Created by:

Thomas Bronack, CBCP
Bronackt@gmail.com
Cell: (917) 673-6992

Thomas Bronack
Overview of Services

Enterprise Resiliency

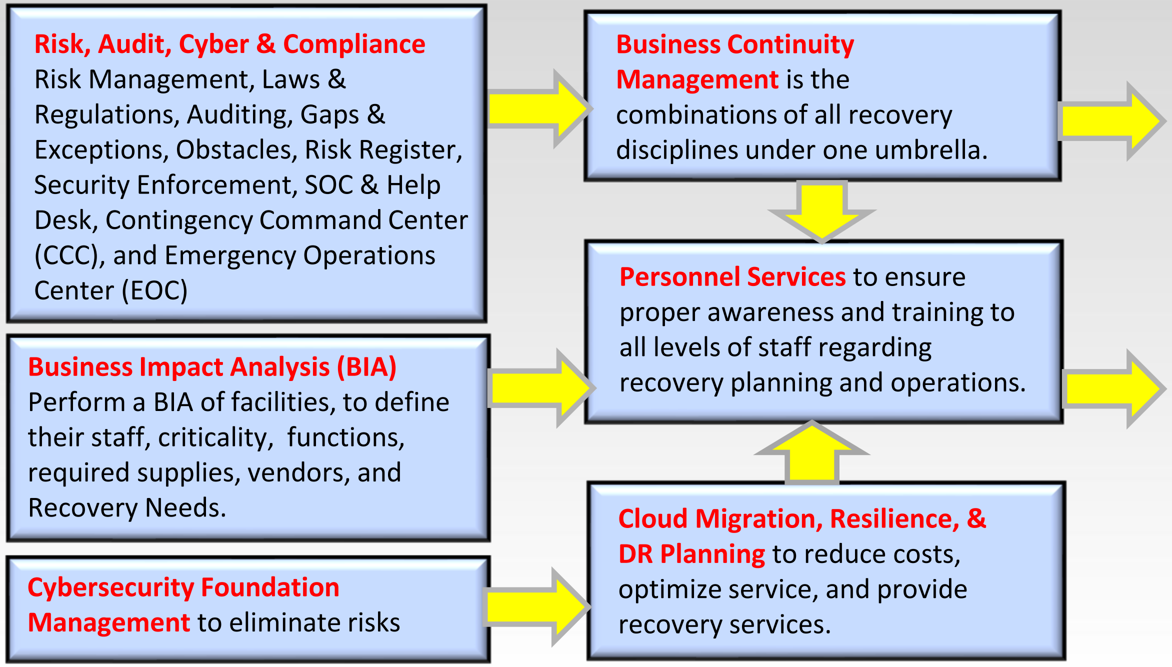
Including

Business Continuity & Disaster Recovery

with

Tom Bronack

Business Continuity, IT Disaster Recovery, Business Location Recovery (COOP), Workplace Safety and Violence Prevention, Emergency Management, Crisis Management, Supply Chain Management, Site Security / Salvage / Restoration, and Application Cloud Migration for Efficiency and Failover / Failback Recovery Operations, with Identity Management, Risk / Audit Management, Asset Management, and Infrastructure Management



Risk, Audit, Cyber & Compliance Risk Management, Laws & Regulations, Auditing, Gaps & Exceptions, Obstacles, Risk Register, Security Enforcement, SOC & Help Desk, Contingency Command Center (CCC), and Emergency Operations Center (EOC)

Business Impact Analysis (BIA) Perform a BIA of facilities, to define their staff, criticality, functions, required supplies, vendors, and Recovery Needs.

Cybersecurity Foundation Management to eliminate risks

Business Continuity Management is the combinations of all recovery disciplines under one umbrella.

Personnel Services to ensure proper awareness and training to all levels of staff regarding recovery planning and operations.

Cloud Migration, Resilience, & DR Planning to reduce costs, optimize service, and provide recovery services.

Enterprise Resilience components and disciplines, include:

- **IT Disaster Recovery** – to protect the data center and its infrastructure
- **Business Location Recovery –** to protect business locations and their staff.
- **Workplace Safety and Violence Prevention** – to protect personnel from harm or Active Shooter situations.
- **Emergency Management** – to protect the company from interruptions due to natural and man-made disaster events. Adherence to OSHA regulations.
- **Crisis Management** – to protect the company and its staff from Crisis Situations that can cause harm to staff and interrupt the business from delivering services.
- **Supply Chain Management** – to ensure the continuous supply of materials as needed supplies during normal and recovery operations in compliance to government regulations.
- **Site Security, Salvage, and Restoration** during and after a business location has a disaster event.
- **Application Migration and DR Planning** for On-Premises, Cloud, and Hybrid applications to improve efficiency, performance, and Failover / Failback operations
- **Infrastructure as Code (IaC), Observability as Code (OaC)** and **Performance Monitoring**.

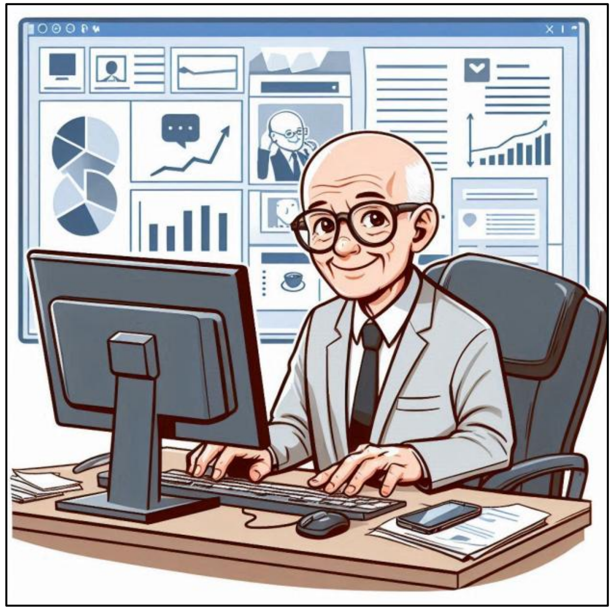
A word from Thomas Bronack

I am a **senior level manager** with in-depth experience in E**nterprise Resilience, Vulnerability Management, Operations Support, 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.

This document provides guidelines on **protecting your 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.

I hope you find the information contained in this presentation interesting and helpful!



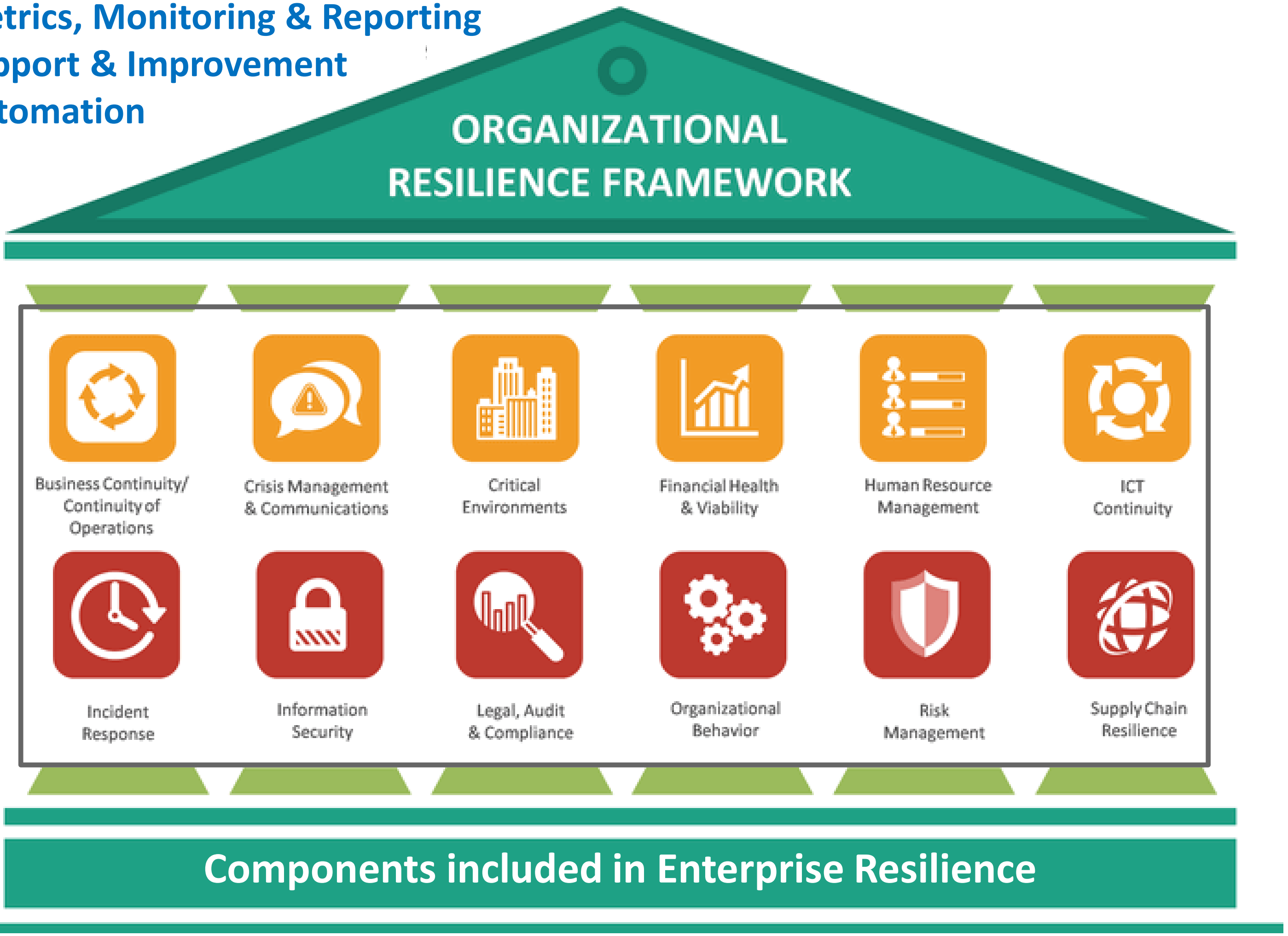
A strong generalist with extensive IT industry experience, ready to help you.

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

What is Enterprise Resilience comprised of?

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

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


ORGANIZATIONAL RESILIENCE FRAMEWORK
Business Continuity/ Continuity of Operations
Crisis Management & Communications
Critical Environments
Financial Health & Viability
Human Resource Management
ICT Continuity
Incident Response
Information Security
Legal, Audit & Compliance
Organizational Behavior
Risk Management
Supply Chain Resilience
Components included in Enterprise Resilience

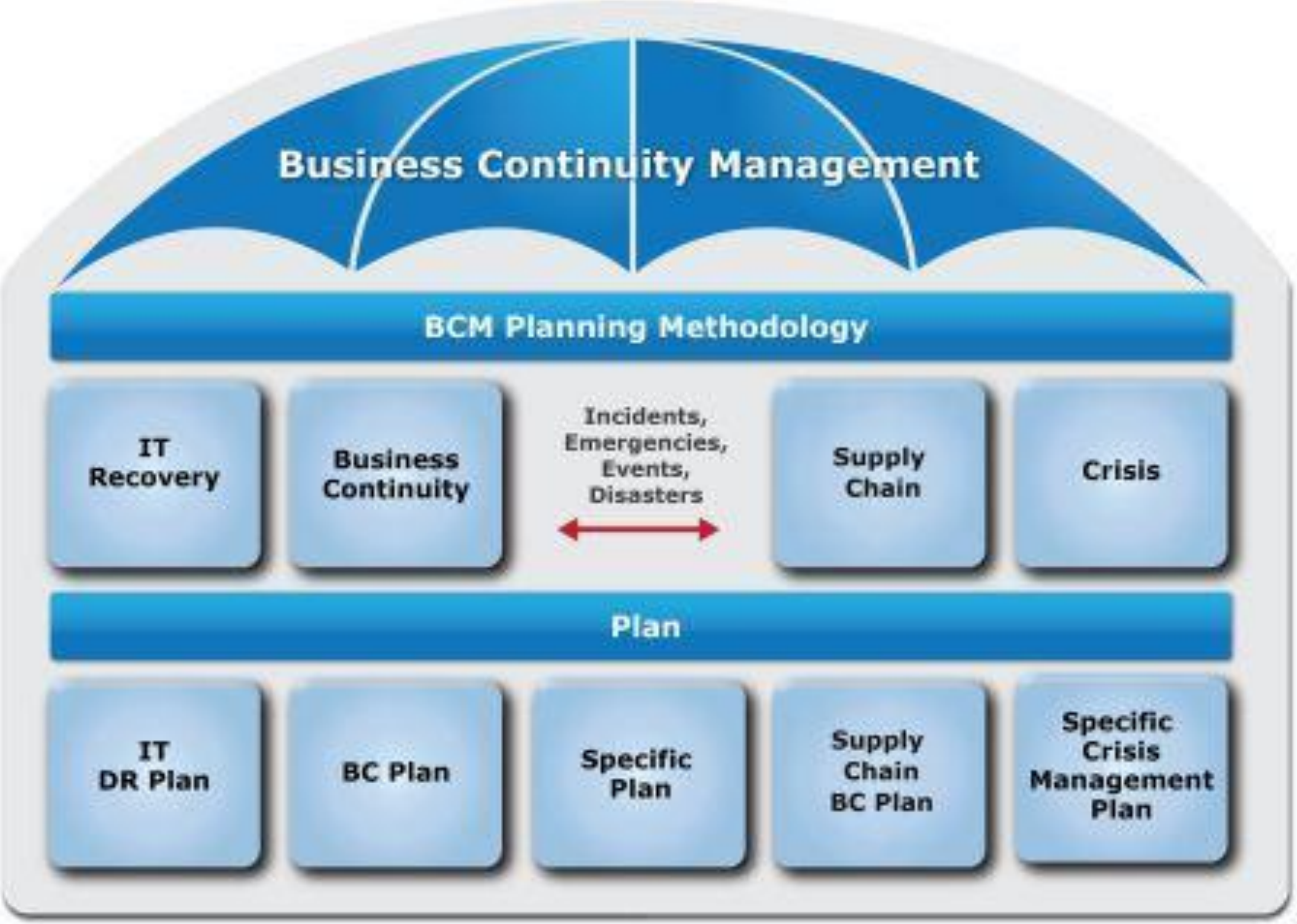
Enterprise Resilience consists of:

- 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

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

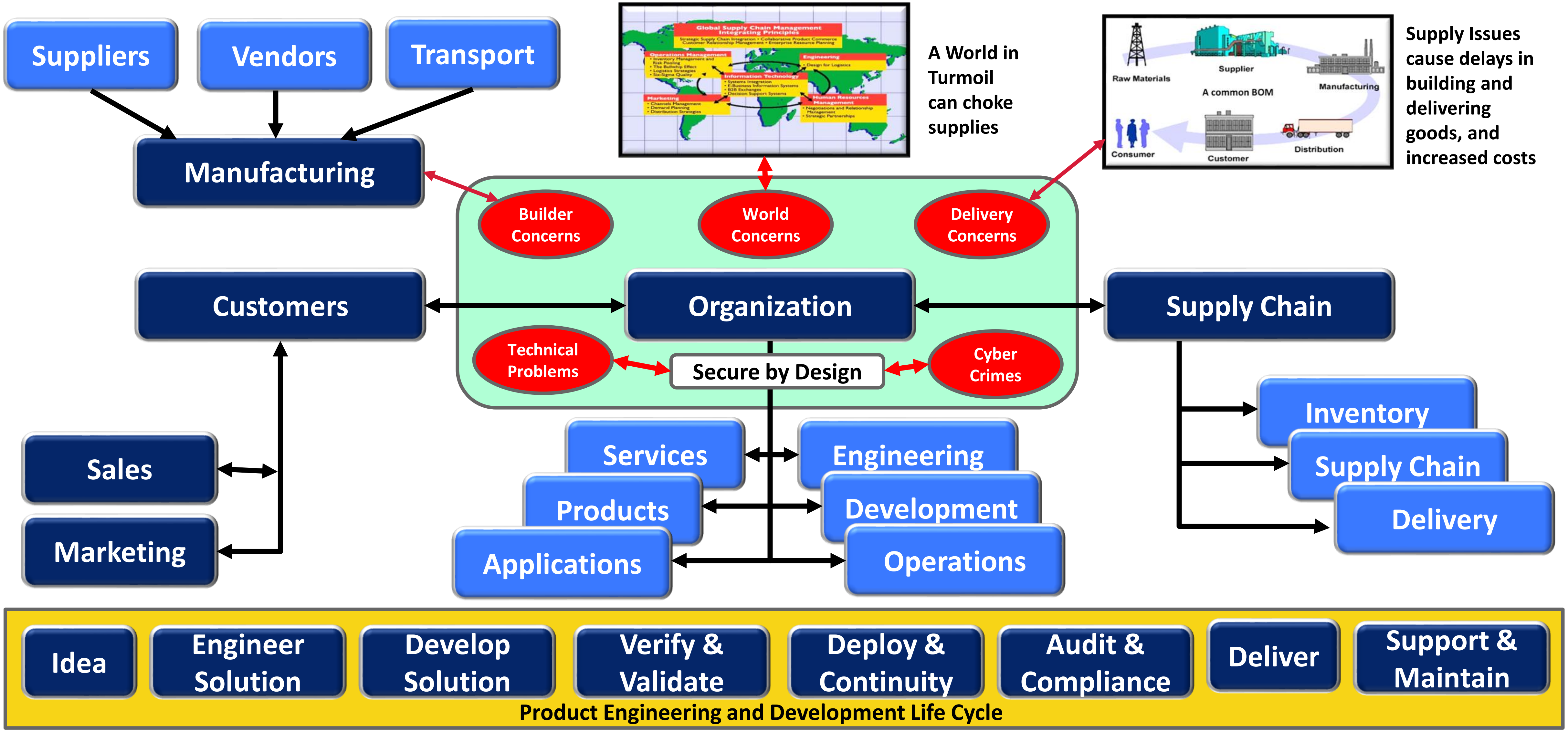
- **Preserve** the company Brand and Reputation, while protecting personnel.
- **Plan** for natural and man-made disaster events to reduce / eliminate outages.
- **Identify** and eliminate Risks and Business Flow Impacts to the company, its people, and resources.
- **Eliminate** Single-Point-Of-Failure.
- **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

Protecting Organization is more difficult than ever

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



Global Supply Chain Management
Integrating Principles
Strategic Supply Chain Integration • Collaborative Product Commerce
Customer Relationship Management • Enterprise Resource Planning
Operations Management
• Inventory Management and Risk Pooling
• The Bullwhip Effect
• Logistics Strategies
• Six-Sigma Quality
Engineering
• Design for Logistics
Information Technology
• Systems Integration
• E-Business Information Systems
• B2B Exchanges
• Decision Support Systems
Marketing
• Channels Management
• Demand Planning
• Distribution Strategies
Human Resources Management
• Negotiations and Relationship Management
• Strategic Partnerships
Raw Materials
Supplier
Manufacturing
A common BOM
Consumer
Customer
Distribution

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

Sales

Marketing

Services

Engineering

Products

Development

Applications

Operations

Inventory

Supply Chain

Delivery

Idea

Engineer Solution

Develop Solution

Verify & Validate

Deploy & Continuity

Audit & Compliance

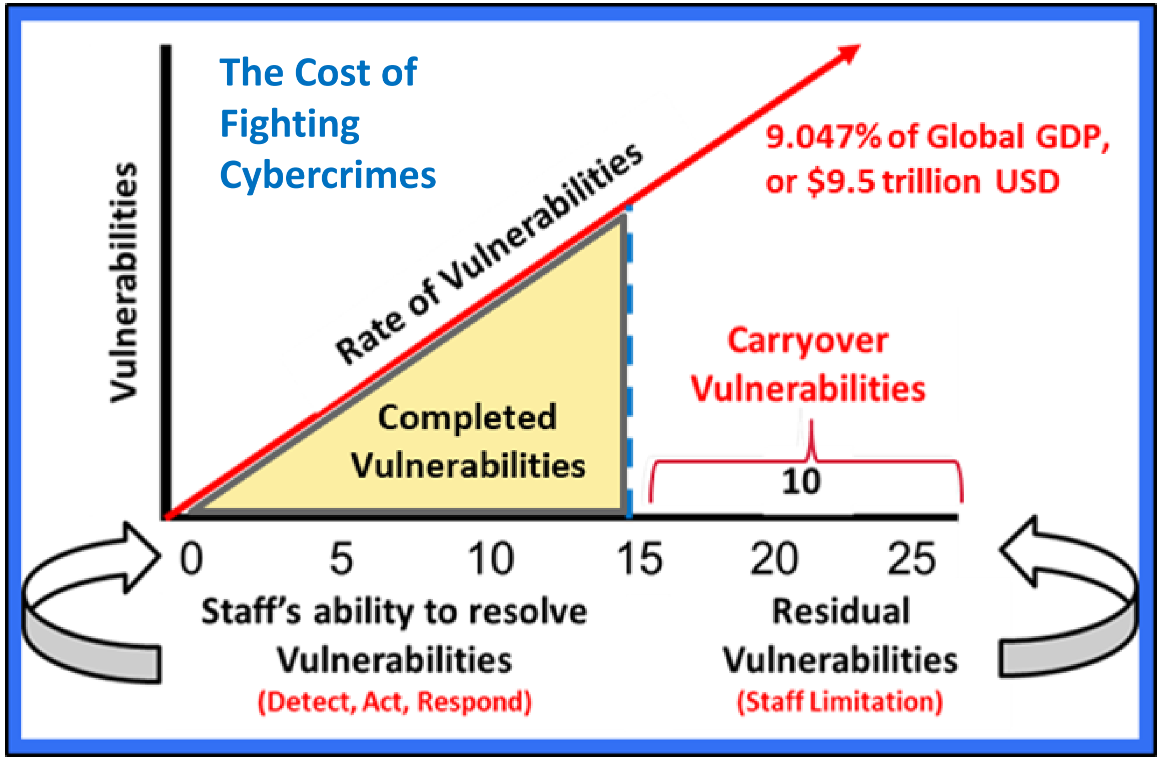
Deliver

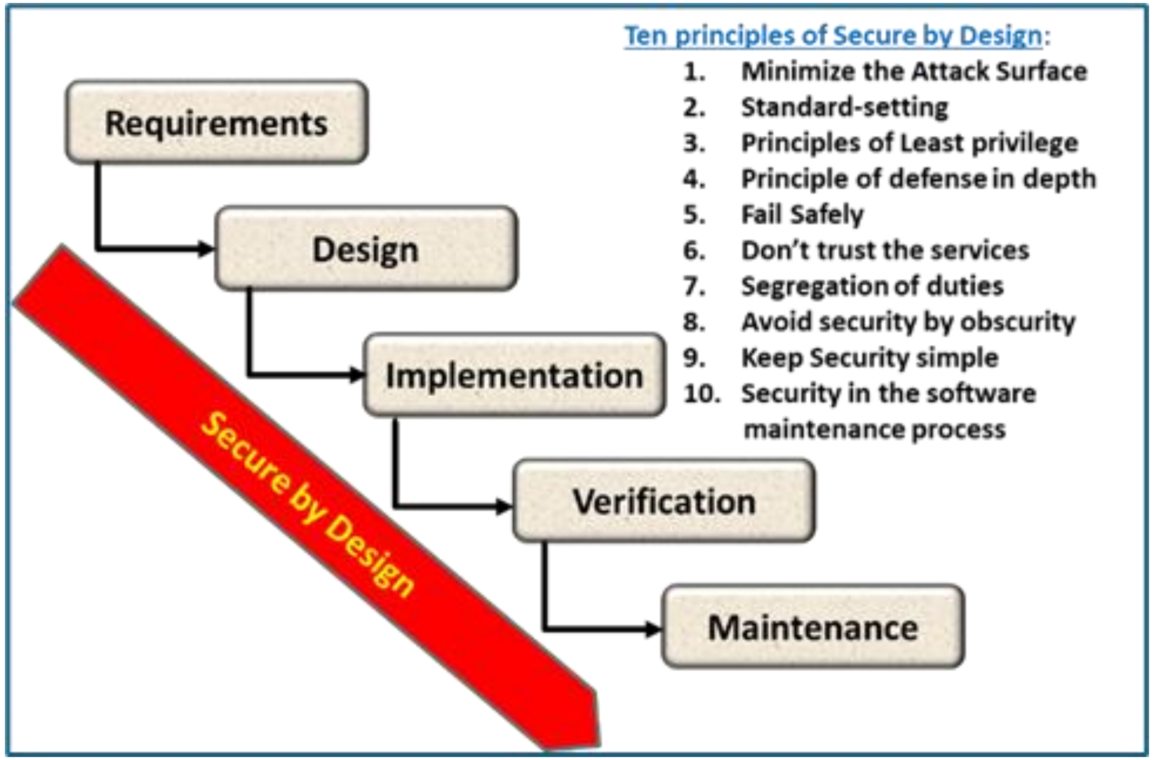
Support & Maintain

Product Engineering and Development Life Cycle

Fighting Cybercrime Costs with Secure by Design

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





Ten principles of Secure by Design:

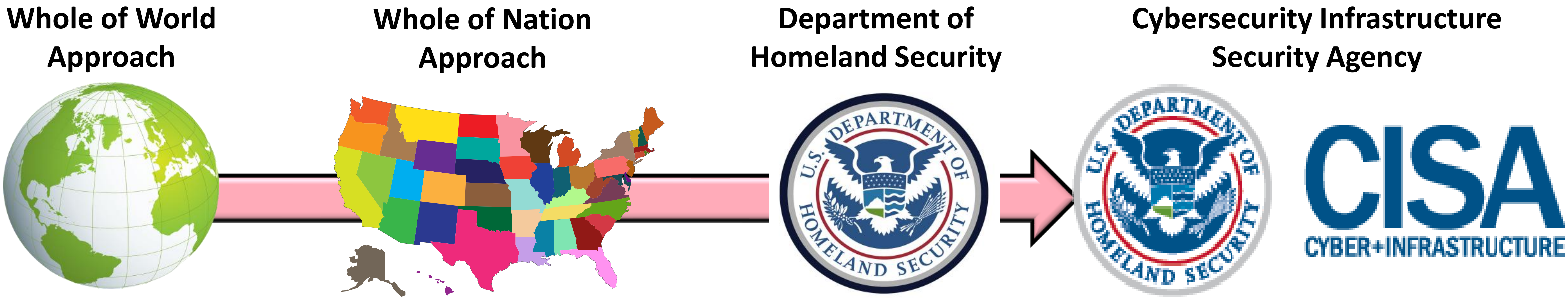
1. Minimize the Attack Surface
2. Standard-setting
3. Principles of Least privilege
4. Principle of defense in depth
5. Fail Safely
6. Don't trust the services
7. Segregation of duties
8. Avoid security by obscurity
9. Keep Security simple
10. Security in the software maintenance process

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
Phone: (917) 673-6992



Whole of World Approach

Whole of Nation Approach

Department of Homeland Security

Cybersecurity Infrastructure Security Agency

U.S. DEPARTMENT OF HOMELAND SECURITY
U.S. DEPARTMENT OF HOMELAND SECURITY
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:

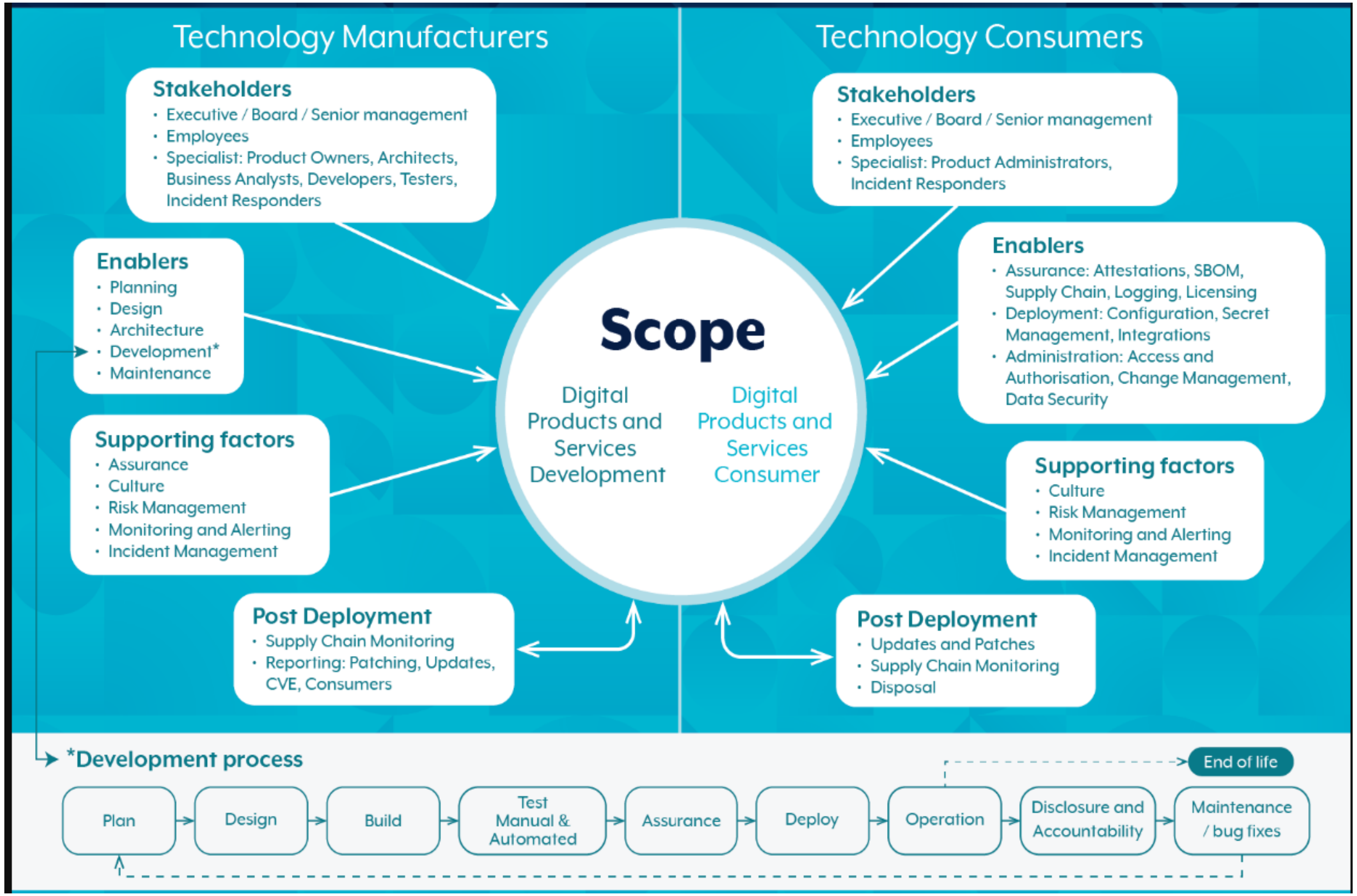
1. Detect Vulnerability (SBOM)
2. Assess the Risk (CVE)
3. Prioritize Remediation (CVSS, KVE, EPSS)
4. Confirm Remediation
5. Optimize through automation
6. Advance the use of BOMs for Software, Release Control, and Artificial Intelligence

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
Phone: (917) 673-6992



Technology Manufacturers

Stakeholders
- Executive / Board / Senior management
- Employees
- Specialist: Product Owners, Architects, Business Analysts, Developers, Testers, Incident Responders

Enablers
- Planning
- Design
- Architecture
- Development*
- Maintenance

Supporting factors
- Assurance
- Culture
- Risk Management
- Monitoring and Alerting
- Incident Management

Post Deployment
- Supply Chain Monitoring
- Reporting: Patching, Updates, CVE, Consumers

Technology Consumers

Stakeholders
- Executive / Board / Senior management
- Employees
- Specialist: Product Administrators, Incident Responders

Enablers
- Assurance: Attestations, SBOM, Supply Chain, Logging, Licensing
- Deployment: Configuration, Secret Management, Integrations
- Administration: Access and Authorisation, Change Management, Data Security

Supporting factors
- Culture
- Risk Management
- Monitoring and Alerting
- Incident Management

Post Deployment
- Updates and Patches
- Supply Chain Monitoring
- Disposal

Scope

Digital Products and Services Development

Digital Products and Services Consumer

*Development process

Plan → Design → Build → Test Manual & Automated → Assurance → Deploy → Operation → Disclosure and Accountability → Maintenance / bug fixes

End of life

<u>What is Secure by Design:</u>

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.

New Laws and Regulations requiring SBOMs

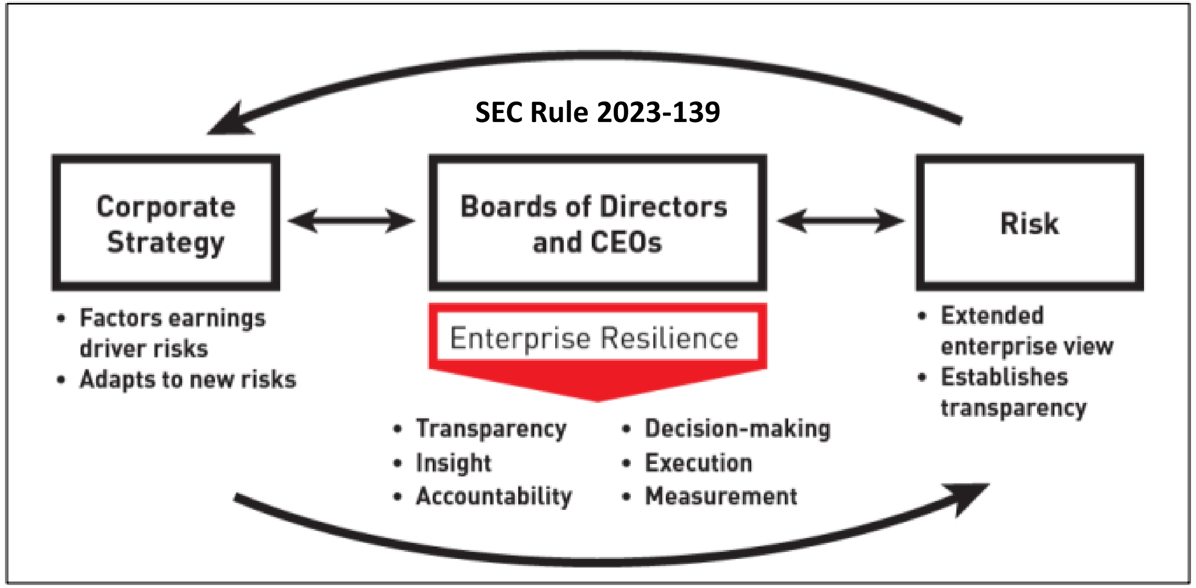
Thomas Bronack
Email: bronackt@dcag.com
Phone: (917) 673-6992

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

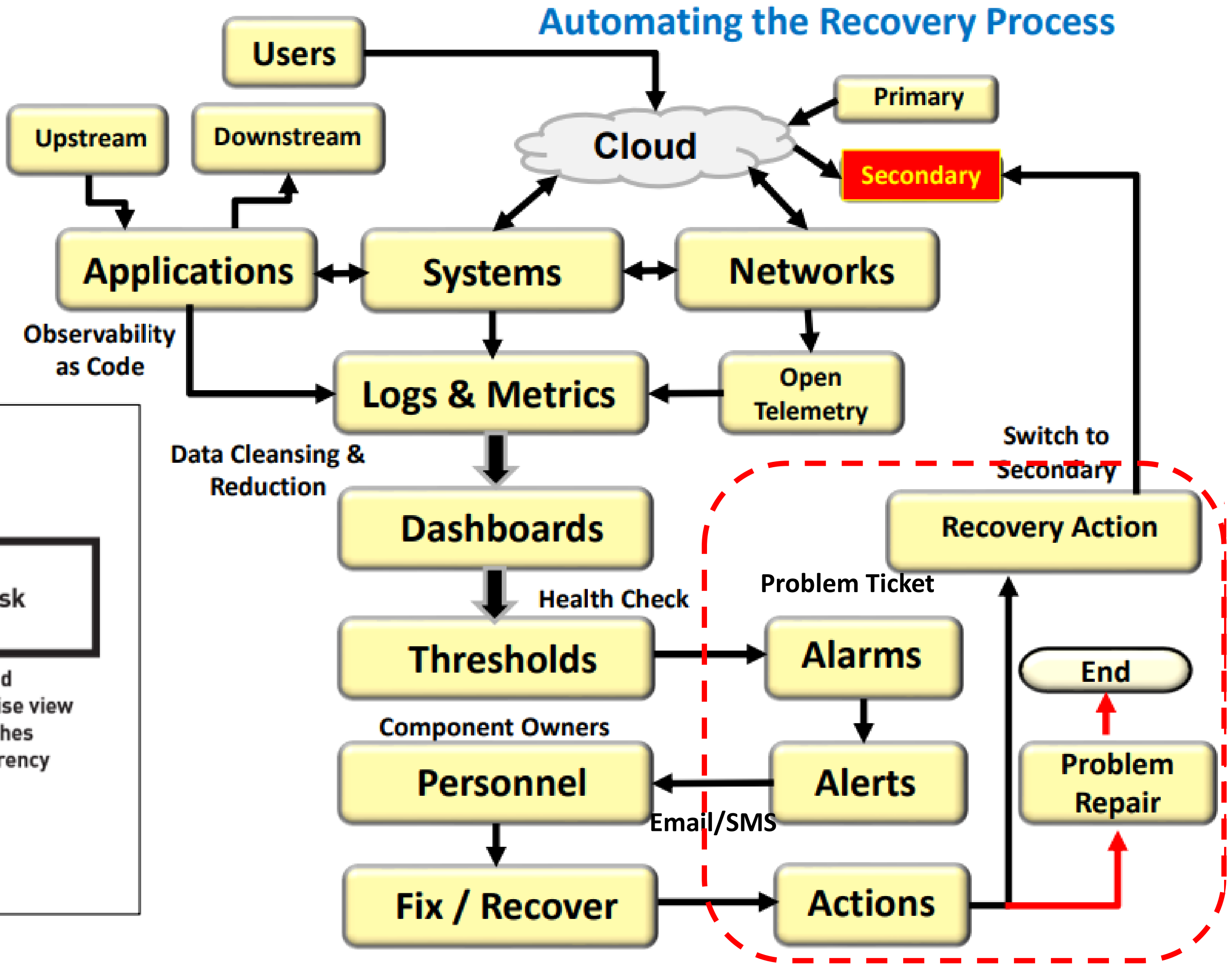
Board of Directors concerns

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

The Board of Director's is responsible for protecting the company, providing continued operation and services, 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.

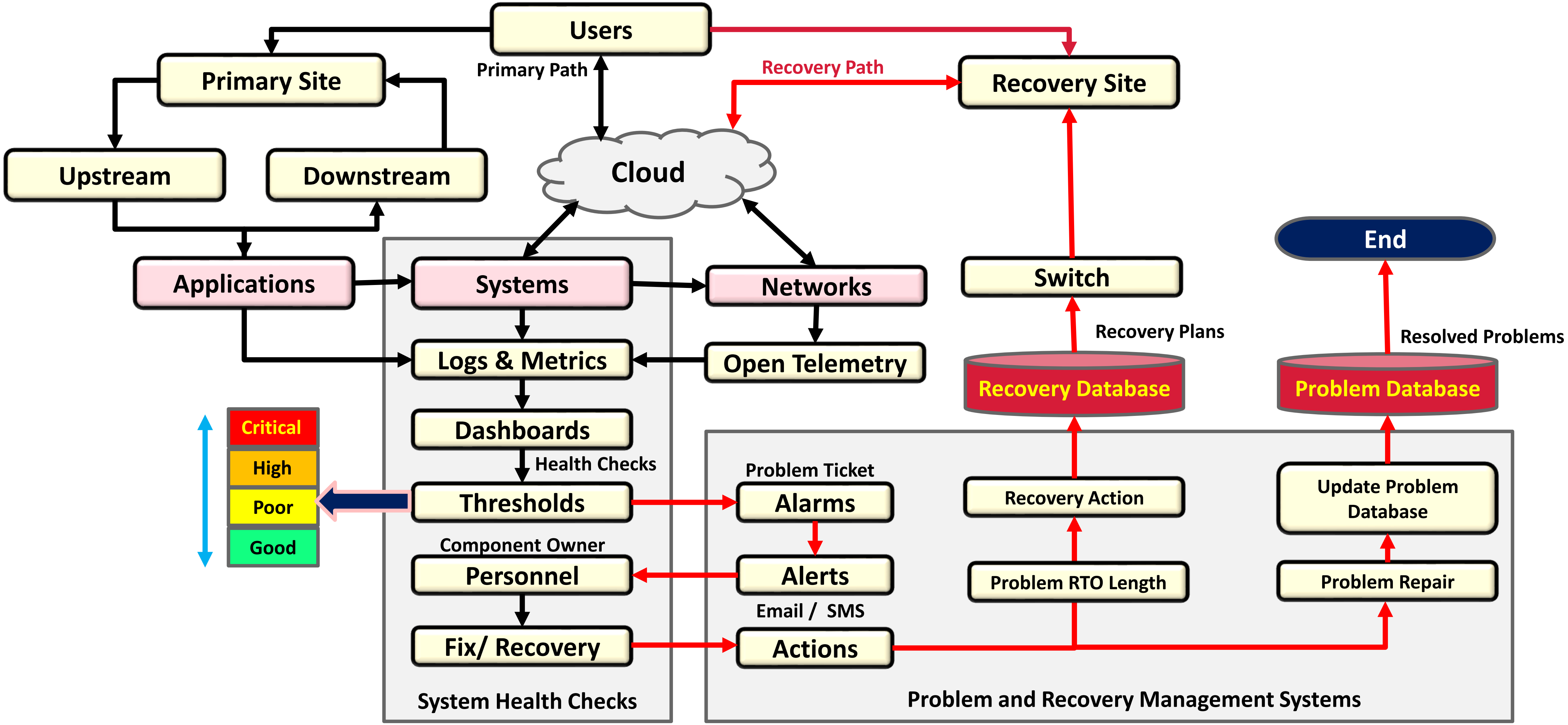


Risk Management Life Cycle


Automating the Recovery Process

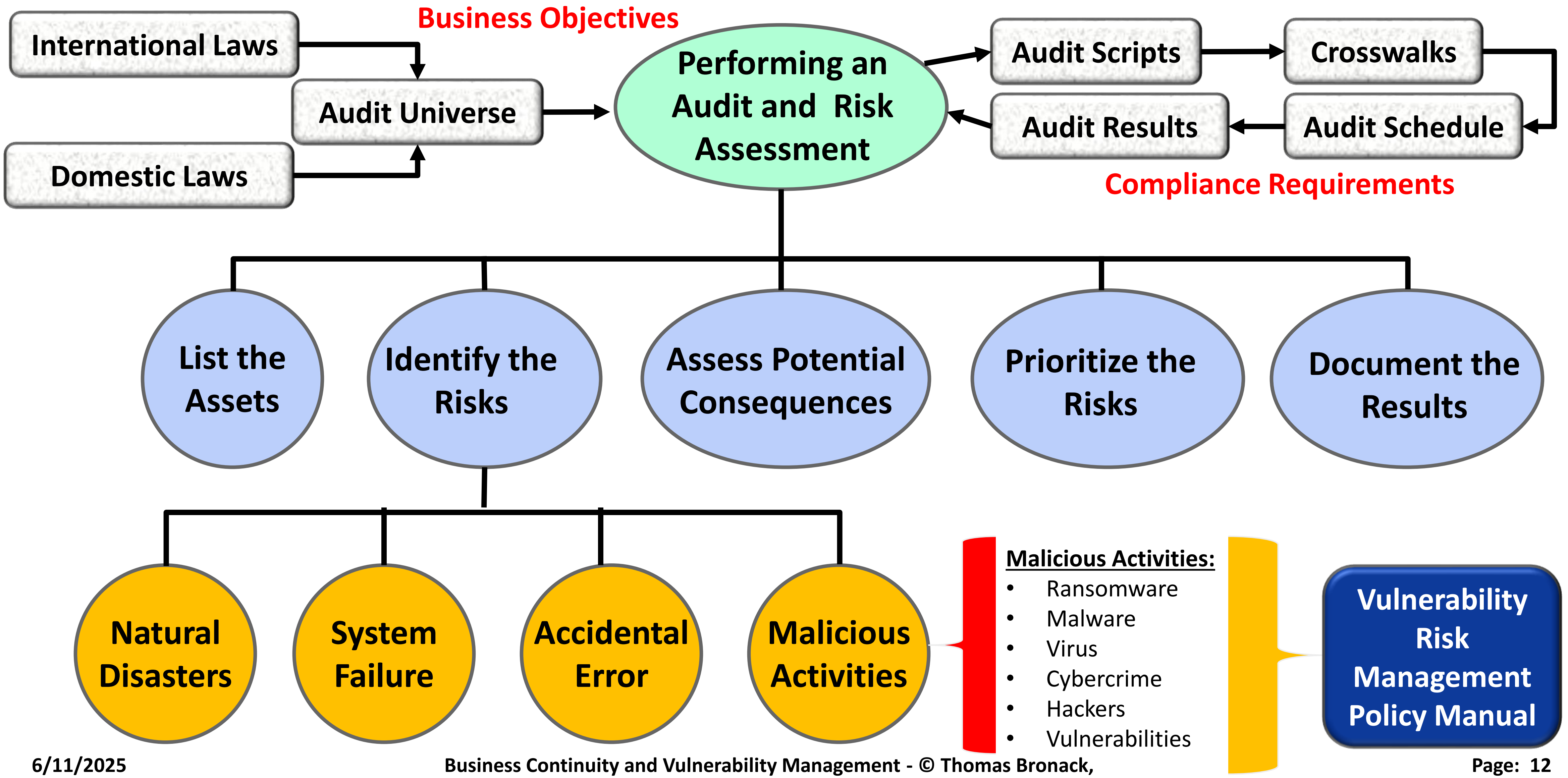
Automated Problem Management and Recovery

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



Performing an Audit and Risk Assessment

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



International Laws

Domestic Laws

Audit Universe

Business Objectives

Performing an Audit and Risk Assessment

Audit Scripts

Crosswalks

Audit Schedule

Audit Results

Compliance Requirements

List the Assets

Identify the Risks

Assess Potential Consequences

Prioritize the Risks

Document the Results

Natural Disasters

System Failure

Accidental Error

Malicious Activities

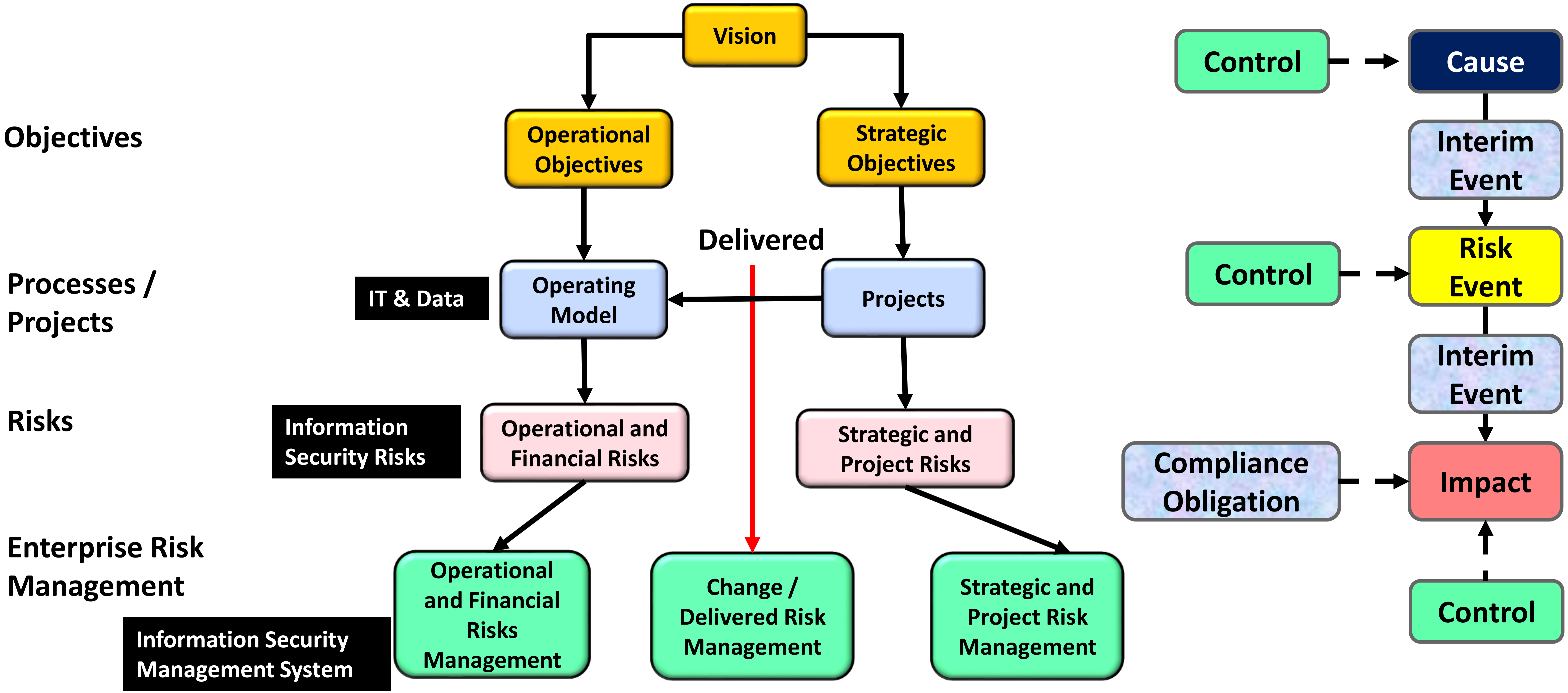
Malicious Activities:

- Ransomware
- Malware
- Virus
- Cybercrime
- Hackers
- Vulnerabilities

Vulnerability Risk Management Policy Manual

Risk and Reward Framework

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



Objectives

Processes / Projects

Risks

Enterprise Risk Management

Vision

Operational Objectives

Strategic Objectives

Delivered

IT & Data

Operating Model

Projects

Information Security Risks

Operational and Financial Risks

Strategic and Project Risks

Information Security Management System

Operational and Financial Risks Management

Change / Delivered Risk Management

Strategic and Project Risk Management

Control

Cause

Interim Event

Control

Risk Event

Interim Event

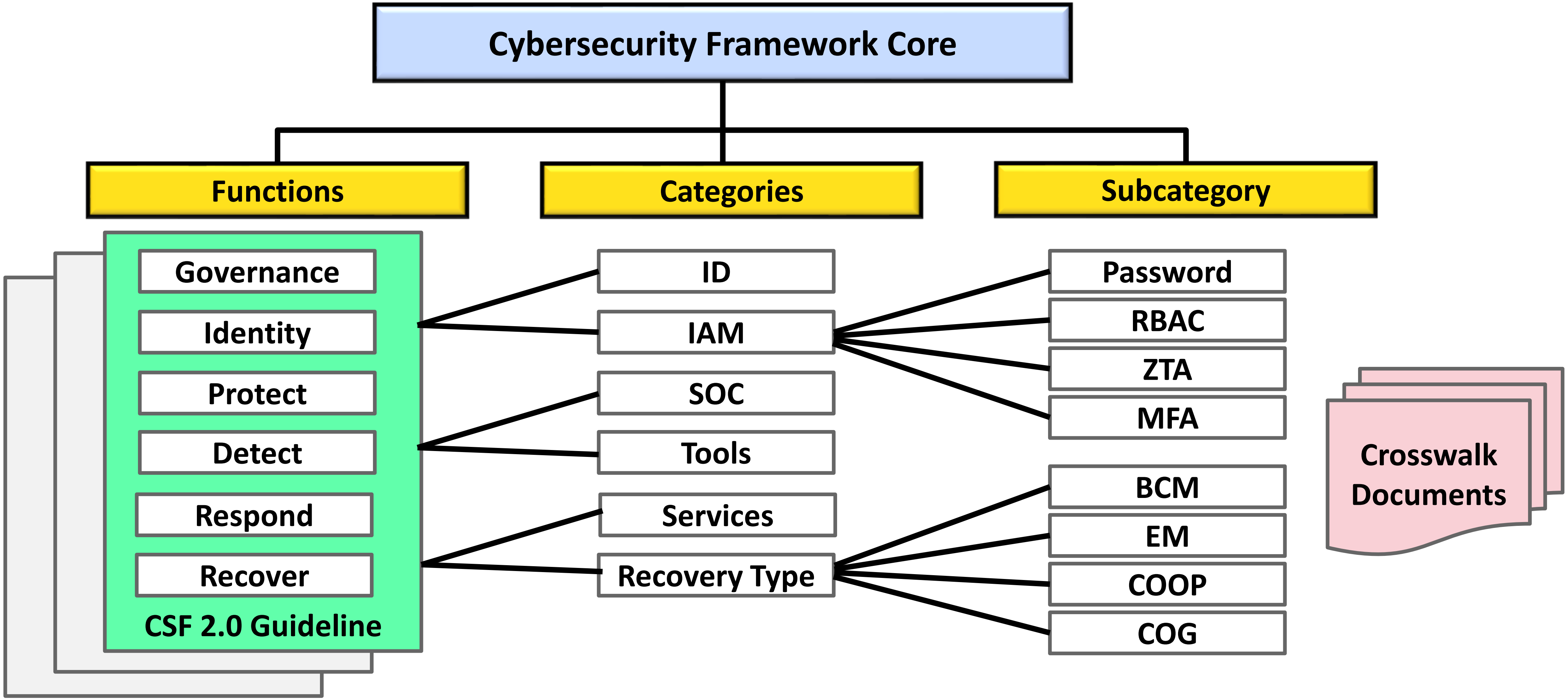
Compliance Obligation

Impact

Control

Creating a Crosswalk Audit Document

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



All Framework Functions

Categories within Functions

Subcategory within Functions

Getting started with facts and a defined direction

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

Know your company:

1. Most Important Applications & Services (**Family Jewels**).
2. Damage caused if lost and maximum duration of survival without the application or service.
3. Define Requirements, Risk, Security, DevSecOps, Testing, Recovery, Acceptance, Deployment, and ITSM, ITOM.
4. Define Audit Universe implement legal & auditing functions.
5. Implement Systems Engineering Life Cycle (SELC) to respond to new ideas or business opportunities.
6. Implement Systems Development Life Cycle (SDLC) to deploy new products and services.
7. 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.

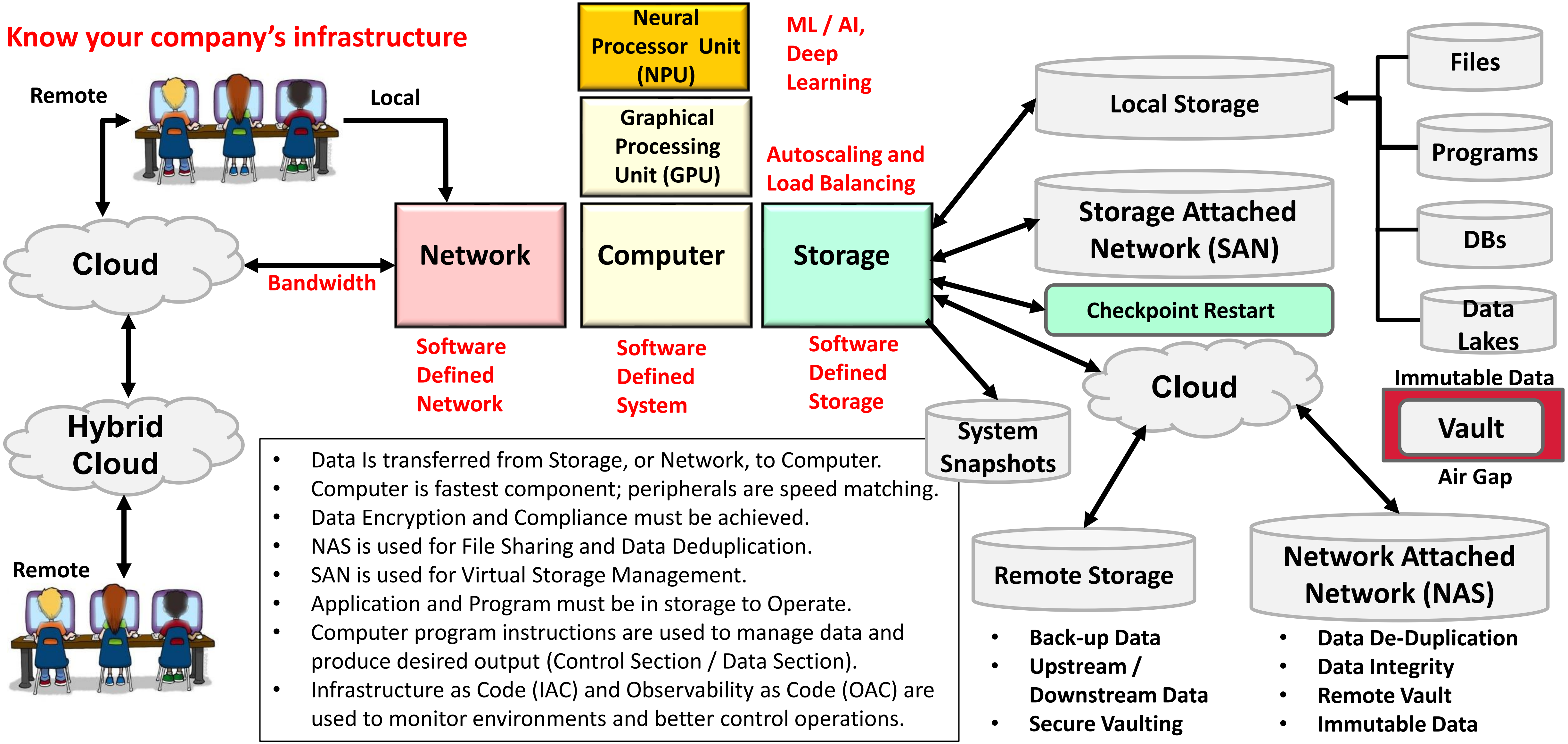
Set you direction:

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.

Monitoring Operations and Controlling Resources

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

Know your company's infrastructure



Remote

Local

Cloud

Bandwidth

Hybrid Cloud

Remote

Neural Processor Unit (NPU)

ML / AI, Deep Learning

Graphical Processing Unit (GPU)

Autoscaling and Load Balancing

Network

Computer

Storage

Software Defined Network

Software Defined System

Software Defined Storage

Local Storage

Files

Programs

DBs

Data Lakes

Storage Attached Network (SAN)

Checkpoint Restart

Cloud

System Snapshots

Immutable Data

Vault

Air Gap

Remote Storage

- Back-up Data
- Upstream / Downstream Data
- Secure Vaulting

Network Attached Network (NAS)

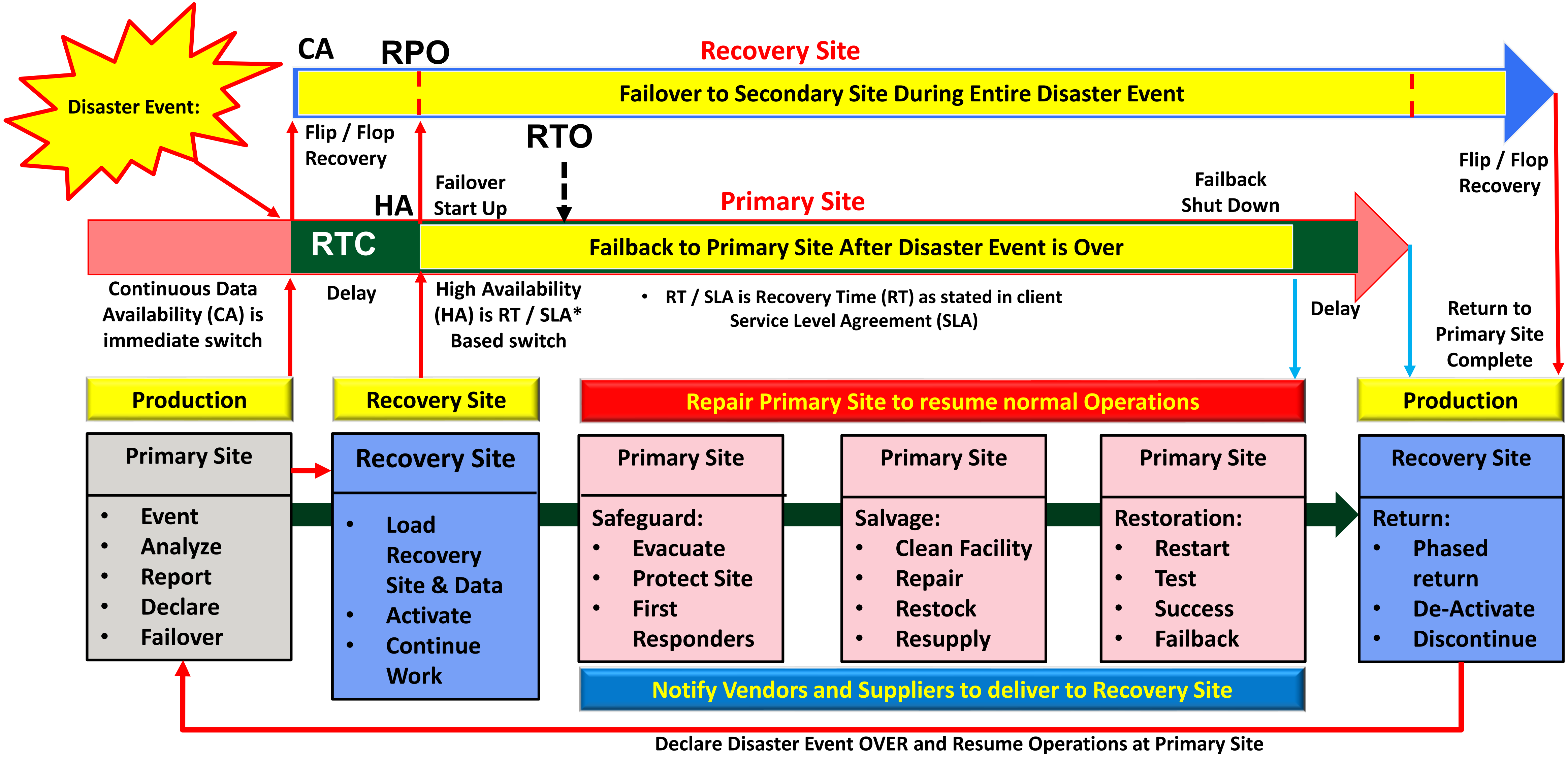
- Data De-Duplication
- Data Integrity
- Remote Vault
- Immutable Data

- Data Is transferred from Storage, or Network, to Computer.
- Computer is fastest component; peripherals are speed matching.
- Data Encryption and Compliance must be achieved.
- NAS is used for File Sharing and Data Deduplication.
- SAN is used for Virtual Storage Management.
- Application and Program must be in storage to Operate.
- Computer program instructions are used to manage data and produce desired output (Control Section / Data Section).
- Infrastructure as Code (IAC) and Observability as Code (OAC) are used to monitor environments and better control operations.

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
Phone: (917) 673-6992



Disaster Event:

CA

RPO

Recovery Site

Failover to Secondary Site During Entire Disaster Event

Flip / Flop Recovery

RTO

Failover Start Up

HA

Primary Site

Failback Shut Down

Flip / Flop Recovery

RTC

Failback to Primary Site After Disaster Event is Over

Continuous Data Availability (CA) is immediate switch

Delay

High Availability (HA) is RT / SLA* Based switch

- RT / SLA is Recovery Time (RT) as stated in client Service Level Agreement (SLA)

Delay

Return to Primary Site Complete

Production

Recovery Site

Repair Primary Site to resume normal Operations

Production

Primary Site
- Event
- Analyze
- Report
- Declare
- Failover

Recovery Site
- Load Recovery Site & Data
- Activate
- Continue Work

Primary Site
Safeguard:
- Evacuate
- Protect Site
- First Responders

Primary Site
Salvage:
- Clean Facility
- Repair
- Restock
- Resupply

Primary Site
Restoration:
- Restart
- Test
- Success
- Failback

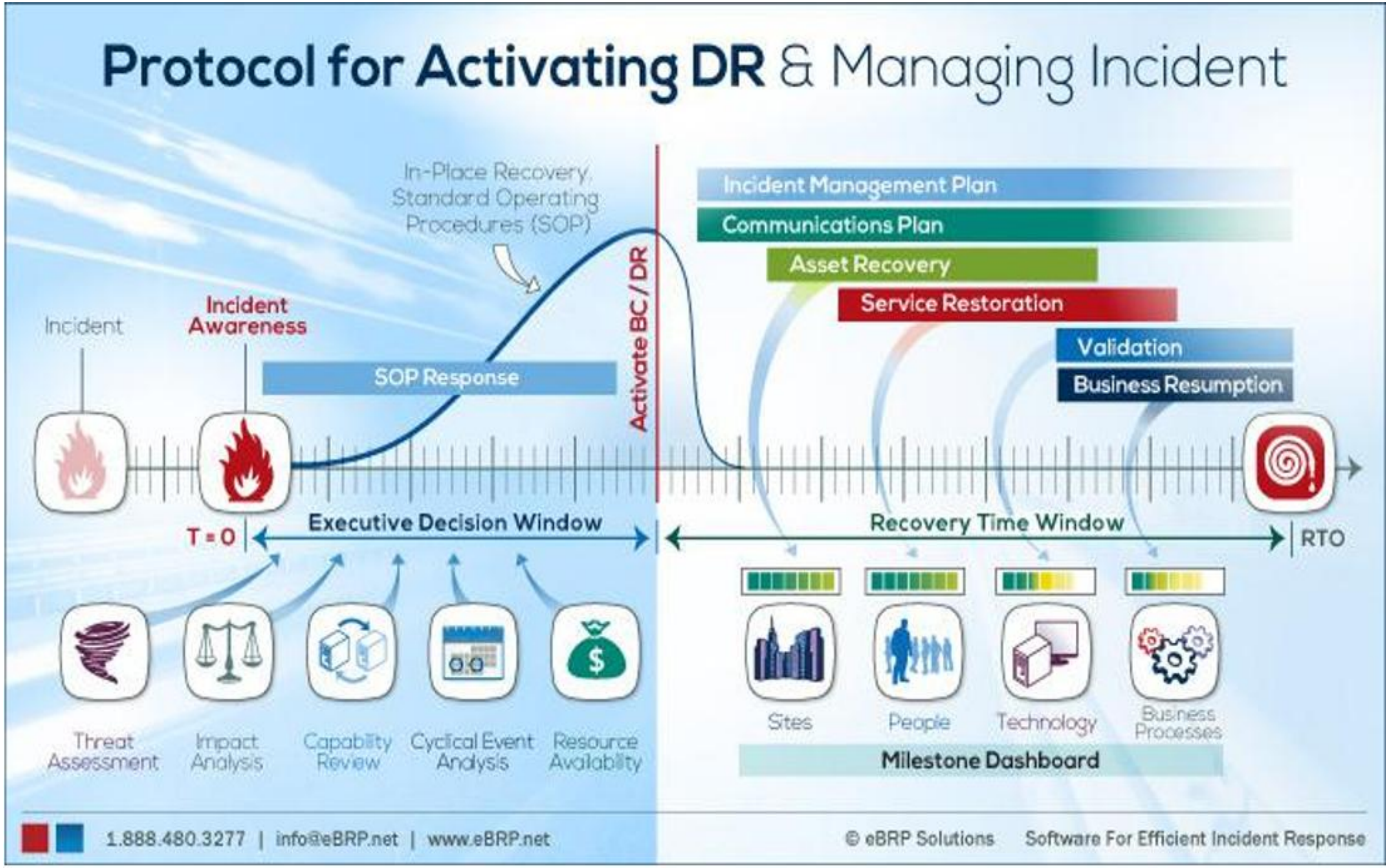
Recovery Site
Return:
- Phased return
- De-Activate
- Discontinue

Notify Vendors and Suppliers to deliver to Recovery Site

Declare Disaster Event OVER and Resume Operations at Primary Site

The Business Recovery Life Cycle

Thomas Bronack
Email: 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

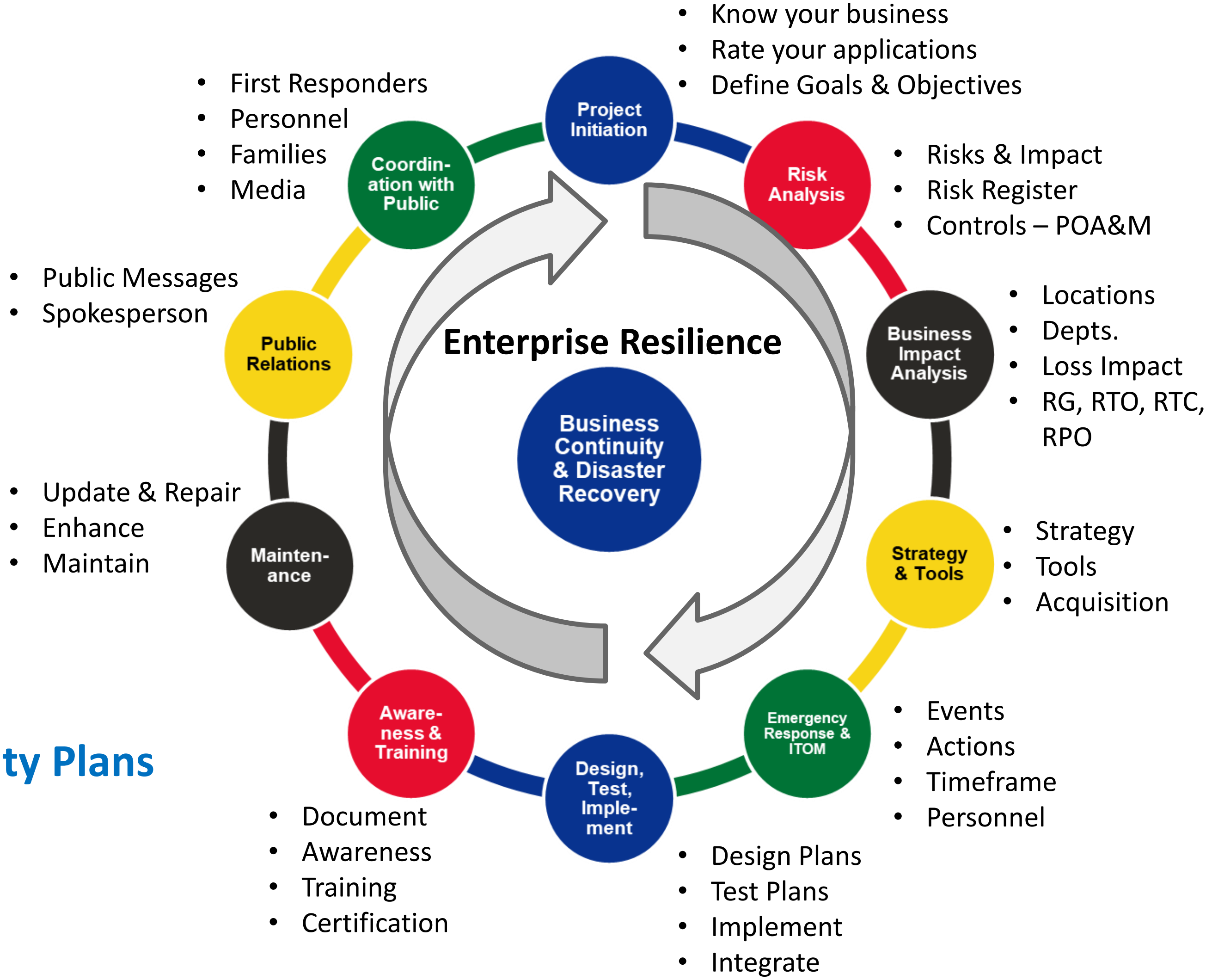
Ten Step Process to establish BCM/DR Practice

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



- Know your business
- Rate your applications
- Define Goals & Objectives

- Risks & Impact
- Risk Register
- Controls – POA&M

- Locations
- Depts.
- Loss Impact
- RG, RTO, RTC, RPO

- Strategy
- Tools
- Acquisition

- Events
- Actions
- Timeframe
- Personnel

- Design Plans
- Test Plans
- Implement
- Integrate

- Document
- Awareness
- Training
- Certification

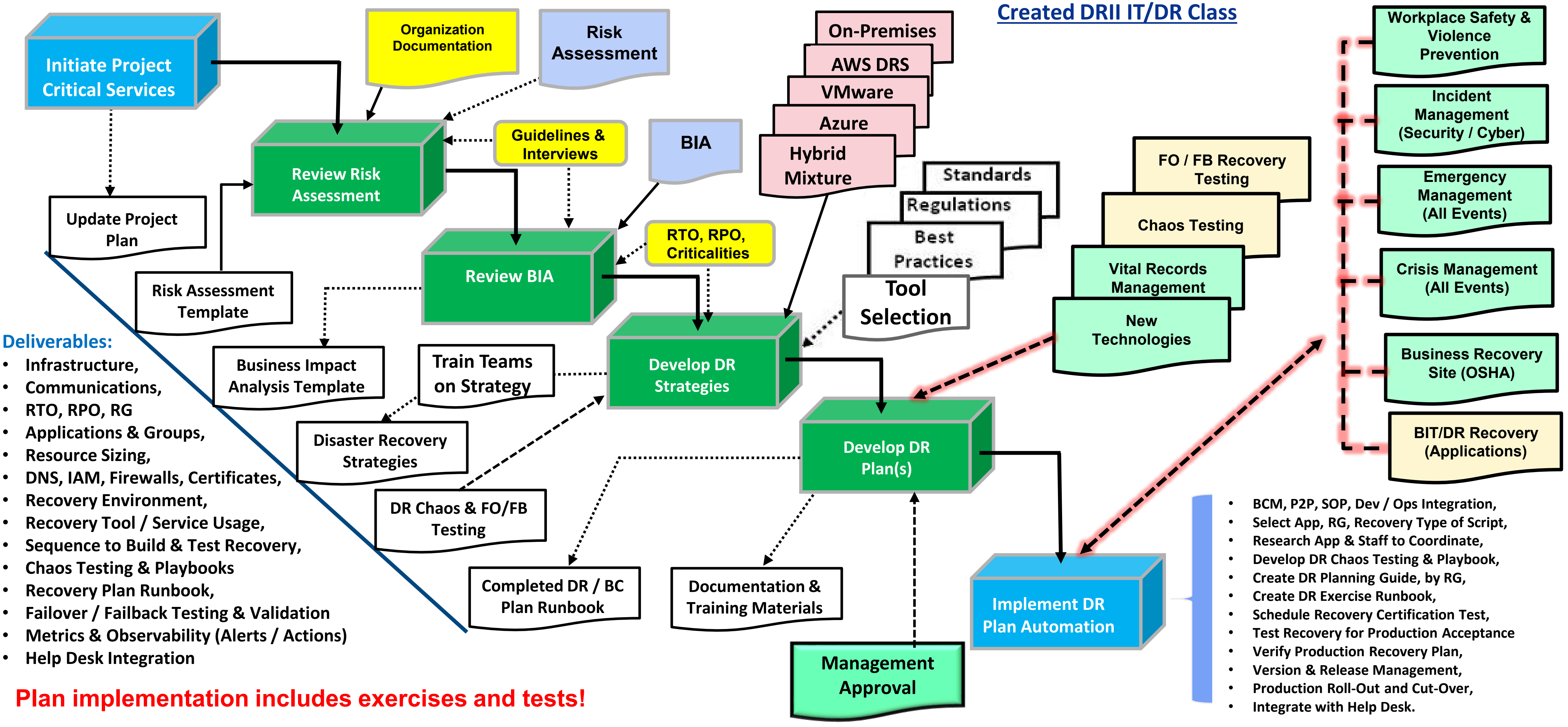
- Update & Repair
- Enhance
- Maintain

- Public Messages
- Spokesperson

- First Responders
- Personnel
- Families
- Media

Sample Recovery Plan Methodology

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



Created DRII IT/DR Class

Initiate Project Critical Services

Update Project Plan

Organization Documentation

Risk Assessment

Review Risk Assessment

Guidelines & Interviews

Risk Assessment Template

BIA

Review BIA

RTO, RPO, Criticalities

Business Impact Analysis Template

On-Premises

AWS DRS

VMware

Azure

Hybrid Mixture

Standards

Regulations

Best Practices

Tool Selection

Develop DR Strategies

Train Teams on Strategy

Disaster Recovery Strategies

DR Chaos & FO/FB Testing

Develop DR Plan(s)

Completed DR / BC Plan Runbook

Documentation & Training Materials

Management Approval

Implement DR Plan Automation

FO / FB Recovery Testing

Chaos Testing

Vital Records Management

New Technologies

Workplace Safety & Violence Prevention

Incident Management (Security / Cyber)

Emergency Management (All Events)

Crisis Management (All Events)

Business Recovery Site (OSHA)

BIT/DR Recovery (Applications)

Deliverables:

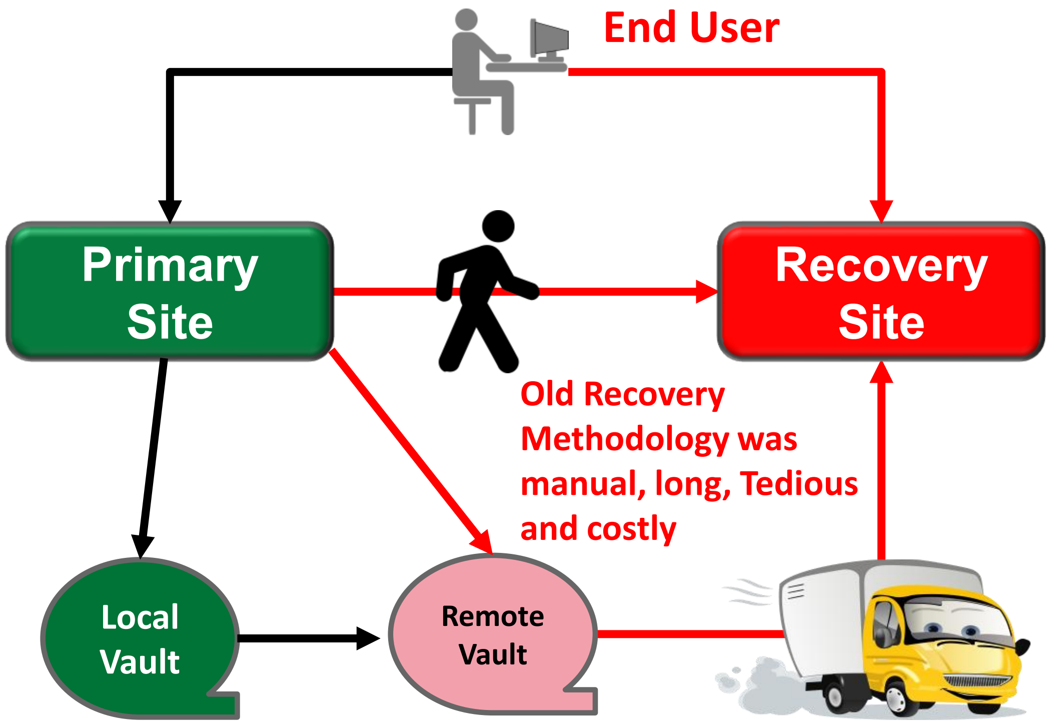
- Infrastructure,
- Communications,
- RTO, RPO, RG
- Applications & Groups,
- Resource Sizing,
- DNS, IAM, Firewalls, Certificates,
- Recovery Environment,
- Recovery Tool / Service Usage,
- Sequence to Build & Test Recovery,
- Chaos Testing & Playbooks
- Recovery Plan Runbook,
- Failover / Failback Testing & Validation
- Metrics & Observability (Alerts / Actions)
- Help Desk Integration

- BCM, P2P, SOP, Dev / Ops Integration,
- Select App, RG, Recovery Type of Script,
- Research App & Staff to Coordinate,
- Develop DR Chaos Testing & Playbook,
- Create DR Planning Guide, by RG,
- Create DR Exercise Runbook,
- Schedule Recovery Certification Test,
- Test Recovery for Production Acceptance
- Verify Production Recovery Plan,
- Version & Release Management,
- Production Roll-Out and Cut-Over,
- Integrate with Help Desk.

Plan implementation includes exercises and tests!

Evolution of Recovery Management

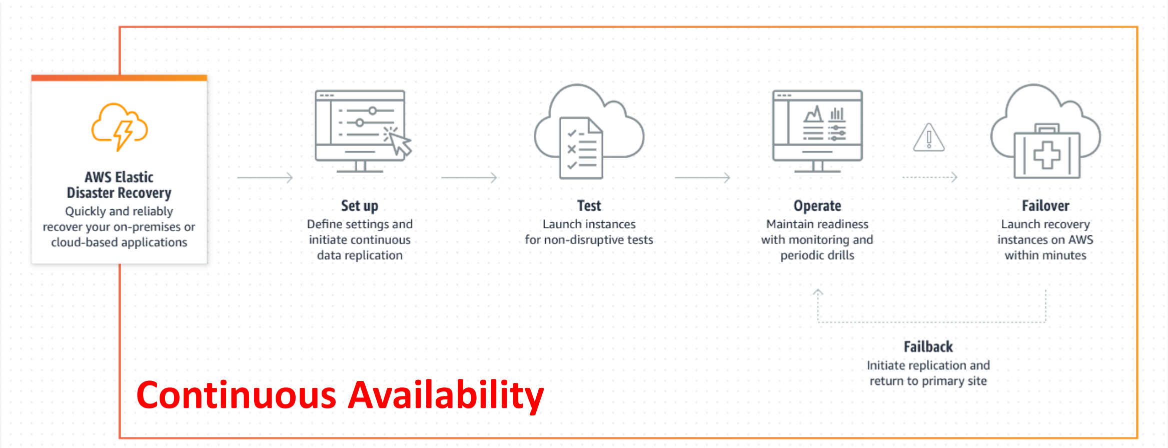
Thomas Bronack
Email: bronackt@dcag.com
Phone: (917) 673-6992



Old Recovery Methodology was manual, long, Tedious and costly

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

AWS Failover / Failback



AWS Elastic Disaster Recovery
Quickly and reliably recover your on-premises or cloud-based applications

Set up
Define settings and initiate continuous data replication

Test
Launch instances for non-disruptive tests

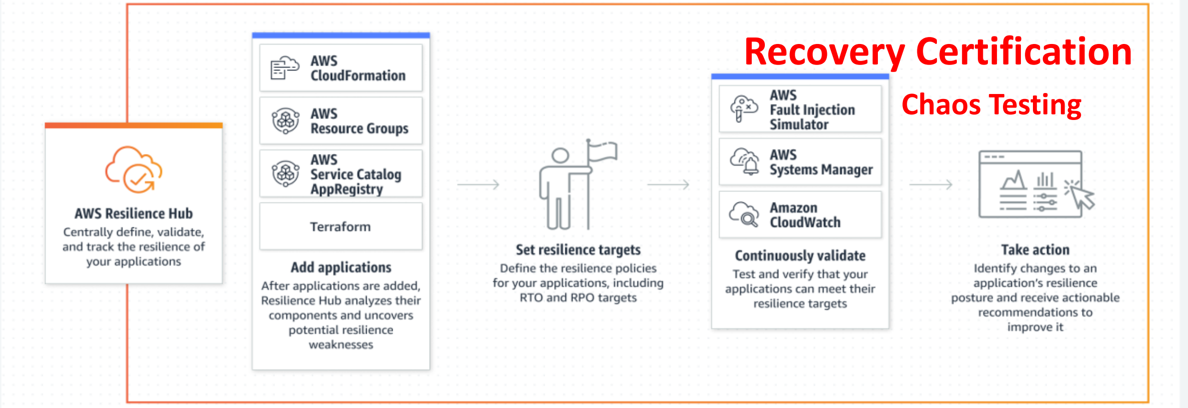
Operate
Maintain readiness with monitoring and periodic drills

Failover
Launch recovery instances on AWS within minutes

Failback
Initiate replication and return to primary site

Continuous Availability

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



AWS Resilience Hub
Centrally define, validate, and track the resilience of your applications

AWS CloudFormation
AWS Resource Groups
AWS Service Catalog AppRegistry
Terraform

Add applications
After applications are added, Resilience Hub analyzes their components and uncovers potential resilience weaknesses

Set resilience targets
Define the resilience policies for your applications, including RTO and RPO targets

Recovery Certification

Chaos Testing

AWS Fault Injection Simulator
AWS Systems Manager
Amazon CloudWatch

Continuously validate
Test and verify that your applications can meet their resilience targets

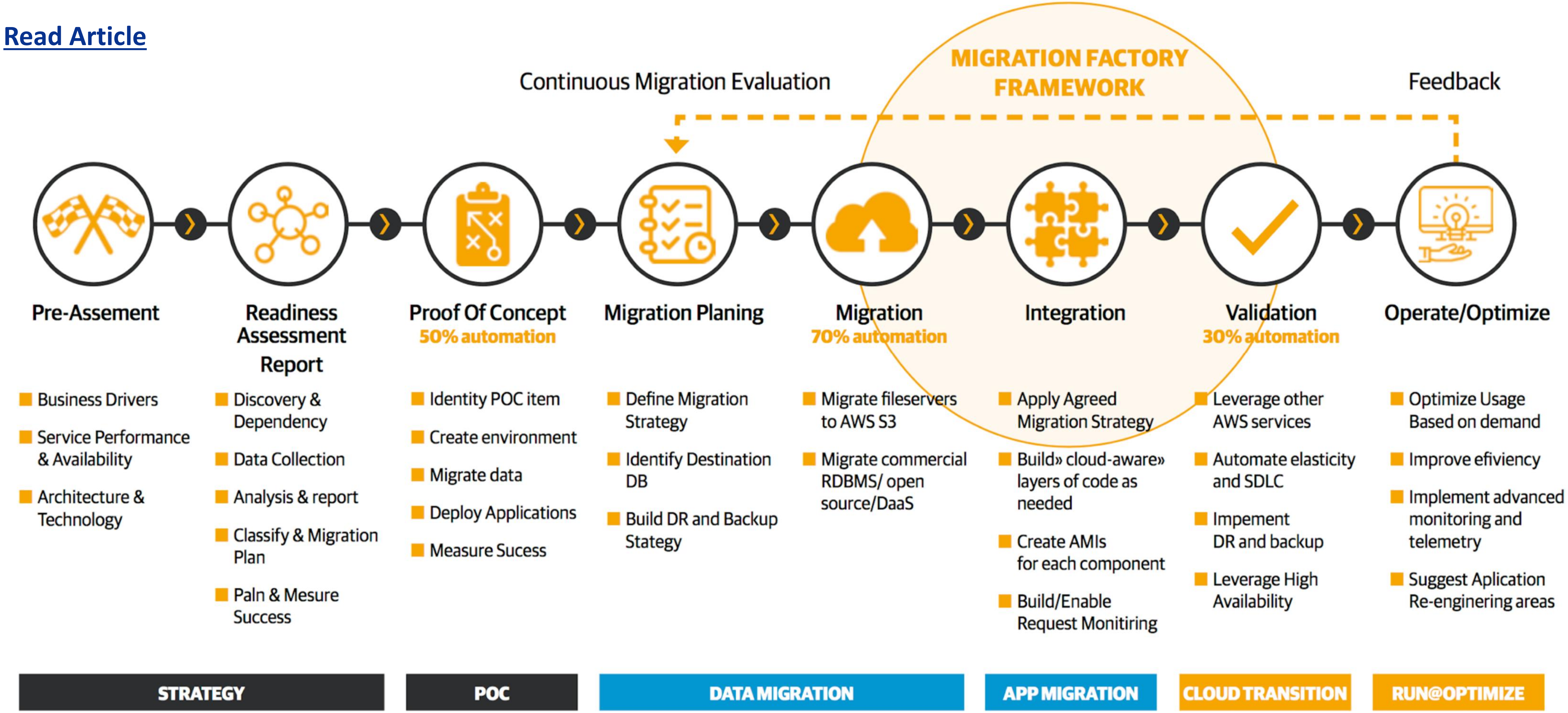
Take action
Identify changes to an application's resilience posture and receive actionable recommendations to improve it

AWS Resiliency Hub

Planning Application Migrating to the AWS Cloud

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

Read Article



Continuous Migration Evaluation

MIGRATION FACTORY FRAMEWORK

Feedback

Pre-Assement

- Business Drivers
- Service Performance & Availability
- Architecture & Technology

Readiness Assessment Report

- Discovery & Dependency
- Data Collection
- Analysis & report
- Classify & Migration Plan
- Paln & Mesure Success

Proof Of Concept
50% automation

- Identity POC item
- Create environment
- Migrate data
- Deploy Applications
- Measure Sucess

Migration Planing

- Define Migration Strategy
- Identify Destination DB
- Build DR and Backup Stategy

Migration
70% automation

- Migrate fileservers to AWS S3
- Migrate commercial RDBMS/ open source/DaaS

Integration

- Apply Agreed Migration Strategy
- Build» cloud-aware» layers of code as needed
- Create AMIs for each component
- Build/Enable Request Monitiring

Validation
30% automation

- Leverage other AWS services
- Automate elasticity and SDLC
- Impement DR and backup
- Leverage High Availability

Operate/Optimize

- Optimize Usage Based on demand
- Improve efiviency
- Implement advanced monitoring and telemetry
- Suggest Aplication Re-enginering areas

STRATEGY | POC | DATA MIGRATION | APP MIGRATION | CLOUD TRANSITION | RUN@OPTIMIZE

AWS DR Strategies

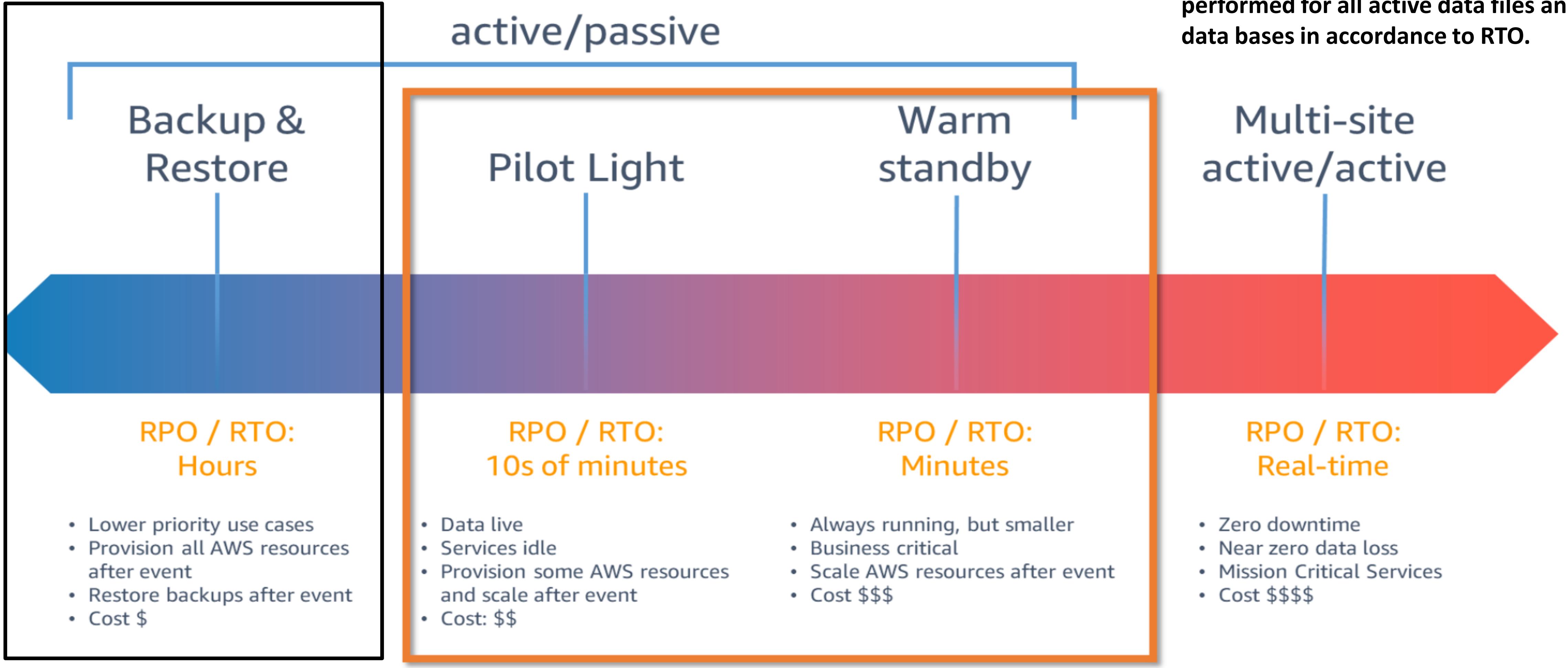
Link to AWS Disaster Recovery Strategies

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

Single Region

Availability Zones

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



active/passive

Backup & Restore

RPO / RTO: Hours

- Lower priority use cases
- Provision all AWS resources after event
- Restore backups after event
- Cost $

Pilot Light

RPO / RTO: 10s of minutes

- Data live
- Services idle
- Provision some AWS resources and scale after event
- Cost: $$

Warm standby

RPO / RTO: Minutes

- Always running, but smaller
- Business critical
- Scale AWS resources after event
- Cost $$$

Multi-site active/active

RPO / RTO: Real-time

- Zero downtime
- Near zero data loss
- Mission Critical Services
- Cost $$$$

Standby **COLD** **WARM** **HOT**

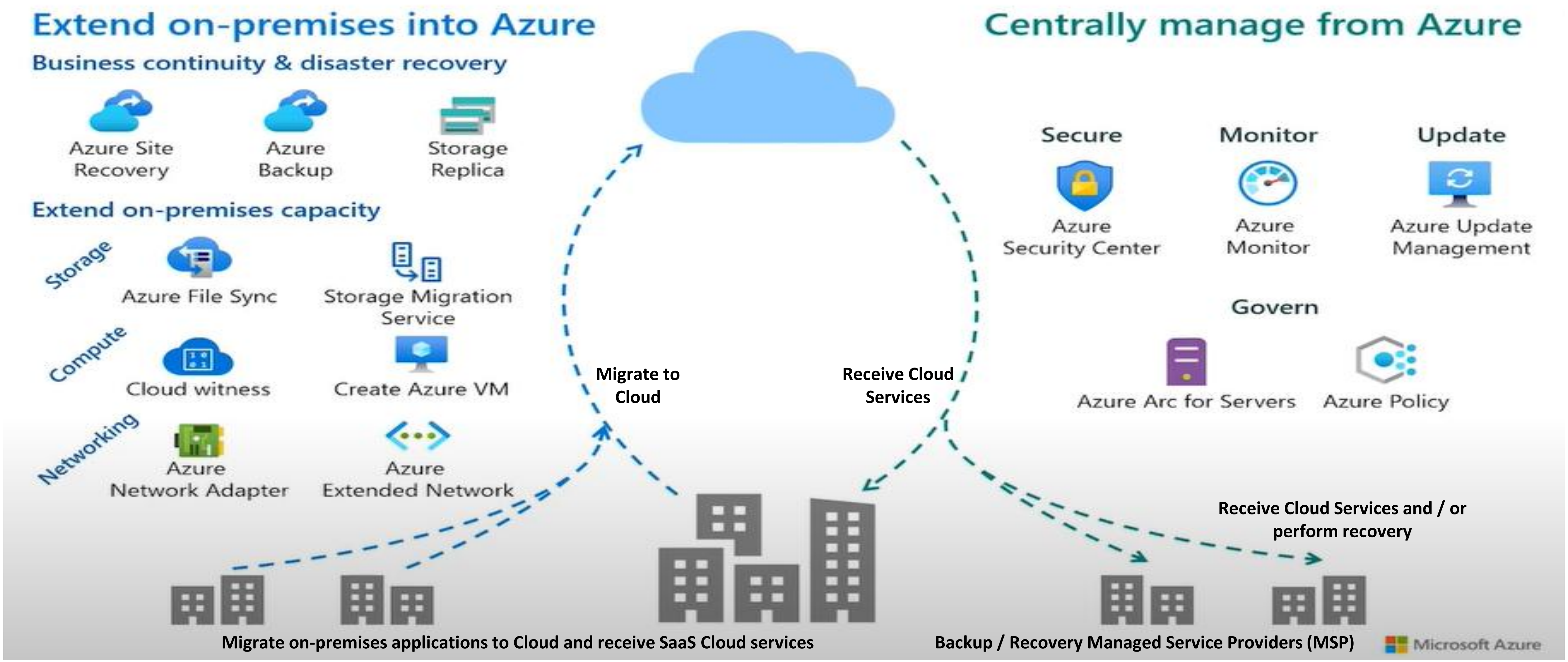
Resilience Patterns and Recovery Groups

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**		

Azure Environment and Recovery Management

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



Extend on-premises into Azure

Business continuity & disaster recovery

Extend on-premises capacity

Centrally manage from Azure

Migrate to Cloud

Receive Cloud Services

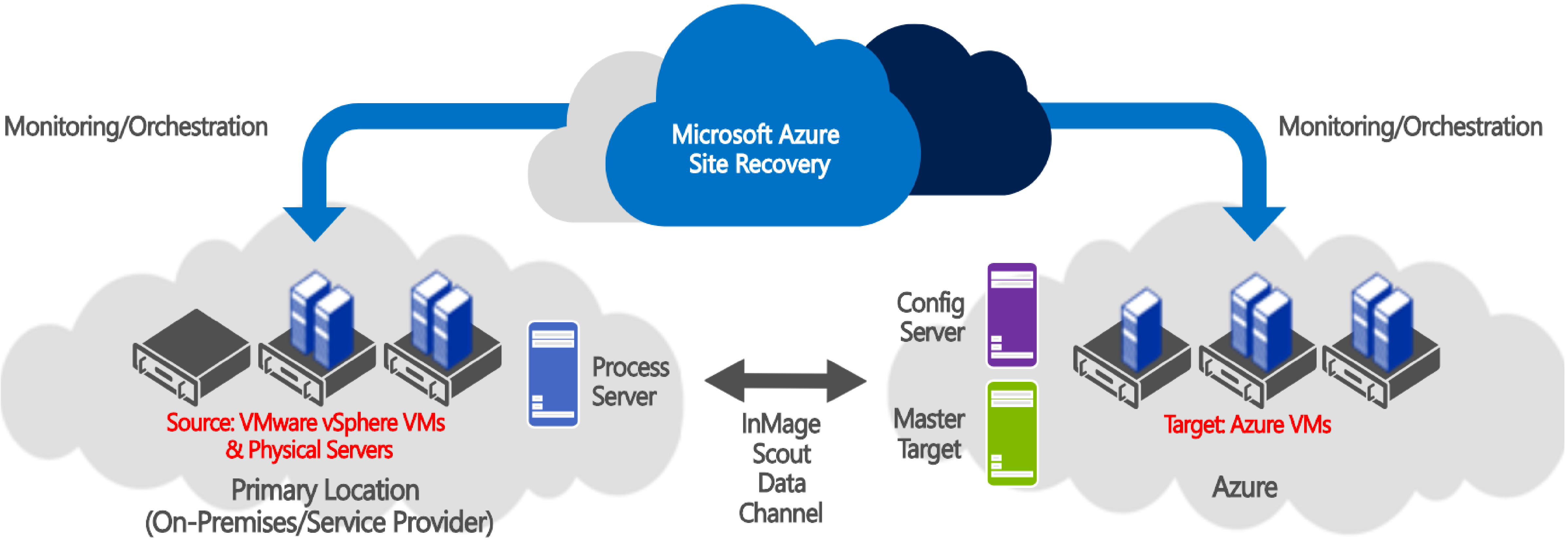
Receive Cloud Services and / or perform recovery

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

Backup / Recovery Managed Service Providers (MSP)

Azure Recovery Management Environment

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



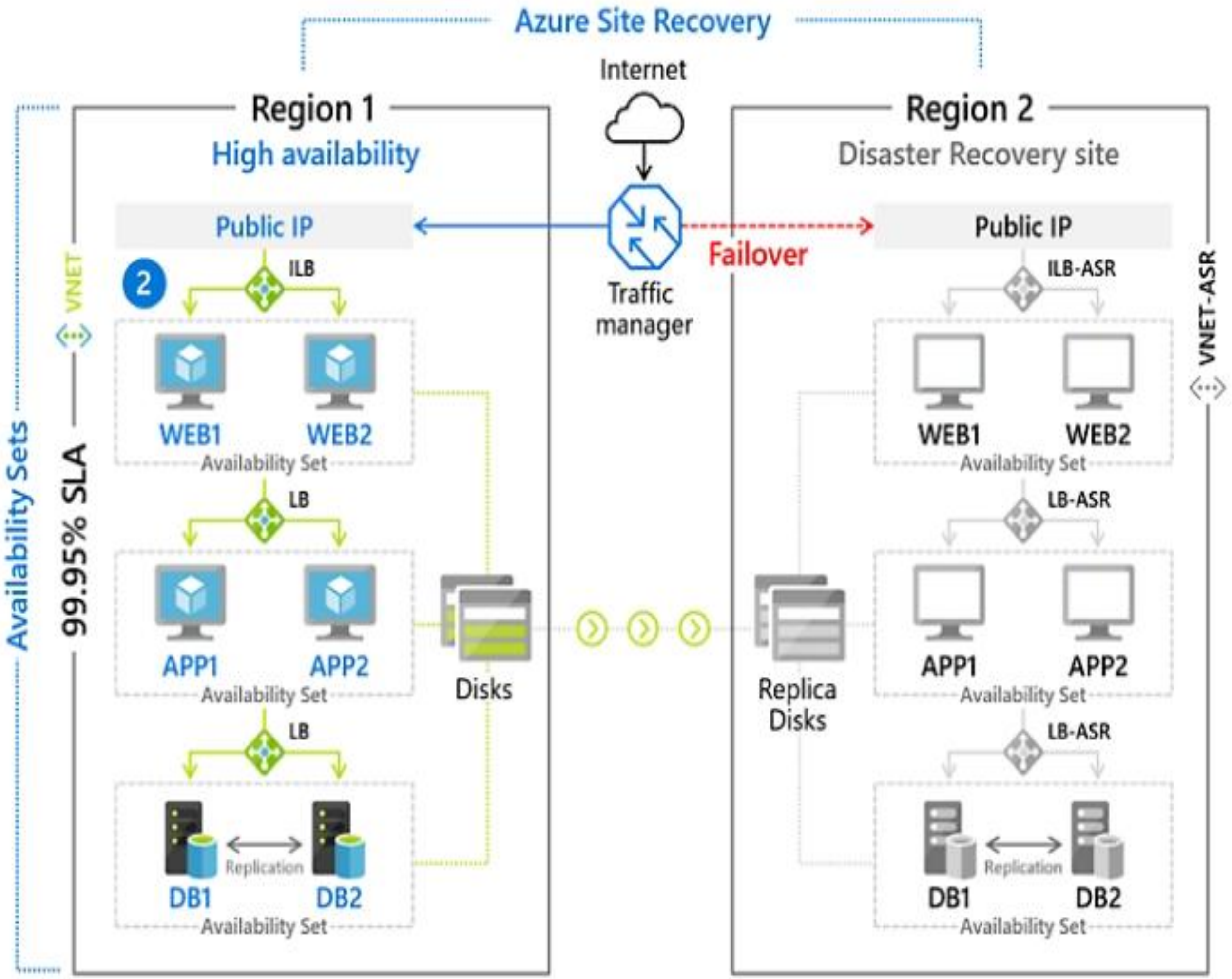
Process Server – Used for Caching, Compression & Encryption

Config Server – Used for Centralized Management of InMage Scout

Master Target – Used as a repository & for retention

Azure Site Recovery Management

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



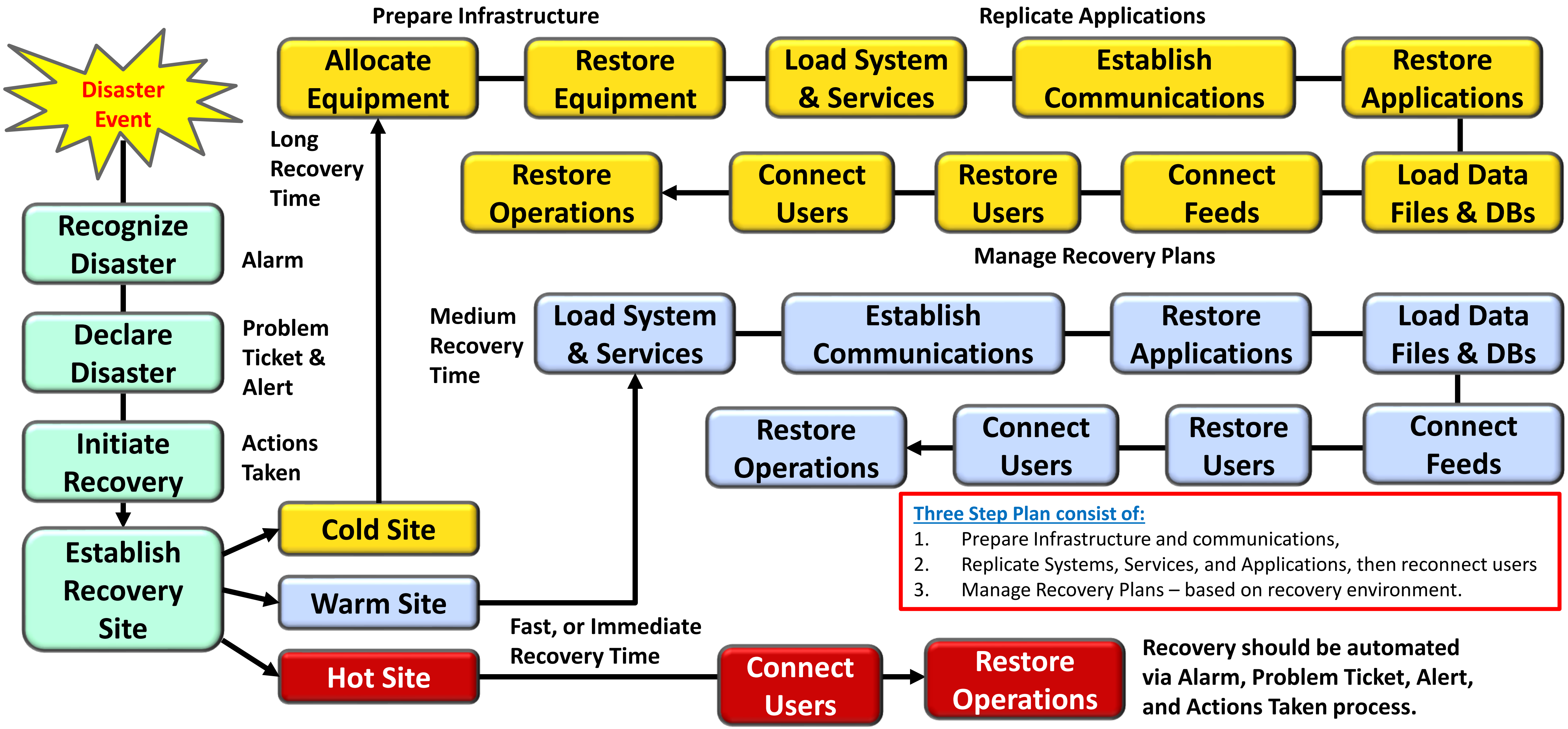
Simple to deploy and manage

- 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

Sequence of Events to enact a Recovery Operation

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



Three Step Plan consist of:

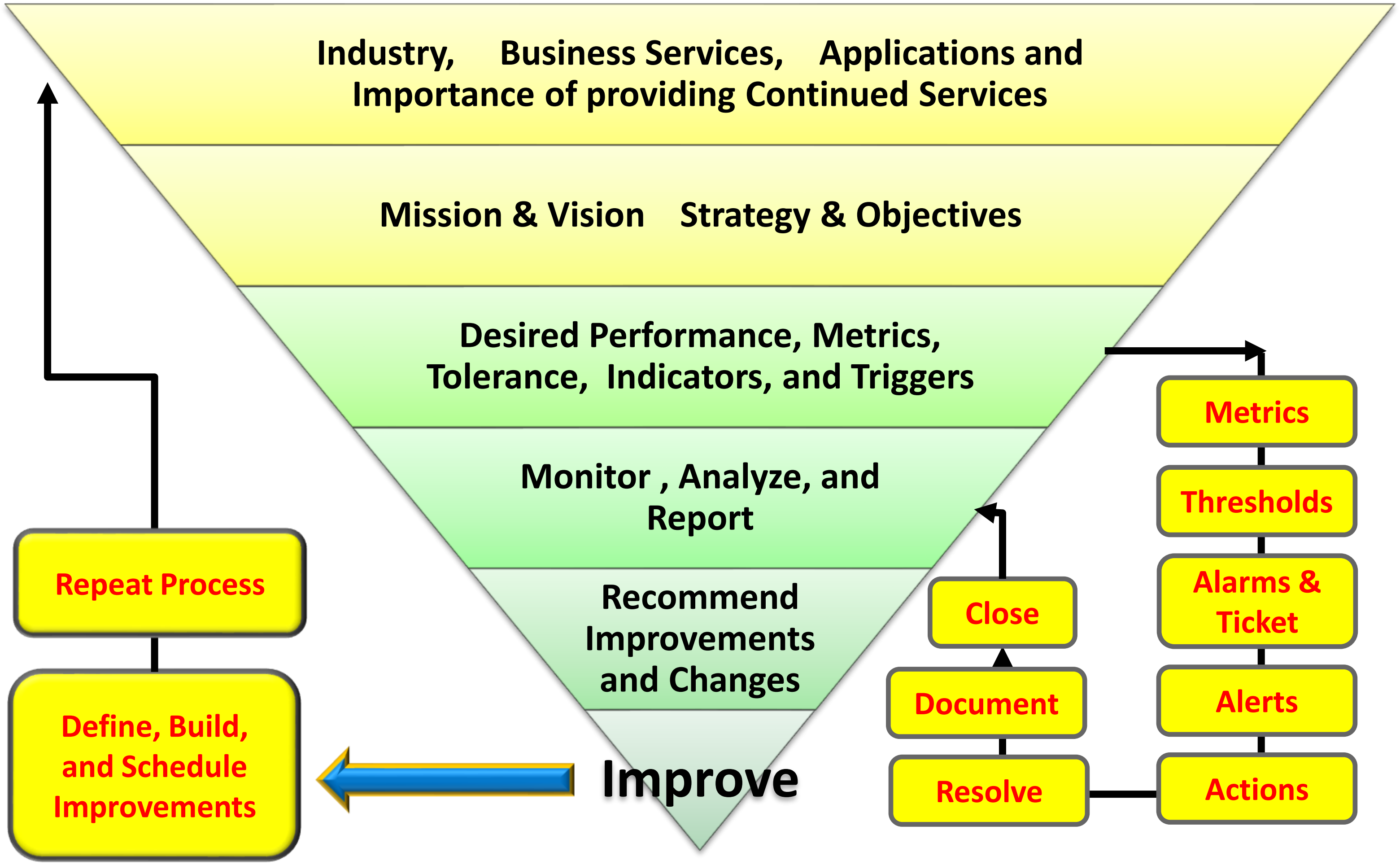
1. Prepare Infrastructure and communications,
2. Replicate Systems, Services, and Applications, then reconnect users
3. Manage Recovery Plans – based on recovery environment.

Recovery should be automated via Alarm, Problem Ticket, Alert, and Actions Taken process.

The Risk Evaluation Process Using COSO

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

Defining the Risk Appetite using COSO

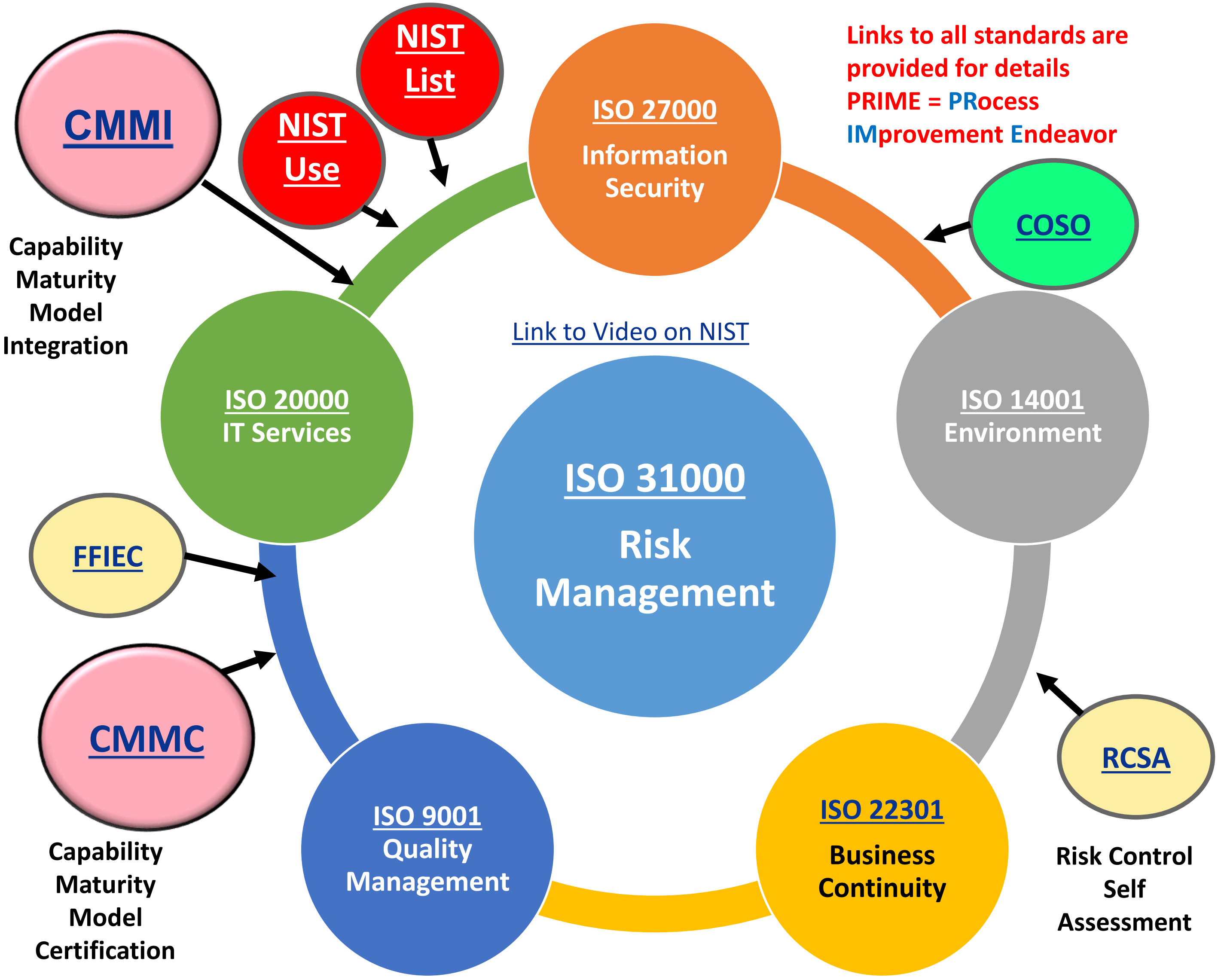

Industry, Business Services, Applications and Importance of providing Continued Services
Mission & Vision Strategy & Objectives
Desired Performance, Metrics, Tolerance, Indicators, and Triggers
Monitor , Analyze, and Report
Recommend Improvements and Changes
Improve
Repeat Process
Define, Build, and Schedule Improvements
Metrics
Thresholds
Alarms & Ticket
Alerts
Actions
Resolve
Document
Close

COSO for Risk Appetite & Evaluation:

1. Review Business Mission and Vision
2. Consider Board and Management perspectives and Risk Appetites
3. Incorporates current strategic direction, risk profile, and culture.
4. Identifies and evaluates alternate strategies.
5. Choose preferred strategy to enhance value.
6. Establish Business Objectives.
7. Set tolerance, define and measure metrics, indicators, and triggers.
8. Include changing context of the business culture and competitive environment.
9. Monitors performance and revises appetite or strategy, as needed.
10. Purchase Insurance and Off-Load responsibilities here possible.

The newest Integration Model – PRIME Approach

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



Links to all standards are provided for details
PRIME = PRocess IMprovement Endeavor

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.

Ensuring Compliance via GRC and Risk Assessment

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

Governance

Risk

Compliance

- Laws
- Statutes
- Regulations

Statutory and Regulatory

- ISO
- NIST

Standards

- Organizational
- Info Technology
- Info Security

Policies

Contract Commitments

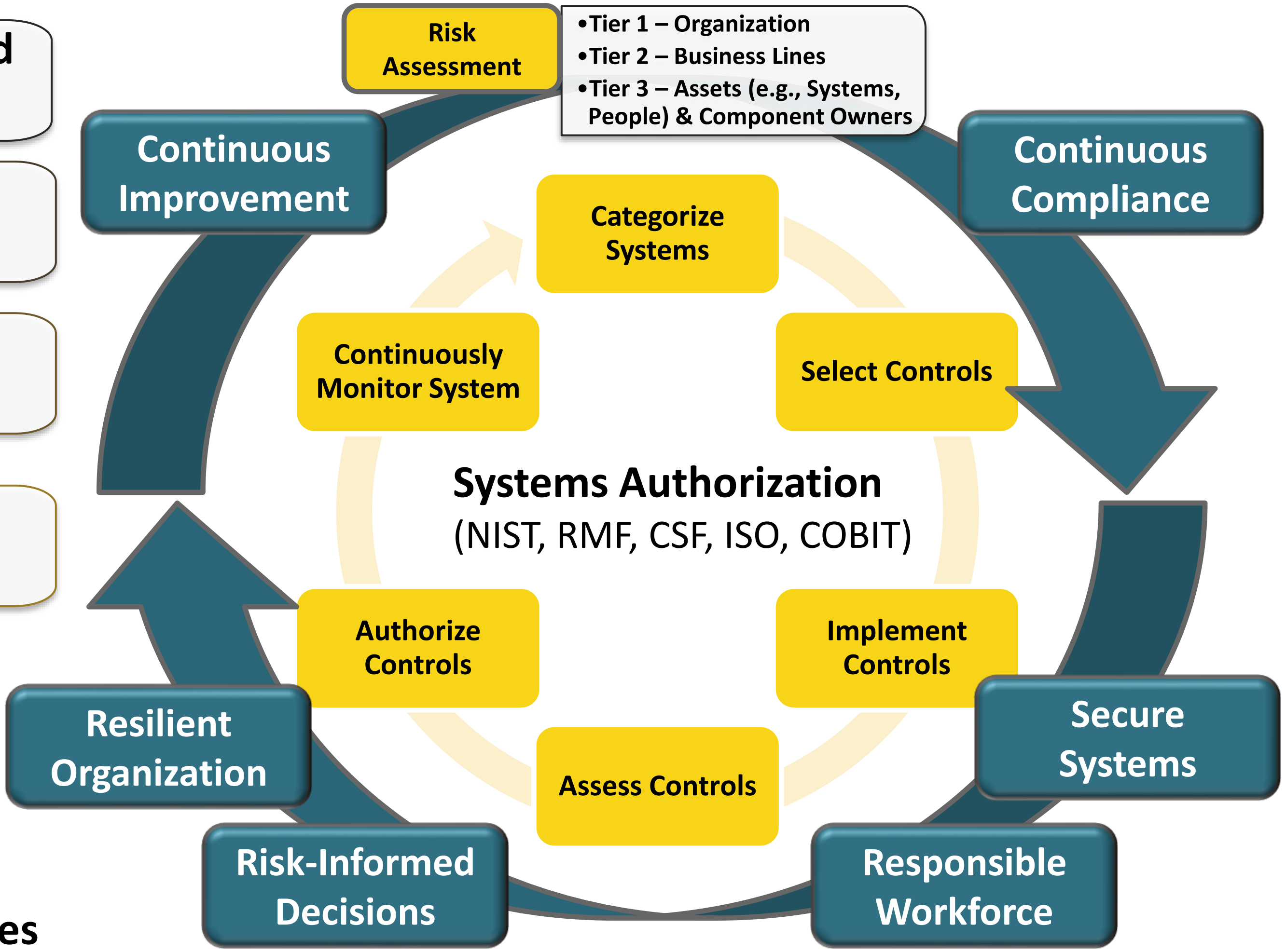
- PCI/DSS
- Customer Contracts
- B2B Agreements

- Administrative
- Physical
- Technical

Contracts

- NIST, CSF, RMF
- ISO
- Organizational

Processes and Procedures



Monitor

- Threat Landscape
- Implemented Controls
- Insider Behavioral Analysis

Self Assessment

- Systems
- Practices
- Audit Preparations

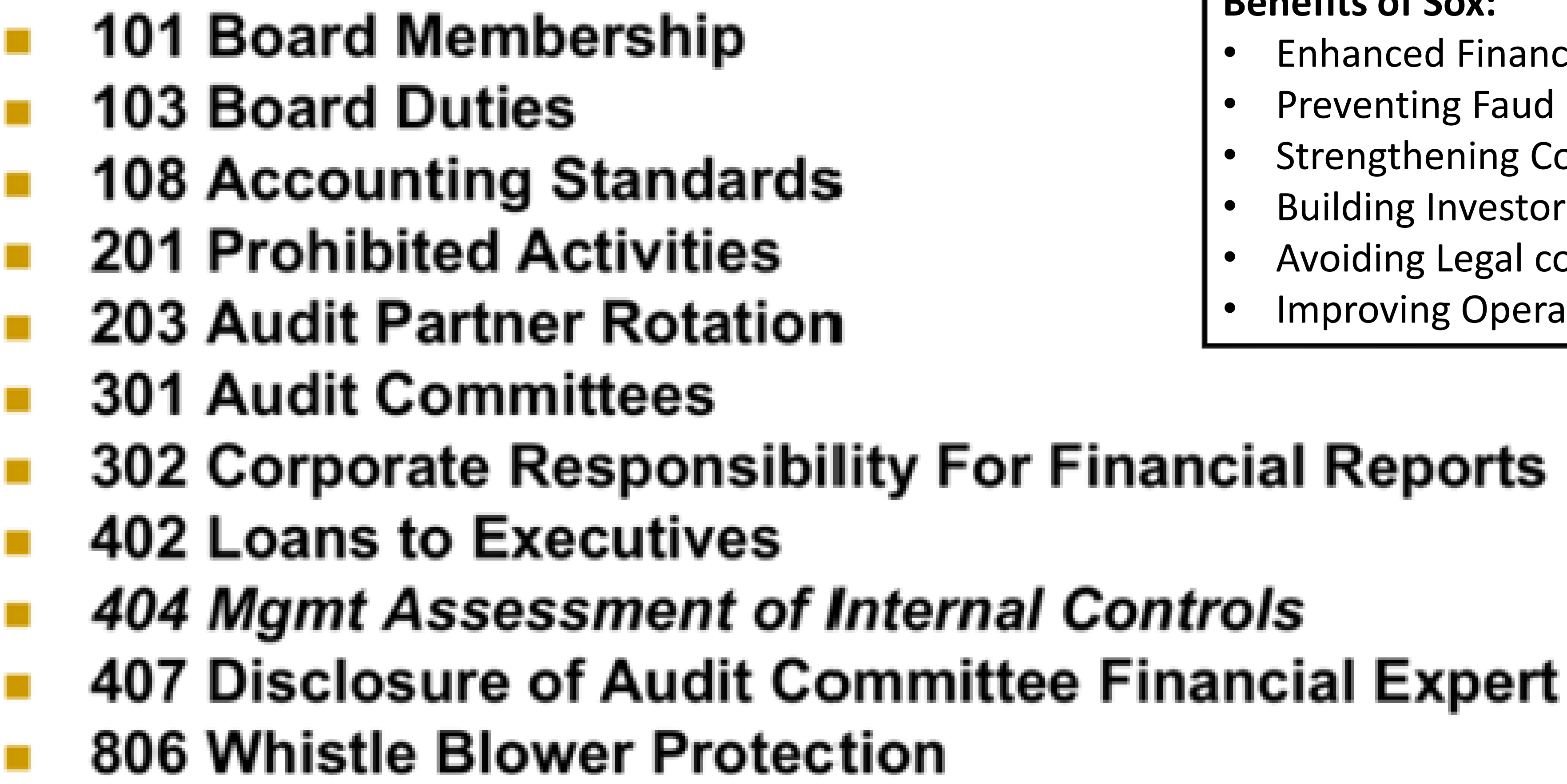
External Audits

- Regulatory Audits
- Standards Audits (e.g.,   ISO)
- Contractual Audits (e.g., PCI)

Reporting

- Internal
- Regulatory Bodies
- Customers

Sarbanes-Oxley Act



- 101 Board Membership
- 103 Board Duties
- 108 Accounting Standards
- 201 Prohibited Activities
- 203 Audit Partner Rotation
- 301 Audit Committees
- 302 Corporate Responsibility For Financial Reports
- 402 Loans to Executives
- *404 Mgmt Assessment of Internal Controls*
- 407 Disclosure of Audit Committee Financial Expert
- 806 Whistle Blower Protection

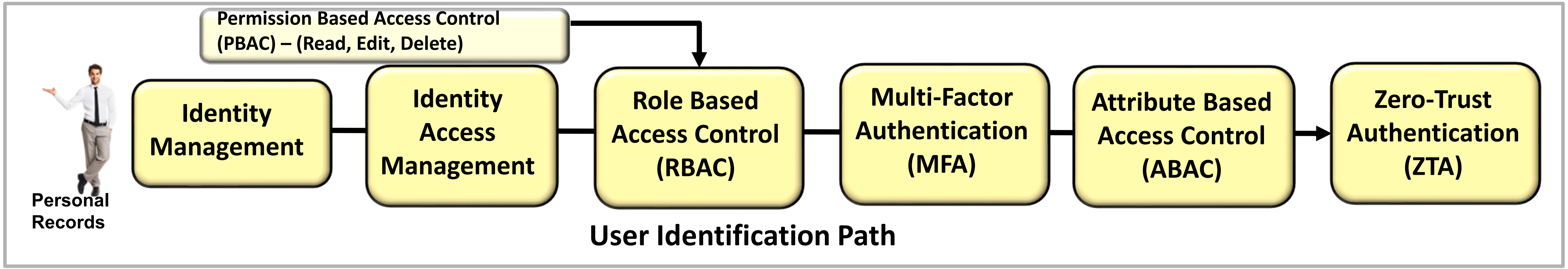
Benefits of Sox:

- Enhanced Financial Reporting Accuracy
- Preventing Faud and misconduct
- Strengthening Corporate Governance
- Building Investor trust
- Avoiding Legal consequences
- Improving Operational Efficiency

List of Sarbanes-Oxley Act Sections and their responsibilities

Identity and Access Management technologies

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



Permission Based Access Control (PBAC) – (Read, Edit, Delete)

Personal Records

Identity Management

Identity Access Management

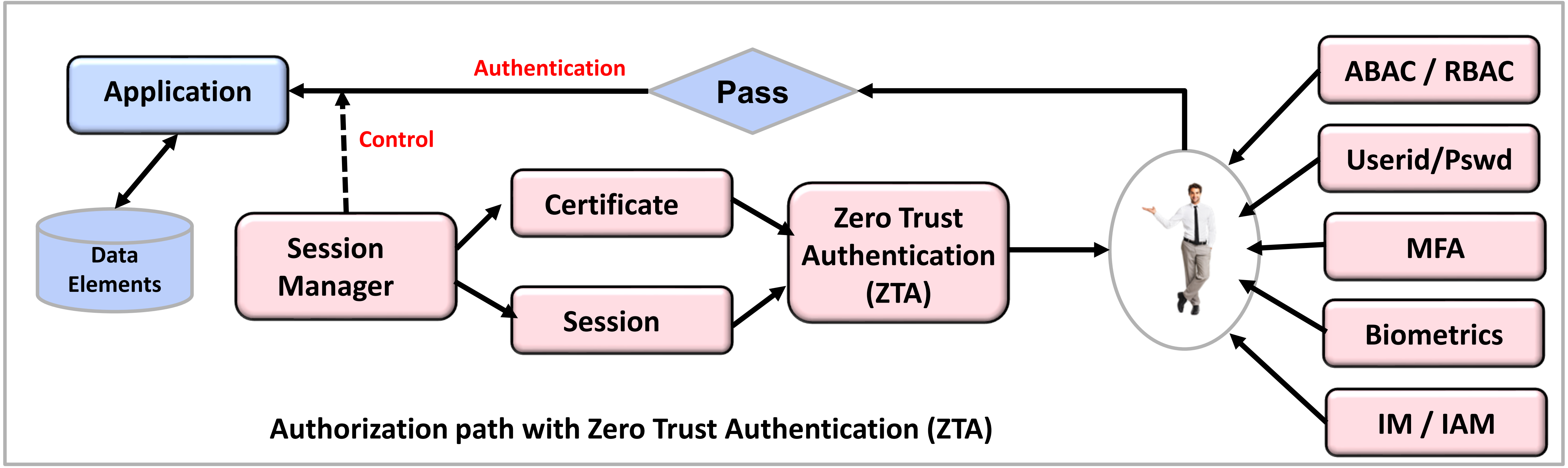
Role Based Access Control (RBAC)

Multi-Factor Authentication (MFA)

Attribute Based Access Control (ABAC)

Zero-Trust Authentication (ZTA)

User Identification Path



Application

Authentication

Pass

Control

Data Elements

Session Manager

Certificate

Session

Zero Trust Authentication (ZTA)

ABAC / RBAC

Userid/Pswd

MFA

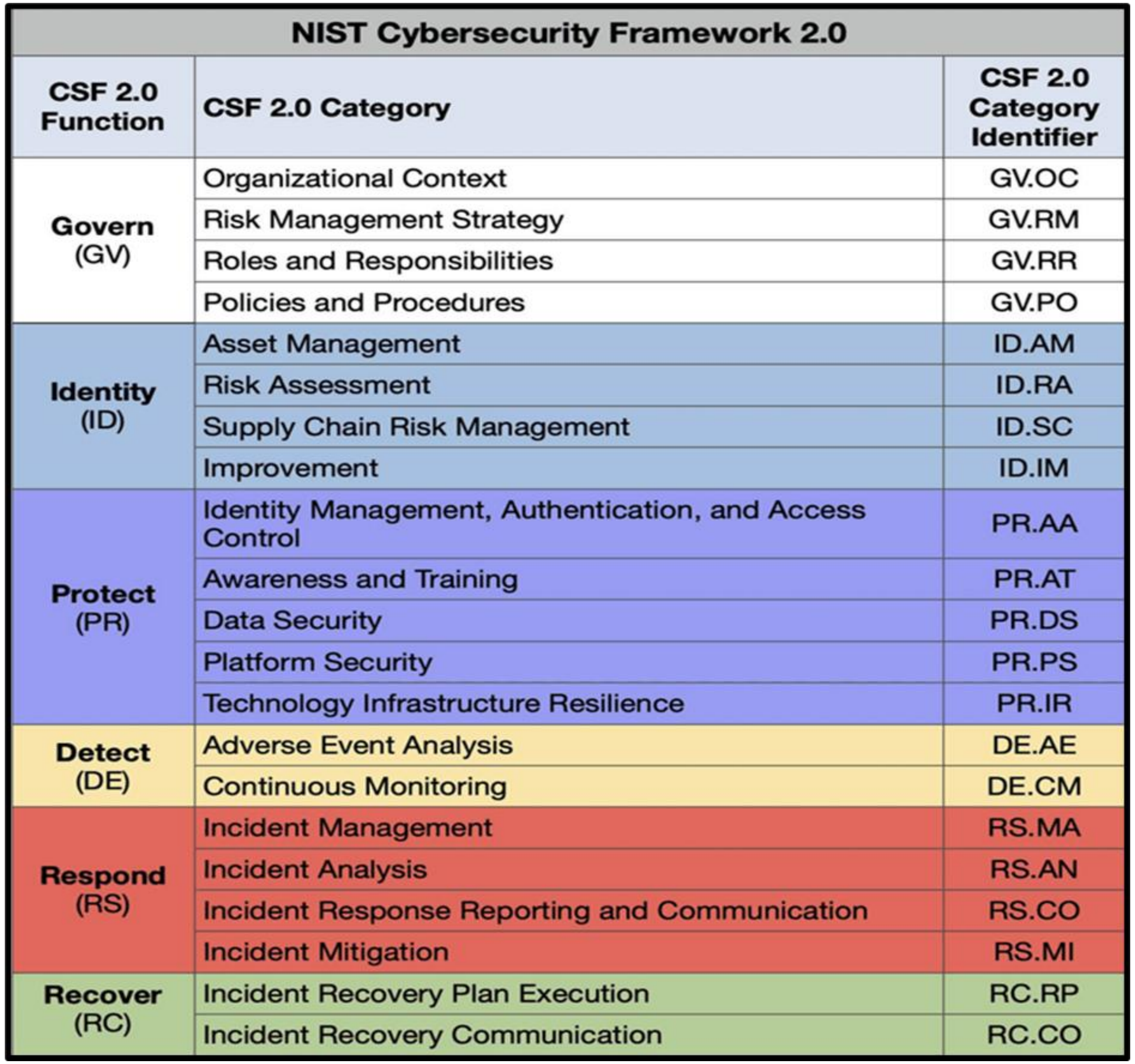
Biometrics

IM / IAM

Authorization path with Zero Trust Authentication (ZTA)

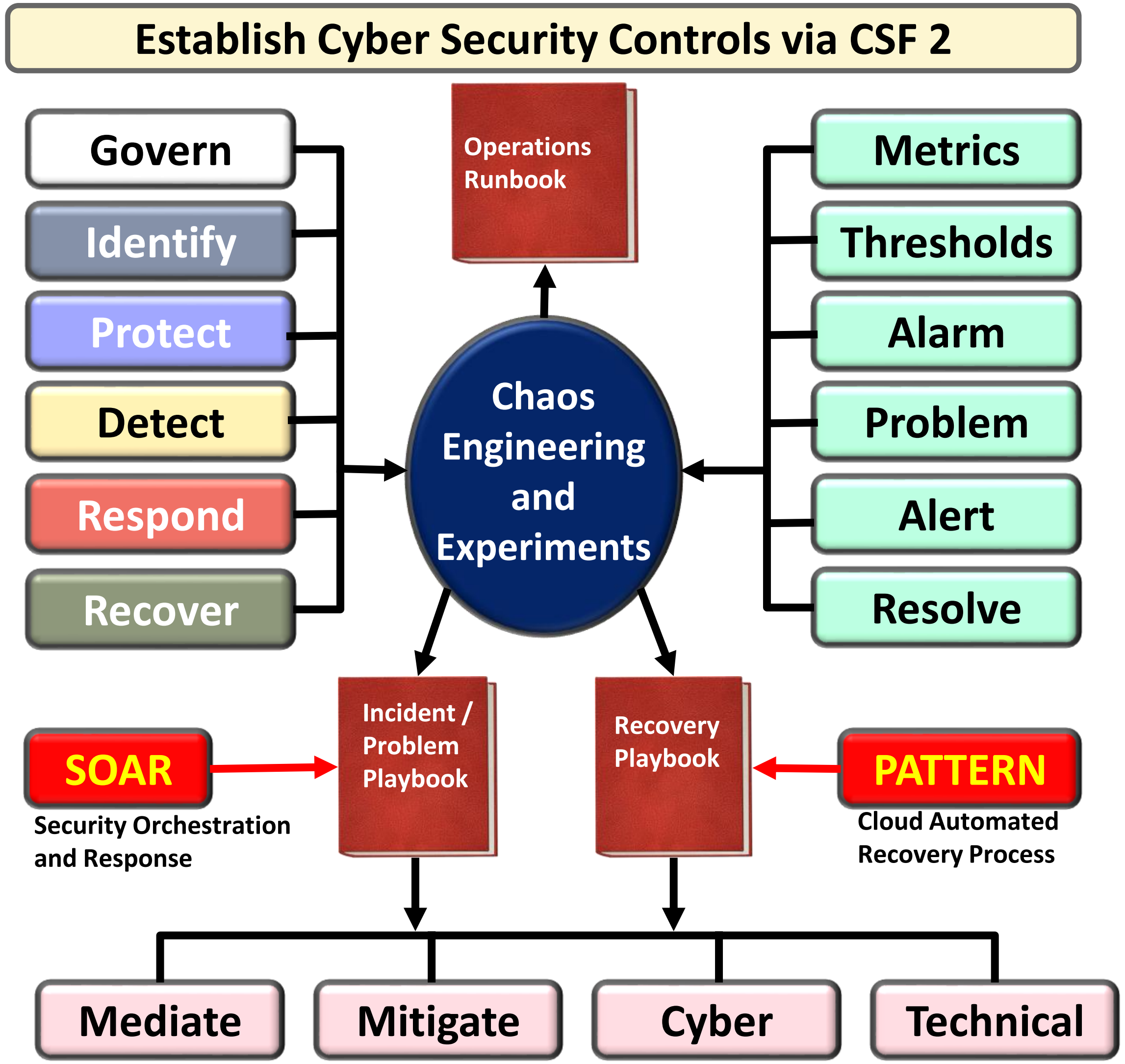
NIST CSF 2.0 Categories and Application

Thomas Bronack
Email: 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



Continuity of Operations Planning - COOP

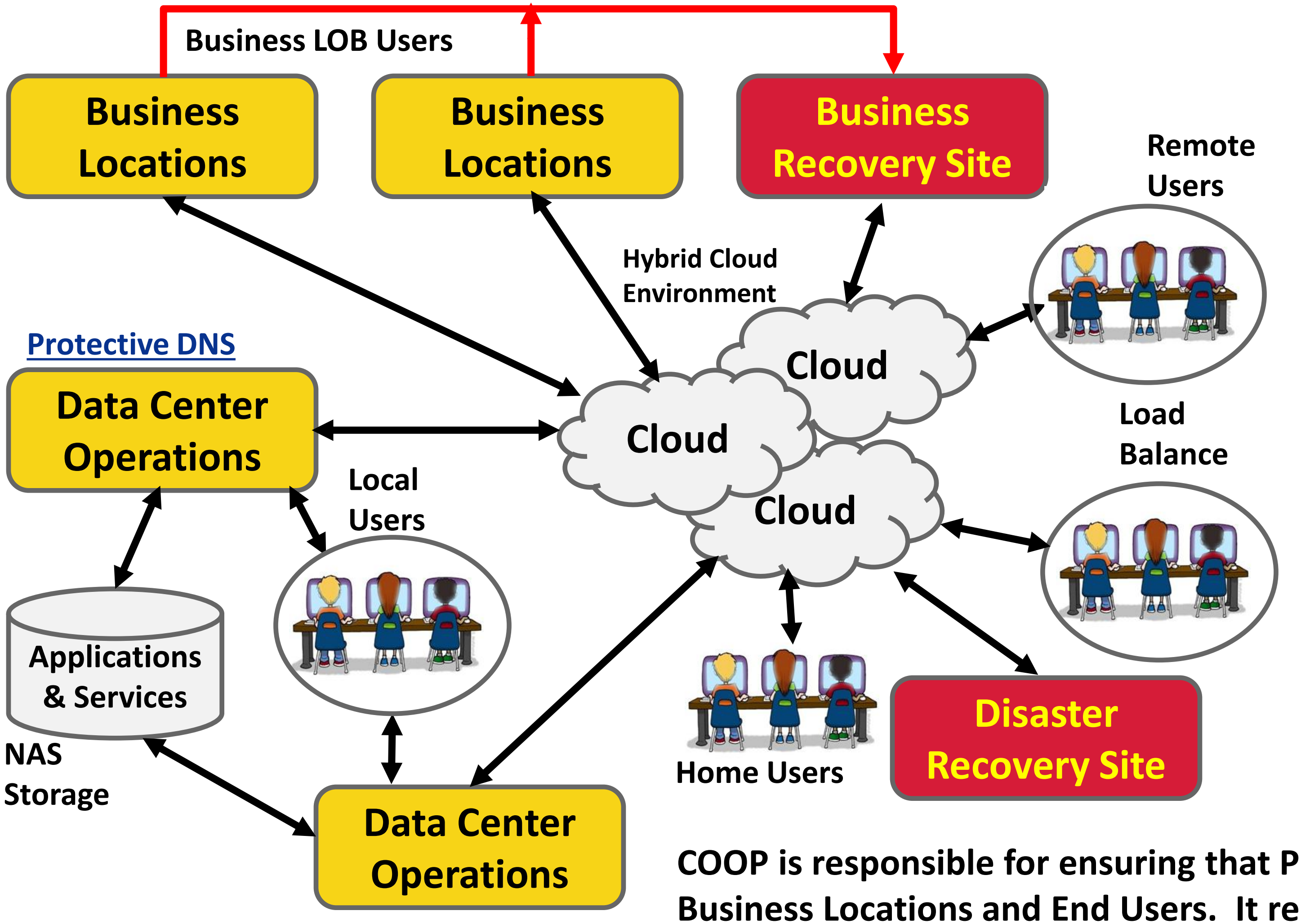
COOP – FEMA Overview

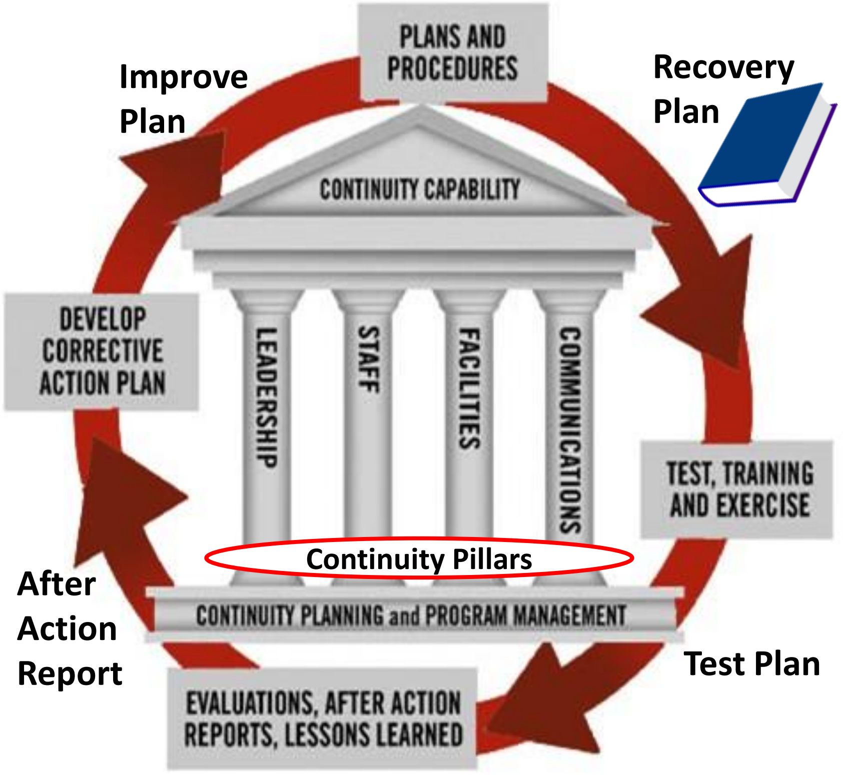
NSPD=51/HSDP-20

National Essential Functions - NEF

Primary Mission Essential Programs - PMEF

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





COOP Lifecycle and Functions – Continuity of Operations and Government Programs

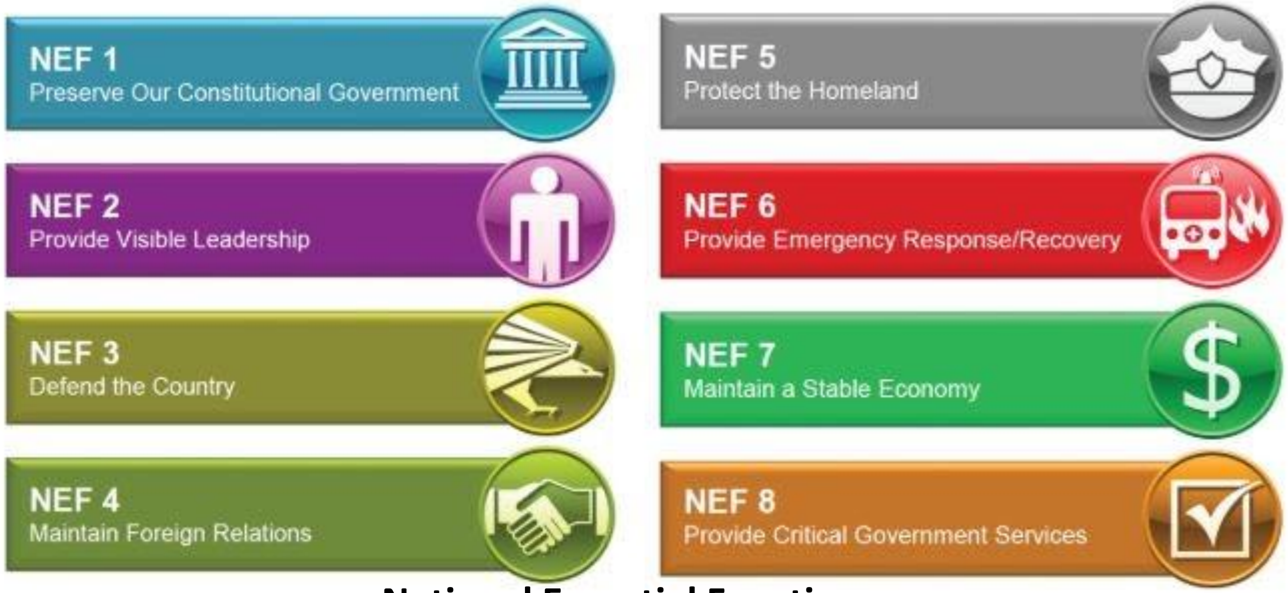
COOP is responsible for ensuring that Production Operations is always available to Business Locations and End Users. It requires a recovery capability for Business Locations and Data Center Operations that is satisfied by Business and Disaster Recovery Sites.

Continuity Of Operations Planning - Guidelines

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

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


NEF 1
Preserve Our Constitutional Government
NEF 2
Provide Visible Leadership
NEF 3
Defend the Country
NEF 4
Maintain Foreign Relations
NEF 5
Protect the Homeland
NEF 6
Provide Emergency Response/Recovery
NEF 7
Maintain a Stable Economy
NEF 8
Provide Critical Government Services

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[2].

Stages of the COOP Plan

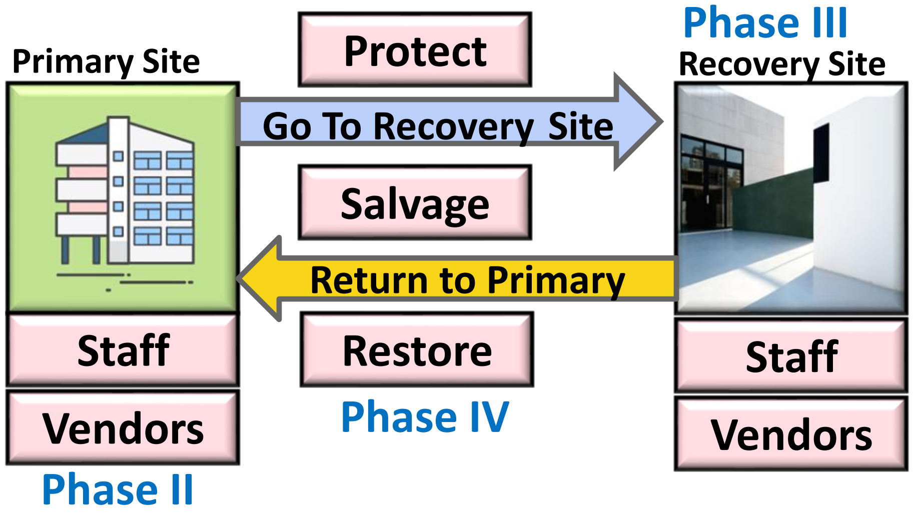
Thomas Bronack
Email: bronackt@dcag.com
Phone: (917) 673-6992

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)

Phase I

- Business Recovery Plan
- Disaster Recovery Plan
- Crisis Management Plan
- Emergency Management Plan



COOP Testing Process

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).

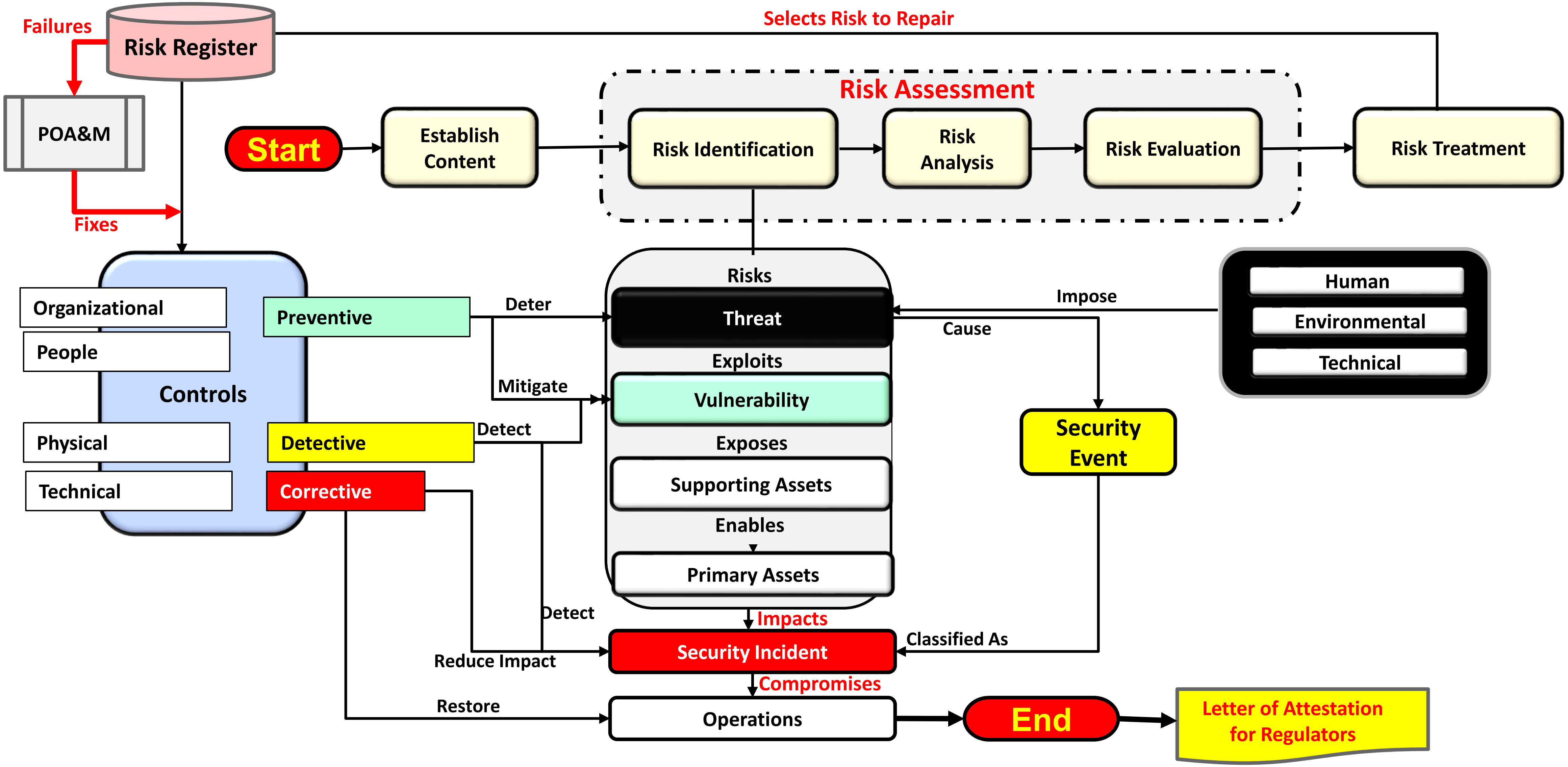
Remember that testing continuity capability involves a combination of training, exercises, and strategic planning to ensure readiness during emergencies[1234].

Learn more

1 fema.gov   2 en.wikipedia.org   3 fema.gov   4 jensenhughes.com

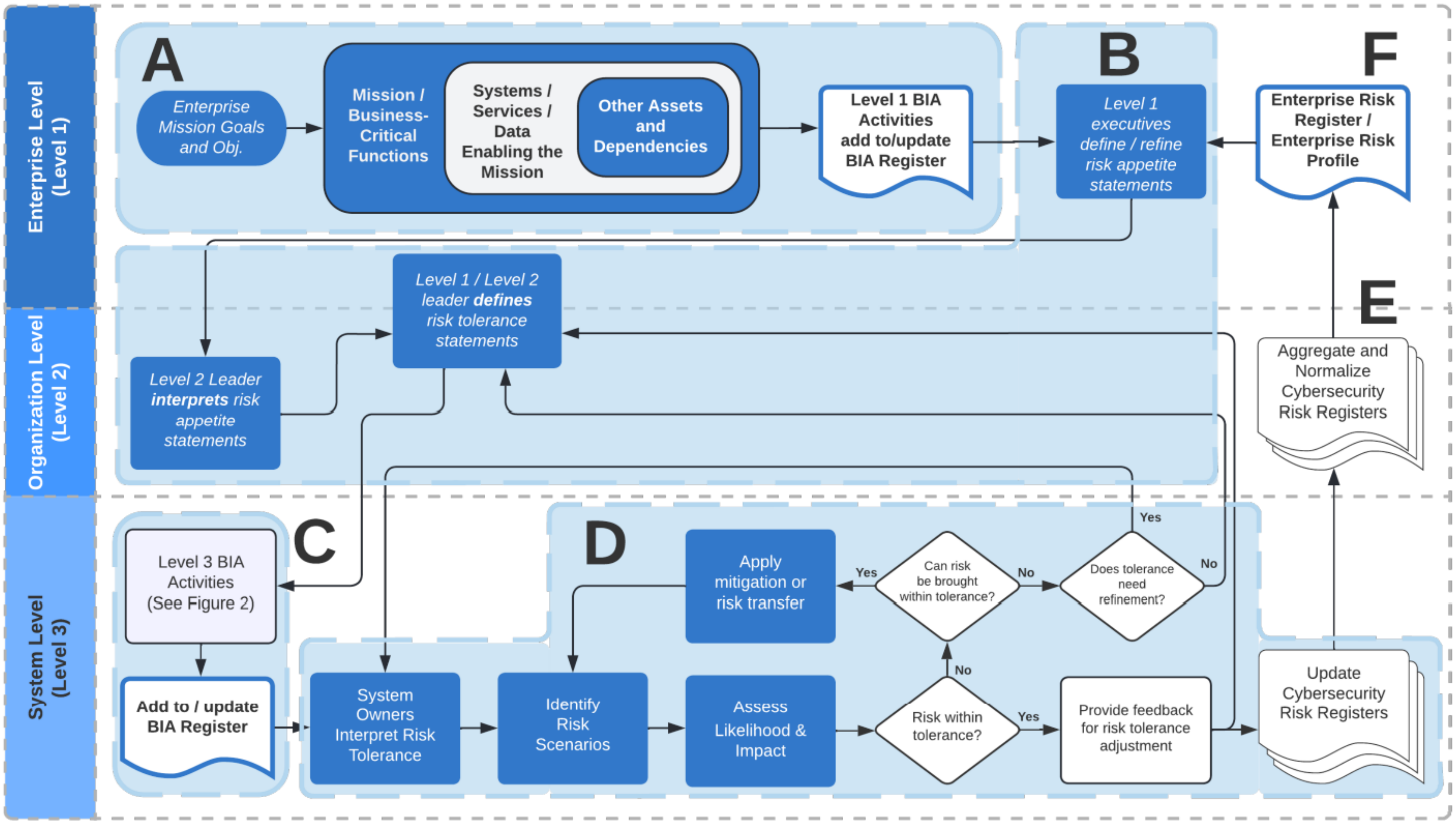
Risk Management with ISO 27000: 2022

Thomas Bronack
Email: 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
Phone: (917) 673-6992

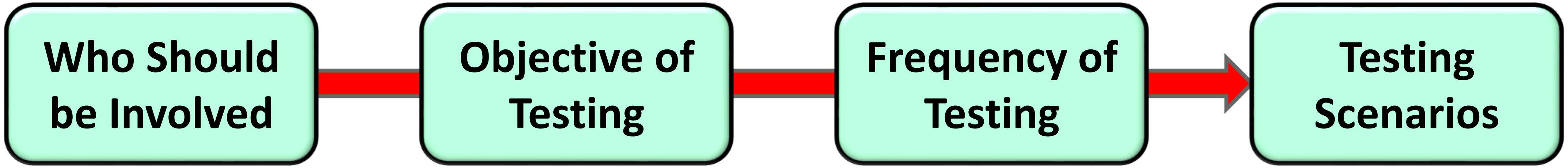

Enterprise Level (Level 1)
Organization Level (Level 2)
System Level (Level 3)
A
Enterprise Mission Goals and Obj.
Mission / Business-Critical Functions
Systems / Services / Data Enabling the Mission
Other Assets and Dependencies
Level 1 BIA Activities add to/update BIA Register
B
Level 1 executives define / refine risk appetite statements
F
Enterprise Risk Register / Enterprise Risk Profile
Level 1 / Level 2 leader defines risk tolerance statements
Level 2 Leader interprets risk appetite statements
E
Aggregate and Normalize Cybersecurity Risk Registers
C
Level 3 BIA Activities (See Figure 2)
Add to / update BIA Register
D
Apply mitigation or risk transfer
Yes
Can risk be brought within tolerance?
No
Yes
Does tolerance need refinement?
No
System Owners Interpret Risk Tolerance
Identify Risk Scenarios
Assess Likelihood & Impact
No
Risk within tolerance?
Yes
Provide feedback for risk tolerance adjustment
Update Cybersecurity Risk Registers

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

Testing Business Continuity Plans

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



Who Should be Involved

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

Objective of Testing

- 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.

Frequency of Testing

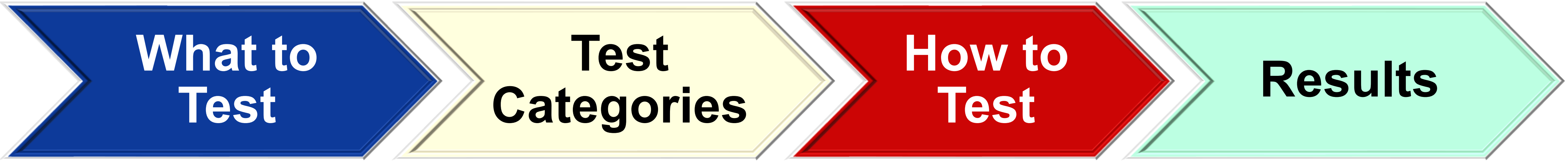
- Business Continuity and Disaster Recovery Plan review and testing should be performed at least quarterly.
- Shift from one application / service to another to provide continuous testing and protection

Testing Scenarios

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

IT/DR Testing Process Overview

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



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

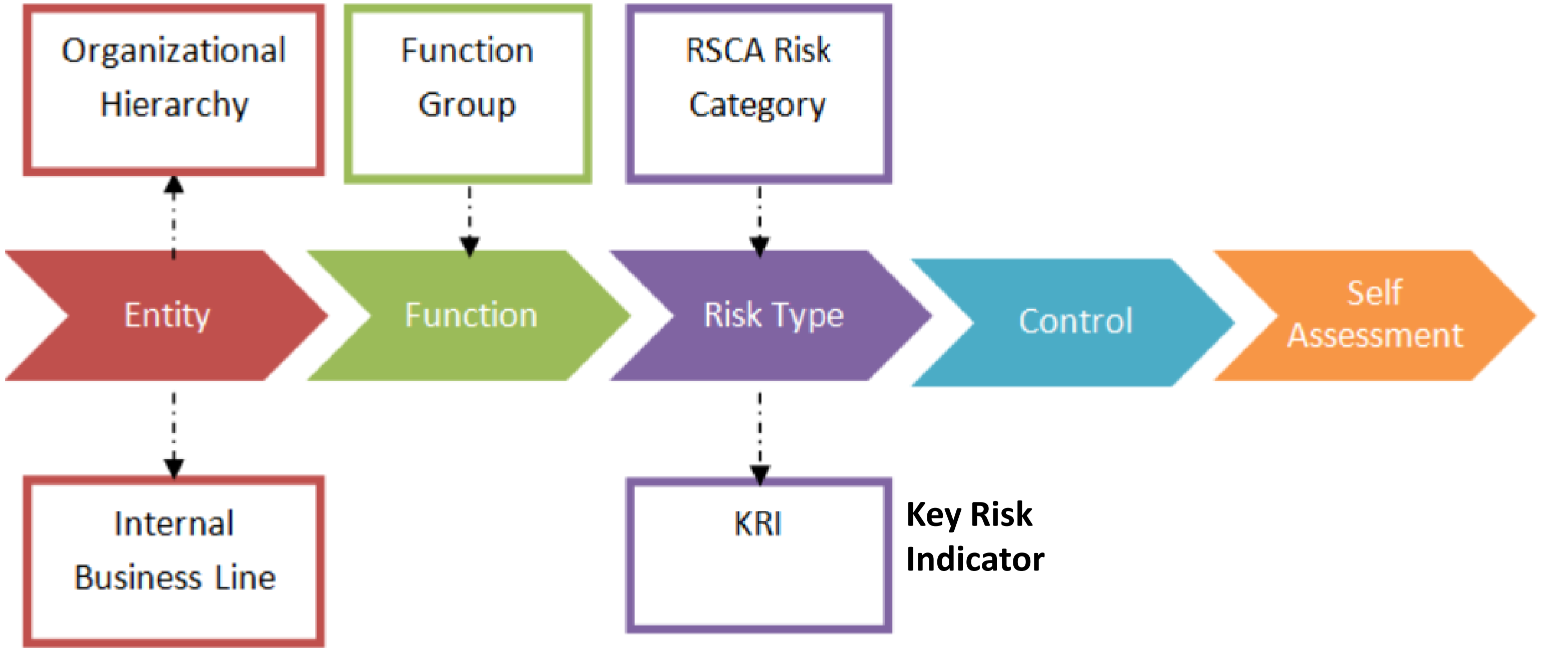
- Data Sensitivity. Including:
  - Ownership;
  - Data Criticality;
  - Legal & Regulatory;
  - Usage Categories (Create, Read, Update, Delete).
  - Access Controls using:
    - Application ID,
    - User ID;
    - Password;
    - Single Log-On;
    - Group Log-on.
- Vital Records Management:
  - Backup / 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

Risk Control Self Assessment (RCSA)

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

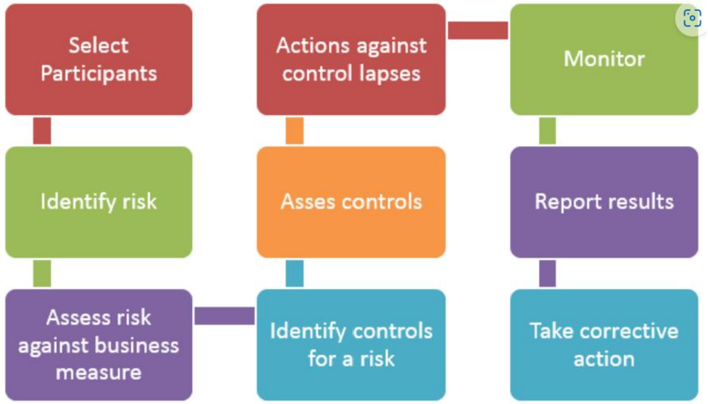


RCSA (Risk Control Self Assessment) is an empowering method/process by which management and staff of all levels collectively identify and evaluate risks and associated controls. It adds value by increasing an operating unit's involvement in designing and maintaining control and risk systems, identifying 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

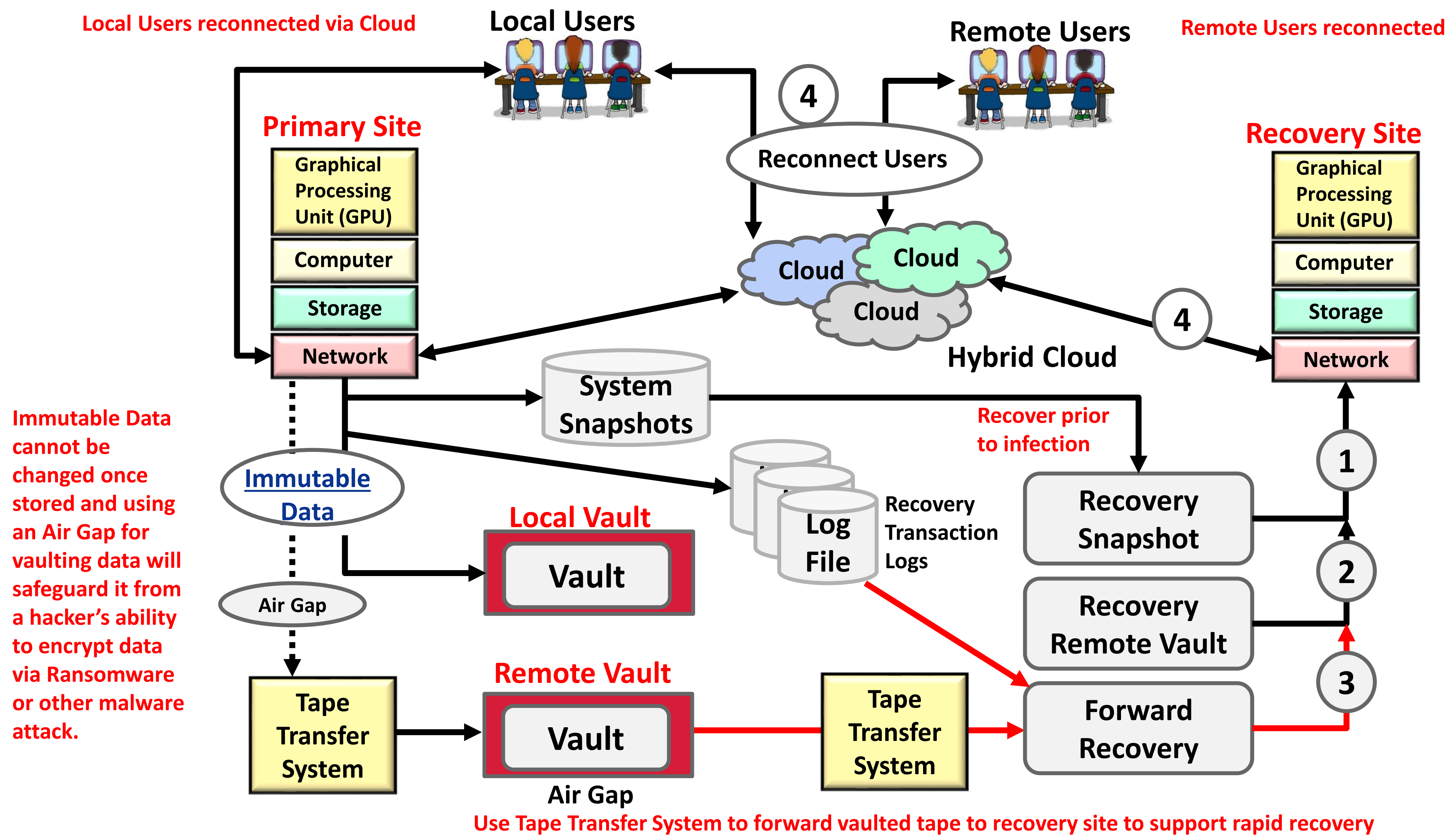
Steps within a RCSA are:

1. Select Participants
2. Identify Risks
3. Assess Risk aginst 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


Select Participants
Identify risk
Assess risk against business measure
Identify controls for a risk
Asses controls
Actions against control lapses
Monitor
Report results
Take corrective action

System Recovery – Even with Ransomware

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



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.

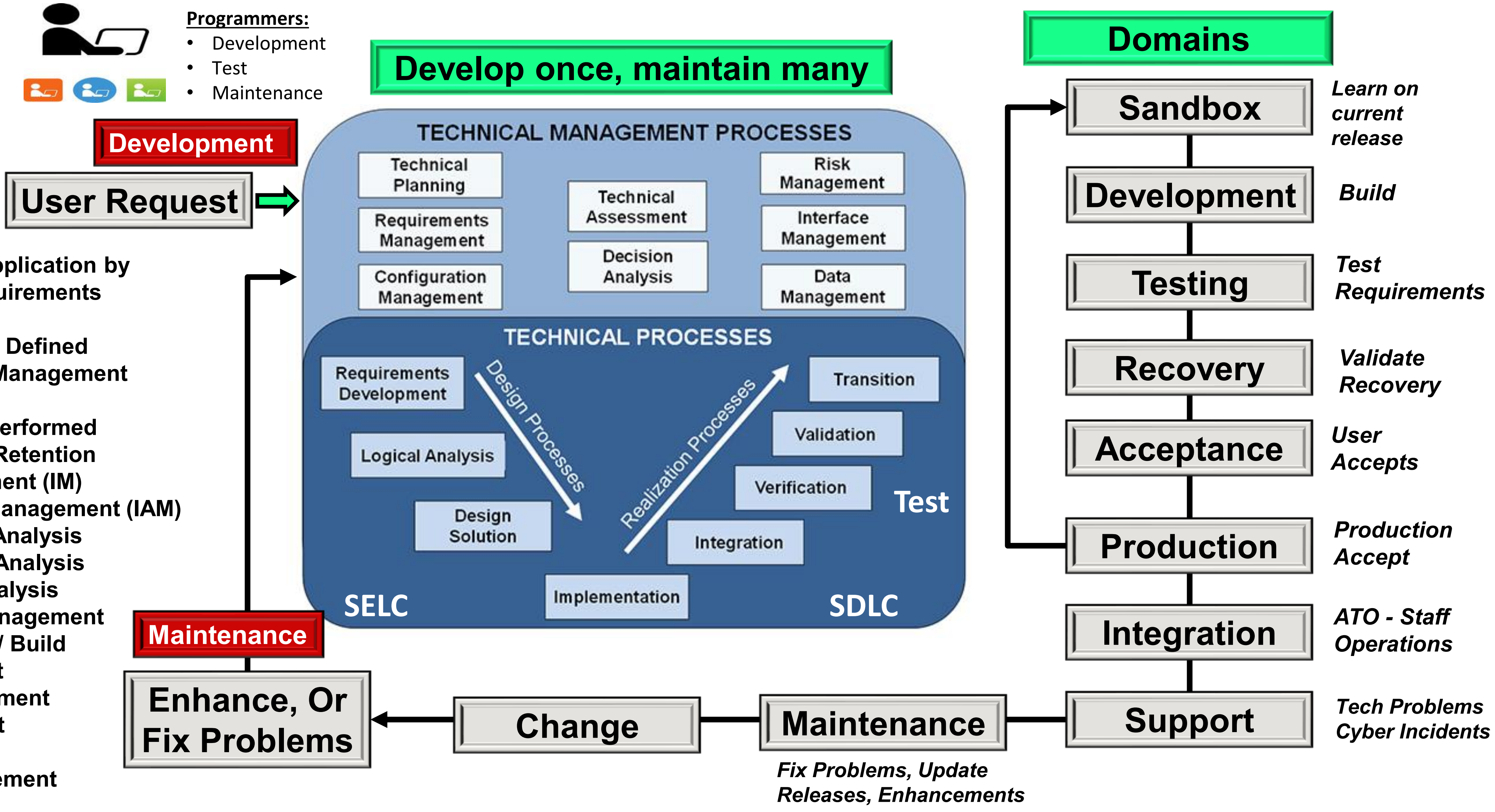
Use Tape Transfer System to forward vaulted tape to recovery site to support rapid recovery

Recovery Process:

1. Recover System Snapshot prior to infection to restore system.
2. Recovery 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.

Building and Implementing an Application

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



Programmers:

- Development
- Test
- Maintenance

Domain	Purpose
Sandbox	*Learn on current release*
Development	*Build*
Testing	*Test Requirements*
Recovery	*Validate Recovery*
Acceptance	*User Accepts*
Production	*Production Accept*
Integration	*ATO - Staff Operations*
Support	*Tech Problems Cyber Incidents*

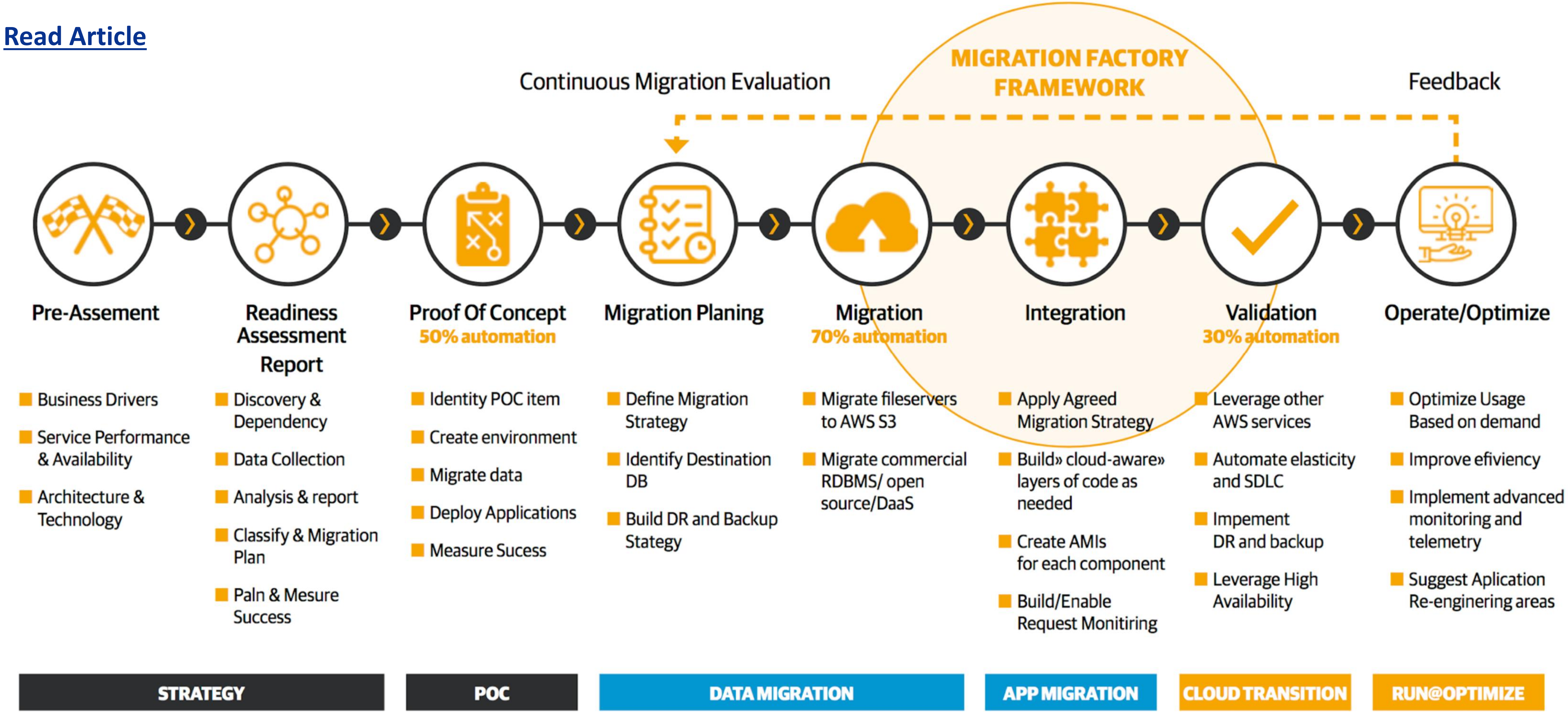
Maintenance: *Fix Problems, Update Releases, Enhancements*

- User Requests Application by providing a “Requirements Definition”
- Business Reason Defined
- Asset Definition Management (ADM)
- Data Sensitivity performed
- Data Handling & Retention
- Identity Management (IM)
- Identity Access Management (IAM)
- Business Needs Analysis
- Technical Needs Analysis
- Requirements Analysis
- Configuration Management
- Decision for Buy / Build
- Risk Management
- Interface Management
- Data Management
- Vital Records
- Recovery Management

Planning for Migrating Applications to the Cloud

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

Read Article



Continuous Migration Evaluation

MIGRATION FACTORY FRAMEWORK

Feedback

Pre-Assement
- Business Drivers
- Service Performance & Availability
- Architecture & Technology

Readiness Assessment Report
- Discovery & Dependency
- Data Collection
- Analysis & report
- Classify & Migration Plan
- Paln & Mesure Success

Proof Of Concept
50% automation
- Identity POC item
- Create environment
- Migrate data
- Deploy Applications
- Measure Sucess

Migration Planing
- Define Migration Strategy
- Identify Destination DB
- Build DR and Backup Stategy

Migration
70% automation
- Migrate fileservers to AWS S3
- Migrate commercial RDBMS/ open source/DaaS

Integration
- Apply Agreed Migration Strategy
- Build» cloud-aware» layers of code as needed
- Create AMIs for each component
- Build/Enable Request Monitiring

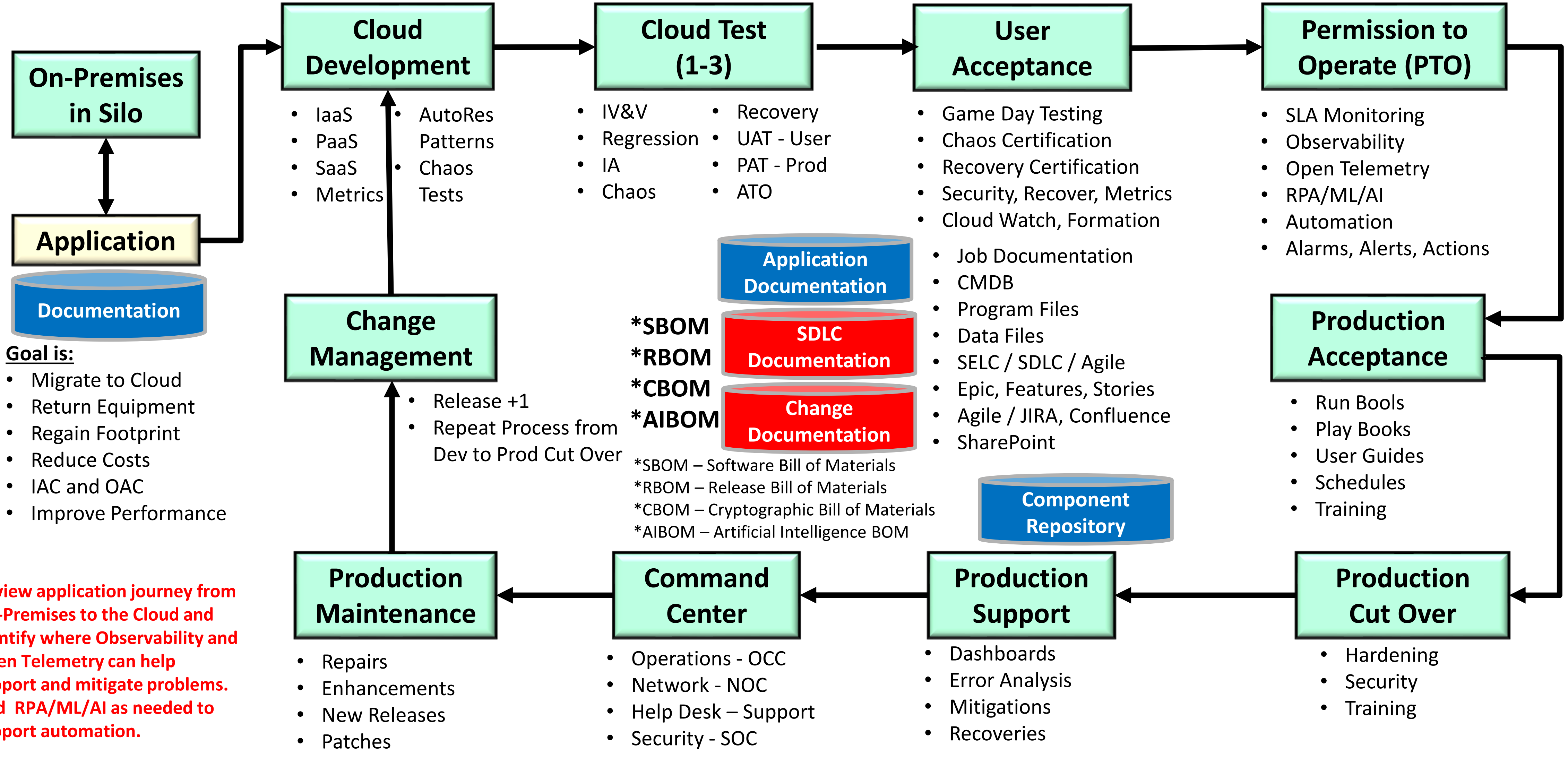
Validation
30% automation
- Leverage other AWS services
- Automate elasticity and SDLC
- Impement DR and backup
- Leverage High Availability

Operate/Optimize
- Optimize Usage Based on demand
- Improve efiviency
- Implement advanced monitoring and telemetry
- Suggest Aplication Re-enginering areas

STRATEGY | POC | DATA MIGRATION | APP MIGRATION | CLOUD TRANSITION | RUN@OPTIMIZE

Migrating Applications to the Cloud

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



On-Premises in Silo

Application

Documentation

Goal is:

- Migrate to Cloud
- Return Equipment
- Regain Footprint
- Reduce Costs
- IAC and OAC
- Improve Performance

Cloud Development

- IaaS
- PaaS
- SaaS
- Metrics

- AutoRes Patterns
- Chaos Tests

Cloud Test (1-3)

- IV&V
- Regression
- IA
- Chaos

- Recovery
- UAT - User
- PAT - Prod
- ATO

User Acceptance

- Game Day Testing
- Chaos Certification
- Recovery Certification
- Security, Recover, Metrics
- Cloud Watch, Formation

Permission to Operate (PTO)

- SLA Monitoring
- Observability
- Open Telemetry
- RPA/ML/AI
- Automation
- Alarms, Alerts, Actions

Application Documentation

***SBOM**
***RBOM**
***CBOM**
***AIBOM**

SDLC Documentation

Change Documentation

- Job Documentation
- CMDB
- Program Files
- Data Files
- SELC / SDLC / Agile
- Epic, Features, Stories
- Agile / JIRA, Confluence
- SharePoint

*SBOM – Software Bill of Materials
*RBOM – Release Bill of Materials
*CBOM – Cryptographic Bill of Materials
*AIBOM – Artificial Intelligence BOM

Component Repository

Change Management

- Release +1
- Repeat Process from Dev to Prod Cut Over

Production Acceptance

- Run Bools
- Play Books
- User Guides
- Schedules
- Training

Production Cut Over

- Hardening
- Security
- Training

Production Support

- Dashboards
- Error Analysis
- Mitigations
- Recoveries

Command Center

- Operations - OCC
- Network - NOC
- Help Desk – Support
- Security - SOC

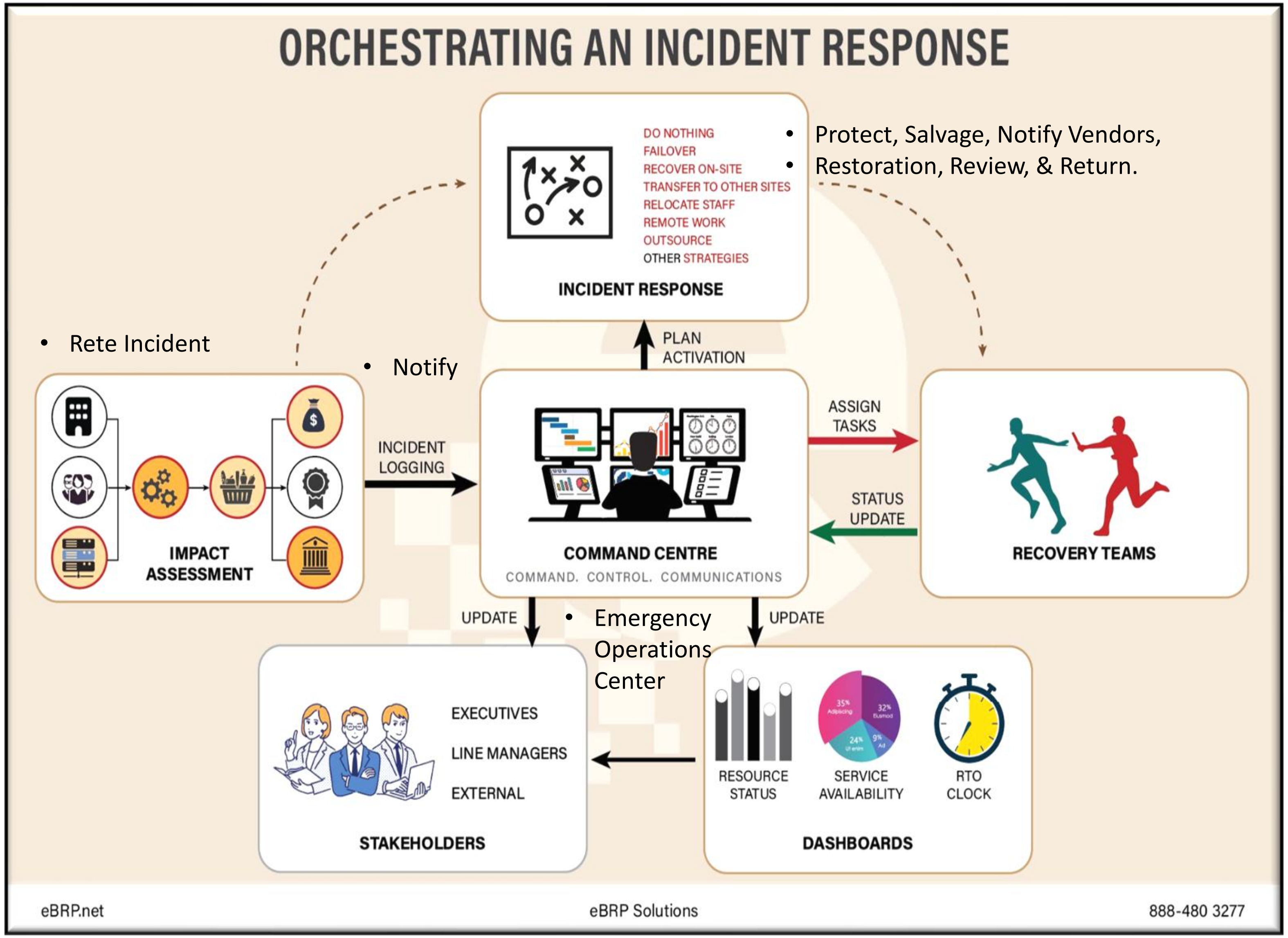
Production Maintenance

- Repairs
- Enhancements
- New Releases
- Patches

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 Center

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



- Protect, Salvage, Notify Vendors,
- Restoration, Review, & Return.

- Rete Incident

- Notify

- Emergency Operations Center

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.

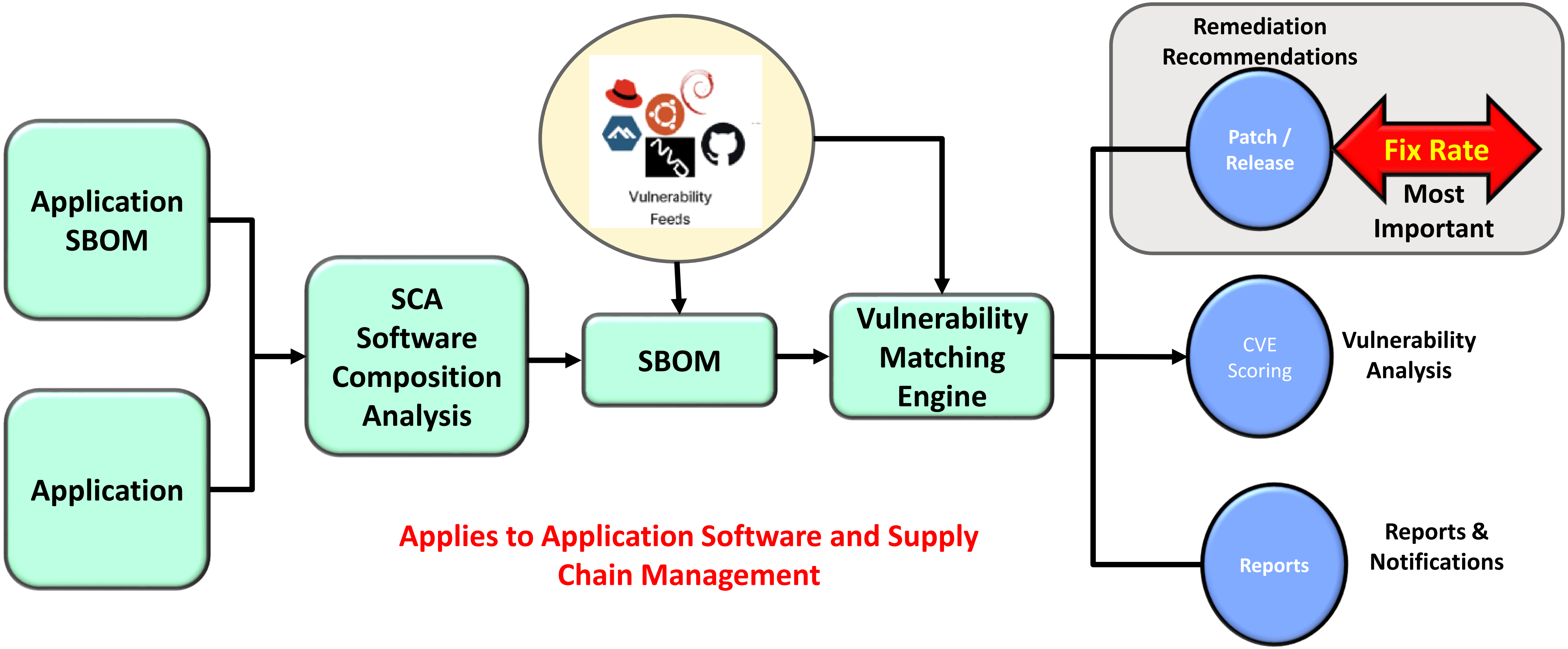
Compliance and Reporting: Ensures that response efforts are documented and reported, meeting regulatory and compliance requirements.

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.



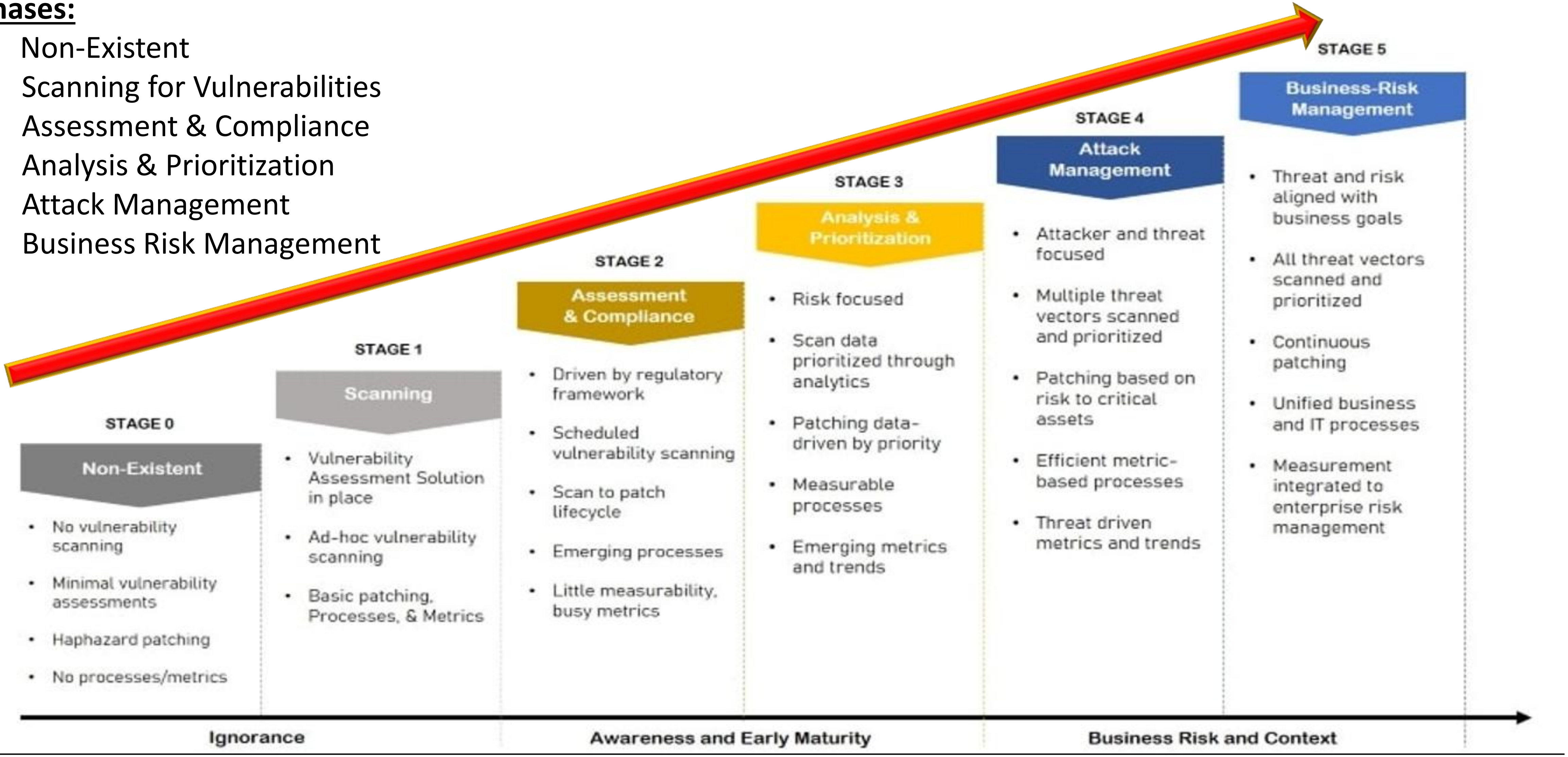
Applies to Application Software and Supply Chain Management

Vulnerability Management Maturity Model

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

Phases:

0. Non-Existent
1. Scanning for Vulnerabilities
2. Assessment & Compliance
3. Analysis & Prioritization
4. Attack Management
5. Business Risk Management



STAGE 0

Non-Existent

- No vulnerability scanning
- Minimal vulnerability assessments
- Haphazard patching
- No processes/metrics

STAGE 1

Scanning

- Vulnerability Assessment Solution in place
- Ad-hoc vulnerability scanning
- Basic patching, Processes, & Metrics

STAGE 2

Assessment & Compliance

- Driven by regulatory framework
- Scheduled vulnerability scanning
- Scan to patch lifecycle
- Emerging processes
- Little measurability, busy metrics

STAGE 3

Analysis & Prioritization

- Risk focused
- Scan data prioritized through analytics
- Patching data-driven by priority
- Measurable processes
- Emerging metrics and trends

STAGE 4

Attack Management

- Attacker and threat focused
- Multiple threat vectors scanned and prioritized
- Patching based on risk to critical assets
- Efficient metric-based processes
- Threat driven metrics and trends

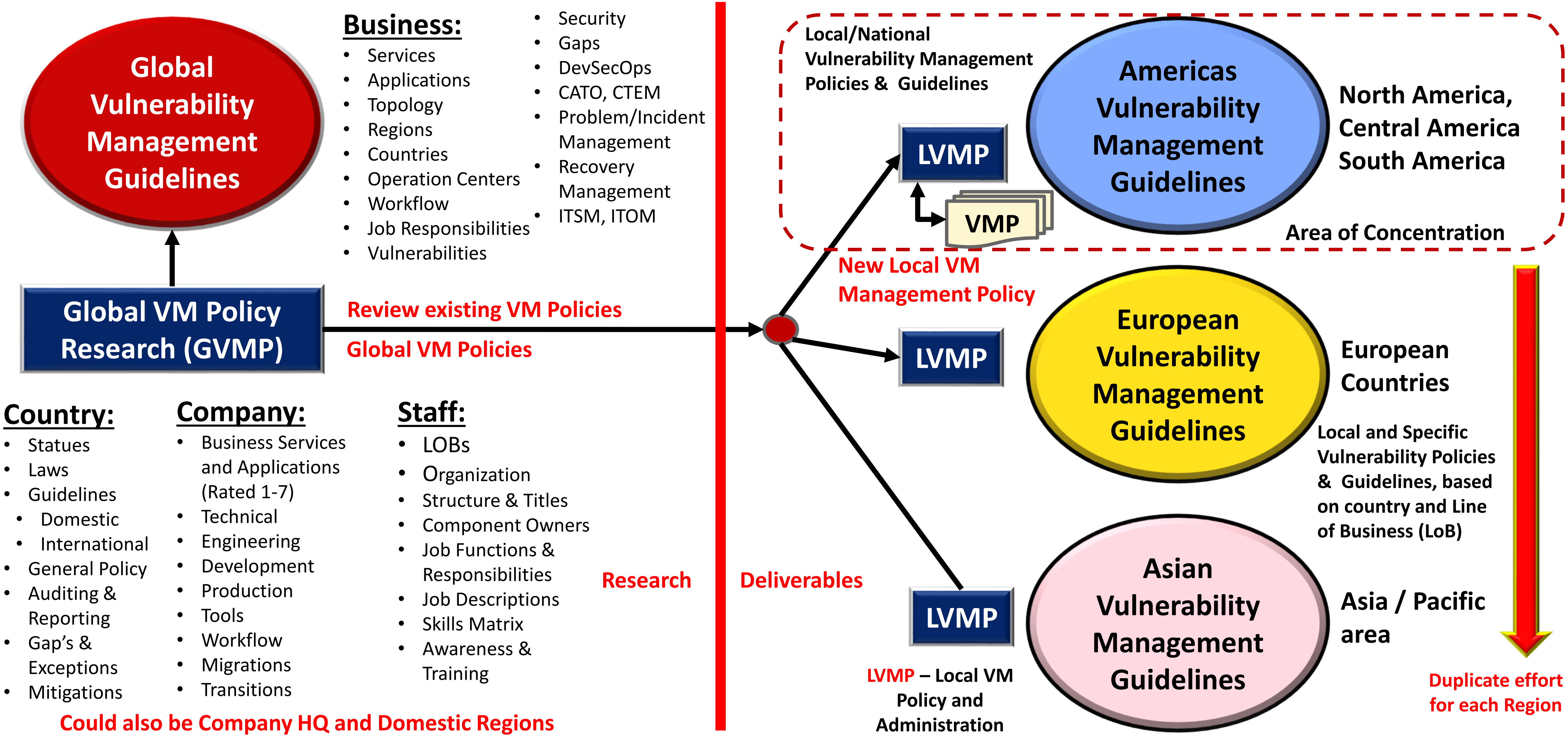
STAGE 5

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 management

Solution - Vulnerability Management Policy

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



Global Vulnerability Management Guidelines
Global VM Policy Research (GVMP)
Review existing VM Policies
Global VM Policies
Research
Deliverables
Local/National Vulnerability Management Policies & Guidelines
LVMP
VMP
Americas Vulnerability Management Guidelines
North America, Central America South America
Area of Concentration
New Local VM Management Policy
LVMP
European Vulnerability Management Guidelines
European Countries
Local and Specific Vulnerability Policies & Guidelines, based on country and Line of Business (LoB)
LVMP
Asian Vulnerability Management Guidelines
Asia / Pacific area
Duplicate effort for each Region

LVMP – Local VM Policy and Administration

Business:

- Services
- Applications
- Topology
- Regions
- Countries
- Operation Centers
- Workflow
- Job Responsibilities
- Vulnerabilities
- Security
- Gaps
- DevSecOps
- CATO, CTEM
- Problem/Incident Management
- Recovery Management
- 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

Resiliency Operations Center (ROC)

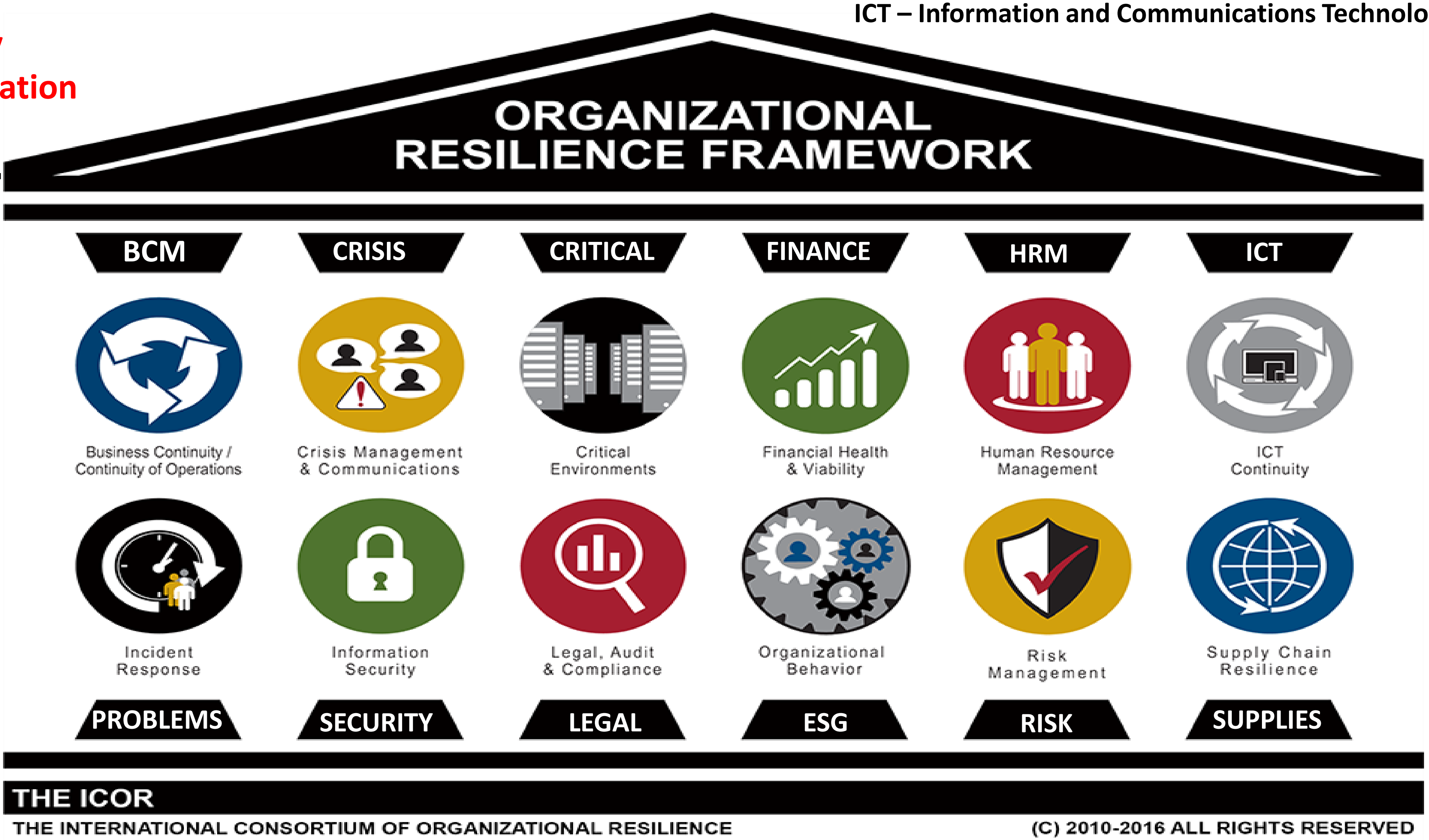
Thomas Bronack
Email: bronackt@dcag.com
Phone: (917) 673-6992

ICT – Information and Communications Technology

Coordinating Resiliency throughout the organization

Resiliency Operations Center (ROC)

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


ORGANIZATIONAL RESILIENCE FRAMEWORK
BCM
CRISIS
CRITICAL
FINANCE
HRM
ICT
Business Continuity / Continuity of Operations
Crisis Management & Communications
Critical Environments
Financial Health & Viability
Human Resource Management
ICT Continuity
Incident Response
Information Security
Legal, Audit & Compliance
Organizational Behavior
Risk Management
Supply Chain Resilience
PROBLEMS
SECURITY
LEGAL
ESG
RISK
SUPPLIES
THE ICOR
THE INTERNATIONAL CONSORTIUM OF ORGANIZATIONAL RESILIENCE
(C) 2010-2016 ALL RIGHTS RESERVED

Resiliency Operational Center (ROC)

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

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[1].
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[1].
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[1].

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

Benefits derived from a Resiliency Operations Center

Thomas Bronack
Email: 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:

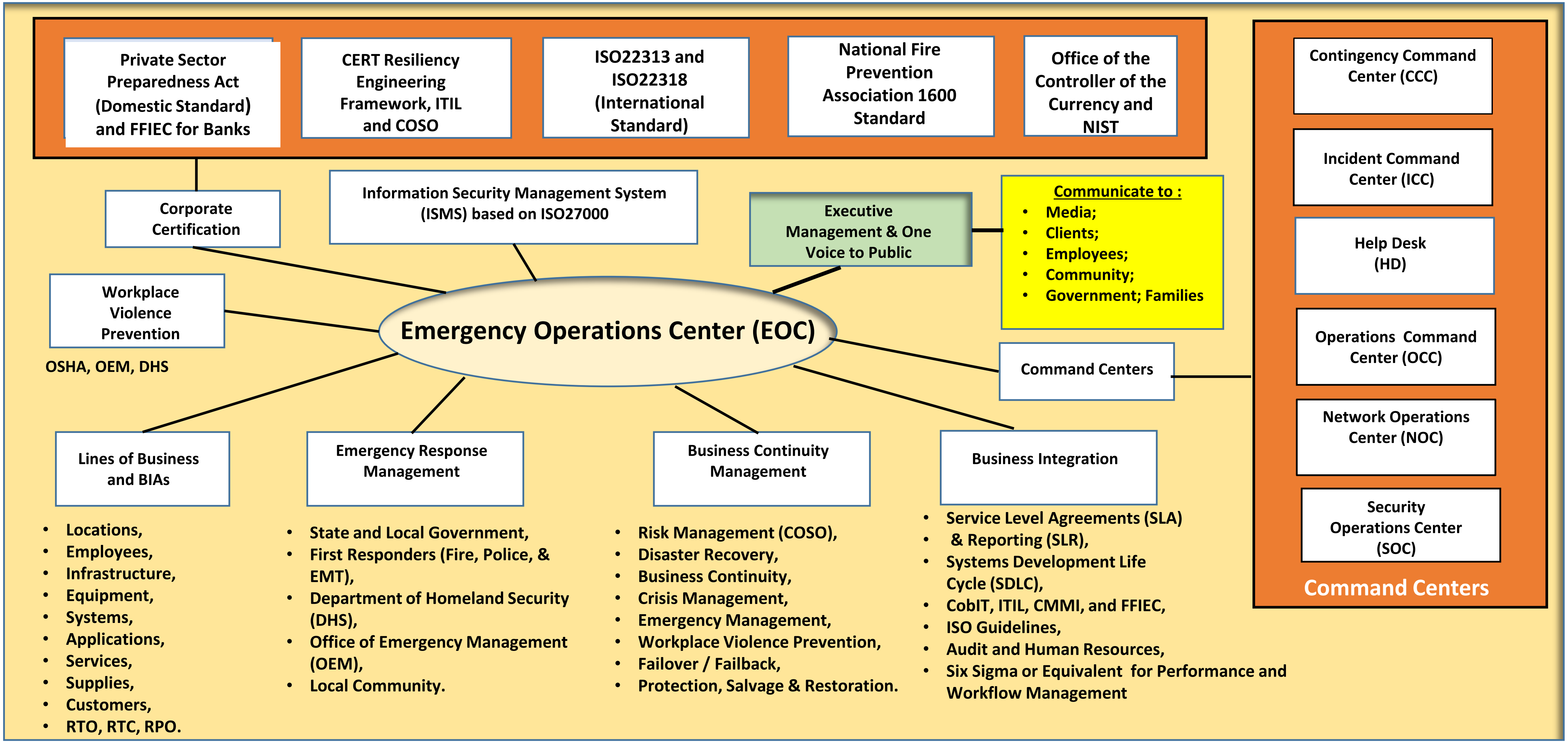
- **Shifting behavior from response to prevention.** Deep, comprehensive planning helps teams anticipate events, evaluate alternatives, prevent disruptions, and model all scenarios and options. Reacting to events as they happen is not sufficient in today's competitive market.

- **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
Phone: (917) 673-6992



Private Sector Preparedness Act (Domestic Standard) and FFIEC for Banks

CERT Resiliency Engineering Framework, ITIL and COSO

ISO22313 and ISO22318 (International Standard)

National Fire Prevention Association 1600 Standard

Office of the Controller of the Currency and NIST

Corporate Certification

Information Security Management System (ISMS) based on ISO27000

Executive Management & One Voice to Public

Communicate to :

- Media;
- Clients;
- Employees;
- Community;
- Government; Families

Workplace Violence Prevention

OSHA, OEM, DHS

Emergency Operations Center (EOC)

Command Centers

Lines of Business and BIAs

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

Emergency Response Management

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

Business Continuity Management

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

Business Integration

- 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

Contingency Command Center (CCC)

Incident Command Center (ICC)

Help Desk (HD)

Operations Command Center (OCC)

Network Operations Center (NOC)

Security Operations Center (SOC)

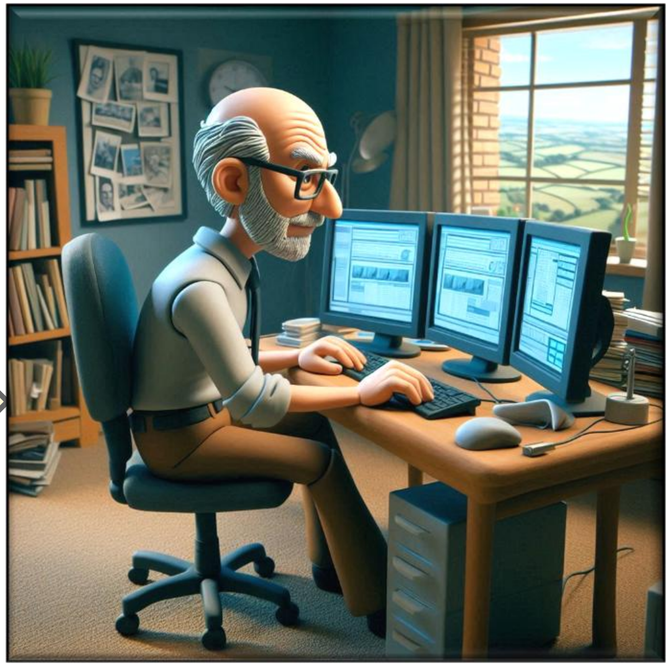
Command Centers

Reaching out to assist our clients

- **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
Website: http://www.dcag.com
bronackt@dcag.com
bronackt@gmail.com
917-673-6992