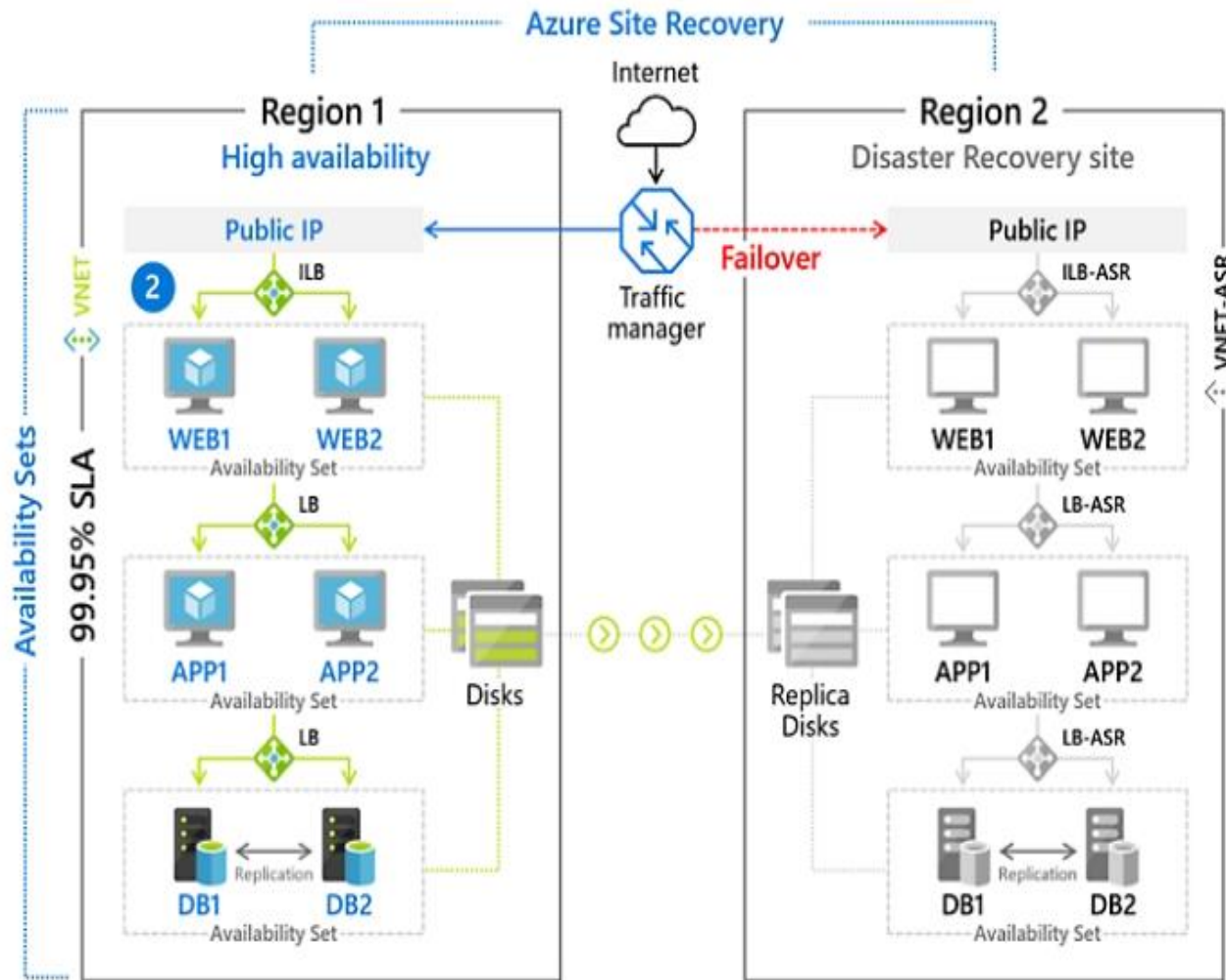


**Config Server** – Used for Centralized Management of InMage Scout



**Master Target** – Used as a repository & for retention

# Azure Site Recovery Management



## Simple to deploy and manage

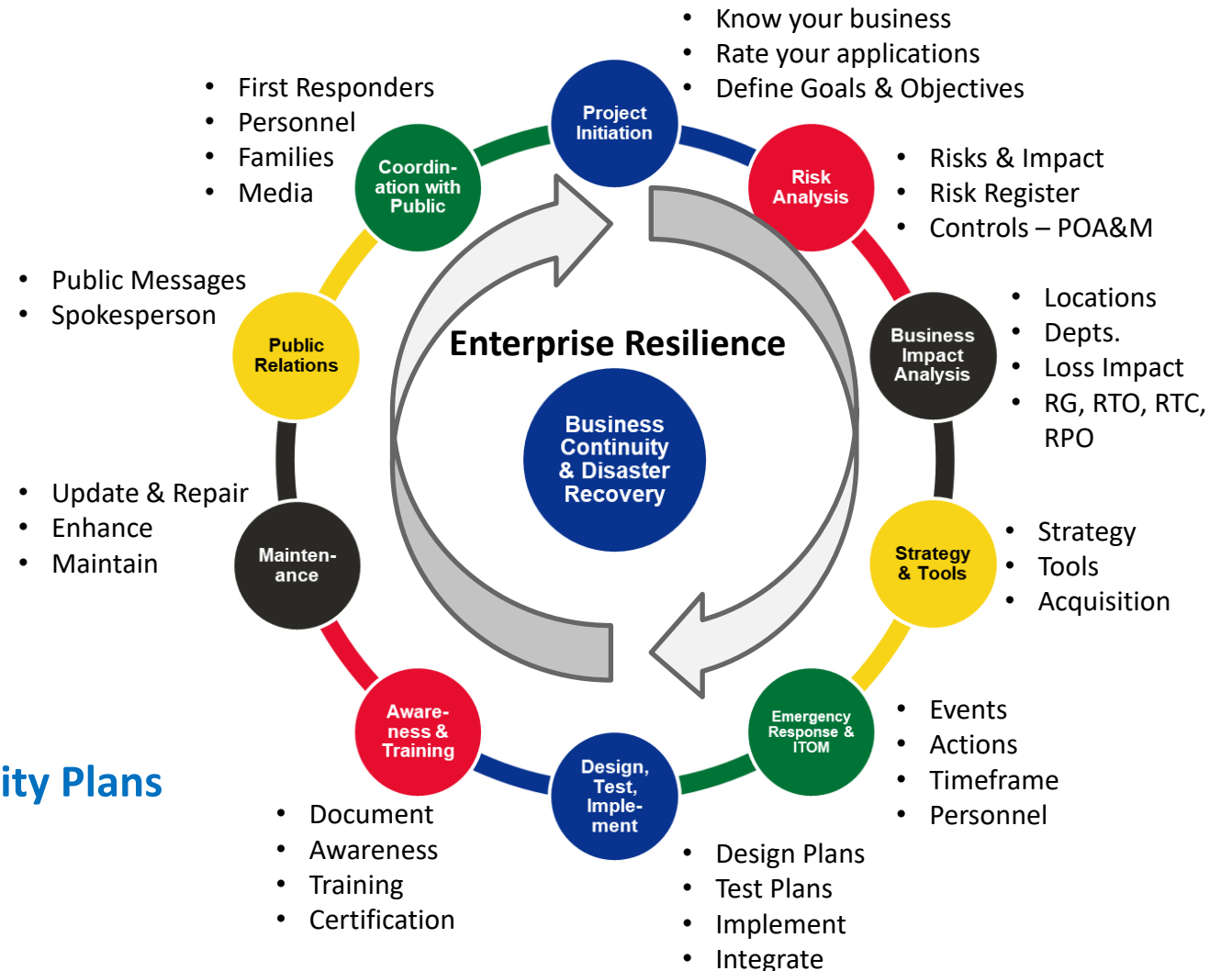
- Set up Azure Site Recovery simply by replicating an Azure VM to a different Azure region directly from the Azure portal.
- As a fully integrated offering, Site Recovery is automatically updated with new Azure features as they're released.
- Minimize recovery issues by sequencing the order of multi-tier applications running on multiple virtual machines.
- Ensure compliance by testing your disaster recovery plan without impacting production workloads or end users.
- And keep applications available during outages with automatic recovery from on-premises to Azure or Azure to another Azure region.

[Link to detailed explanation](#)

# Ten Step Process to establish BCM/DR Practice

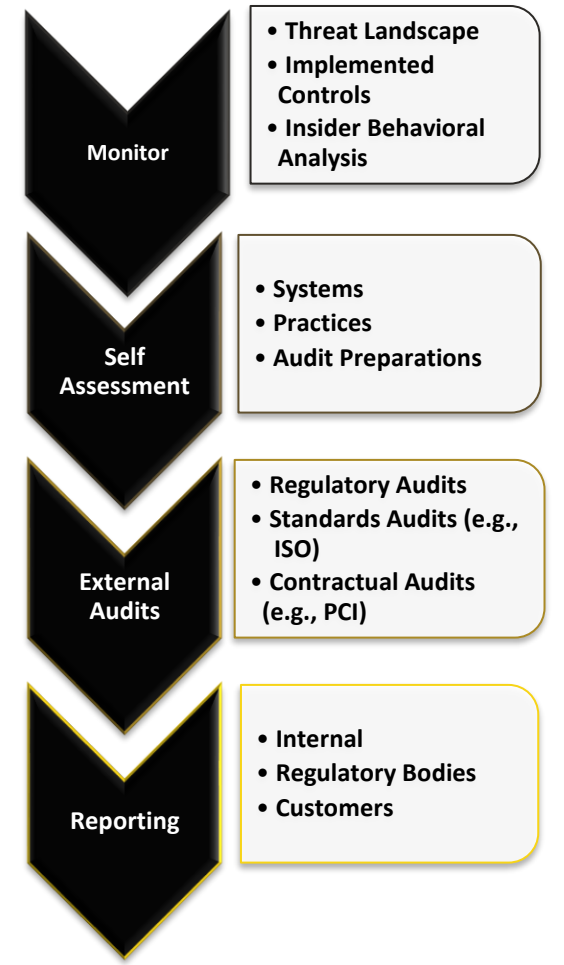
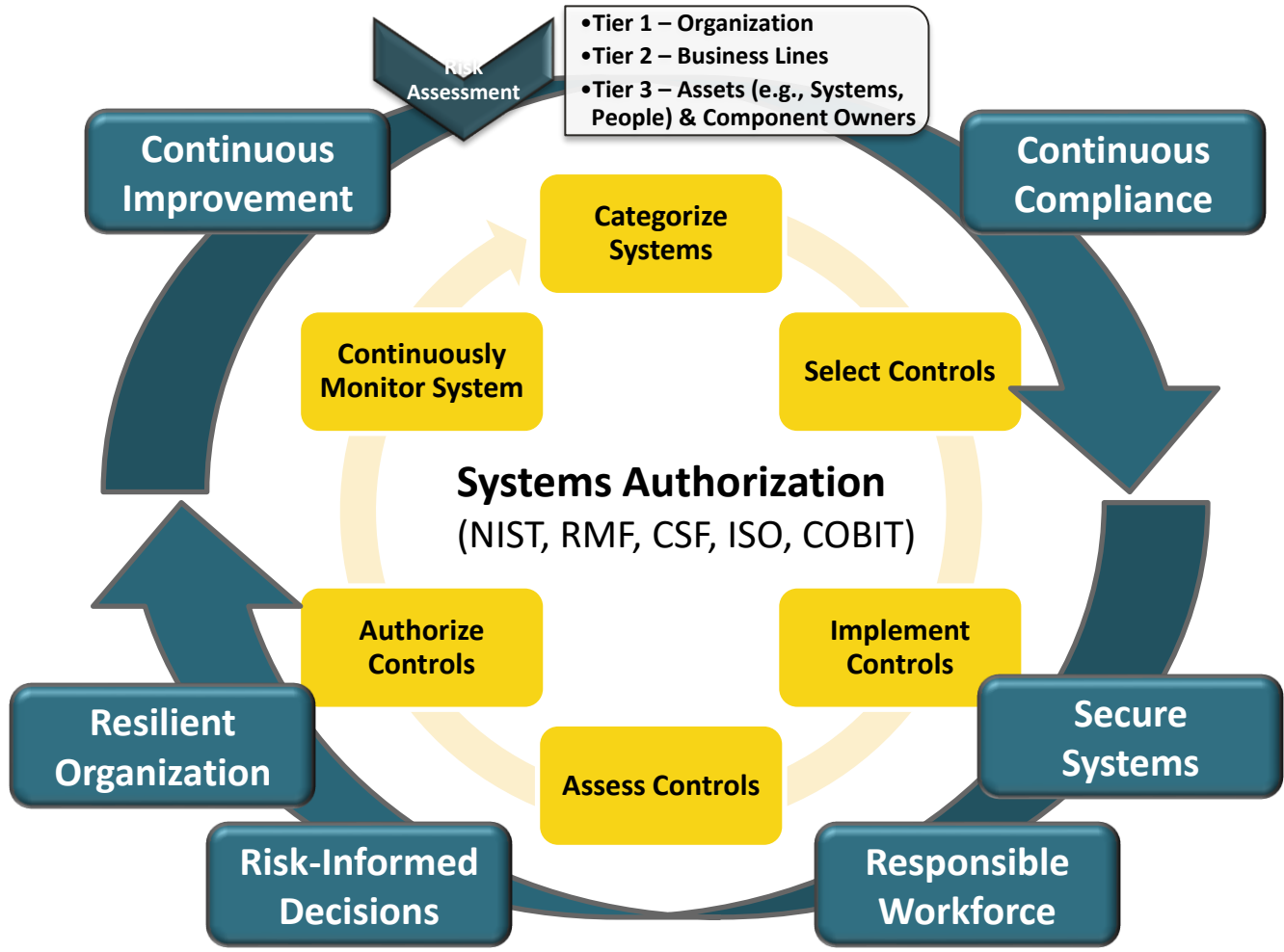
Thomas Bronack  
 Email: [bronackt@dcag.com](mailto:bronackt@dcag.com)  
 Phone: (917) 673-6992

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



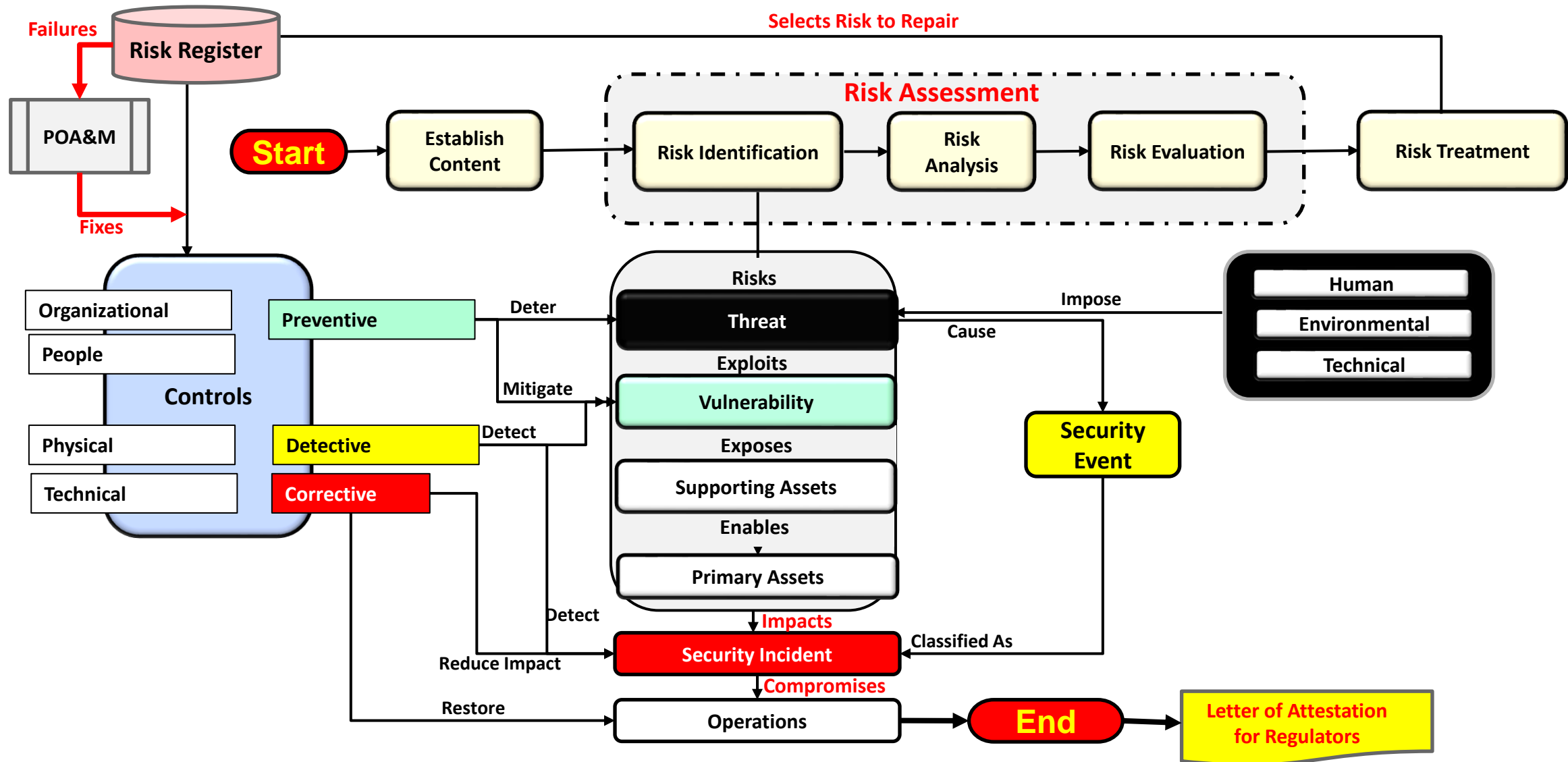
# Ensuring Compliance via GRC and Risk Assessment

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



# Risk Management with ISO 27000: 2022

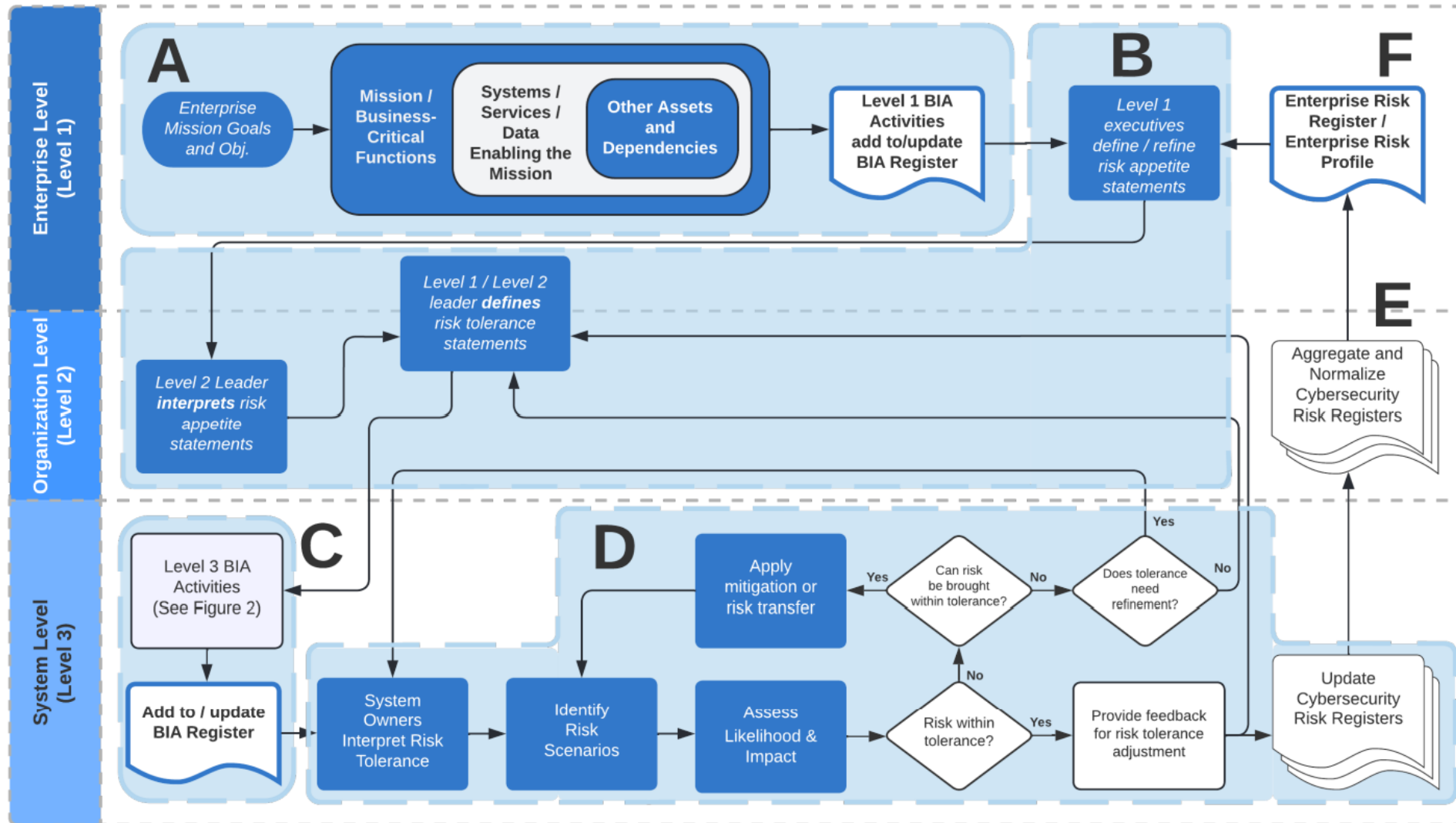
Thomas Bronack  
 Email: [bronackt@dcag.com](mailto:bronackt@dcag.com)  
 Phone: (917) 673-6992





# Business Impact Analysis – BIA (NIST SP 800-34, and NIST IR 8286d)

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



## [Link to Document](#)

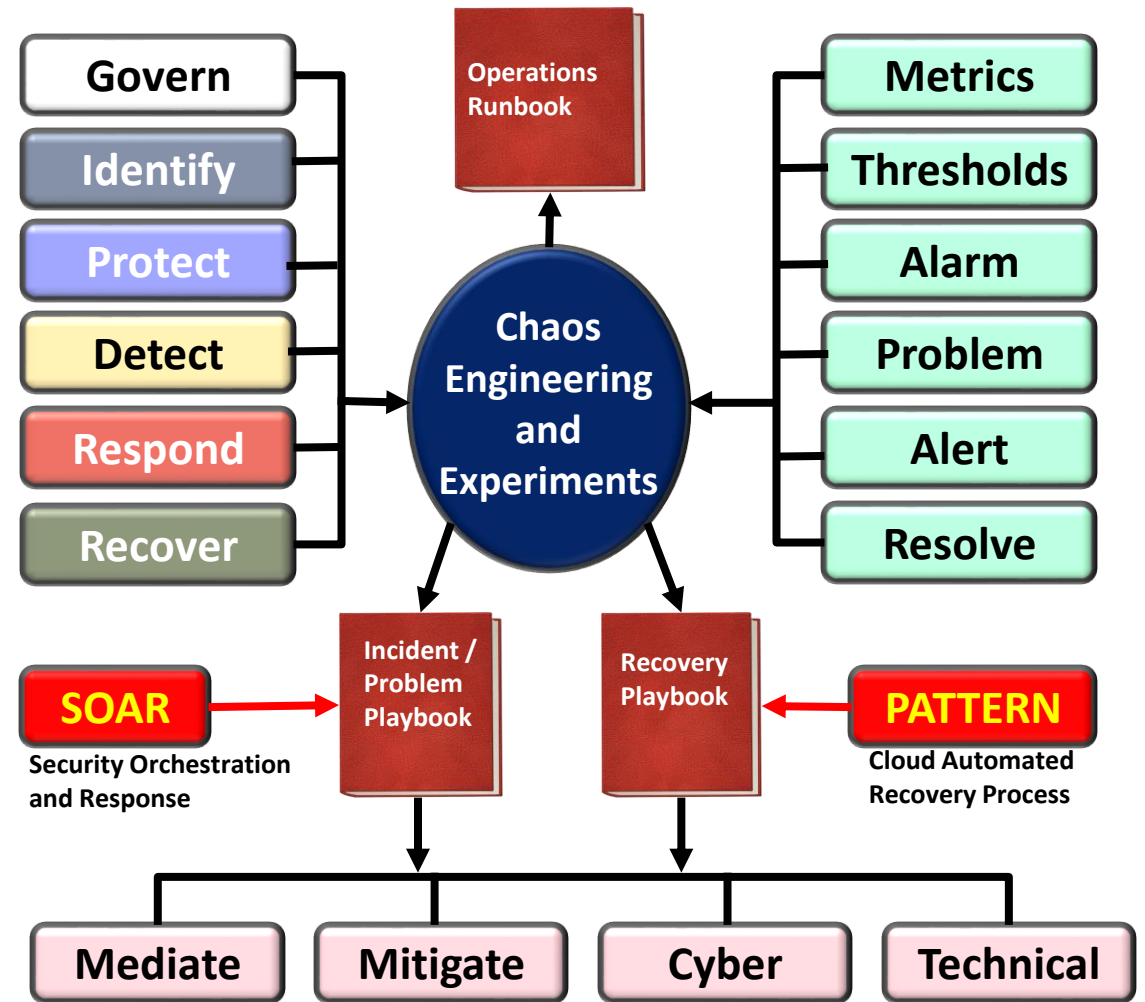
- A. Define Goals
- B. Risk Appetite
- C. BIA Activities
- D. Identify Risks
- E. Normalize Risks
- F. Risk Register with POA&M
- G. RTO / RPO
- H. Feeds (Upstream / Downstream)
- I. Recovery Group
- J. Executive Decision Window & Activities
- K. Recovery Time Window & Activities

# NIST CSF 2.0 Categories and Application

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

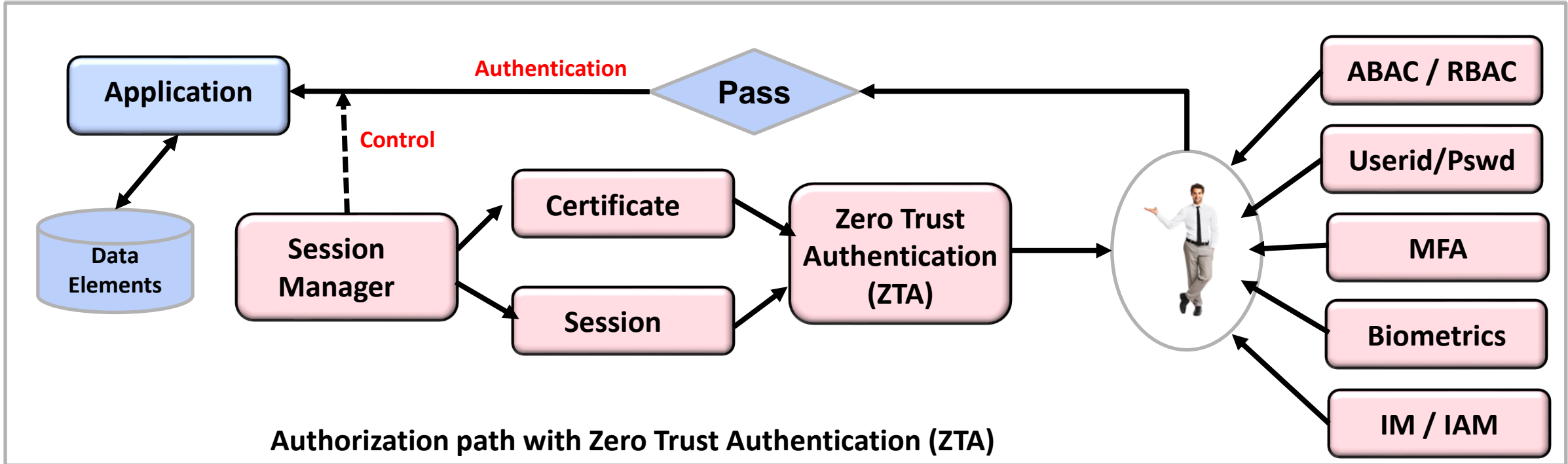
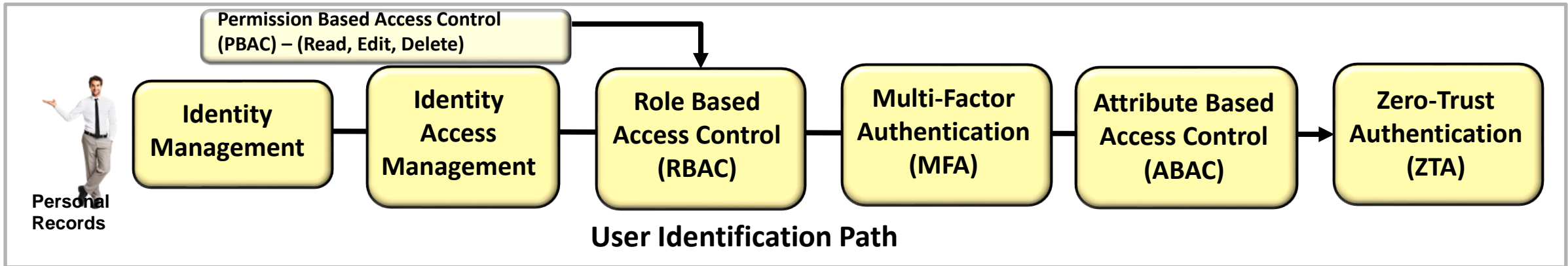
NIST Cybersecurity Framework 2.0		
CSF 2.0 Function	CSF 2.0 Category	CSF 2.0 Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles and Responsibilities	GV.RR
	Policies and Procedures	GV.PO
Identity (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Supply 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

## Establish Cyber Security Controls via CSF 2

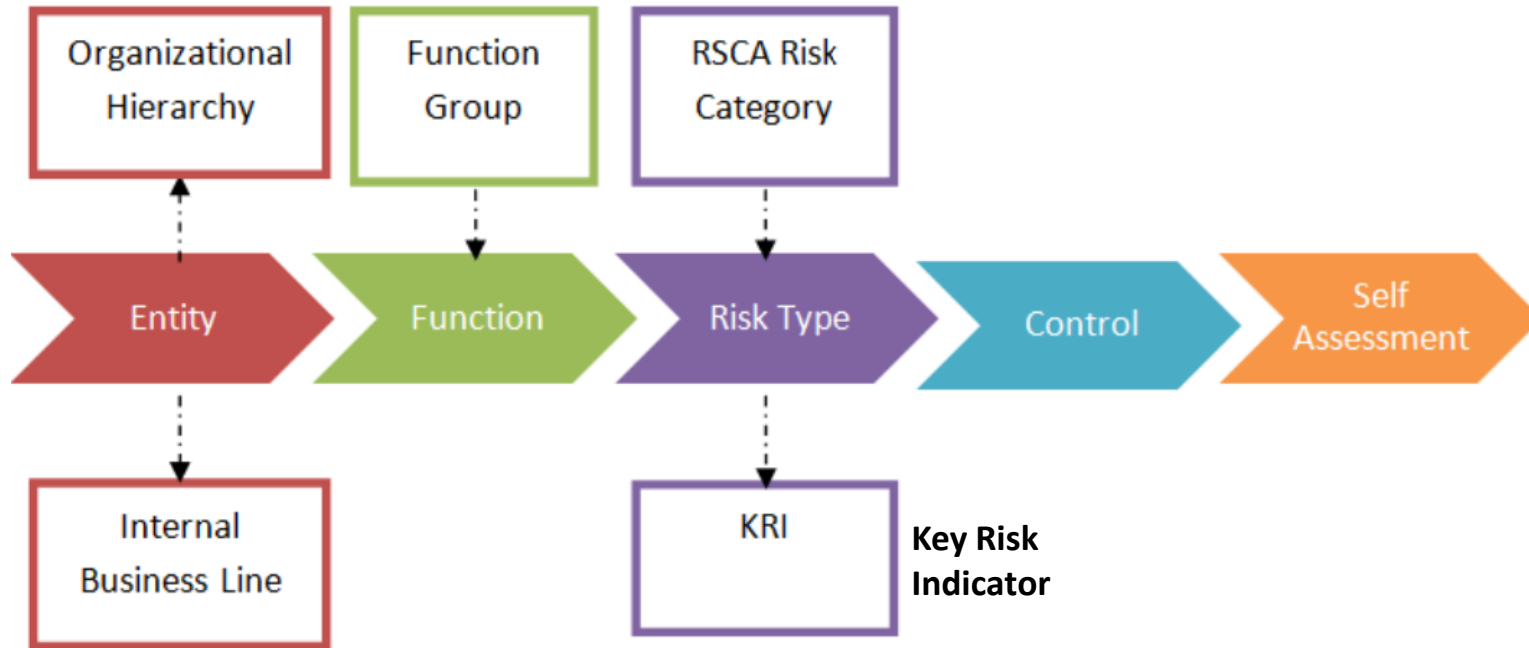


# Identity and Access Management technologies

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



# Risk Control Self Assessment (RCSA)



**RCSA** (Risk Control Self Assessment) is an empowering method/process by which management and staff of all levels collectively identify and evaluate risks and associated controls. It adds value by increasing an operating unit’s involvement in designing and maintaining control and risk systems, identifying risk exposures and determining corrective action. The aim of RCSA is to integrate risk management practices and culture into the way staff undertake their jobs, and business units achieve their objectives. It provides a framework and tools for management and employees to:

- Identify and prioritize their business objectives
- Assess and manage high risk areas of business processes
- Self-evaluate the adequacy of controls
- Develop risk treatment action plans
- Ensure that the identification, recognition and evaluation of business objectives and risks are consistent across all levels of the organization

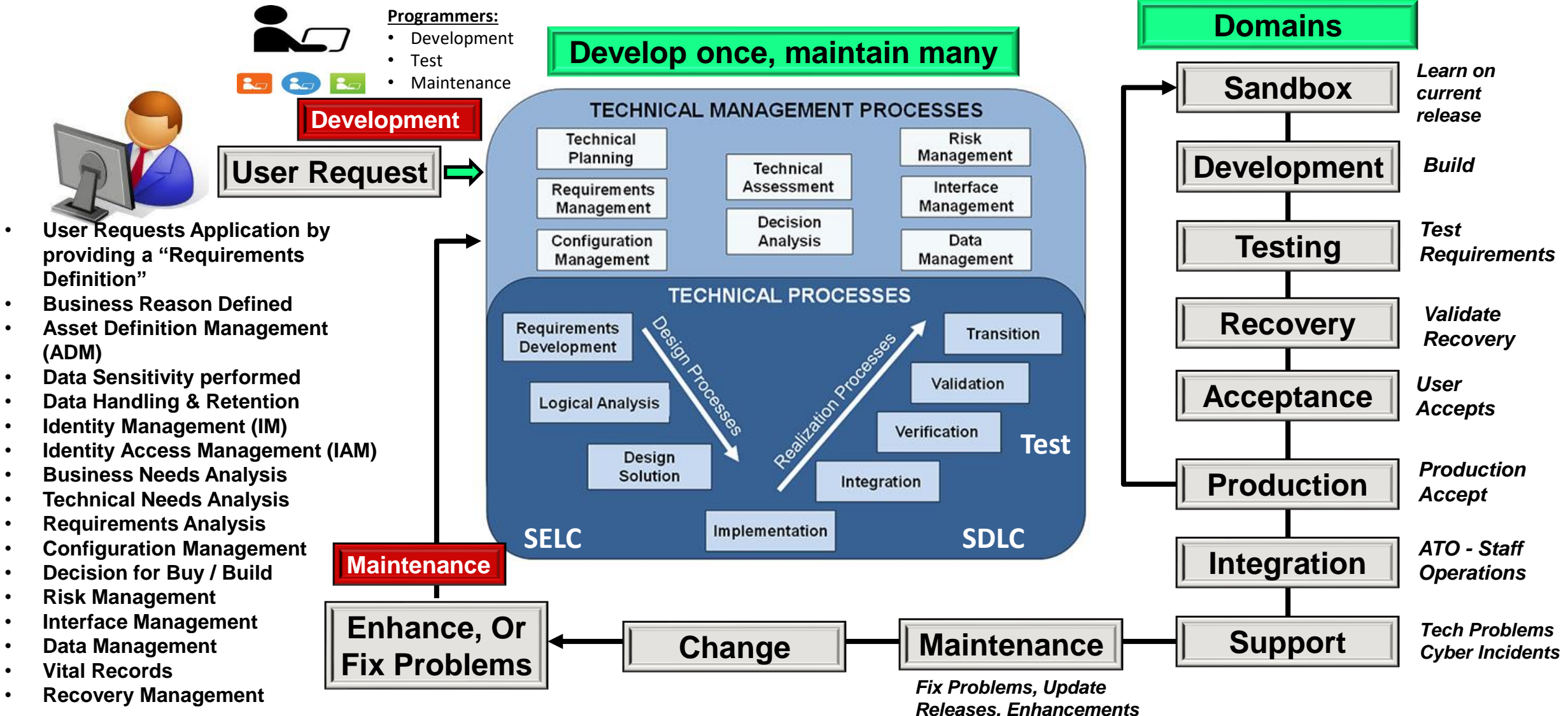
## Steps within a RCSA are:

1. Select Participants
2. Identify Risks
3. Assess Risk against business measure
4. Actions against control lapses
5. Access Controls
6. Identify controls for a risk (KRI)
7. Monitor
8. Report results
9. Take corrective actions to continuously improve process



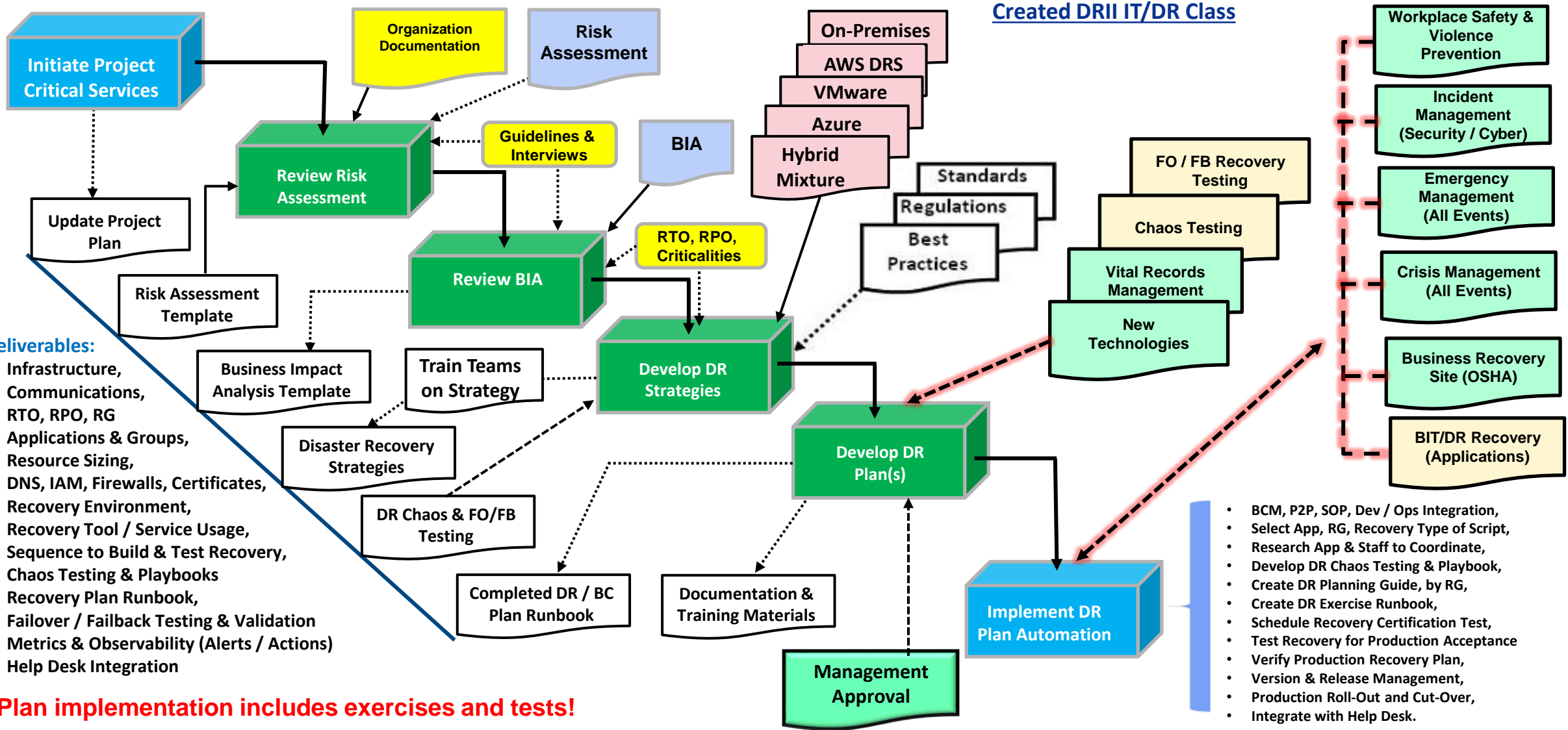
# Building and Implementing an Application

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



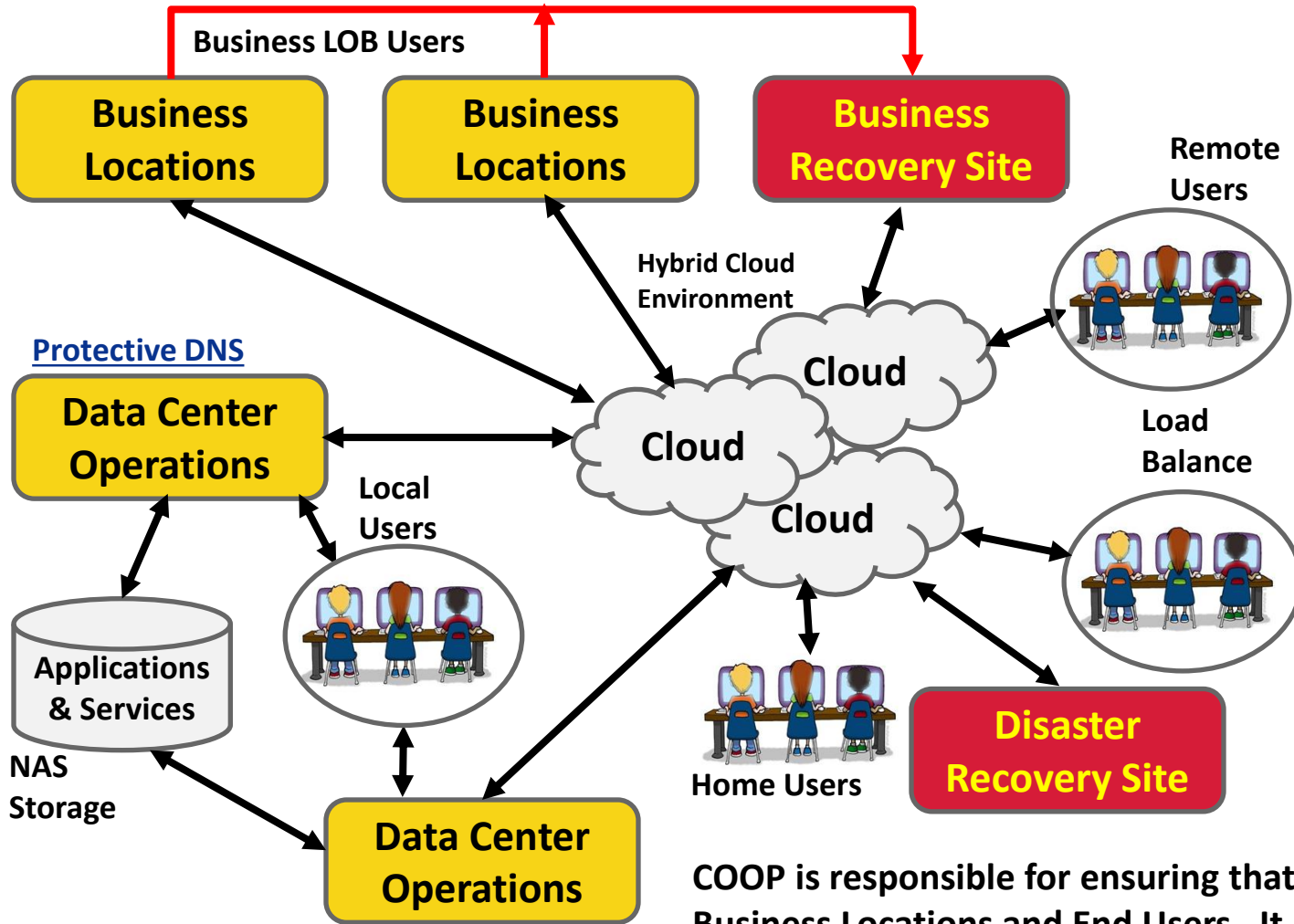
# Sample Recovery Plan Methodology

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



# Continuity of Operations Planning - COOP

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



COOP Lifecycle and Functions – Continuity of Operations and Government Programs

COOP is responsible for ensuring that Production Operations is always available to Business Locations and End Users. It requires a recovery capability for Business Locations and Data Center Operations that is satisfied by Business and Disaster Recovery Sites.

# Continuity Of Operations Planning - Guidelines

## Laws, Regulations, and Guidelines

- [NCPIP](#) - National Continuity Policy Implementation Plan
- [NSPD-51](#) – National Security Presidential Directive
- [HSPD-20](#)- Homeland Security Presidential Directive
- [NEF](#) – National Essential Functions
- [PMEF](#) – Primary Mission Essential Functions



### National Essential Functions

**Primary Mission Essential Functions (PMEFs)** are critical functions that must be continuously performed or resumed within **12 hours** after an event. These functions are essential for supporting or implementing the performance of **National Essential Functions (NEFs)** before, during, and after an emergency. PMEFs are validated by the **Federal Emergency Management Agency (FEMA) National Community Coordinator**. [FCD 1](#), [FCD2](#), [CGC 1](#) (federal Guidelines).

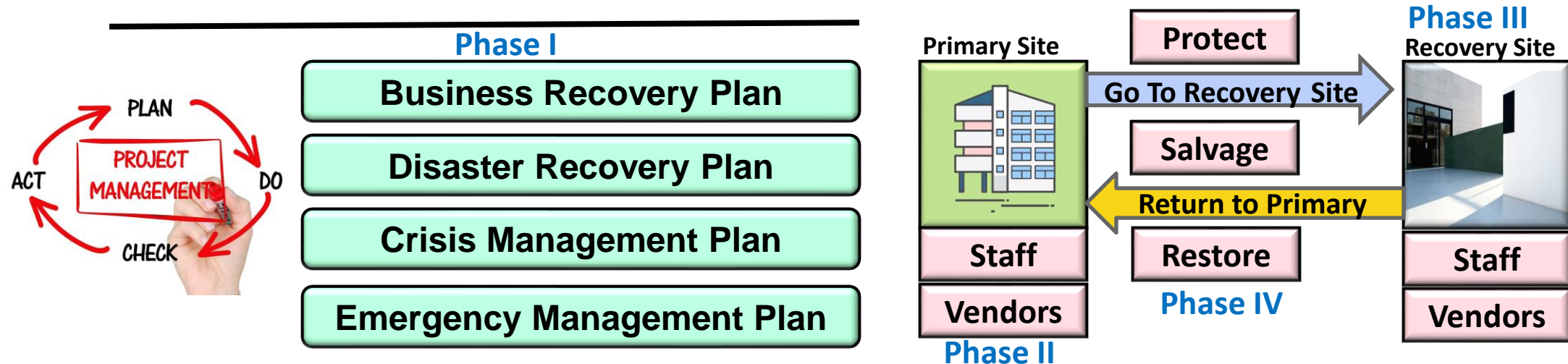
The NEFs serve as the foundation for all continuity programs and capabilities, and they are the primary focus of the Federal Government in catastrophic emergencies. [However, it's important to note that the Federal Government cannot maintain these functions and services without the support of the rest of the nation<sup>2</sup>.](#)



# Stages of the COOP Plan

## Four Phases of Continuity of Operations Activation

- **Phase I - Readiness and Preparedness** (Build and Test a Recovery Plan) – Continuity of Operations and Government Programs.
- **Phase II - Activation and Relocation:** plans, procedures, and schedules to transfer activities, personnel, records, and equipment to alternate facilities are activated (Activate Recovery Plan should a Disaster Event occur).
- **Phase III - Continuity Operations:** full execution of essential operations at alternate operating facilities is commenced (Run Production from an Alternate Site).
- **Phase IV – Reconstitution:** operations at alternate facility are terminated and normal operations resume (Protect, Salvage, Restore Primary Site, approve and return then to normal operations)



Testing continuity capability is crucial to ensure that organizations can effectively maintain essential functions during emergencies. Here are some ways continuity capability is tested:

## 1. Exercises and Drills:

- **Tabletop Exercises (TTX):** These discussions-based exercises simulate emergency scenarios, allowing participants to discuss continuity plans, roles, and responsibilities.
- **Functional Exercises:** These involve real-time actions and coordination among personnel. They test specific aspects of continuity plans.
- **Full-Scale Exercises:** These comprehensive exercises simulate actual emergencies, involving multiple agencies and stakeholders.

## 2. Training Programs:

- FEMA offers courses like "[An Introduction to Exercises](#)" and "[Exercise Evaluation and Improvement Planning](#)" to train continuity practitioners.
- The **Homeland Security Exercise and Evaluation Program (HSEEP)** provides principles for exercise program management.

## 3. Continuity Evaluation Tools:

- The **Continuity Evaluation Tool** assesses federal continuity plans, programs, and procedures.
- The **Continuity Assessment Tool** helps non-federal entities identify strengths and areas for improvement.

## 4. Strategic Planning:

- Organizations use the **Multi-Year Strategic Plan Template** to sustain and enhance continuity capabilities over a five-year period.

## 5. Specific Scenarios:

- Organizations conduct exercises related to specific threats (e.g., pandemic influenza) or operational challenges (e.g., telework scenarios).

[Remember that testing continuity capability involves a combination of training, exercises, and strategic planning to ensure readiness during emergencies<sup>1234</sup>.](#)

Learn more

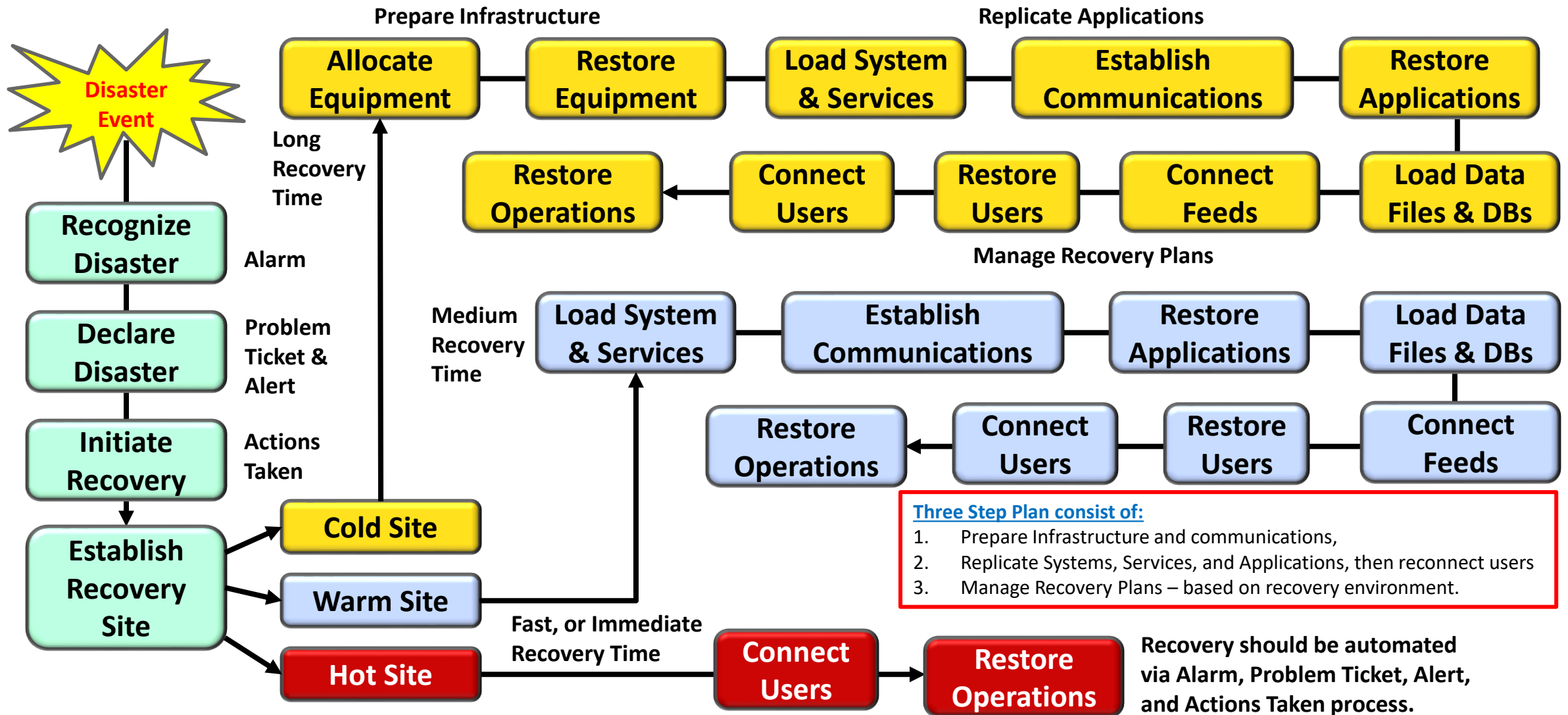
[1 fema.gov](#)

[2 en.wikipedia.org](#)

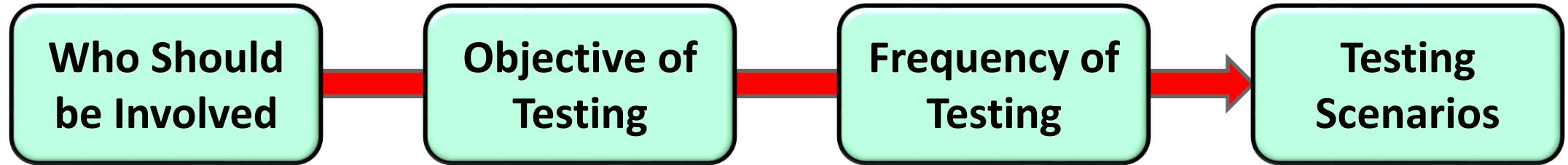
[3 fema.gov](#)

[4 jensenhughes.com](#)

# Sequence of Events to enact a Recovery Operation



# Testing Business Continuity Plans



- All Employees,
- Emergency Response Team
- Business Continuity Team
  - Location
  - Data Center
  - Network
  - Storage
- Crisis Communication Contacts
- Stakeholders
- Management

- Identify Gaps & Weaknesses in Recovery Plans
- Ensure Business Objectives are met
- Review responses to various disruptions
- Recognize areas for improvement, improve process and update,
- Continue until perfect.

- Business Continuity and Disaster Recovery Plan review and testing should be performed at least quarterly.
- Shift from one application / service to another to provide continuous testing and protection

- Data Loss Breach
- Data Recovery
  - What Data
  - Frequency
  - Recovery Solution
  - Test & Monitor
- Power Outage
- Network Outage
- Physical Disruption
- Emergency, or Natural Disaster event.

# IT/DR Testing Process Overview

## What to Test

## Test Categories

## How to Test

## Results

- Business Continuity Management Organization, including:
  - Structure;
  - Services and Functions;
  - Procedures;
  - Job Descriptions
  - Resources;
  - Vendors and Suppliers; and,
  - Personnel.
- Risk Management Guidelines, including:
  - Risk Appetite, GRC, CIA, RMF,CSF;
  - Gaps and Exceptions;
  - Obstacles;
  - Legal and Regulatory;
  - Insurance and Protection.
- Security, including:
  - Vital Records;
  - Firewalls;
  - Intrusion Detection;
  - SIEM, SOAR, Monitoring;
  - Domain Management;
  - Access Controls.
- Production Operations Support

- Data Sensitivity. Including:
  - Ownership;
  - Data Criticality;
  - Legal & Regulatory;
  - Usage Categories (Create, Read, Update, Delete).
  - Access Controls using:
    - Application ID,
    - User ID;
    - Password;
    - Single Log-On;
    - Group Log-on.
- Vital Records Management:
  - Backup / Recovery;
    - Mirroring;
    - Incremental; and,
    - Media Type.
  - RPO, RTO & Ability
  - Vaulting
- IT Operations Management, IT Systems Management, Production Acceptance, Support, Maintenance, Change Management

- Business Continuity Management, including:
  - Disaster Recovery Site;
  - Business Recovery Site;
  - Primary, Secondary Site;
  - Connectivity;
  - Functionality.
- Risk Assessment, including:
  - Laws and Regulations;
  - “Audit Universe”;
  - Audit Schedule;
  - Mitigate & Mediate;
  - Insurance and Protection;
  - Attestation.
- Security, including:
  - Firewalls & Security;
  - Intrusion Detection;
  - Access Controls;
  - Network Communications;
  - Tracking and Logging;
  - Reporting & Actions.
- Recovery Group, RTO, RPO, RTC
- Chaos Testing & Resilience Hub

- Business Continuity Success, including:
  - Business Site Recovery;
  - IT Services Recovered;
  - Validated Plans;
  - Recovery Sites Verified;
  - Personnel Trained.
- Risk Assessment, including:
  - Technology Validated;
  - Financial Needs Met;
  - Supply Chain & Vendors;
  - Legal and Regulatory;
  - Insurance and Protection.
- Security, including:
  - Successfully Tested;
  - Meets all Requirements;
  - Management and User Sign-Off on Testing.
- Production Operations Supported:
- Recovery Certification, by Recovery Grp.
- Documentation & Training
- Problem, Cyber and Recovery Playbooks
- Support and Maintenance
- Change Management and QA

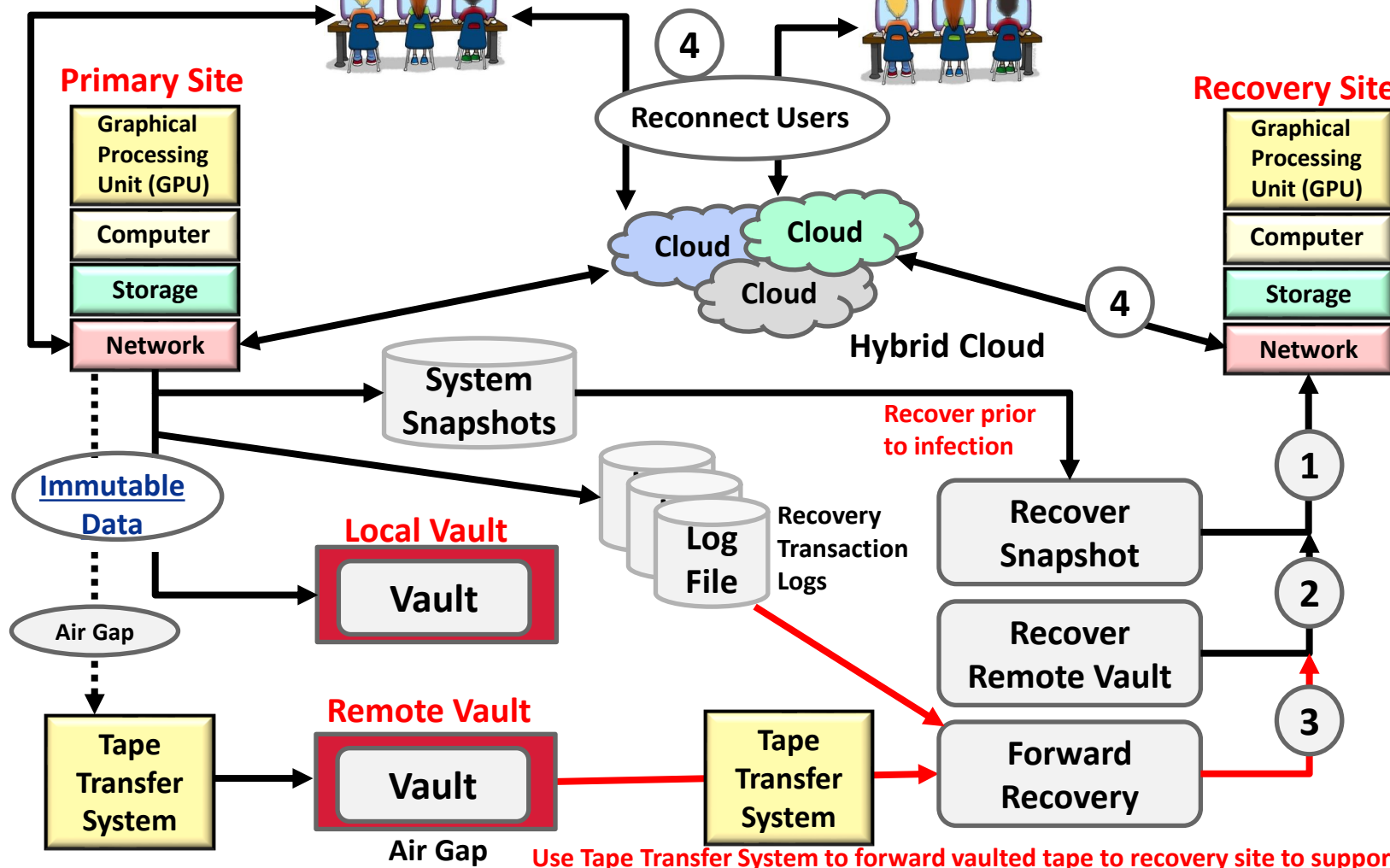
# System Recovery – Even with Ransomware

Local Users reconnected via Cloud

Local Users

Remote Users

Remote Users reconnected via Site Recovery

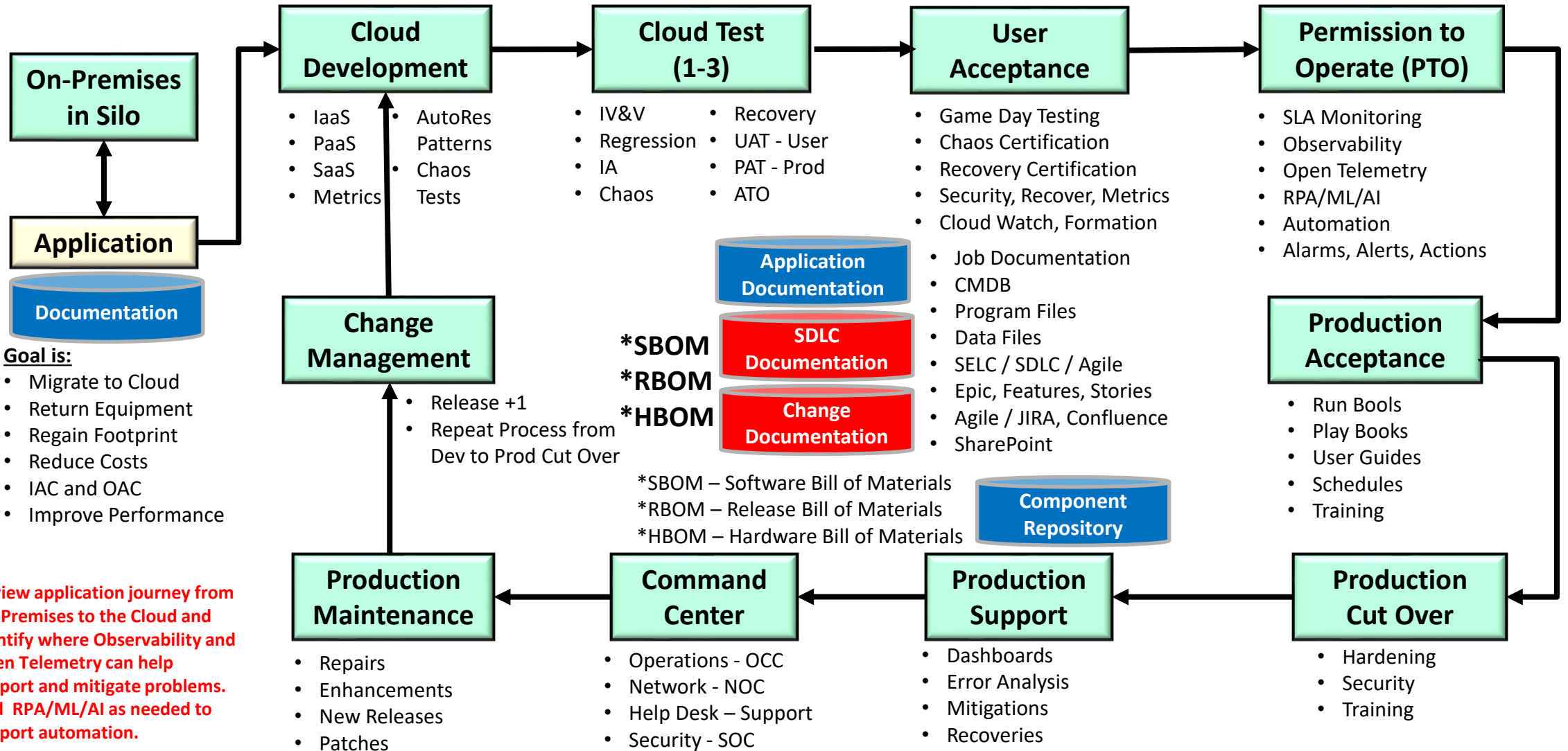


Immutable Data cannot be changed once stored and using an Air Gap for vaulting data will safeguard it from a hacker's ability to encrypt data via Ransomware or other malware attack.

## Recovery Process:

1. Recover System Snapshot prior to infection to restore 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.

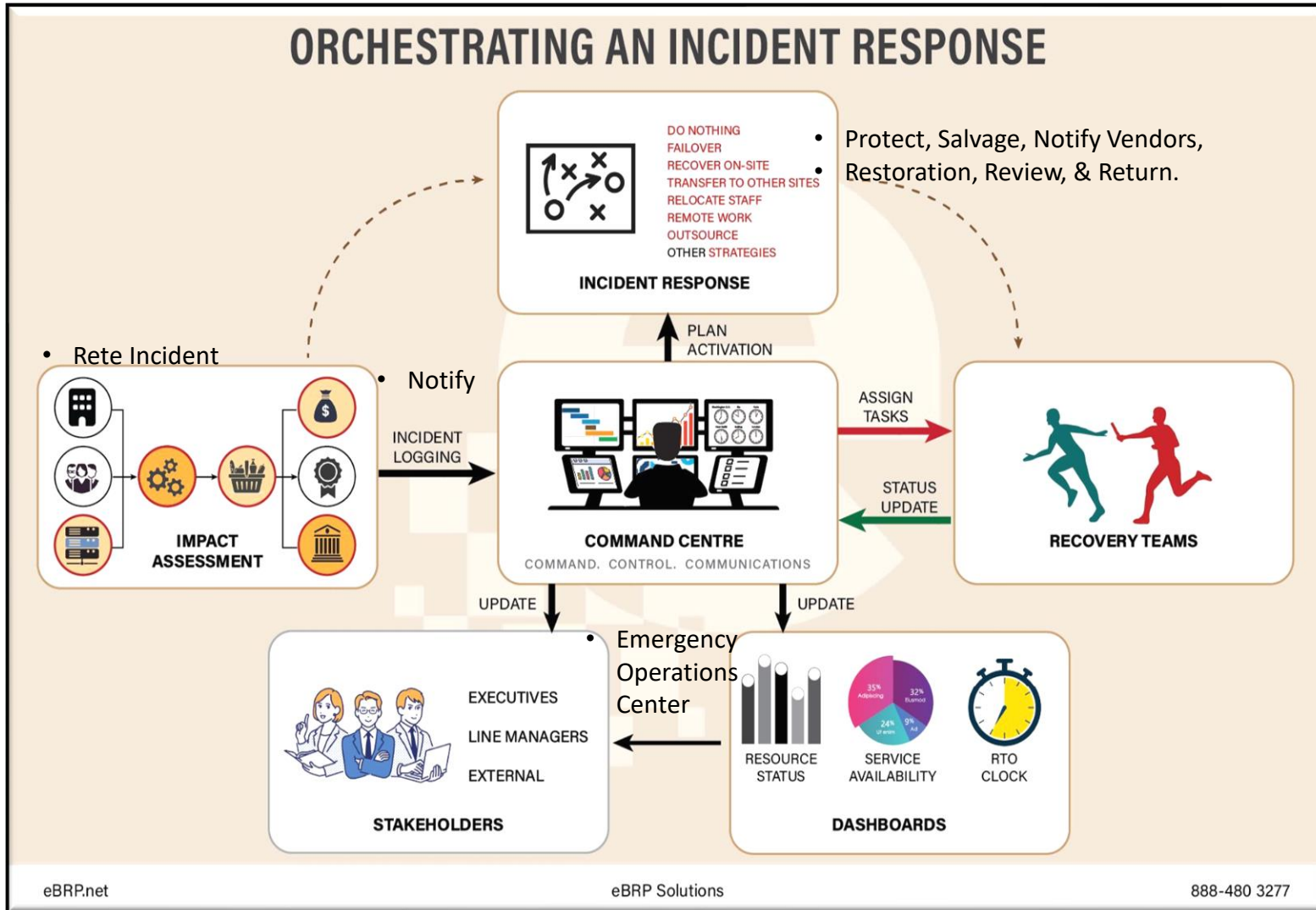
# Migrating Applications to the Cloud



Review application journey from On-Premises to the Cloud and identify where Observability and Open Telemetry can help support and mitigate problems. Add RPA/ML/AI as needed to support automation.

# Business Continuity Command Center

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



## Incident and Recovery Management.

1. Incident Occurs – Problem Ticket, Alarm
2. Impact Assessment performed – Problem Ticket completed and failing component
3. Command Center notifies Recovery Teams
4. Stakeholders are informed
5. Dashboards Maintained
6. Status Reports provided
7. Incident Tracked until Completed
8. Post Incident Review
9. Improvements
10. Update & Maintain Recovery Plans

### Overall Benefits

**Efficiency:** Centralized control improves response times and reduces the duplication of efforts.

**Effectiveness:** Enhanced coordination and resource allocation lead to more effective incident handling.

**Compliance and Reporting:** Ensures that response efforts are documented and reported, meeting regulatory and compliance requirements.



# Resiliency Operations Center (ROC)

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

Coordinating Resiliency throughout the organization

ICT – Information and Communications Technology



**THE ICOR**

THE INTERNATIONAL CONSORTIUM OF ORGANIZATIONAL RESILIENCE

(C) 2010-2016 ALL RIGHTS RESERVED

# Resiliency Operational Center (ROC)

The **Resilience Operations Center (ROC)** is a strategic framework that organizations adopt to enhance their operational resilience and effectively manage supply chain risks. Let's delve into the key aspects of ROC:

## 1. Purpose and Principles:

1. The ROC aims to achieve and maintain operational resilience by aligning risk management with organizational goals.
2. It breaks down silos within an organization and modernizes threat detection and mitigation using technologies like automation, artificial intelligence, and natural language processing.
3. [By adhering to these principles, organizations gain insight and agility to capitalize on unforeseen opportunities<sup>1</sup>.](#)

## 2. Challenges to Operational Resilience:

1. Operational resilience breakdowns can occur due to various factors:
  1. Weak governance processes at different levels (board, senior management, etc.).
  2. Incomplete business continuity management for critical operations functions.
  3. Lack of scenario planning and analysis to anticipate disruptions.
  4. Insecure information systems and ineffective monitoring.
2. [Addressing these inefficiencies is crucial to prevent financial losses and mitigate operational risks<sup>1</sup>.](#)

## 3. ROC Success Factors:

1. Understand industry-specific operational risks.
2. Prioritize IT hygiene, including active threat monitoring and security patching.
3. Combine scenario planning with forecasting to refine plans.
4. [Maintain secure information systems and effective monitoring practices<sup>1</sup>.](#)

[In summary, the ROC framework provides organizations with the tools to proactively manage risks, enhance resilience, and respond effectively to supply chain challenges<sup>2</sup>. Whether it's financial services, manufacturing, or any other industry, the ROC helps organizations stay prepared and agile in the face of modern risks<sup>3</sup>.](#) 🌟

# Benefits derived from a Resiliency Operations Center

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

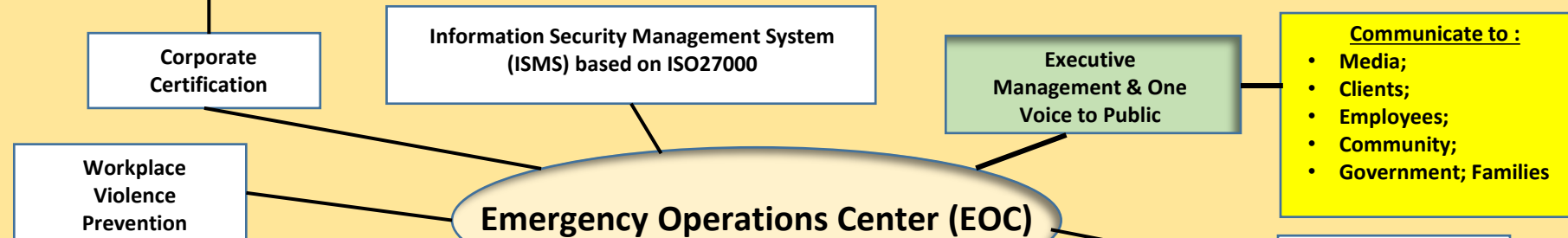
The **Resilience Operations Center (ROC)** represents a new approach to modern supply chain security and continuity, delivered through an enterprise-wide framework that ensures risk management objectives are tied to organizational goals. It brings previously siloed groups together to form agile and informed teams that are empowered to use data intelligently and react quickly to changing circumstances. The ROC framework is deployed in a variety of industries, and they are using ROCs to dramatically change outcomes for the better.

**A ROC is effective at fostering Operational Resilience** because it helps organizations overcome difficult internal challenges, including:

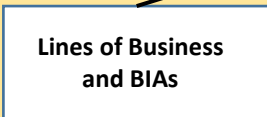
- **Shifting behavior from response to prevention.** Deep, comprehensive planning helps teams anticipate events, evaluate alternatives, prevent disruptions, and model all scenarios and options. Reacting to events as they happen is not sufficient in today's competitive market.
- **Making risk management an organization-wide job,** not the domain of one person or team. Most approaches to managing risk are siloed within business units, such as procurement, supply chain operations, and IT, or in single focus organizations, such as information security and compliance. When everyone is a stakeholder, organizations improve how they coordinate, collaborate, prepare, and respond.
- **Managing risk beyond the walls of your company.** Organizations rely on an extensive network of suppliers and partners for developing and producing their products and services. Identifying relationships in the extended supply chain to the Nth tier helps organizations decide if those connections are good or bad business choices, thereby identifying and preventing potential risk. And, most importantly, remember that you are a third party to myriad other organizations, which are now looking at you through their own risk management lens.

# Emergency Operations Center (EOC)

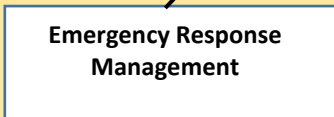
Thomas Bronack  
 Email: [bronackt@dcag.com](mailto:bronackt@dcag.com)  
 Phone: (917) 673-6992



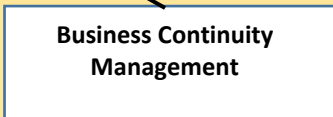
OSHA, OEM, DHS



- Locations,
- Employees,
- Infrastructure,
- Equipment,
- Systems,
- Applications,
- Services,
- Supplies,
- Customers,
- RTO, RTC, RPO.



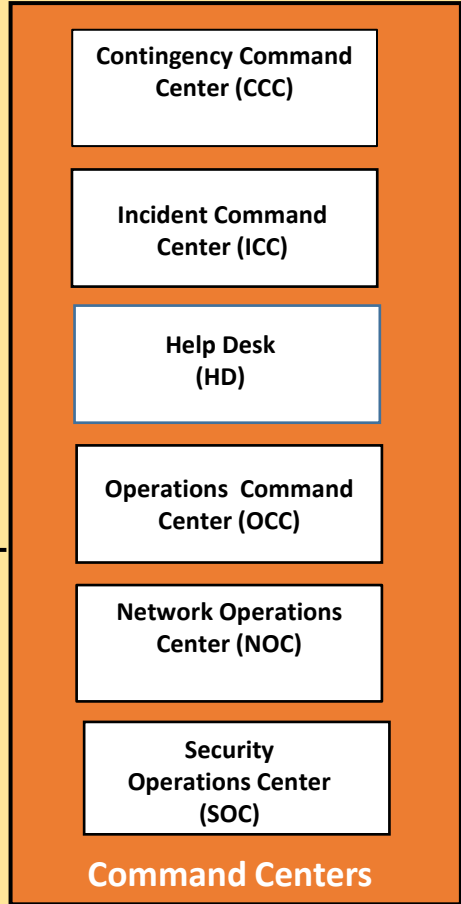
- State and Local Government,
- First Responders (Fire, Police, & EMT),
- Department of Homeland Security (DHS),
- Office of Emergency Management (OEM),
- Local Community.



- Risk Management (COSO),
- Disaster Recovery,
- Business Continuity,
- Crisis Management,
- Emergency Management,
- Workplace Violence Prevention,
- Failover / Failback,
- Protection, Salvage & Restoration.



- Service Level Agreements (SLA) & Reporting (SLR),
- Systems Development Life Cycle (SDLC),
- CobIT, ITIL, CMMI, and FFIEC,
- ISO Guidelines,
- Audit and Human Resources,
- Six Sigma or Equivalent for Performance and Workflow Management



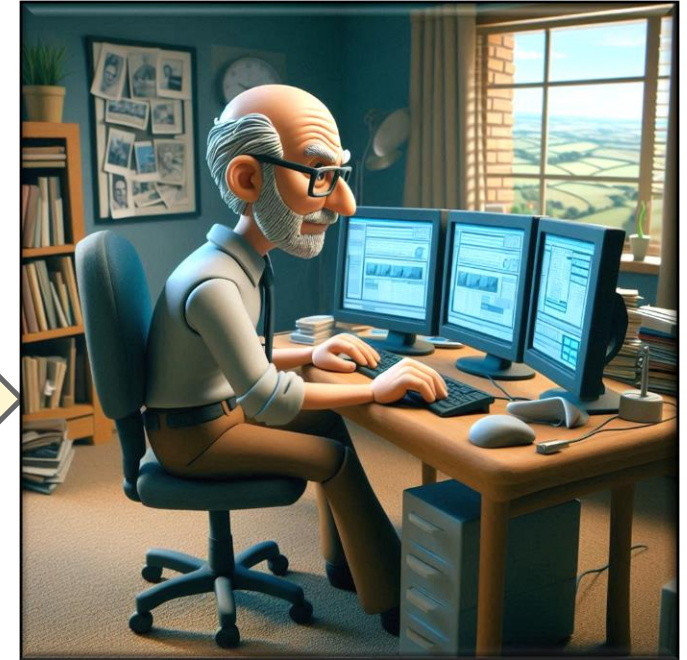
# Reaching out to assist our clients

Thomas Bronack  
Email: [bronackt@dcag.com](mailto: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  
[Website: http://www.dcag.com](http://www.dcag.com)  
[bronackt@dcag.com](mailto:bronackt@dcag.com)  
[bronackt@gmail.com](mailto:bronackt@gmail.com)  
917-673-6992