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**.

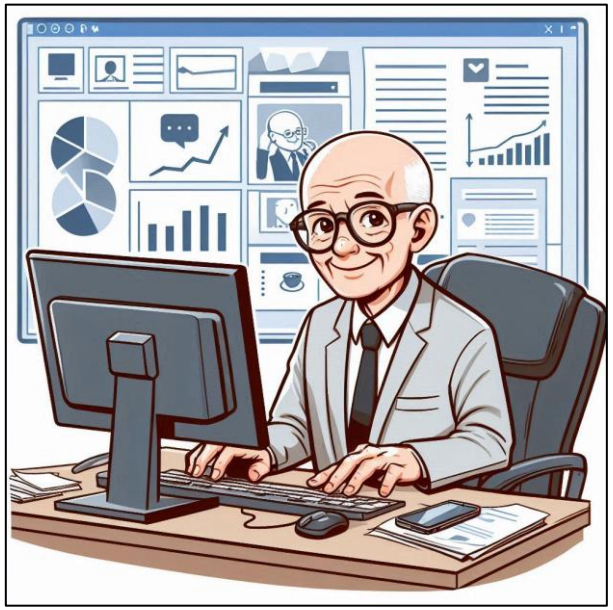
A word from Thomas Bronack

Thomas Bronack
Email: 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.



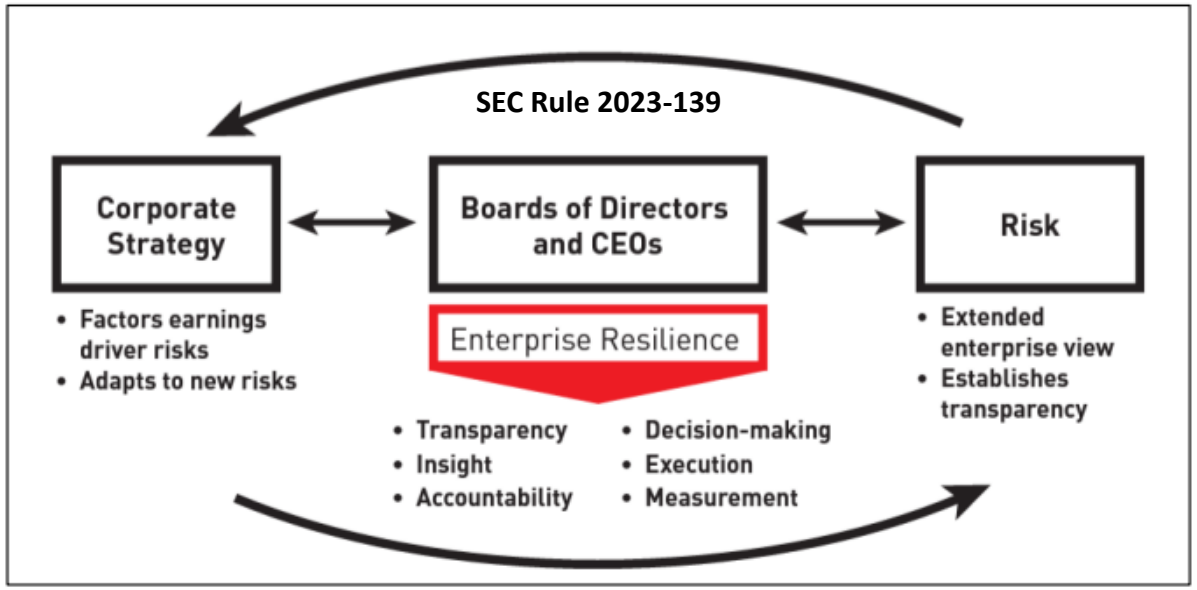
A strong generalist with extensive IT industry experience, ready to help you.

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

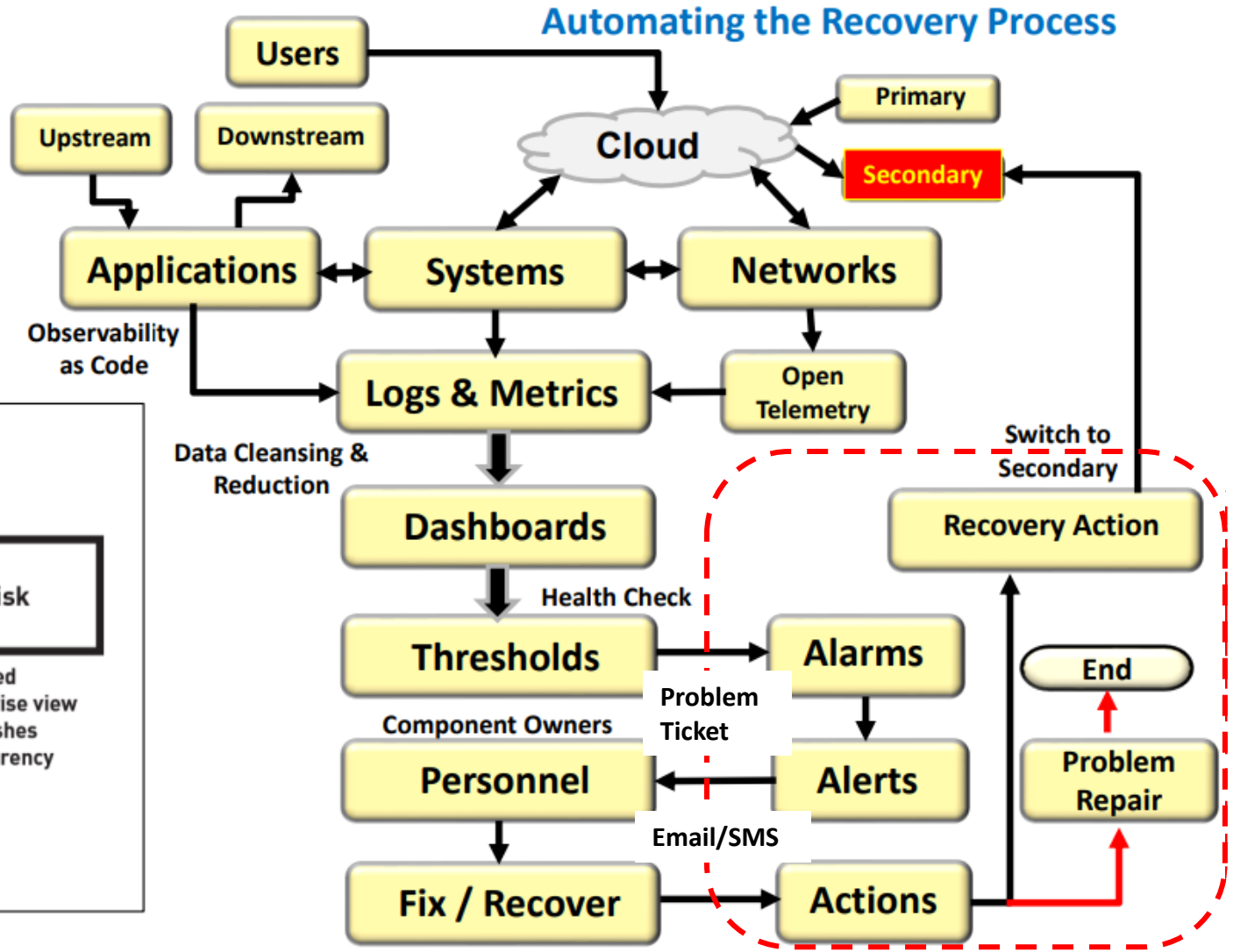
Board of Directors concerns

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

The Board of Director's is responsible for protecting the company 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



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

Know your Environment:

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

Set you direction:

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

Laws and Regulations requiring SBOMs

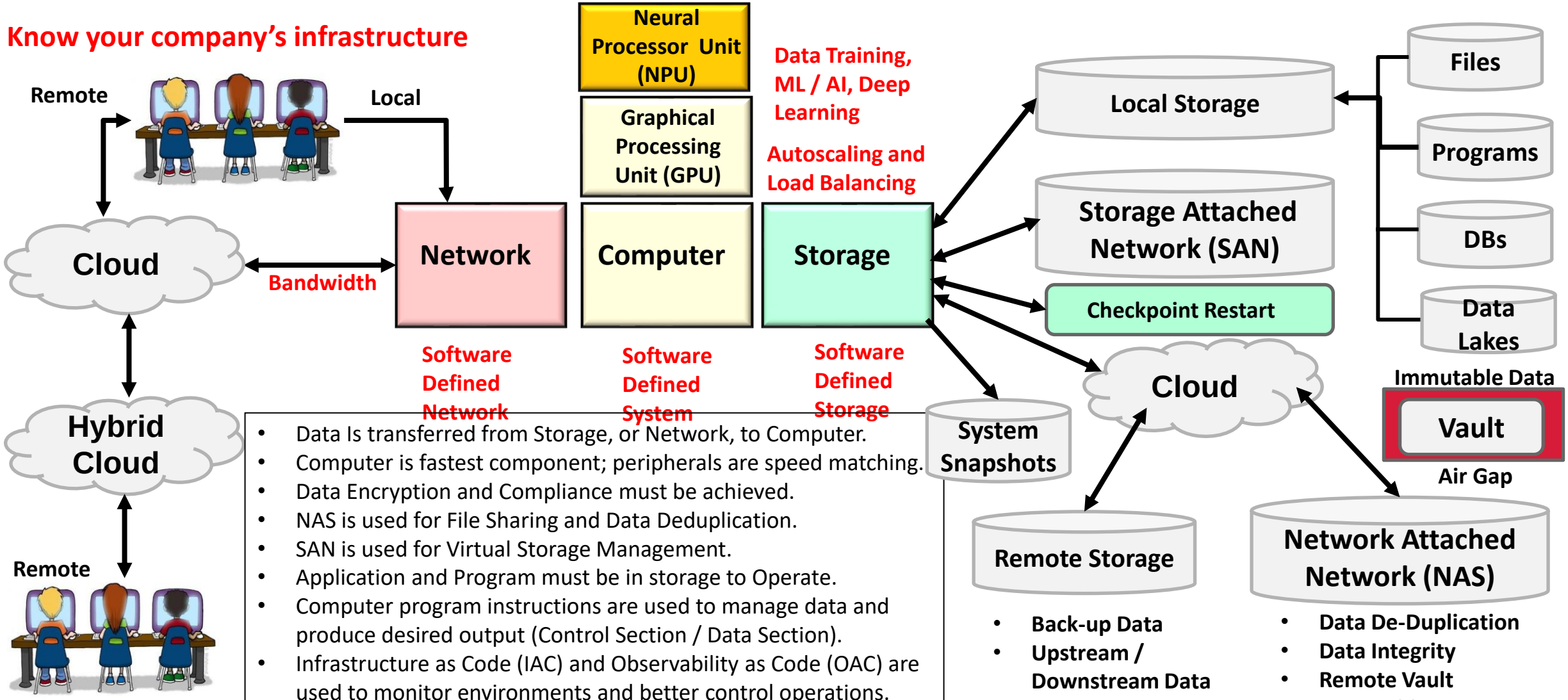
Thomas Bronack
Email: bronackt@dcag.com
Phone: (917) 673-6992

- 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 Procedures must be integrated into the staff's daily process for new and changed applications and services, with automated support through RPAs whenever feasible.

Monitoring Operations and Controlling Resources

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

Know your company's infrastructure



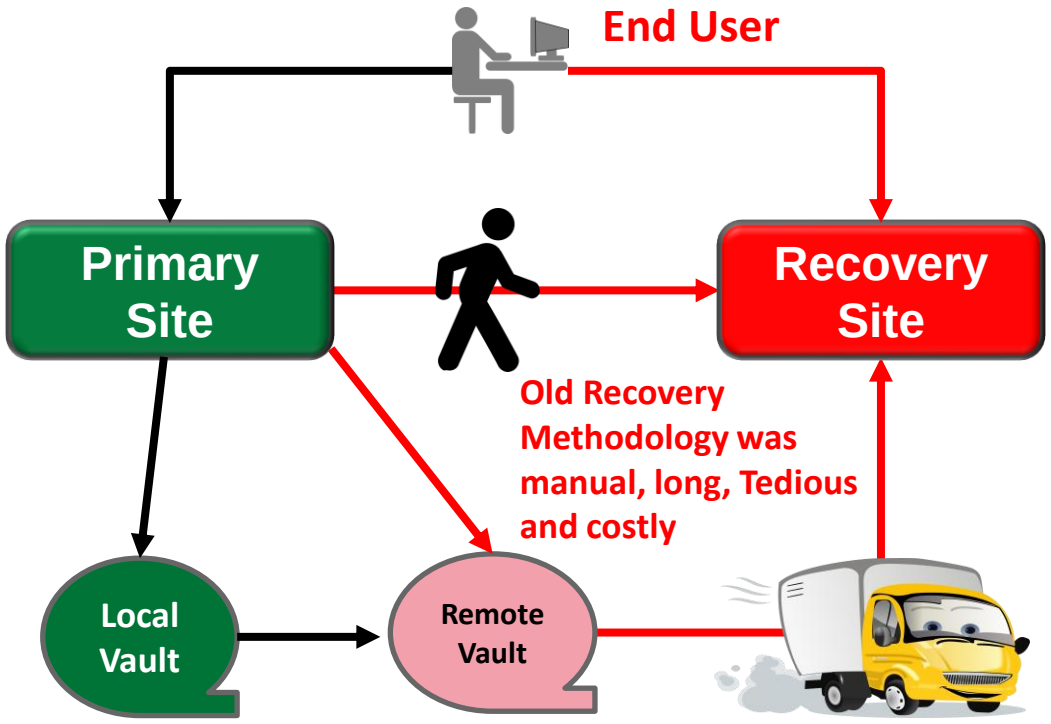
- Data Is transferred from Storage, or Network, to Computer.
- Computer is fastest component; peripherals are speed matching.
- Data Encryption and Compliance must be achieved.
- NAS is used for File Sharing and Data Deduplication.
- SAN is used for Virtual Storage Management.
- Application and Program 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.

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

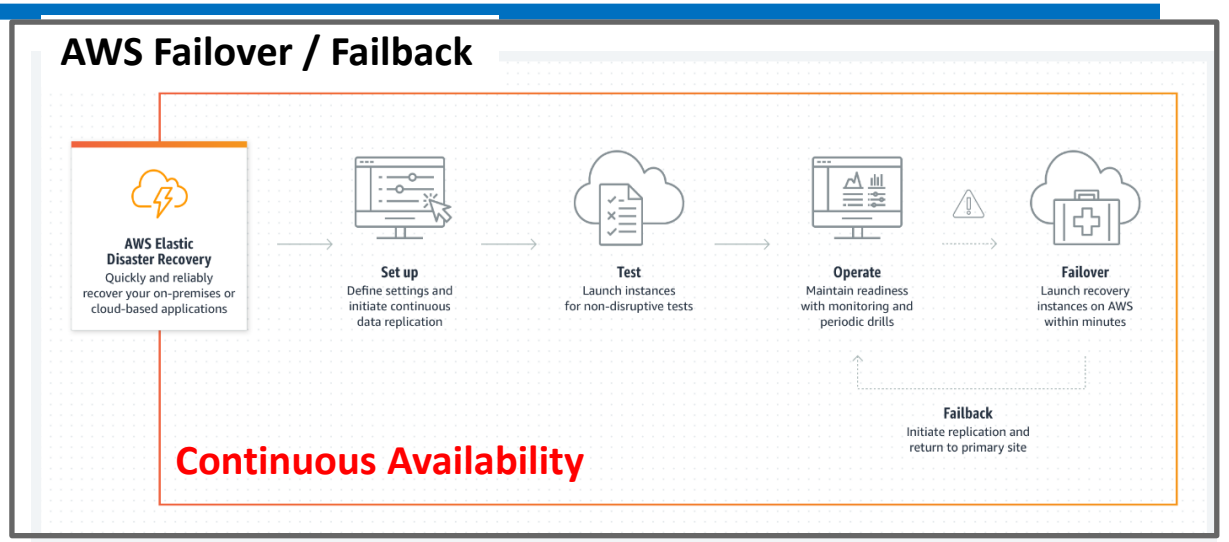
- **Data De-Duplication**
- **Data Integrity**
- **Remote Vault**
- **Immutable Data**

Evolution of Recovery Management

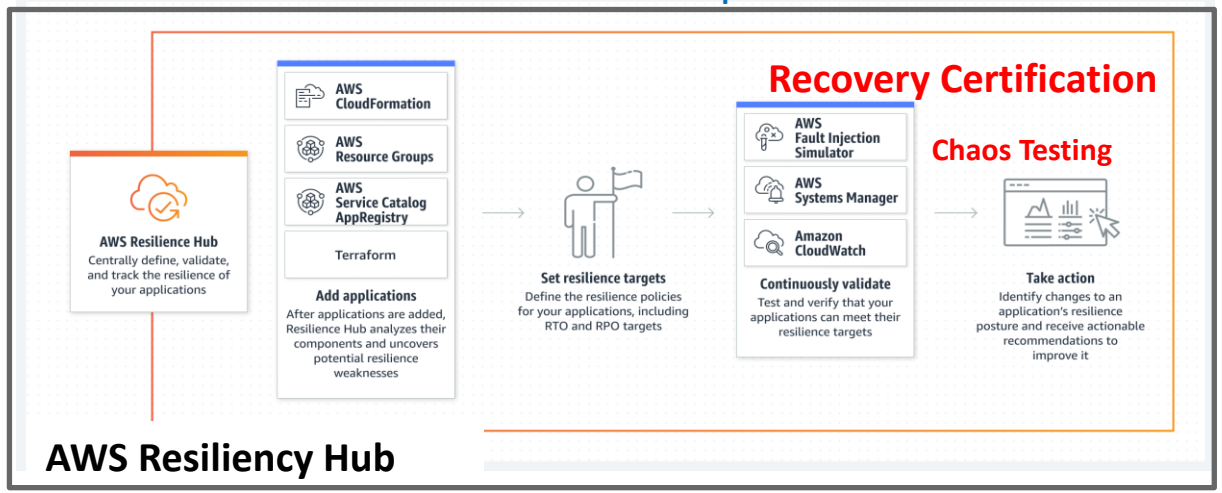
Thomas Bronack
Email: bronackt@dcag.com
Phone: (917) 673-6992



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 Resilience Hub allows for and continuous validation without disruption

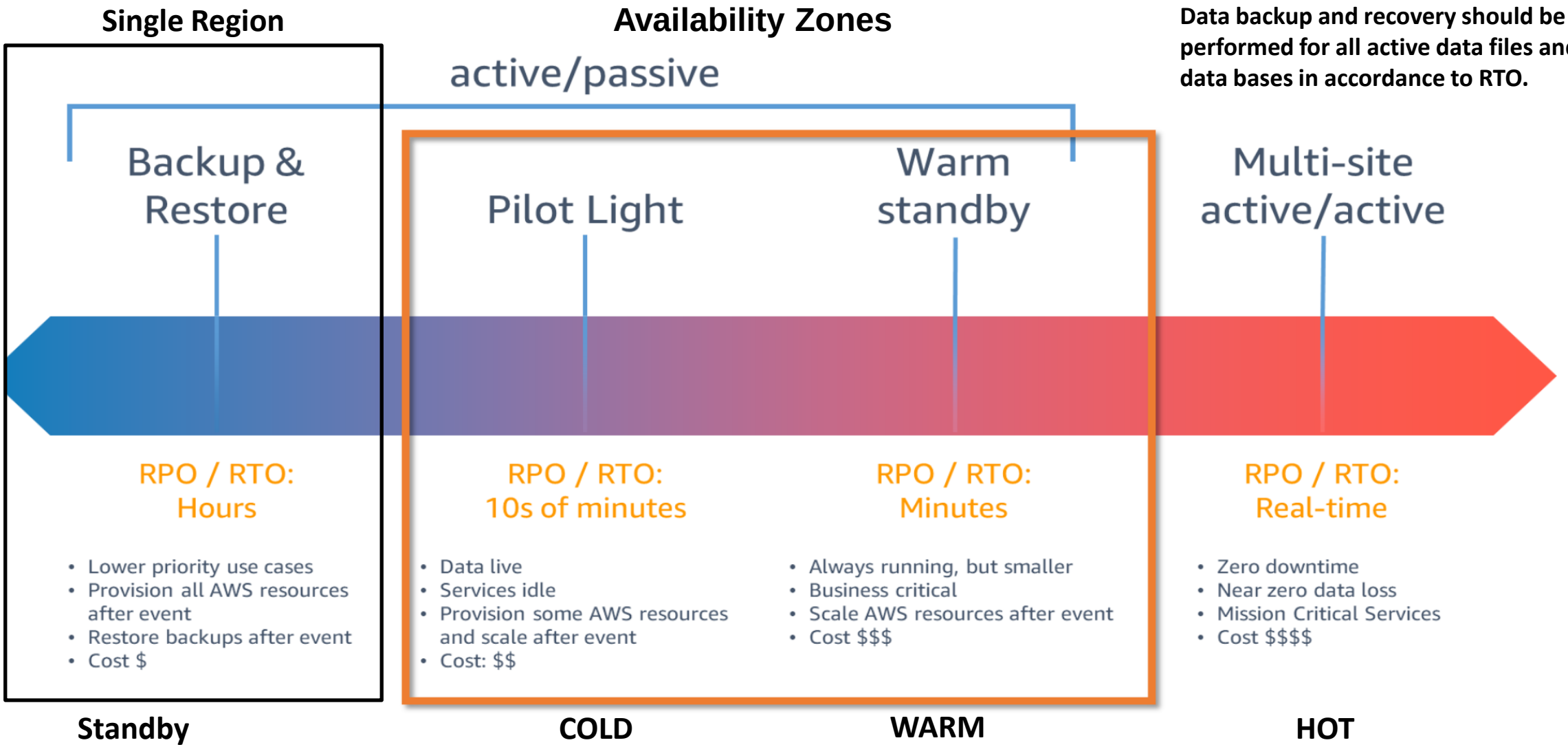


AWS DR Strategies

Link to AWS Disaster Recovery Strategies

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

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



Resilience Patterns and Recovery Groups

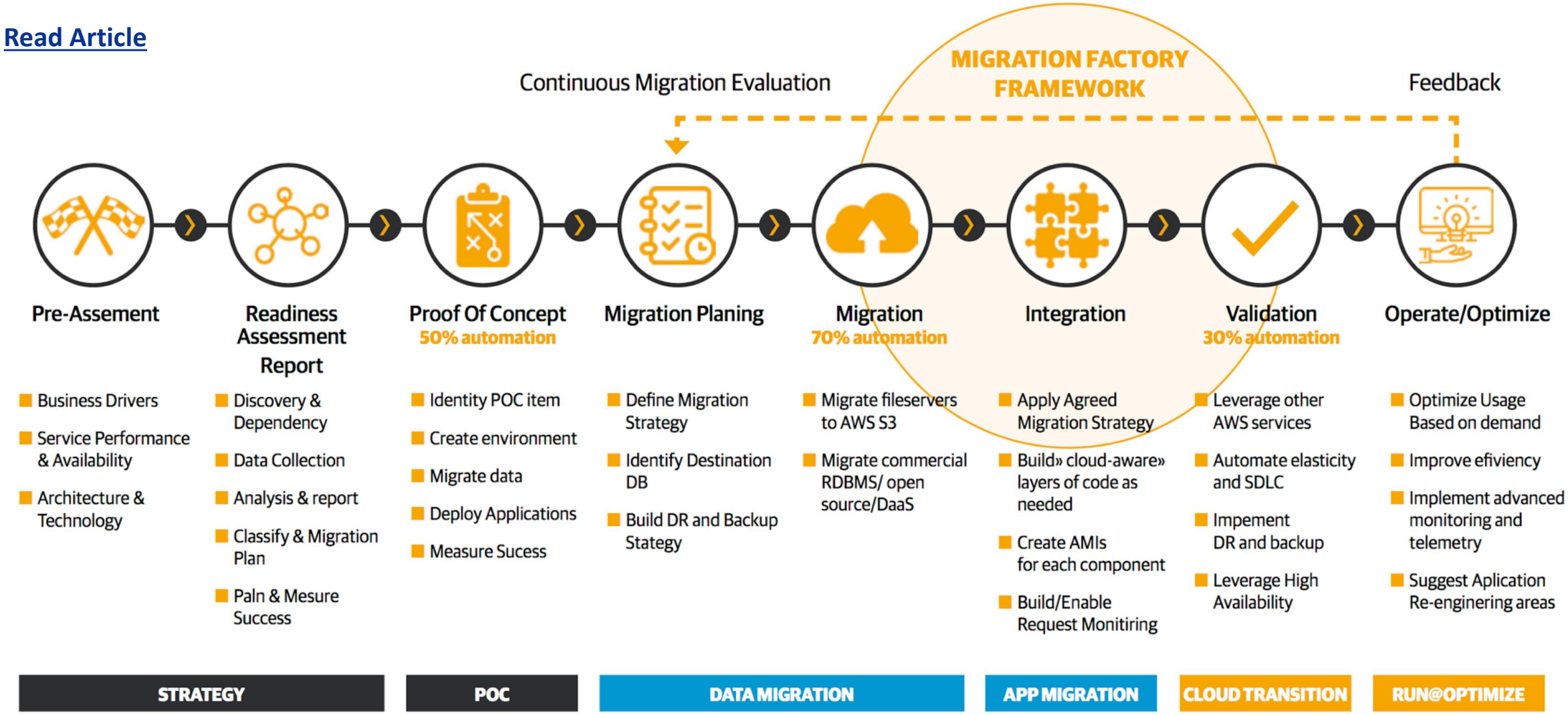
Thomas Bronack
Email: bronackt@dcag.com
Phone: (917) 673-6992

Resiliency Patterns	Single Region	Multiple Regions		
	In-Region	Active Standby (Pilot Ligt)	Active-Passive (Warm Stendby)	Active-Active (Multi-Site)
Pattern Profile	**1. TRANSACTIONAL TRAFFIC** - handled by primary region only 2. No multi-region **INFRASTRUCTURE** 3**. APPLICATION** code only available in single region 4. Multi-region **RECOVERY** not supported	**1. TRANSACTIONAL TRAFFIC** - handled by primary region only 2. **INFRASTRUCTURE available on stand-by** 3**. APPLICATION** provisioned, but in shutdown state	**1. TRANSACTIONAL TRAFFIC** - handled by primary region only 2. **INFRASTRUCTURE available on standby** 3**. Minimal APPLICATION** footprint running in 2nd rerion (all components are spun up and available with min. capacity, where application)	**1. TRANSACTIONAL TRAFFIC** - handled by primary region only 2. **INFRASTRUCTURE always available in both regions** 3**. APPLICATION** stack running active/active multi-region
Reserve Capacity			Required **RESERVE CAPACITY**	Required **RESERVE CAPACITY**
Cross-Region Maintenance	None	1. Maintain **PERSISTENT DATA REPLICATION** infrastructure 2. **APPLICATION CODE** maintaned for currency in **BOTH REGIONS** 3. Operate Production from stand-by region periodically	1. Maintain **PERSISTENT DATA REPLICATION** infrastructure 2. **APPLICATION CODE** maintaned for currency in **BOTH REGIONS** 3. Operate Production from stand-by region periodically	1. Maintain **2-WAY PERSISTENT DATA REPLICATION** 2. **APPLICATION CODE** maintaned for currency in **BOTH REGIONS** 3. Operate Production from stand-by region periodically
Recovery Steps	1. **ACQUIRE INFRASTRUCTURE** 2**. BUILD OU**T 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**		

Using AI Planning for Migrating Applications to AWS Cloud

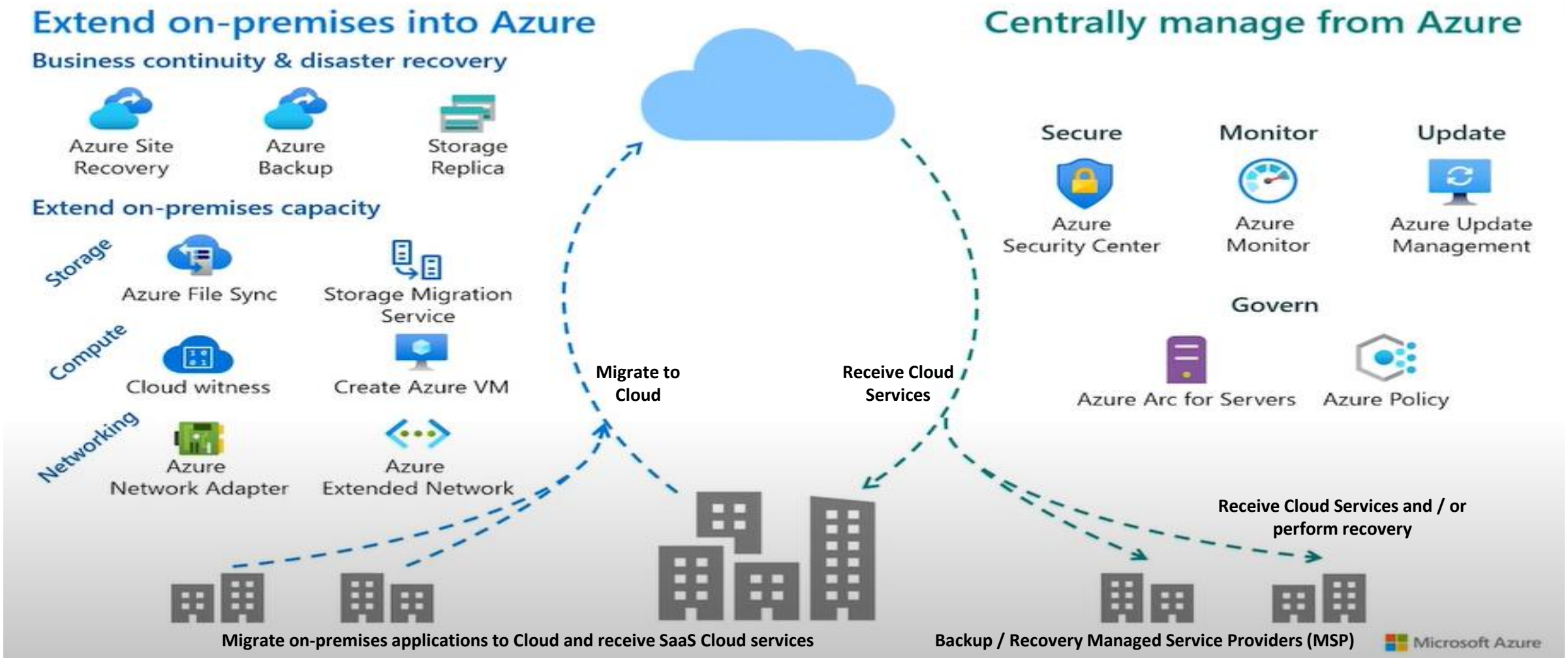
Thomas Bronack
Email: bronackt@dcag.com
Phone: (917) 673-6992

Read Article



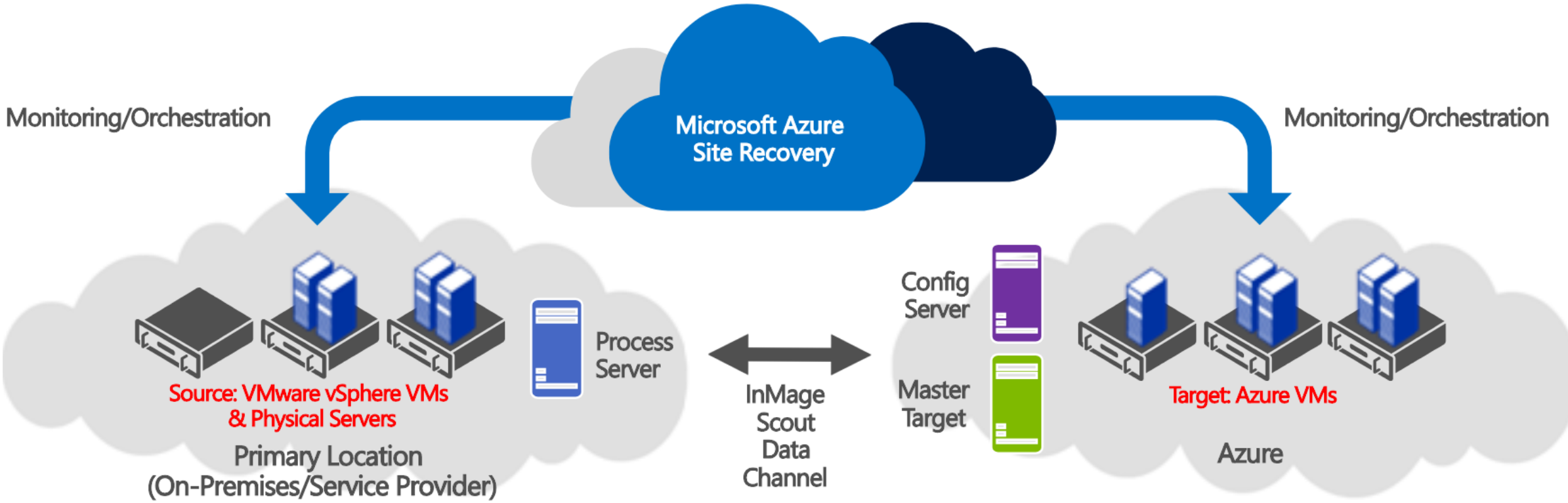
Azure Environment and Recovery Management

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



Azure Recovery Management Environment

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



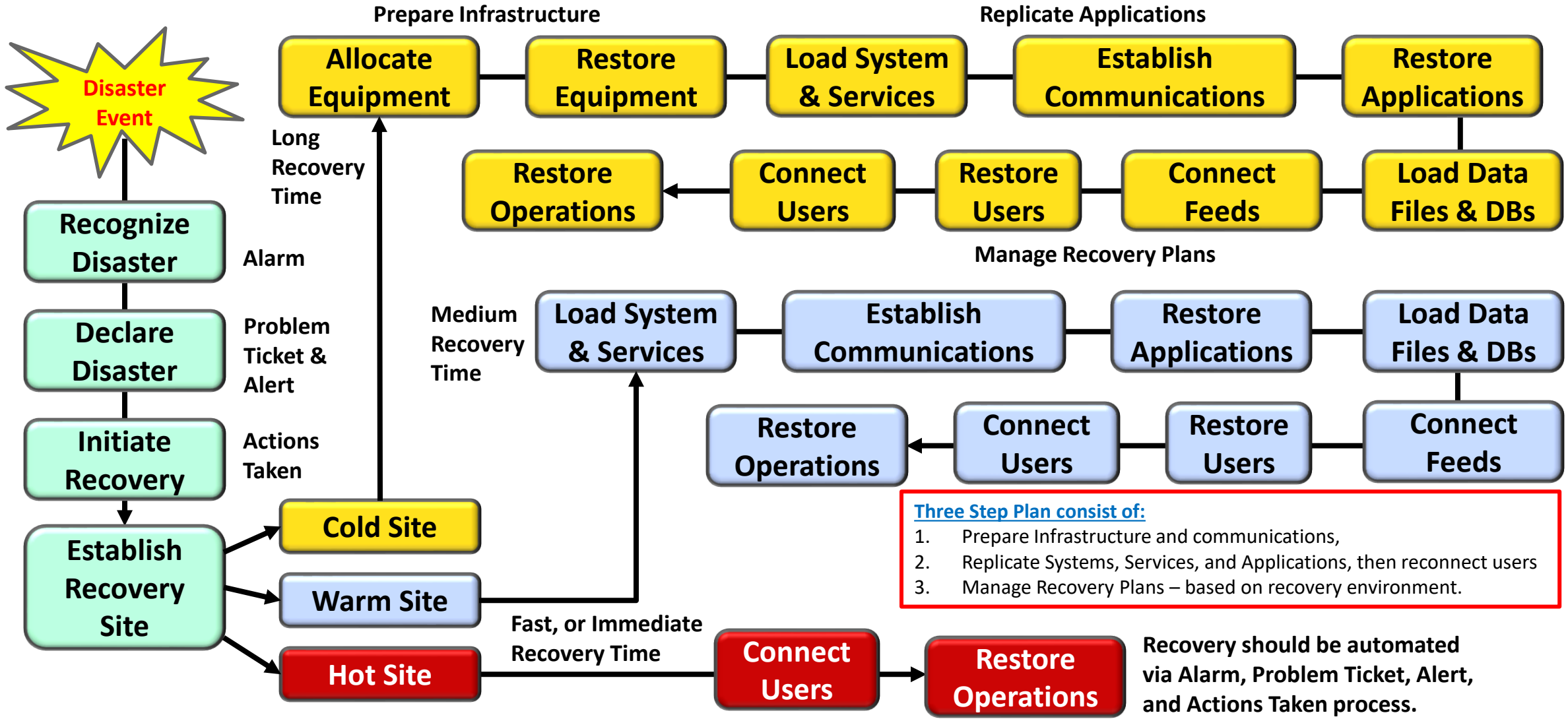
Process Server – Used for Caching, Compression & Encryption

Config Server – Used for Centralized Management of InMage Scout

Master Target – Used as a repository & for retention

Sequence of Events to enact a Recovery Operation

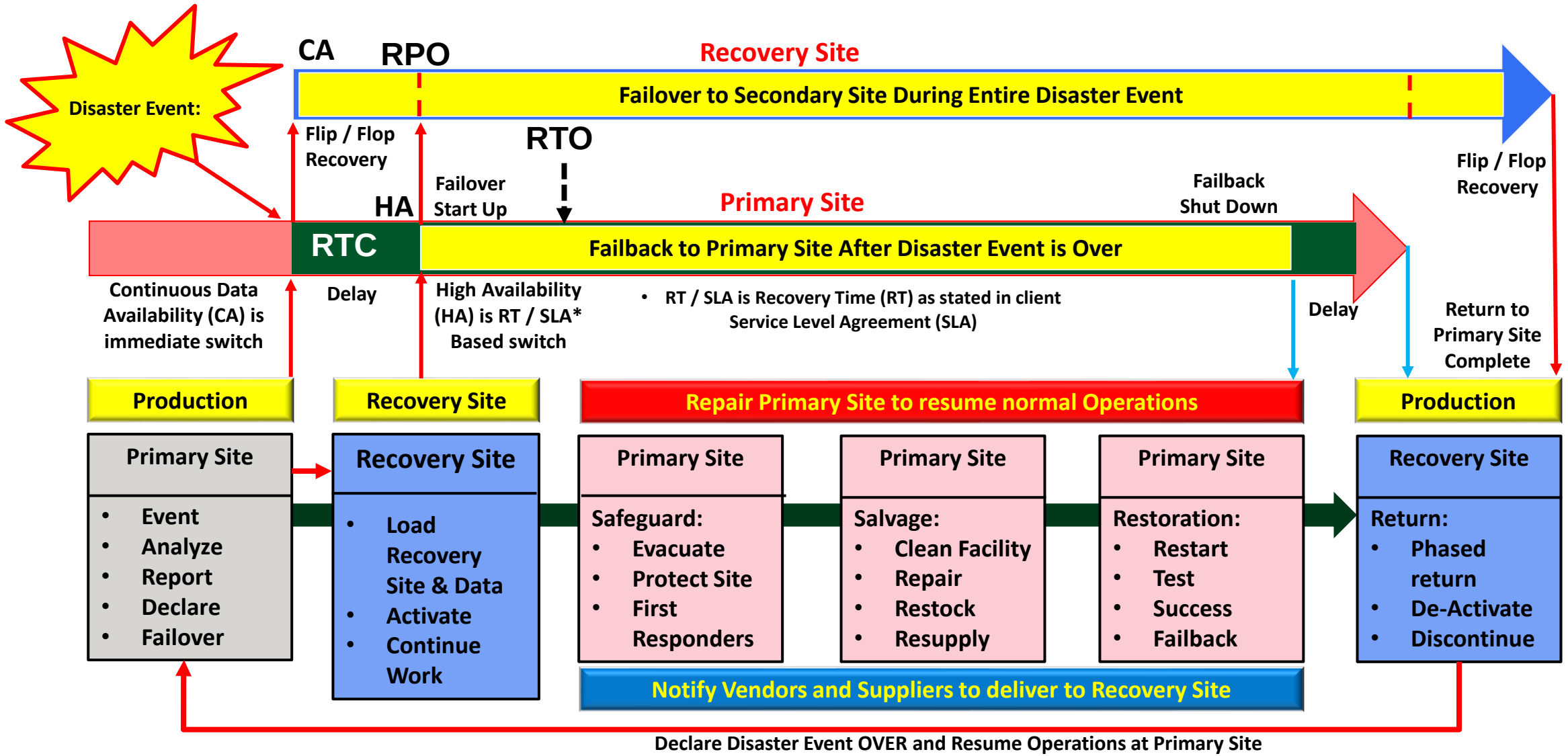
Thomas Bronack
Email: bronackt@dcag.com
Phone: (917) 673-6992



The Disaster Event Life Cycle

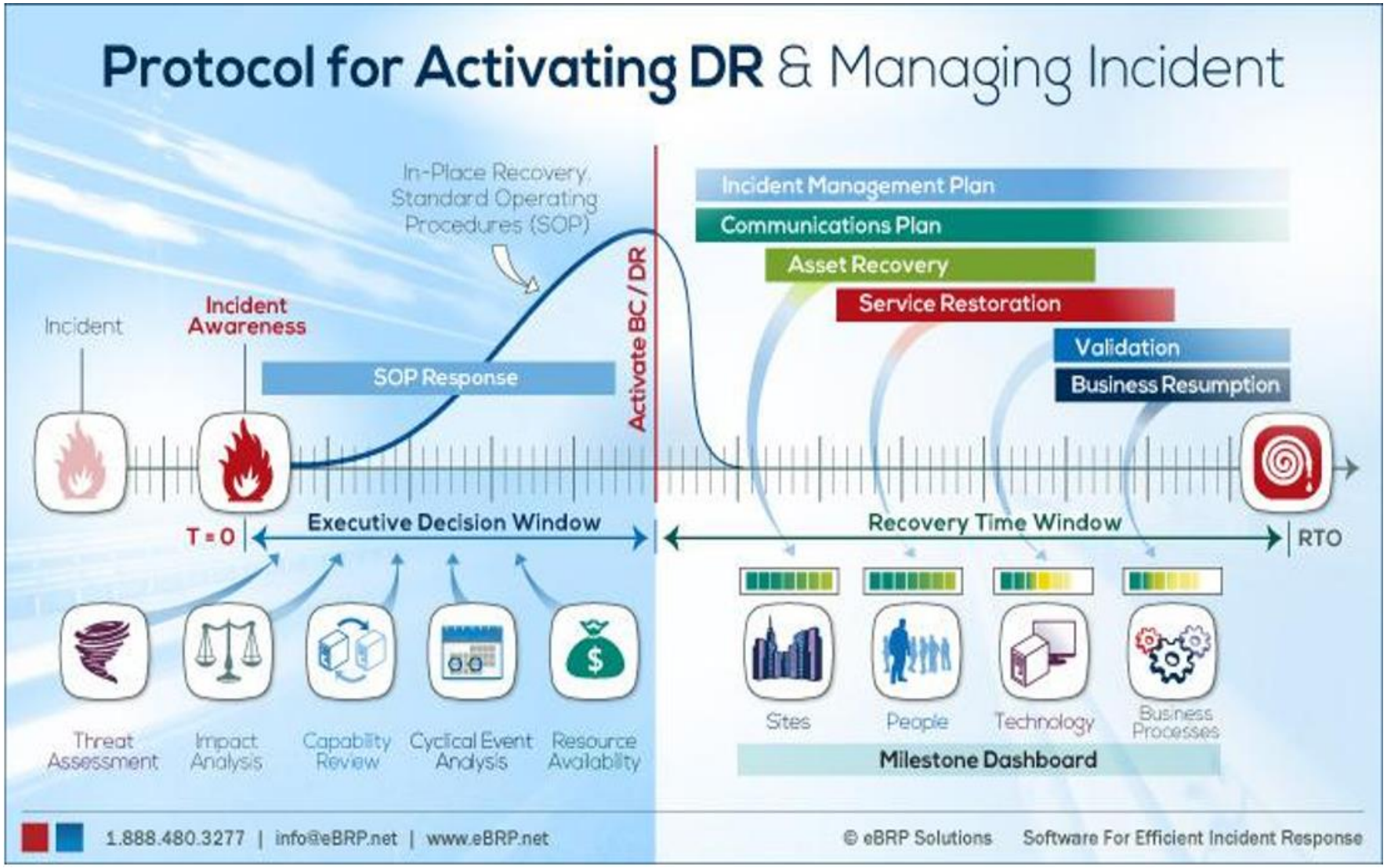
CA is Continuous Availability
HA is High Availability
RTO – Recovery Time Objective
RPO – Recovery Point Objective
RTC – Recovery Time Capability

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



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

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

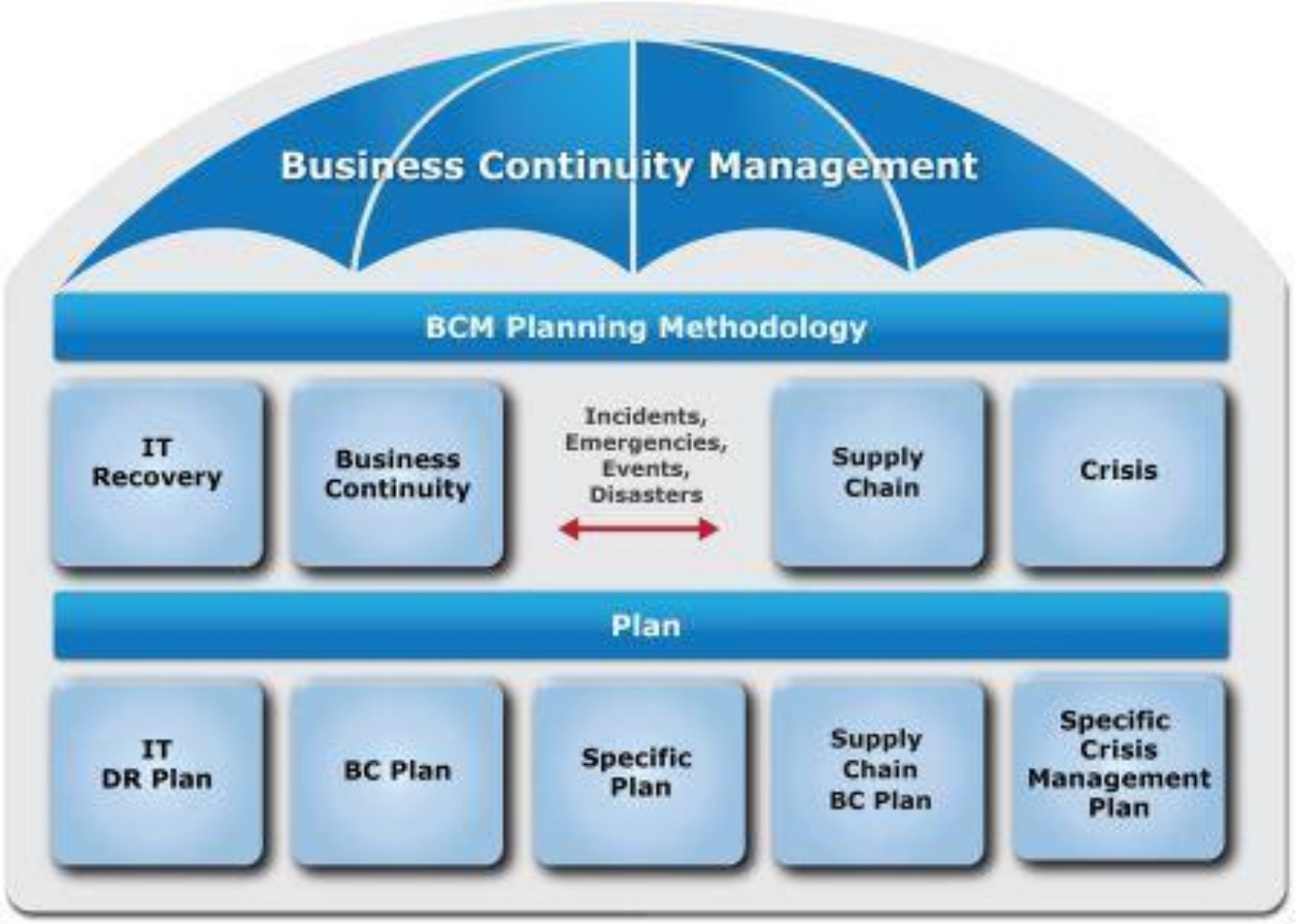
Enterprise Resilience concists of:

- 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

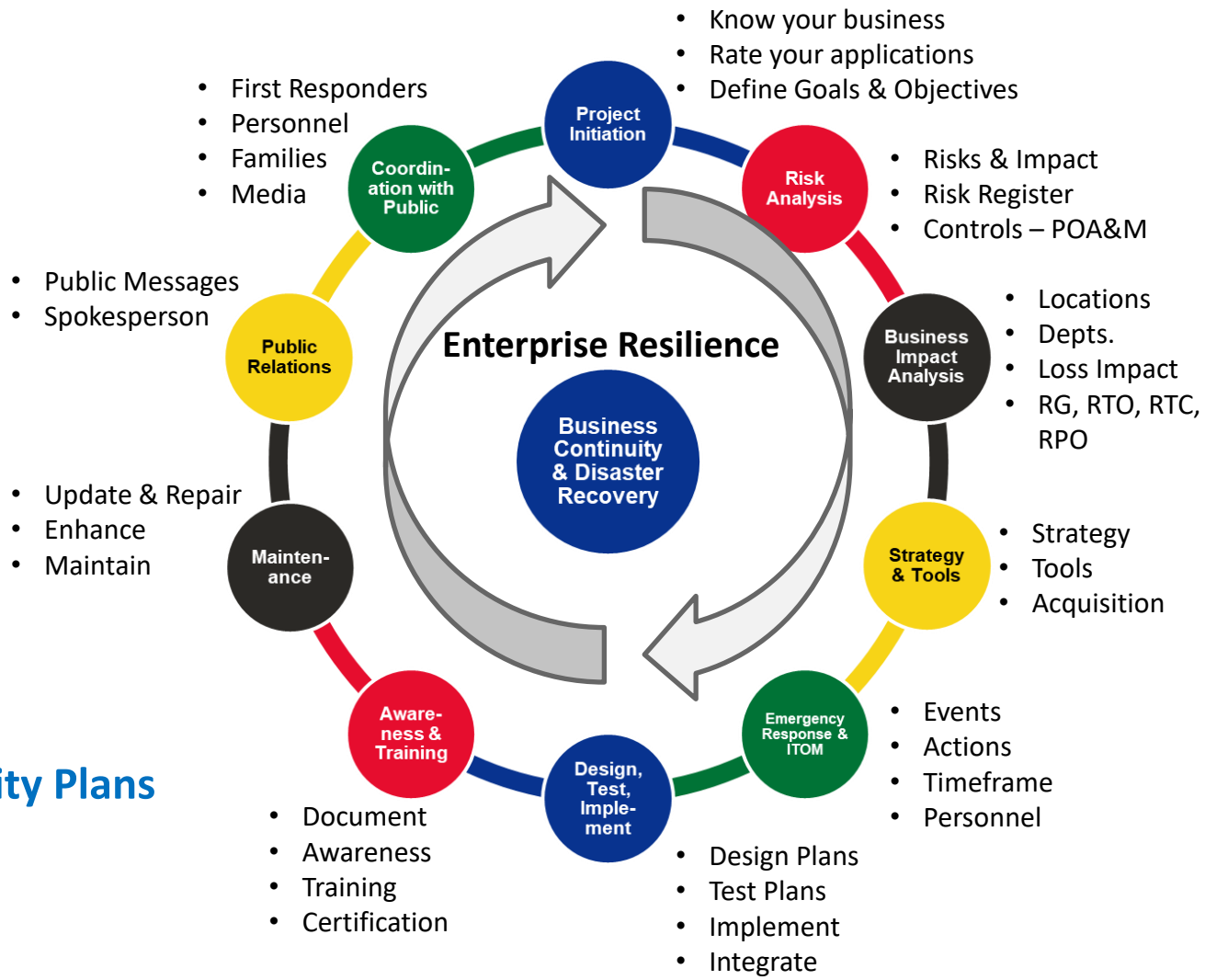
Ten Step Process to establish BCM/DR Practice

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

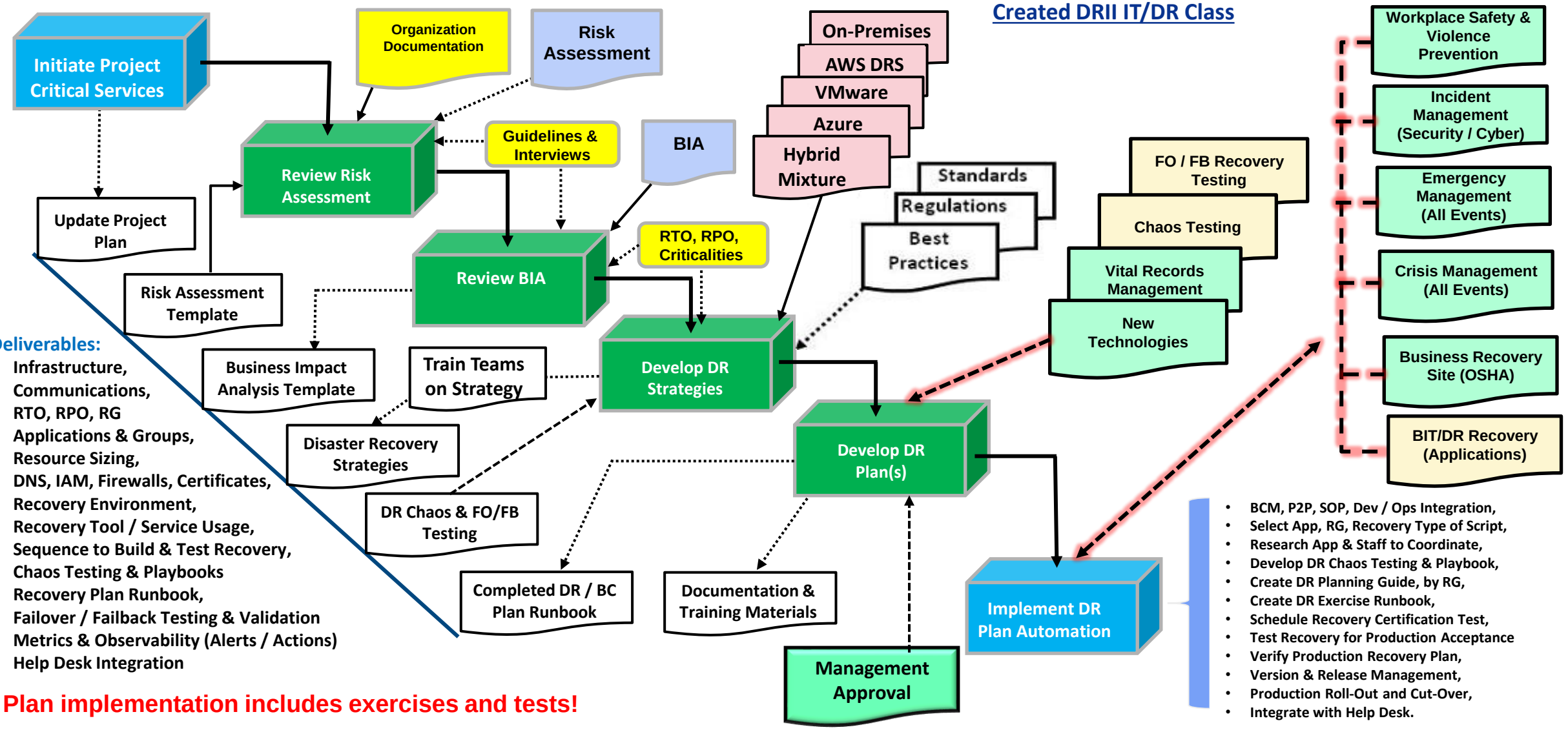
   Restoration (Backup, Vaulting, Restoration)
6. Designing and Implementing Business

   Continuity Plans
7. Awareness and Training
8. Maintaining and Exercising Business Continuity Plans
9. Public Relations and Crisis Communications
10. Coordinating with Public Authorities



Sample Recovery Plan Methodology

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



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

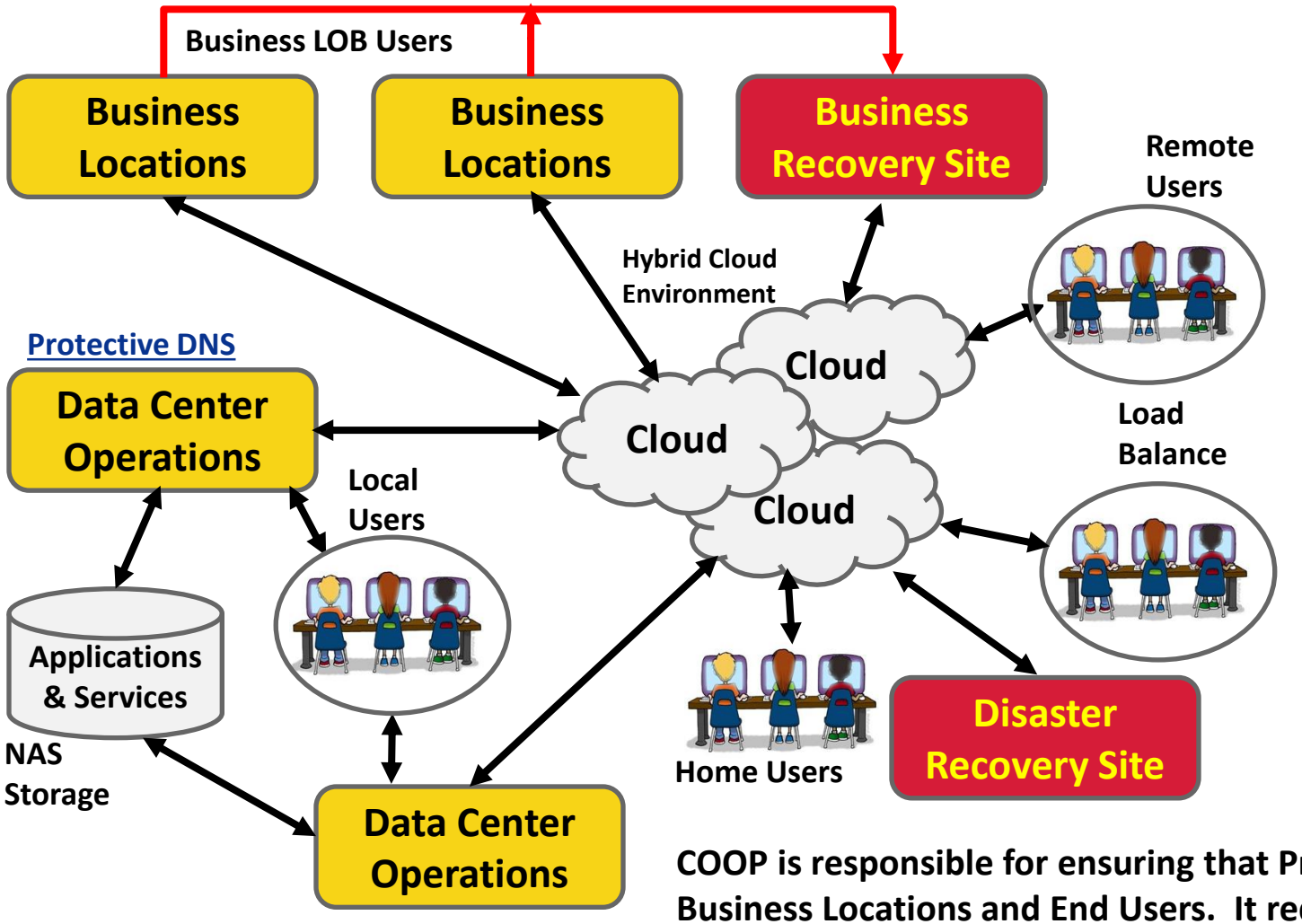
- BCM, P2P, SOP, Dev / Ops Integration,
- Select App, RG, Recovery Type of Script,
- Research App & Staff to Coordinate,
- Develop DR Chaos Testing & Playbook,
- Create DR Planning Guide, by RG,
- Create DR Exercise Runbook,
- Schedule Recovery Certification Test,
- Test Recovery for Production Acceptance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

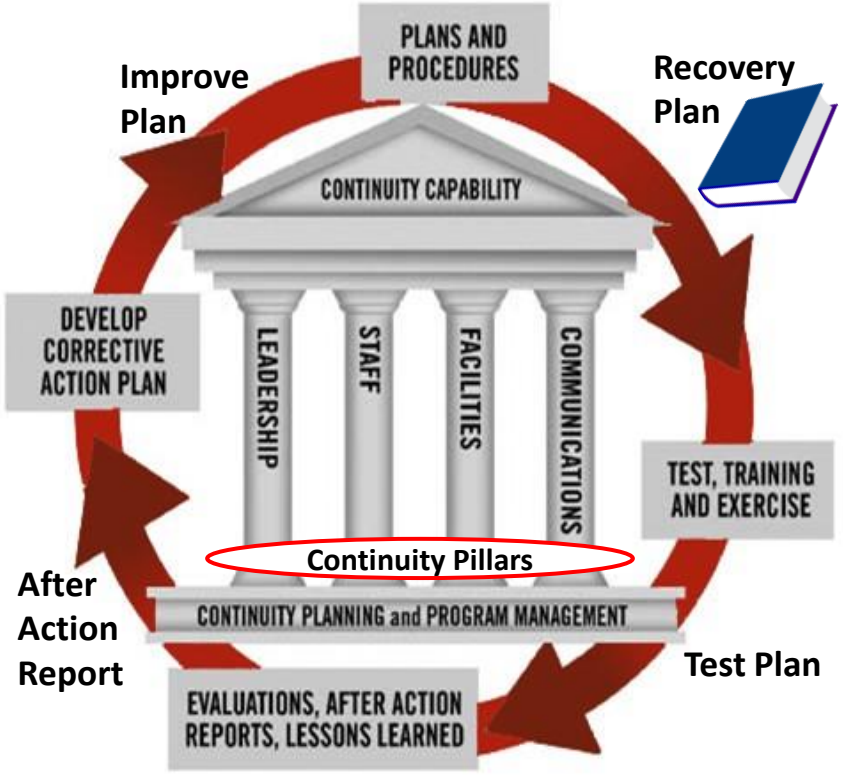
Plan implementation includes exercises and tests!

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

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).

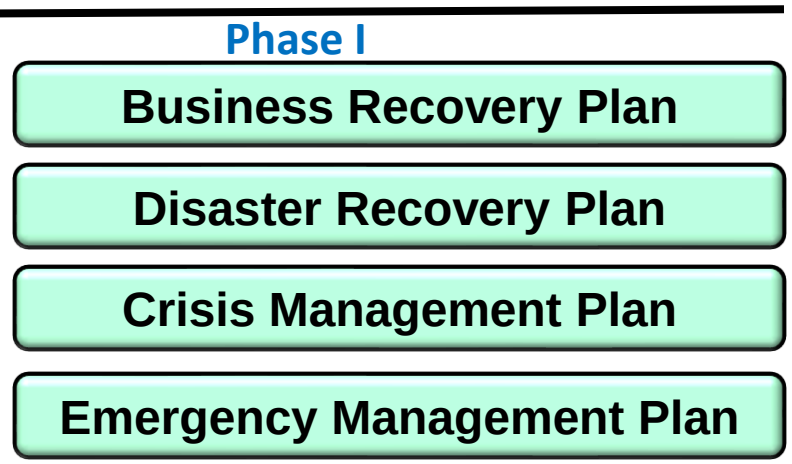
The NEFs serve as the foundation for all continuity programs and capabilities, and they are the primary focus of the Federal Government in catastrophic emergencies. However, it's important to note that the Federal Government cannot maintain these functions and services without the support of the rest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

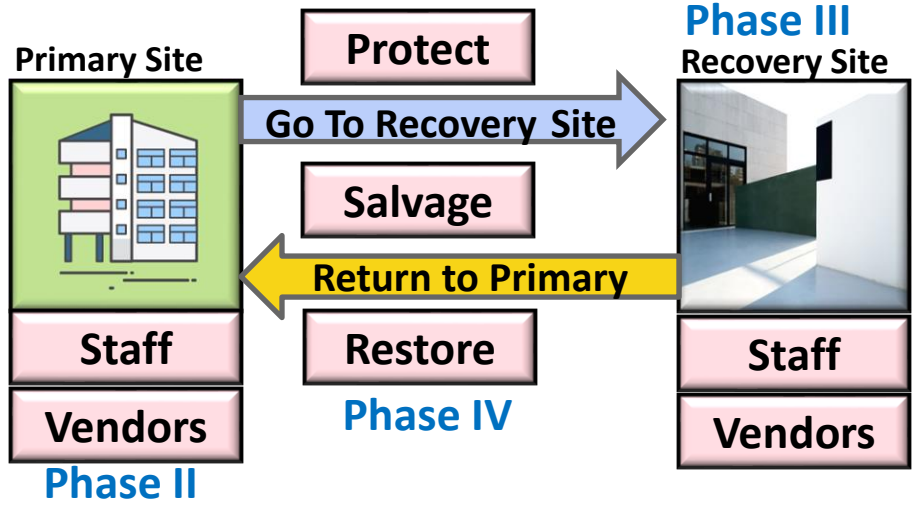
Stages of the COOP Plan

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)





COOP Testing Process

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

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].

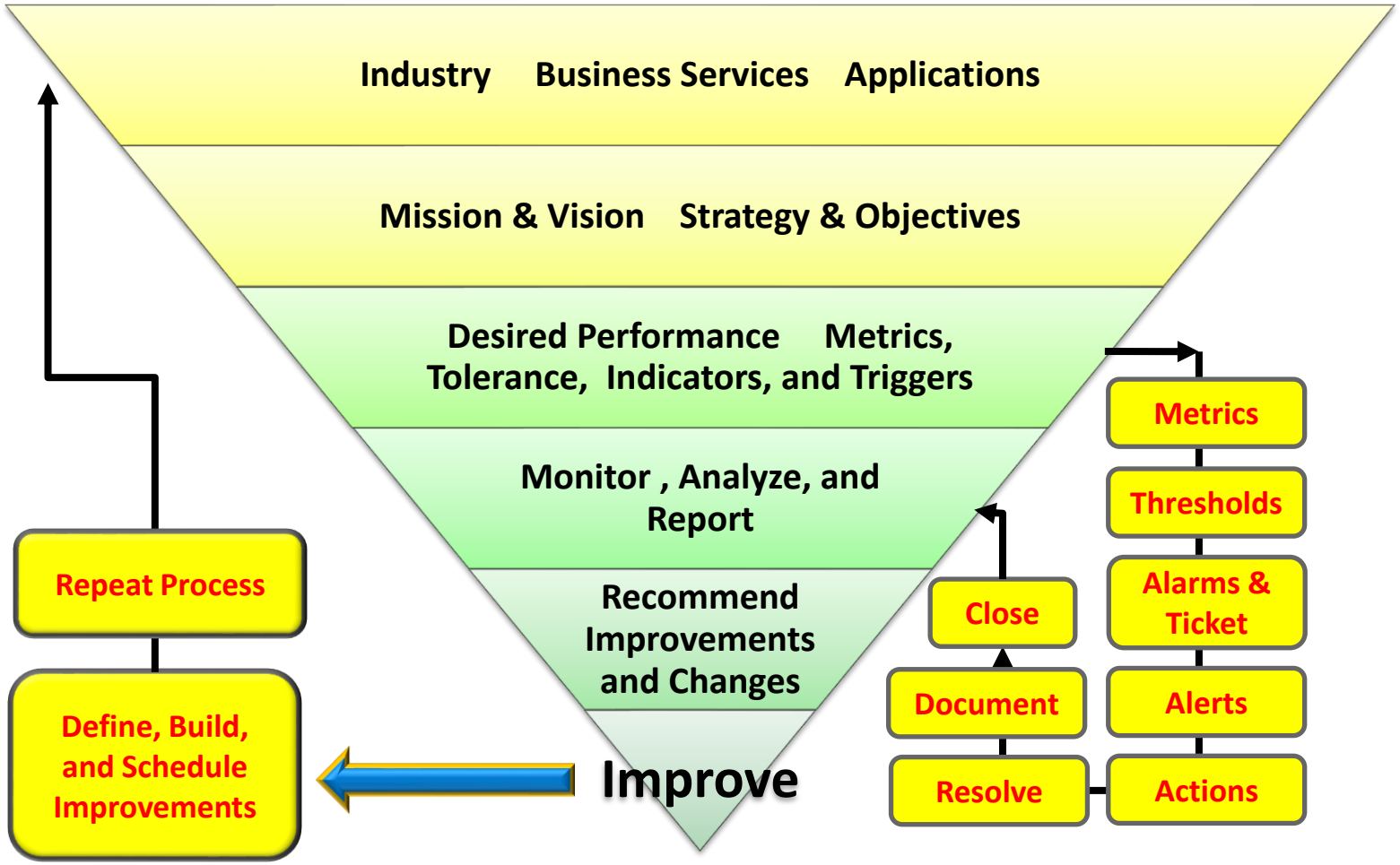
Learn more

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

The Risk Evaluation Process Using COSO

Thomas Bronack
Email: 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.

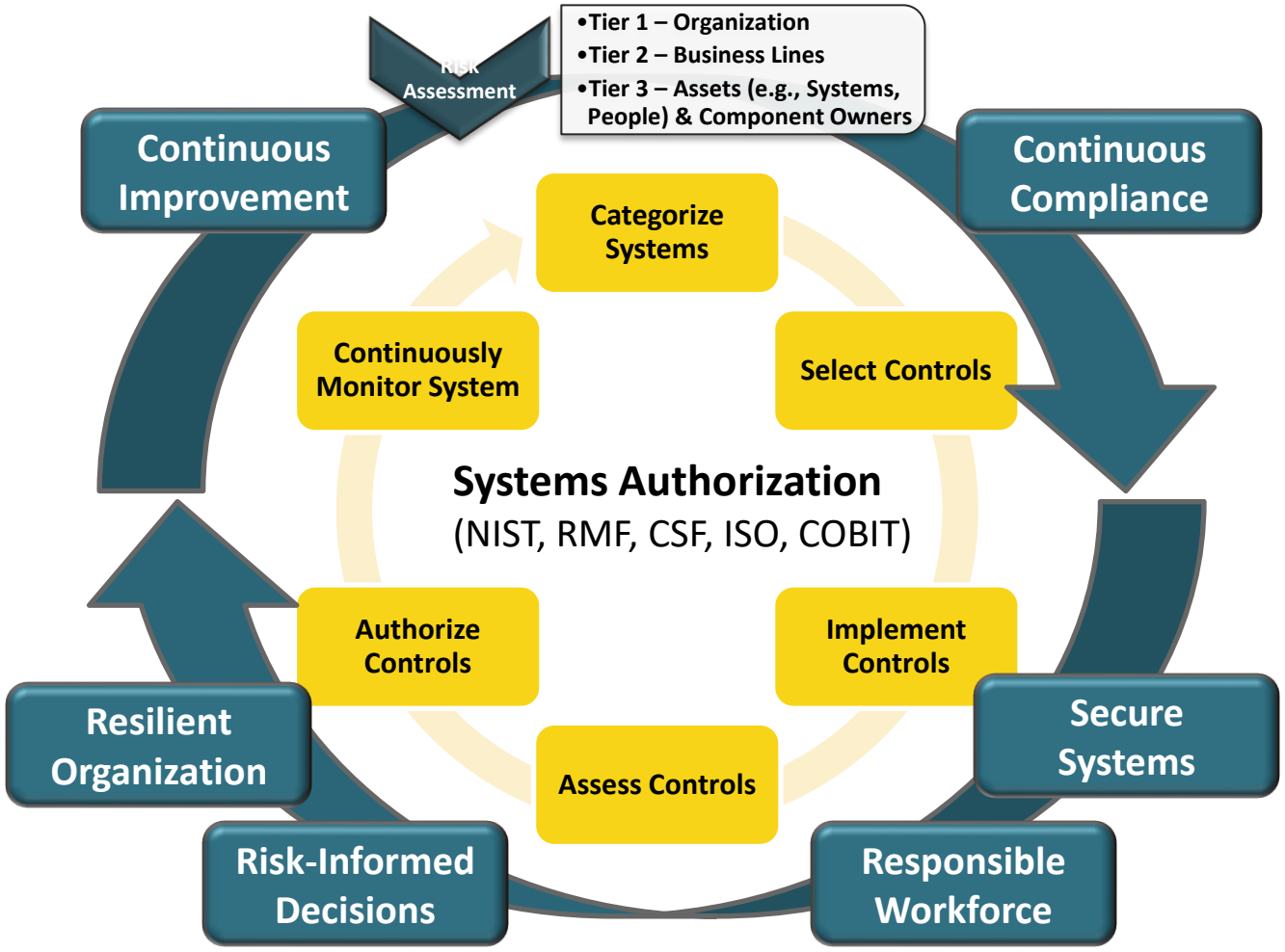
Ensuring Compliance via GRC and Risk Assessment

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

Goverance

- **Statutory and Regulatory**
  - Laws
  - Statutes
  - Regulations
- **Standards**
  - ISO
  - NIST
- **Policies**
  - Organizational
  - InfoTechnology
  - InfoSecurity
- **Contracts / Commitments**
  - PCI/DSS
  - Customer Contracts
  - B2B Agreements
- **Processes & Procedure**
  - NIST, CSF, RMF
  - ISO
  - Organizational
- **Contracts**
  - Administrative
  - Physical
  - Technical

Risk

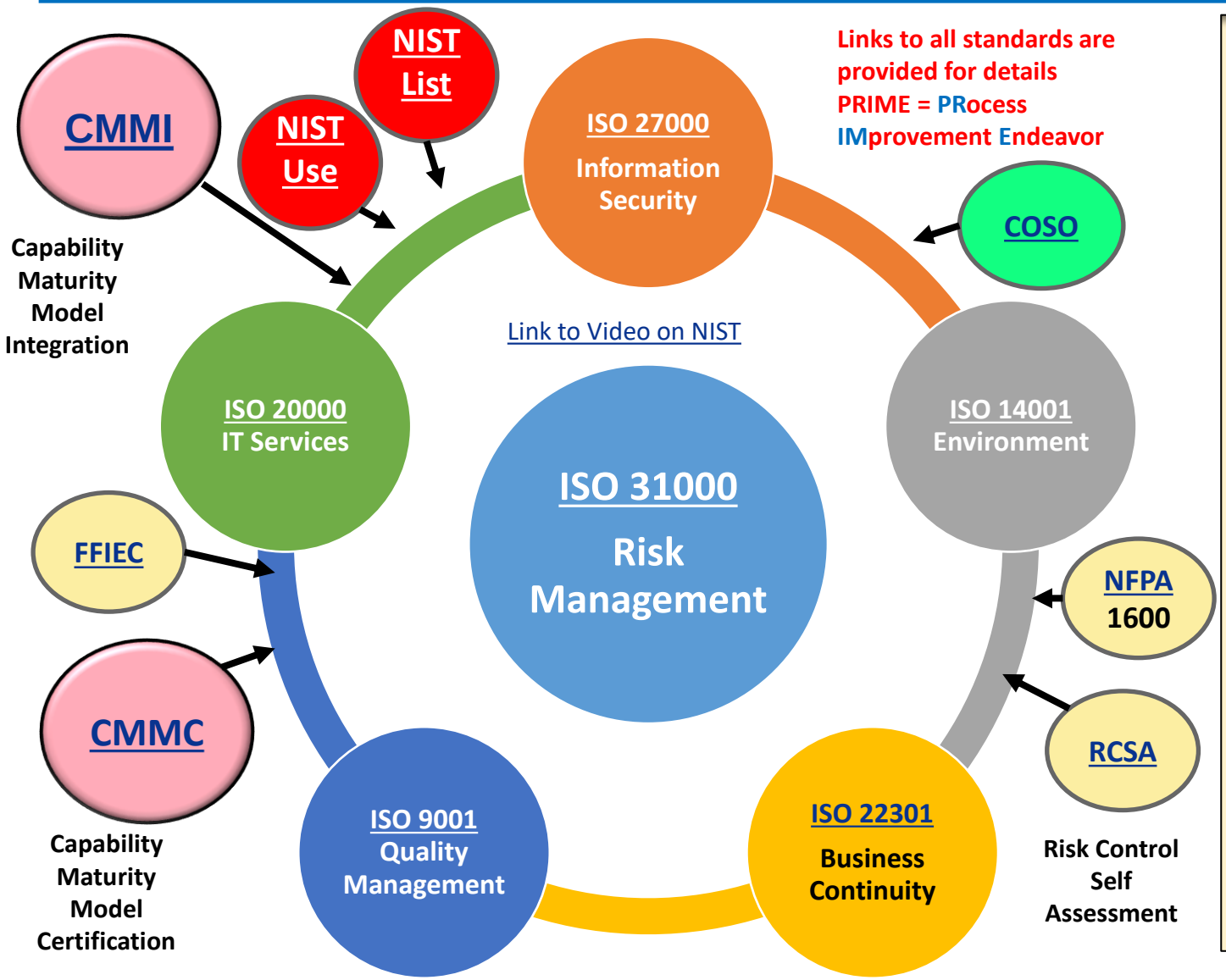


Compliance

- **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

The newest Integration Model – PRIME Approach

Thomas Bronack
Email: 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).

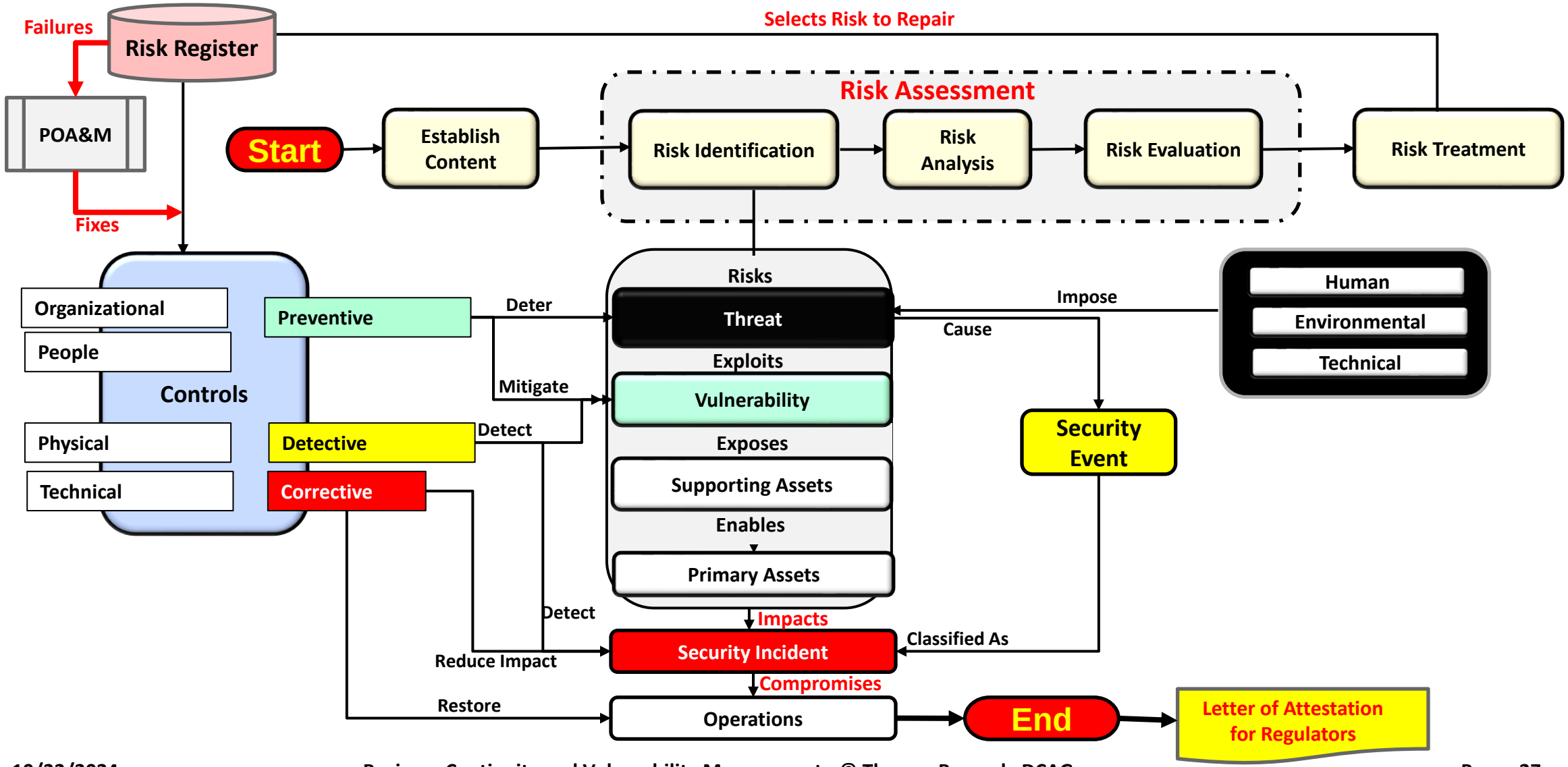
Then implement your **Business Continuity** (ISO 22301) Recovery Certification Process for Emergency, Crisis, Business, and IT Disaster Recovery Management.

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.

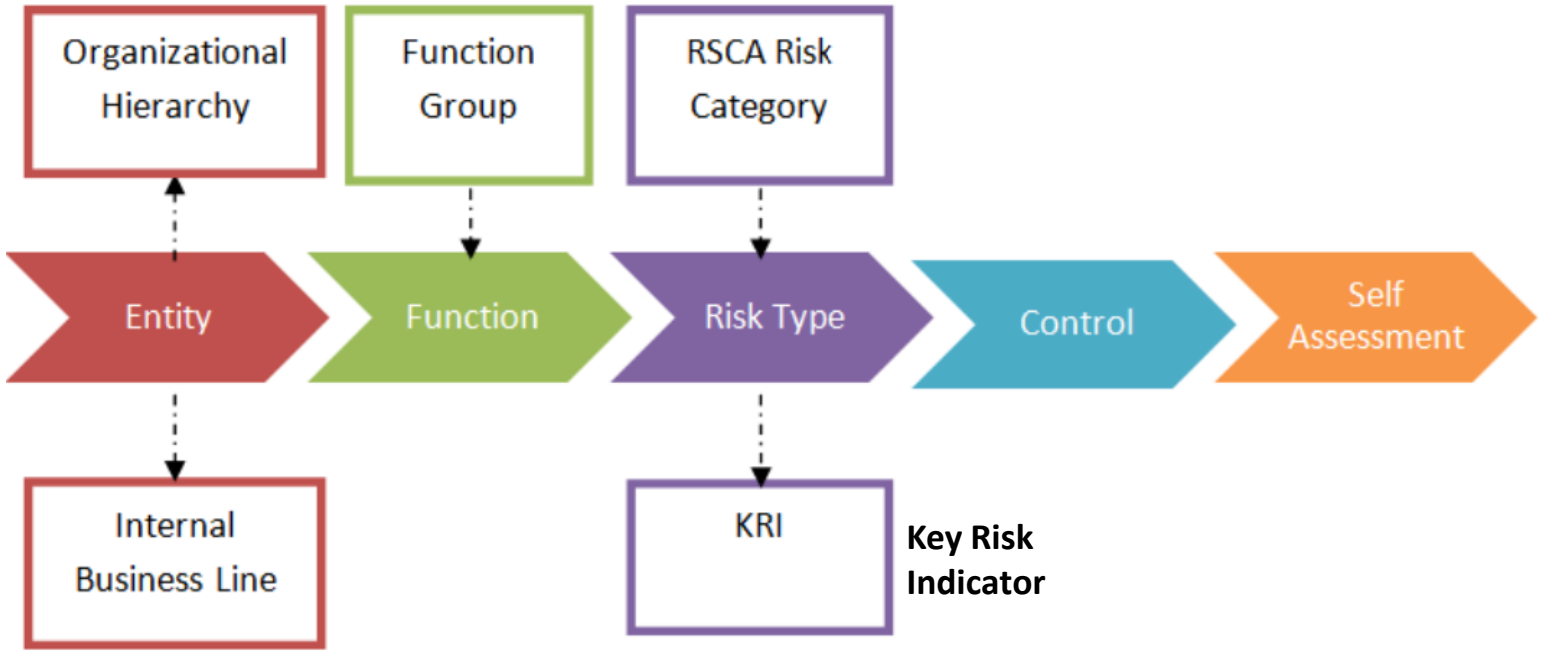
Risk Management with ISO 27000: 2022

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



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:

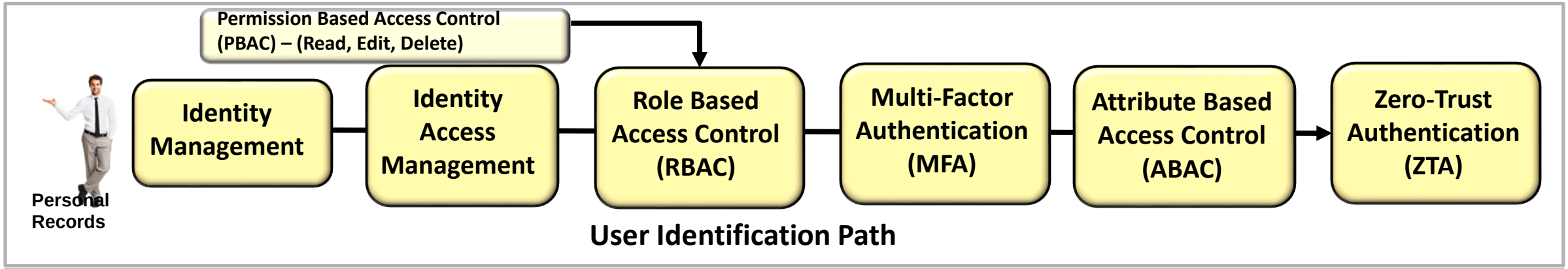
- Identify and prioritize their business objectives
- Assess and manage high risk areas of business processes
- Self-evaluate the adequacy of controls
- Develop risk treatment action plans
- Ensure that the identification, recognition and evaluation of business objectives and risks are consistent across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

Steps within a RCSA are:

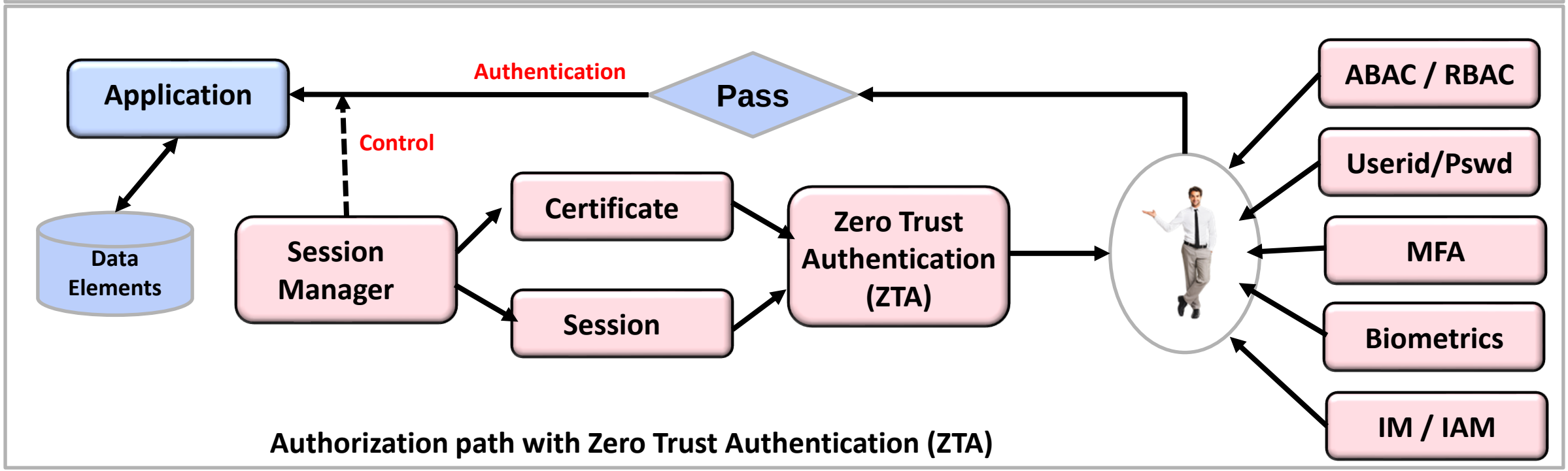
1. Select Participants
2. Identify Risks
3. Assess Risk against business measure
4. Actions against control lapses
5. Access Controls
6. Identify controls for a risk (KRI)
7. Monitor
8. Report results
9. Take corrective actions to continuously improve process

Identity and Access Management technologies

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



User Identification Path

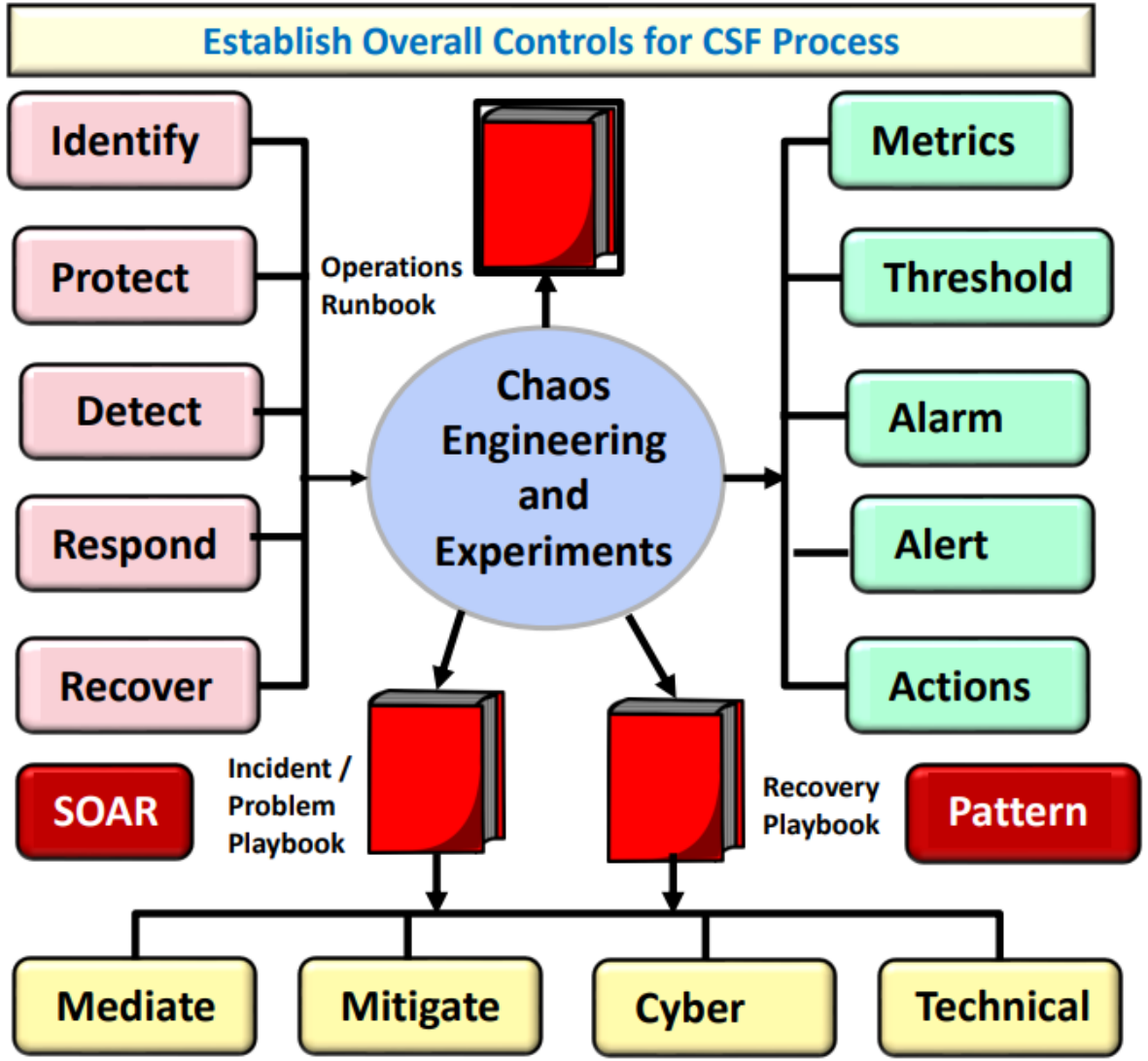


Authorization path with Zero Trust Authentication (ZTA)

Detecting and Responding to Cyber Problems – CSF2

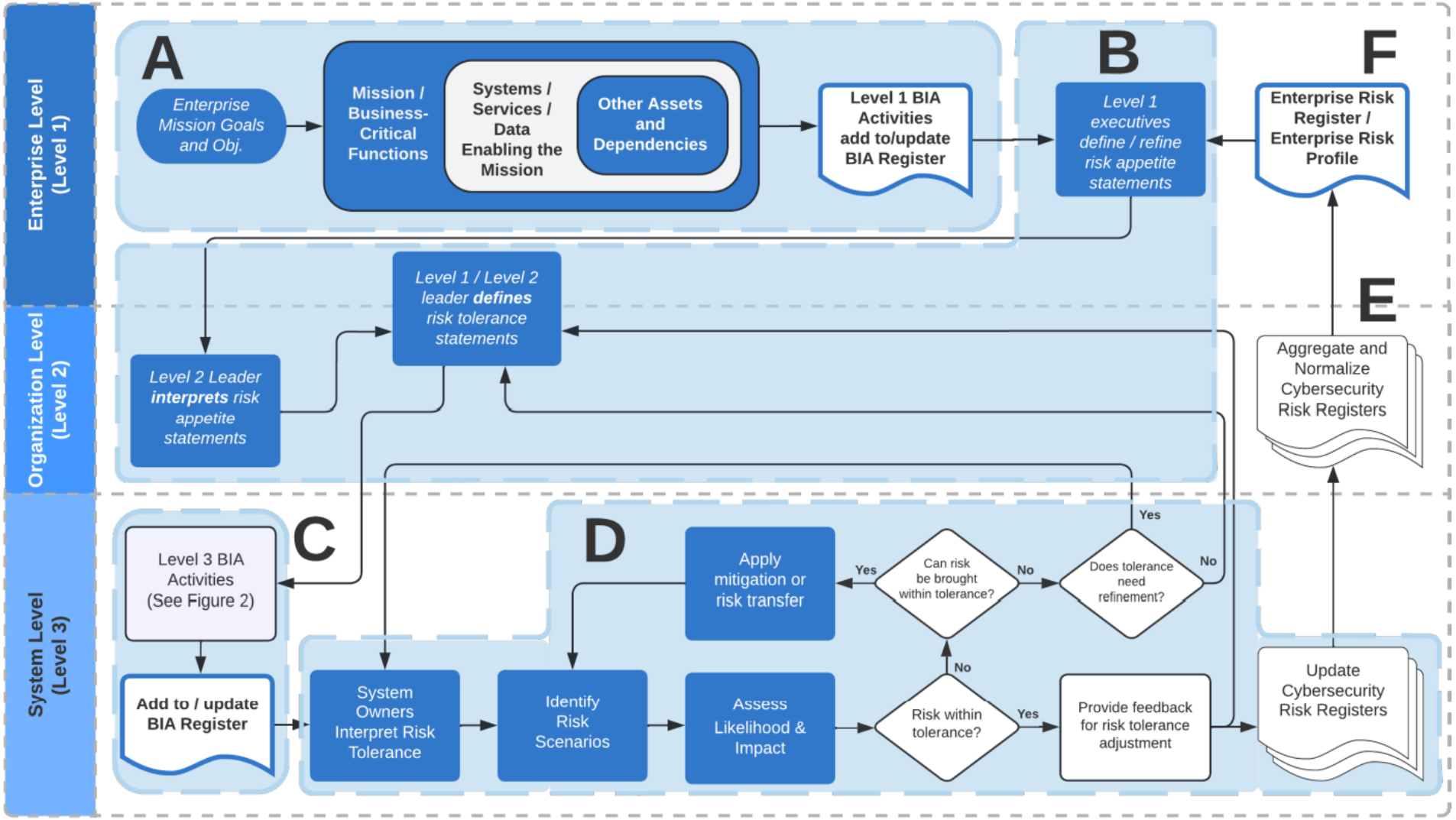
Thomas Bronack
Email: bronackt@dcag.com
Phone: (917) 673-6992

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



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

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

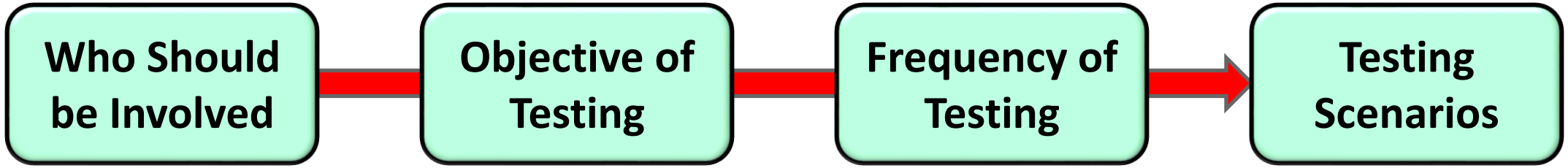


Link to Document

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

Testing Business Continuity Plans

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



- 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

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

What to Test

- 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

Test Categories

- 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

How to Test

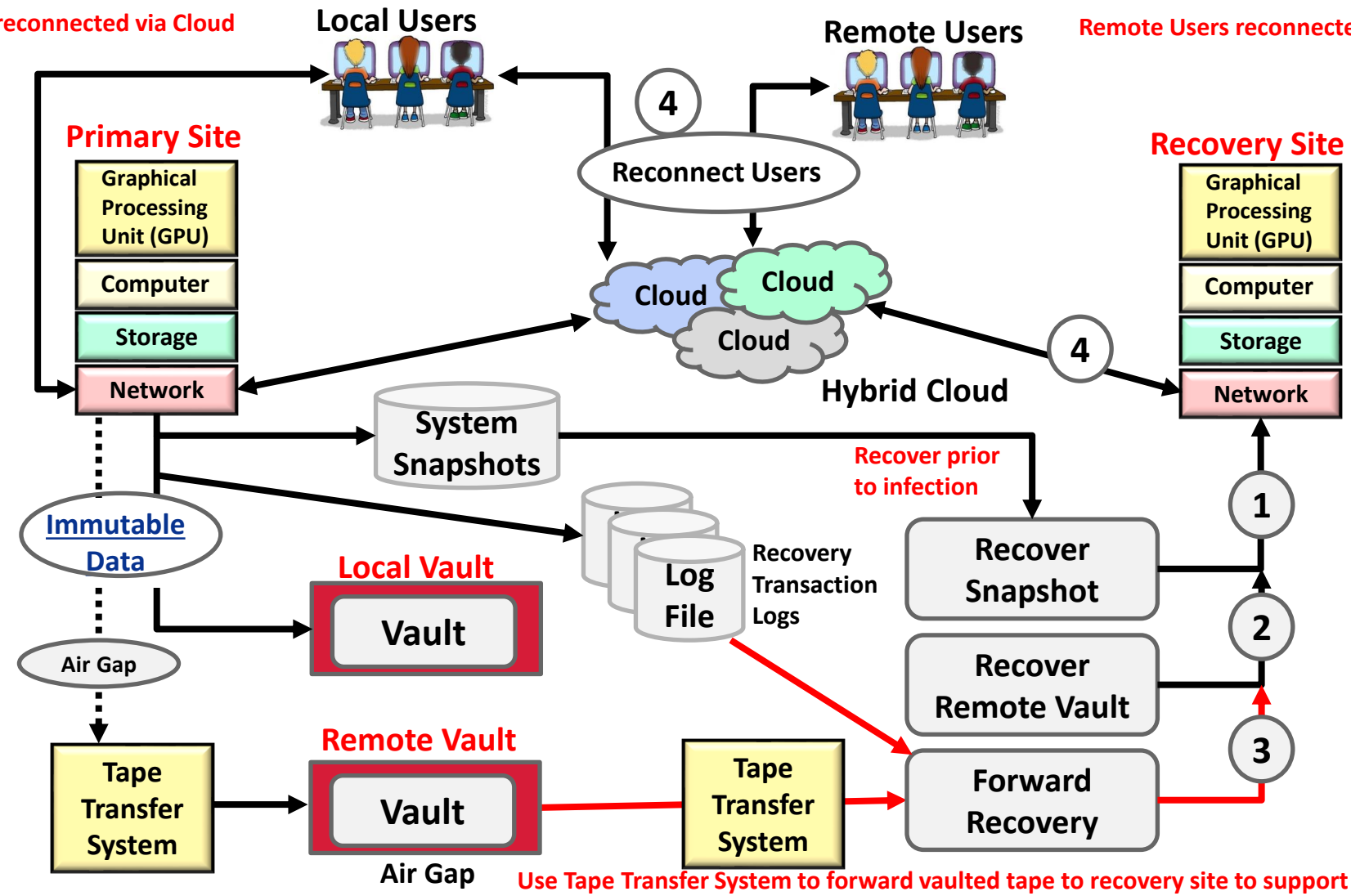
- Business Continuity Management, including:
  - Disaster Recovery Site;
  - Business Recovery Site;
  - Primary, Secondary Site;
  - Connectivity;
  - Functionality.
- Risk Assessment, including:
  - Laws and Regulations;
  - "Audit Universe";
  - Audit Schedule;
  - Mitigate & Mediate;
  - Insurance 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

Results

- 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

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

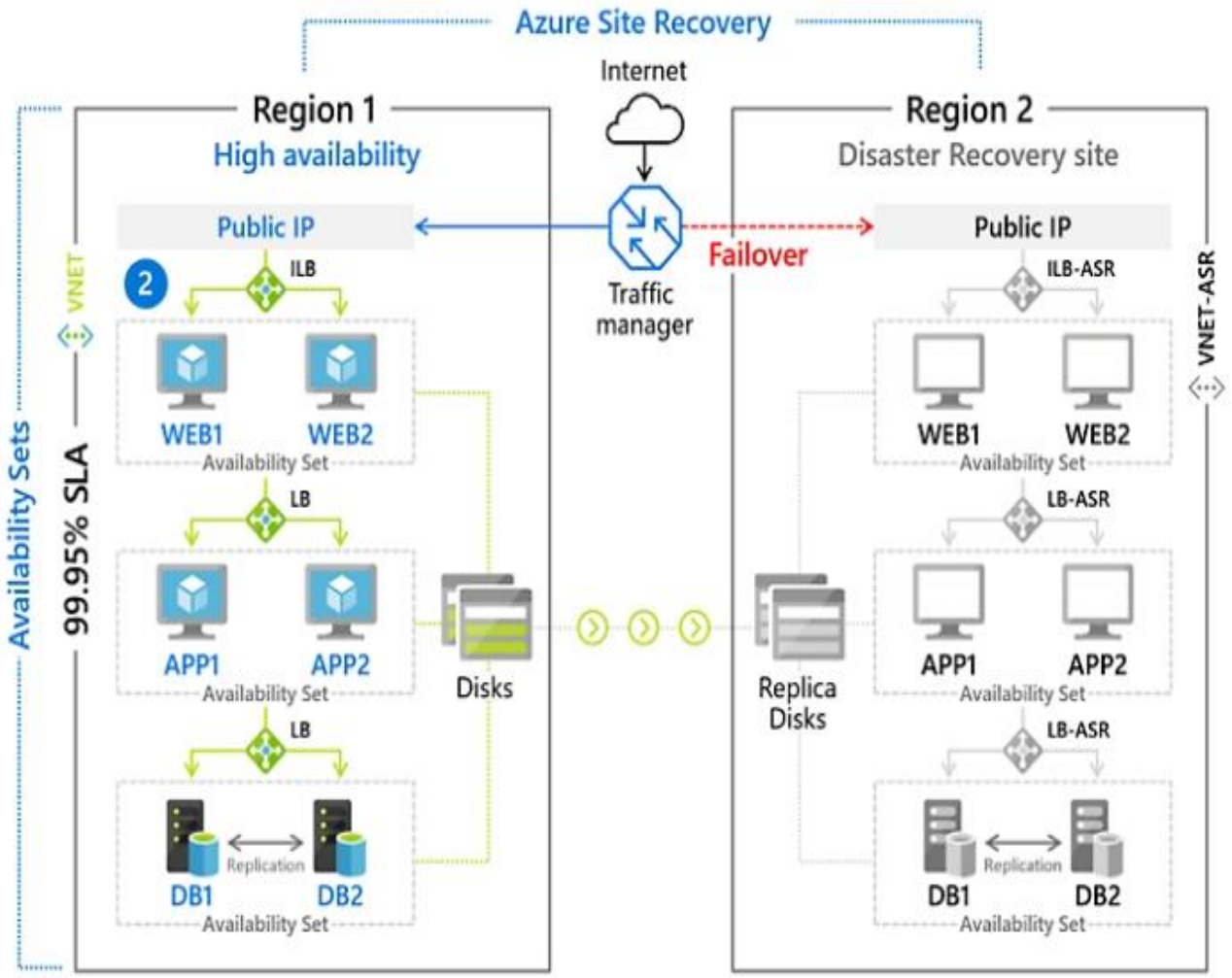


Recovery Process:

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.

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

Building and Implementing an Application

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

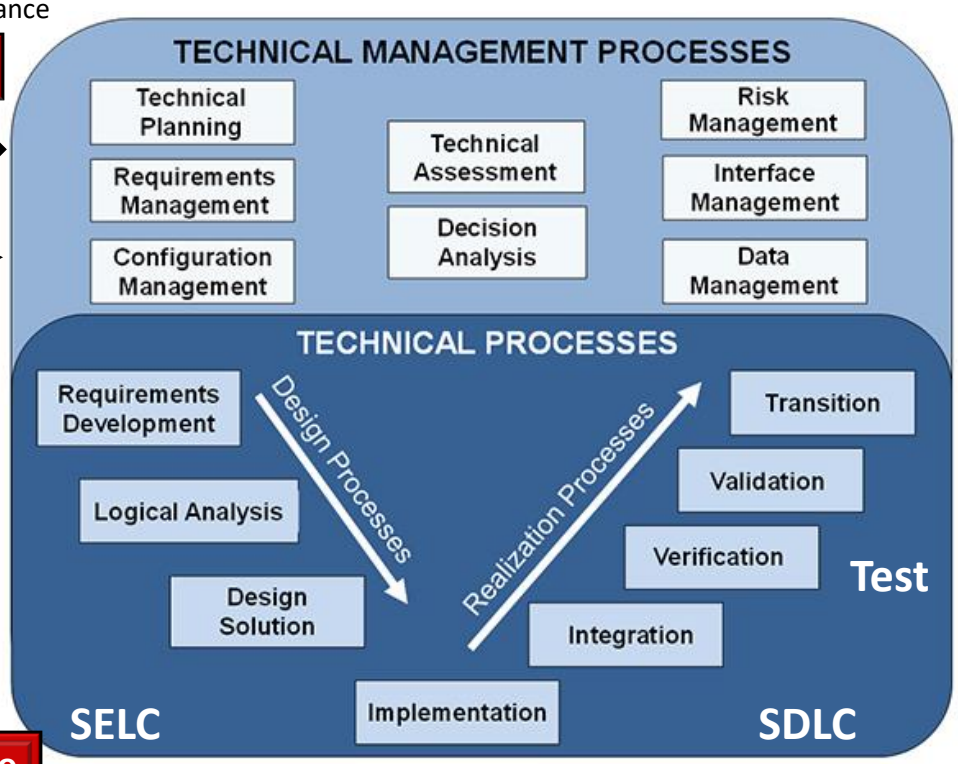
Programmers:
- Development
- Test
- Maintenance

Development

User Request

- 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

Develop once, maintain many



Maintenance

Enhance, Or Fix Problems

Change

Maintenance

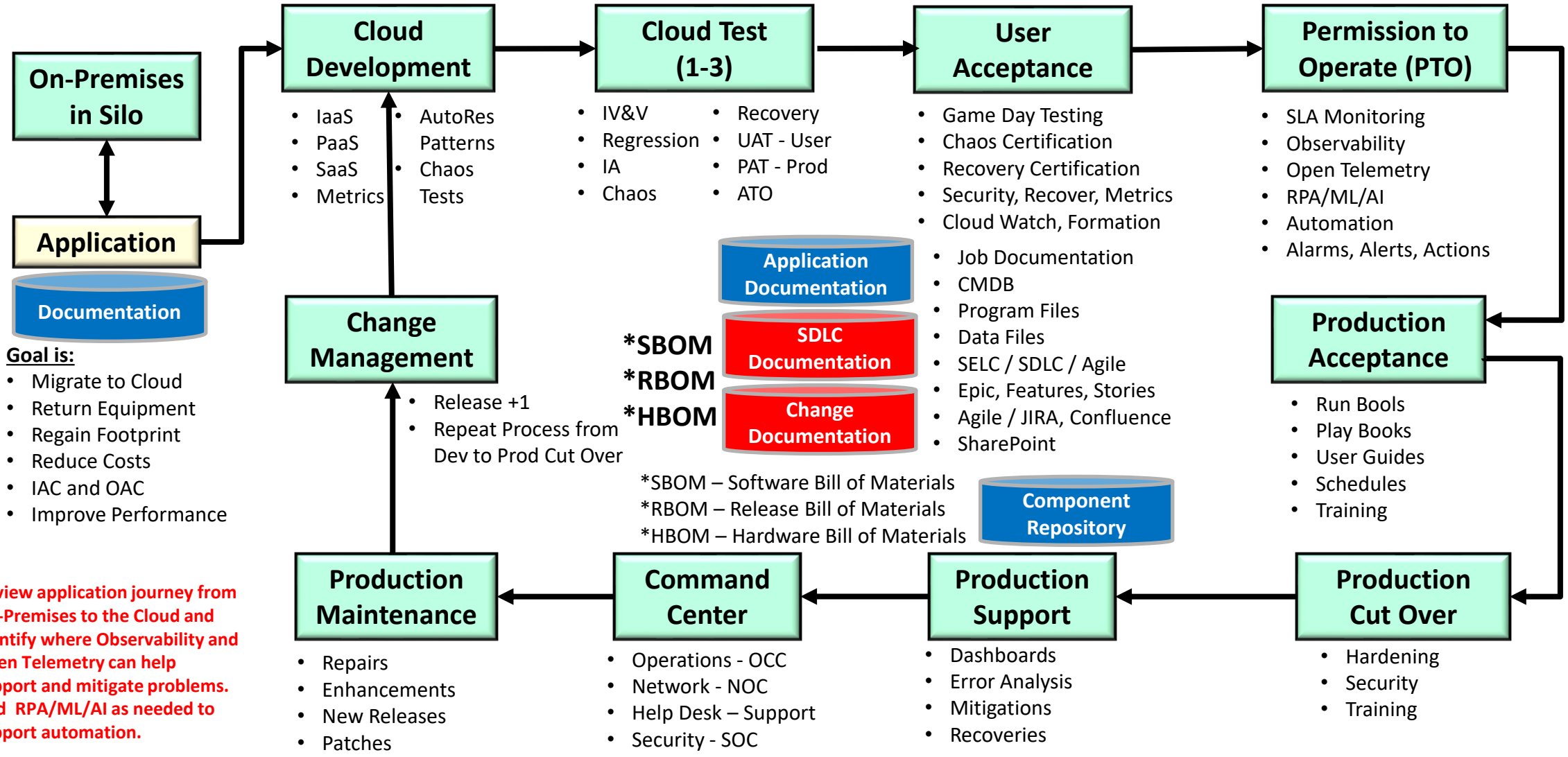
Fix Problems, Update Releases, Enhancements

Domains

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*

Migrating Applications to the Cloud

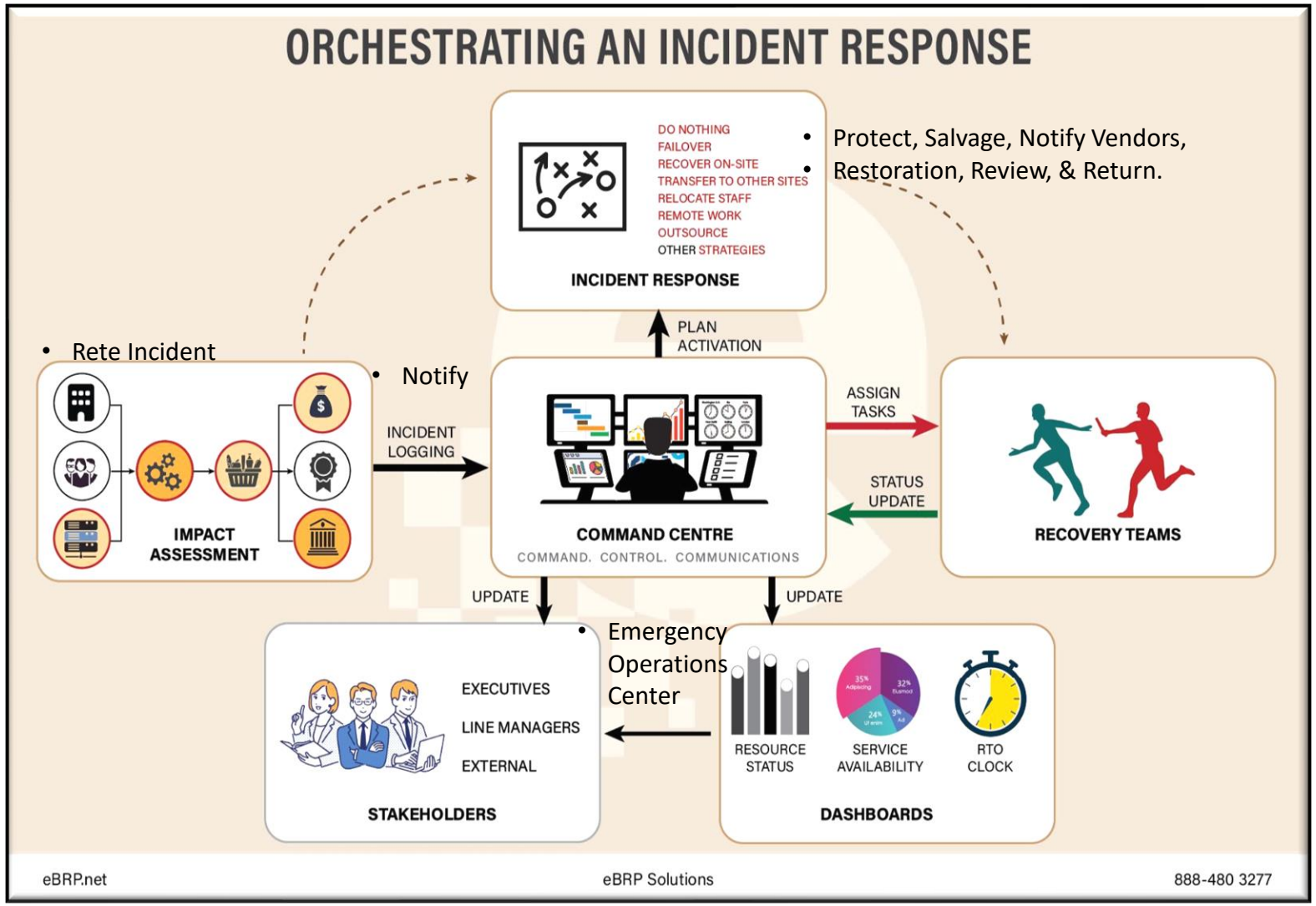
Thomas Bronack
Email: bronackt@dcag.com
Phone: (917) 673-6992



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
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)

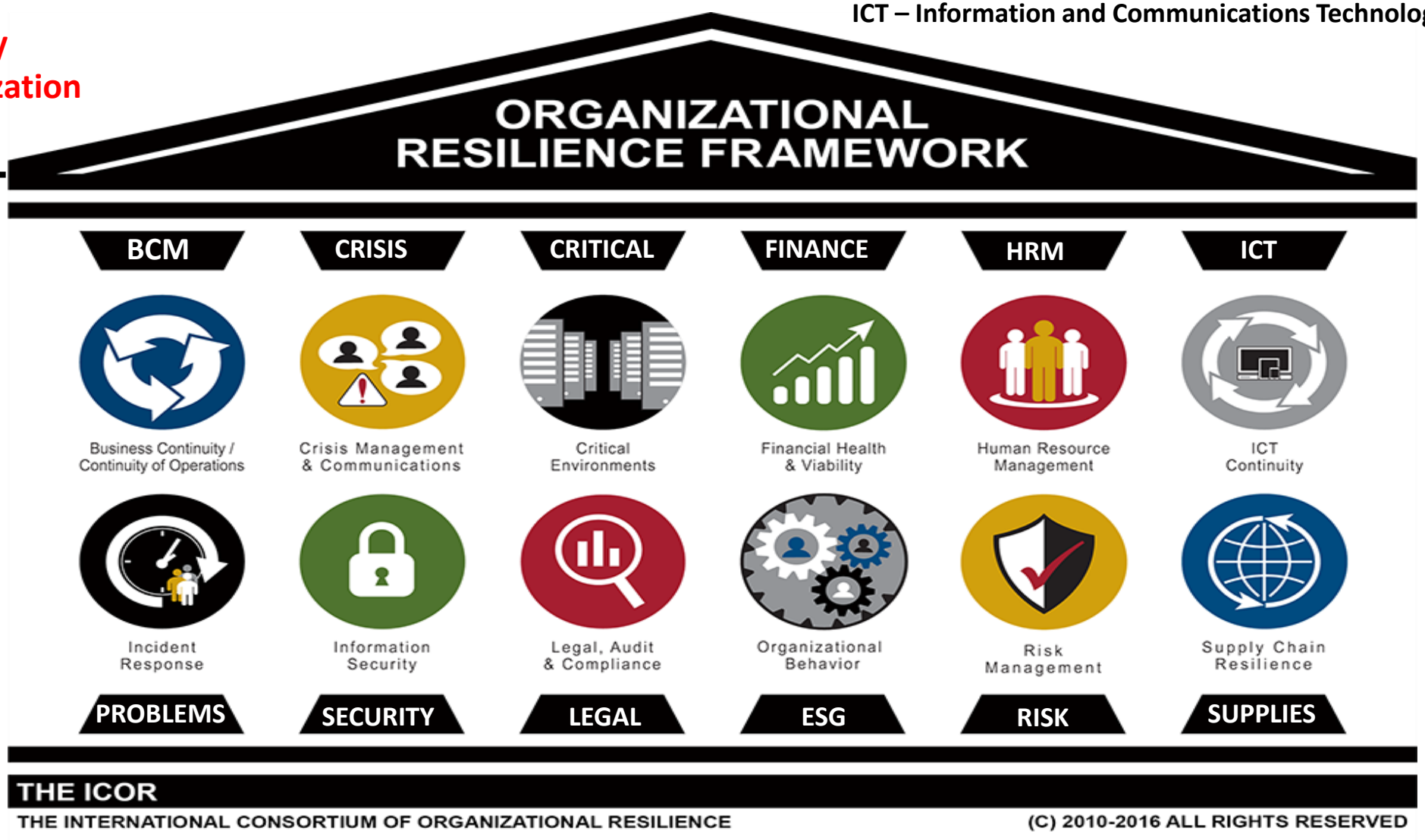
Thomas Bronack
Email: bronackt@dcag.com
Phone: (917) 673-6992

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.



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:

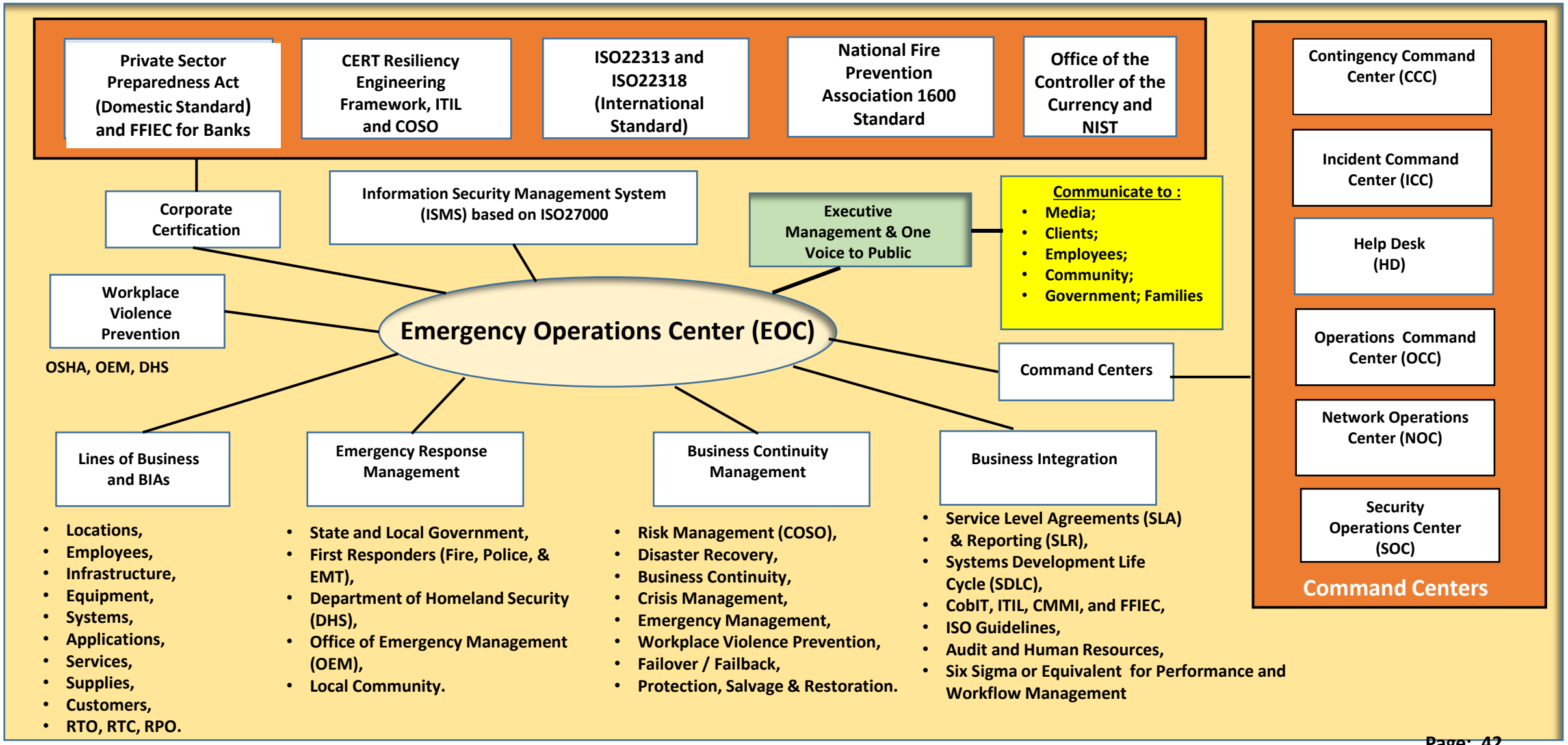
- **Shifting behavior from response to prevention.** Deep, comprehensive planning helps teams anticipate events, evaluate alternatives, prevent disruptions, and model all scenarios and options. Reacting to events as they happen is not sufficient in today's competitive market.

- **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)

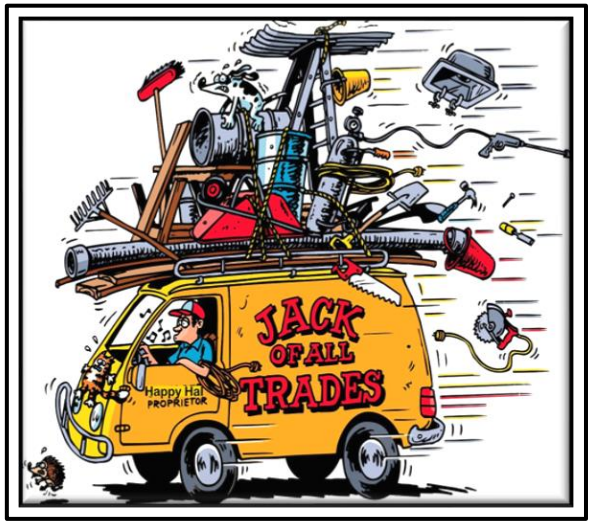
Thomas Bronack
Email: bronackt@dcag.com
Phone: (917) 673-6992



Tom Bronack– A strong Generalist

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

My background is comprised of technical, managerial, sales, and consulting with experience implementing safeguarded environments that comply with business/regulatory requirements. Skilled in Enterprise Resiliency and Corporate Compliance Certification, Risk Management, Operations Analysis, creating Disaster Recovery and Business Continuity plans, integrating process improvements within standards and procedures governing business operations and personnel accountability, adept in planning and improving the efficiency of data processing systems/services; optimizing information technology productivity through system implementation, quality improvements, technical documentation, and Dashboards. Excellent communications and personnel interfacing skills as Team Member or Lead.



Selected Accomplishments

- Provided data center builds, migrations, consolidations, and termination services.
- Defined and conducted Asset Management services for equipment acquisitions, redeployment, and termination.
- Led, conducted, and performed IT Technology and Security Risk Assessments / Audits for regulator attestation and Risk Eliminations (Risk Register with POA&M that mitigates. or mediates, problems associated with Risks).
- Implemented Business Continuity Plans for major organizations in the Banking, Brokerage, Insurance, Service and Product Vendors, Pharmaceutical, Manufacturing, and international industries utilizing best practices and virtualization techniques.
- Designed and implemented High Availability and Continuously Available environments for a major bank to meet recovery RTO and RPO discovered via BIA assessments and Recovery Group definitions. Categorized Applications and Services as Critical t Revenue, Operations, or Brand with Risk Group.
- Sales Agent for IBM Business Recovery Services, bringing Chase, Citibank, and Salomon Brothers in as potential clients.
- Sales Agent for Diversified Software Systems, Inc. (DSSI) selling Docu/Text and Job/Scan products and provided professional services to clients.
- Provided consulting services to established offsite vaulting and recovery facilities for clients (both business and IT) and assisted in implementing an automated file vaulting and recovery management system (automated vaulting system).
- Created first Computer Risk Management Department for a bank, then created first data center recovery center with Comdisco at a joint site in NJ.
- Created Security Pacific Risk Asset Management (SPRAM) and Total Risk Management (TRM) company as a subsidiary to Security Pacific Bank.
- Conducted a one-year audit of Midland Bank in England for Computer Science Corporation and reported to bank president.
- Created Five-Year Business Plan for Information Technology Division of European America Bank.
- Merged ADP Proxy and IECA into new $9.3 million facility, while consulting directly to Brokerage Division President.
- Sr. Systems Developer on team creating DHS CDM Dashboard for detecting cyber-crimes and technology threats in near real-time for entire US Government.
- Created Management Dashboard system for Infrastructure, SDLC, BCM, and Compliance and used system to finalize project for manufacturing company.
- Designed Electronic Voting System based on “One Person – One Vote:” using biometrics to eliminate fraud and corruptions, and blockchain to eliminate data tampering and ensure system guaranteed data integrity, security, accessibility, and audit ability.
- Implemented problem/incident management systems based on metric thresholds, alarms to capture anomalies, alerts to notify component owners, and actions performed by component owners to fix problem and update documentation as needed.
- Developed and presented educational classes on Business Continuity, IT/DR, and general Information Technology topics including developing and instructing the BCP – IT/DR course for the Disaster Recovery Institute International (DRII).

- Enterprise Resilience,
- Corporate Certification,
- Risk Assessment,
- Business Impact Analysis,
- Business and Disaster Recovery,
- Project Management,
- Team Leadership,
- Training & Awareness,
- Optimization & Compliance