Created by:

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

Thomas Bronack
Overview of Services

Enterprise Resiliency

Including

Site Reliability Engineering

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.

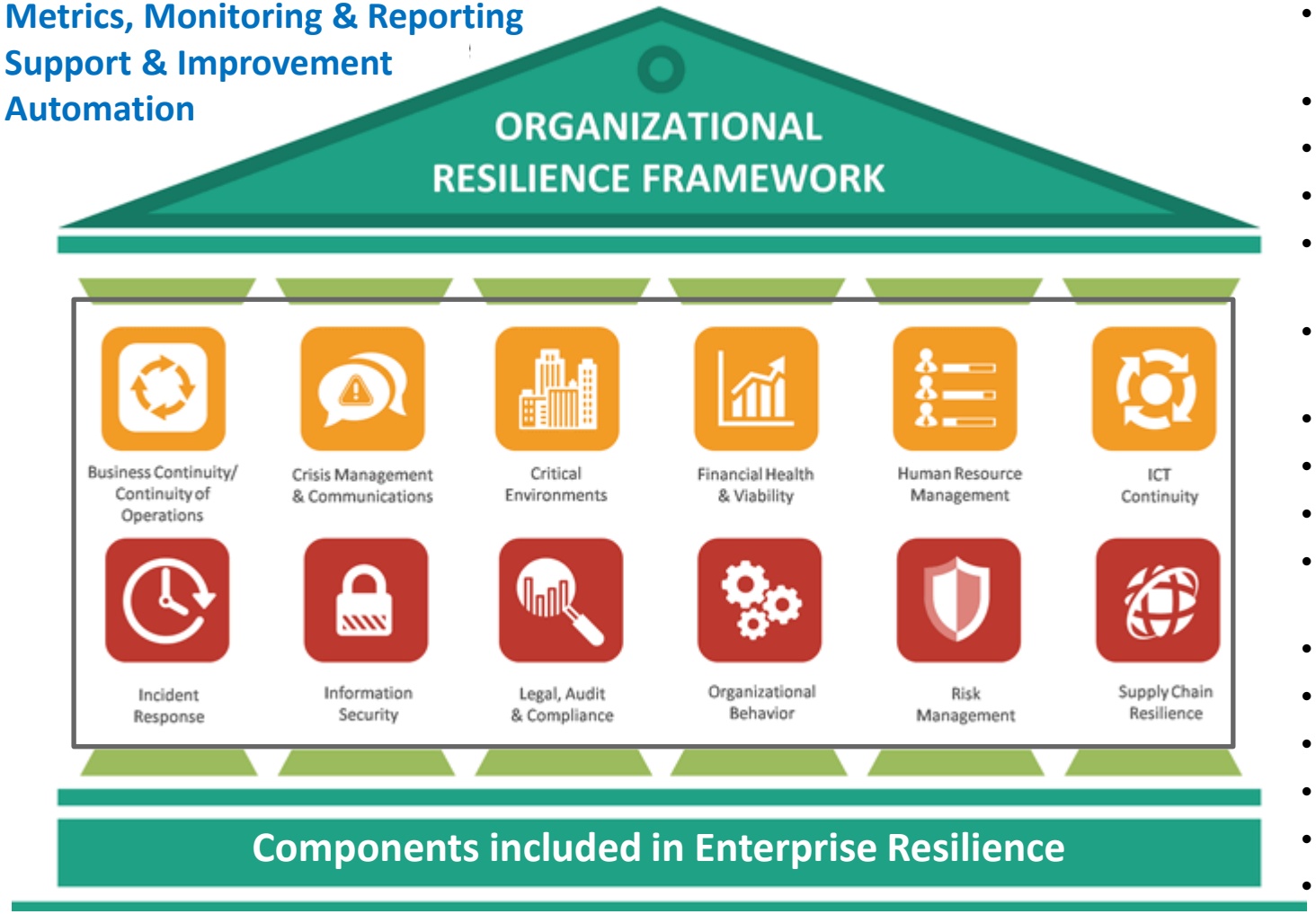
Enterprise Resilience components and disciplines, include:

- **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**.

What does Enterprise Resilience consist 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:

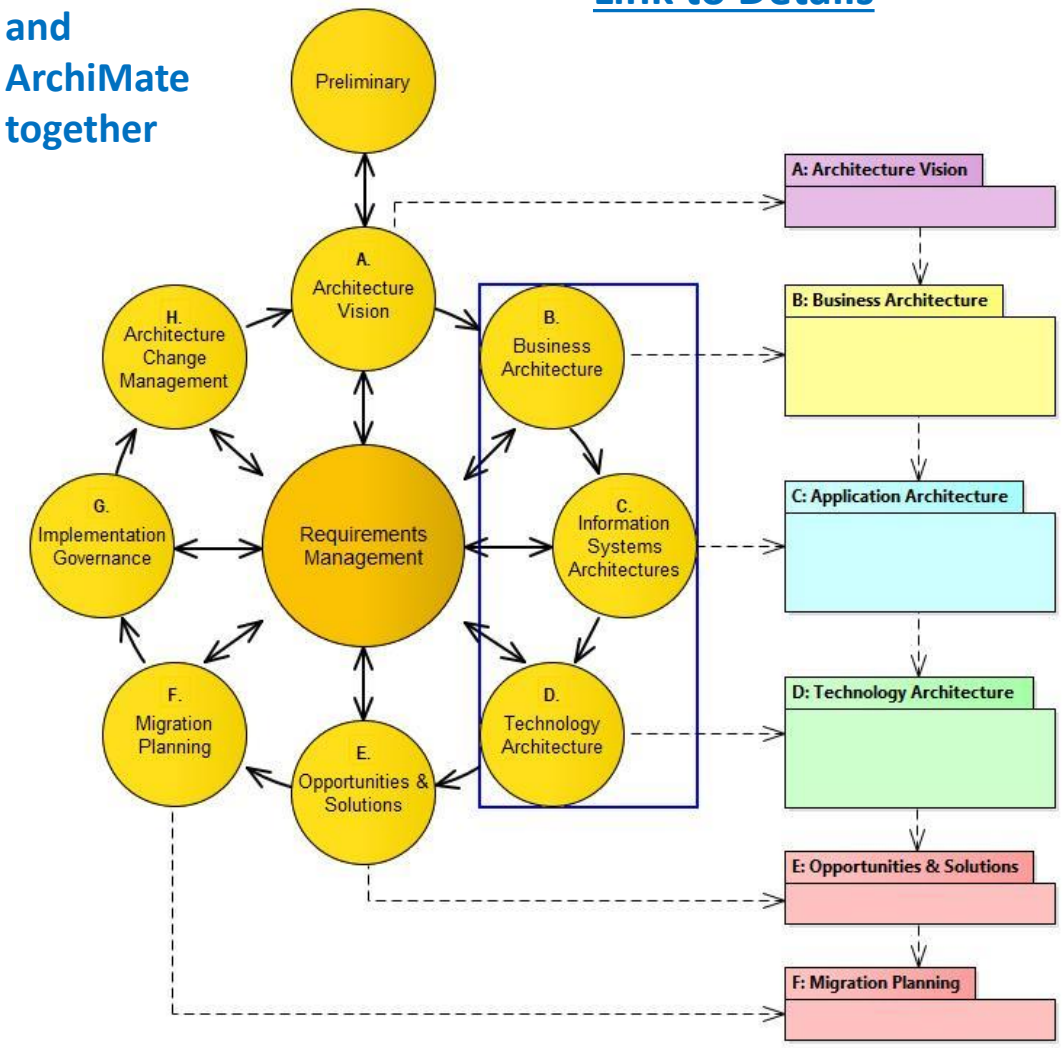
- Enterprise Products & Services (Company Jewels),
- Critical Economic Services & Financial Health & Visibility,
- Brand and Company Reputation,
- Legal, Audits, & Compliance,
- Recovery Groups, RTO, RPO, RTC, Certifications
- Risk Management Foundation (RMF) & Business Impact Analysis (BIA),
- Business 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,
- Incident & Problem Response,
- Organizational Behavior,
- Supply Chain Resilience,
- Migrating to the Cloud and hybrid Environments,
- Center of Excellence (COE) implementation.

TOGAF - The Open Group Architecture Framework

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

TOGAF ADM and ArchiMate together

Link to Details

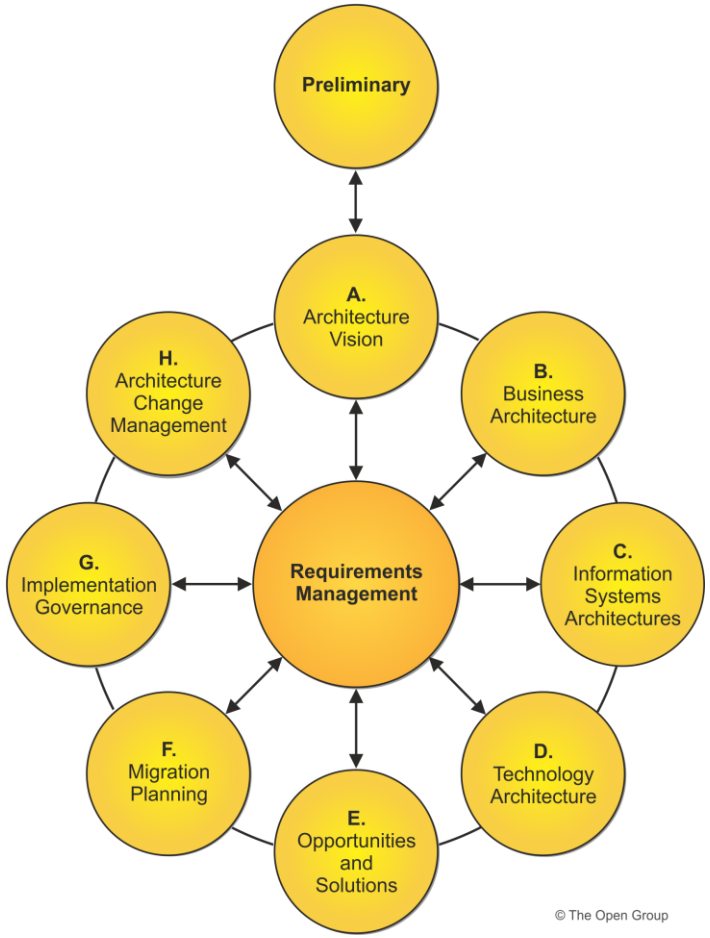


TOGAF Steps:

Preliminary - Understand the business and key services that produce revenue or are customer facing and rate tiers of importance.

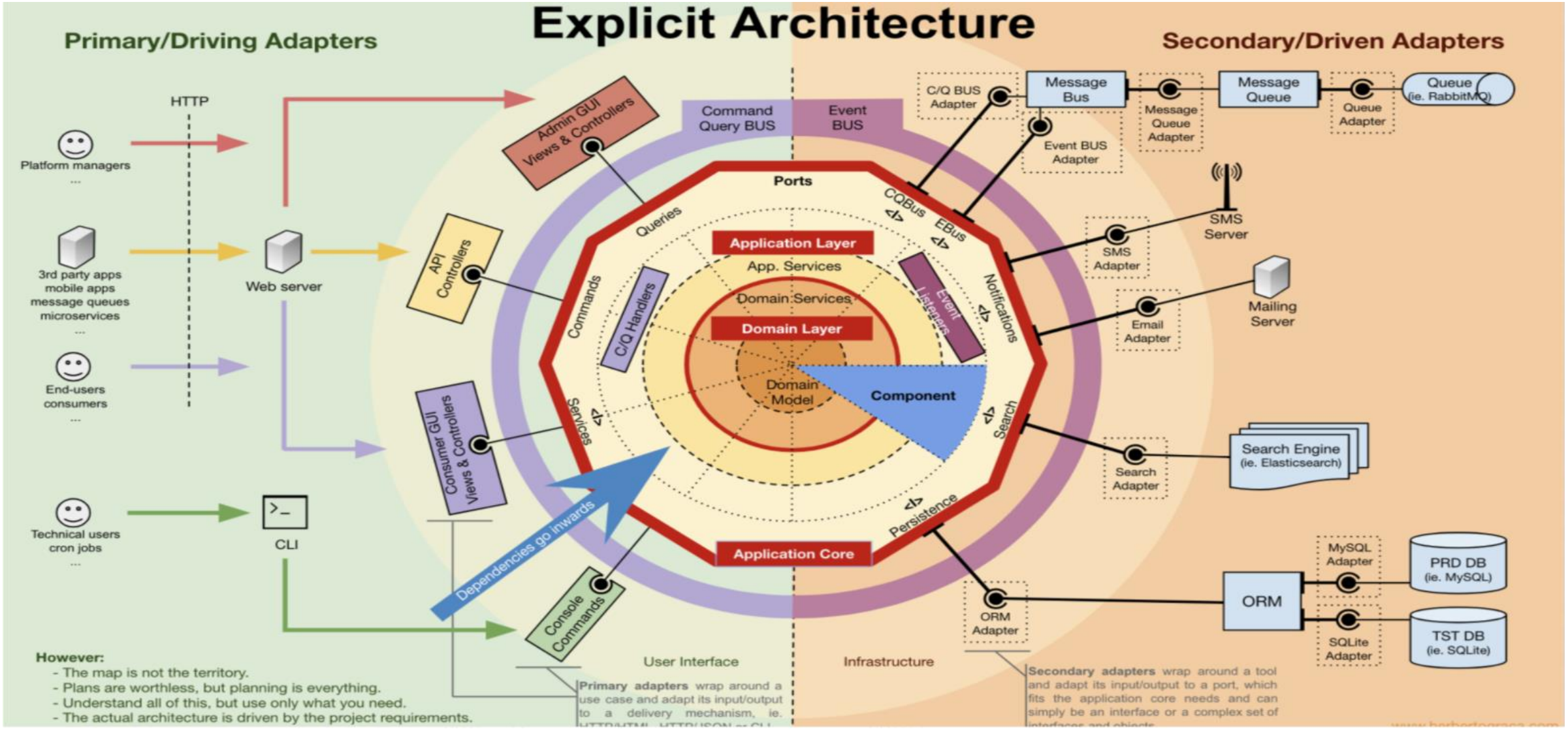
A. Architecture Vision
B. Business Architecture
C. Information Systems Architectures
D. Technology Architecture
E. Opportunities and Solutions
F. Migration Planning
G. Implementation Governance
H. Architecture Change Management

Link to TOGAF Group



Domain-Driven Design overview

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



Why do you need Business Continuity Management

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
- **Integrate** production, testing, validation and continuous Improvement

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

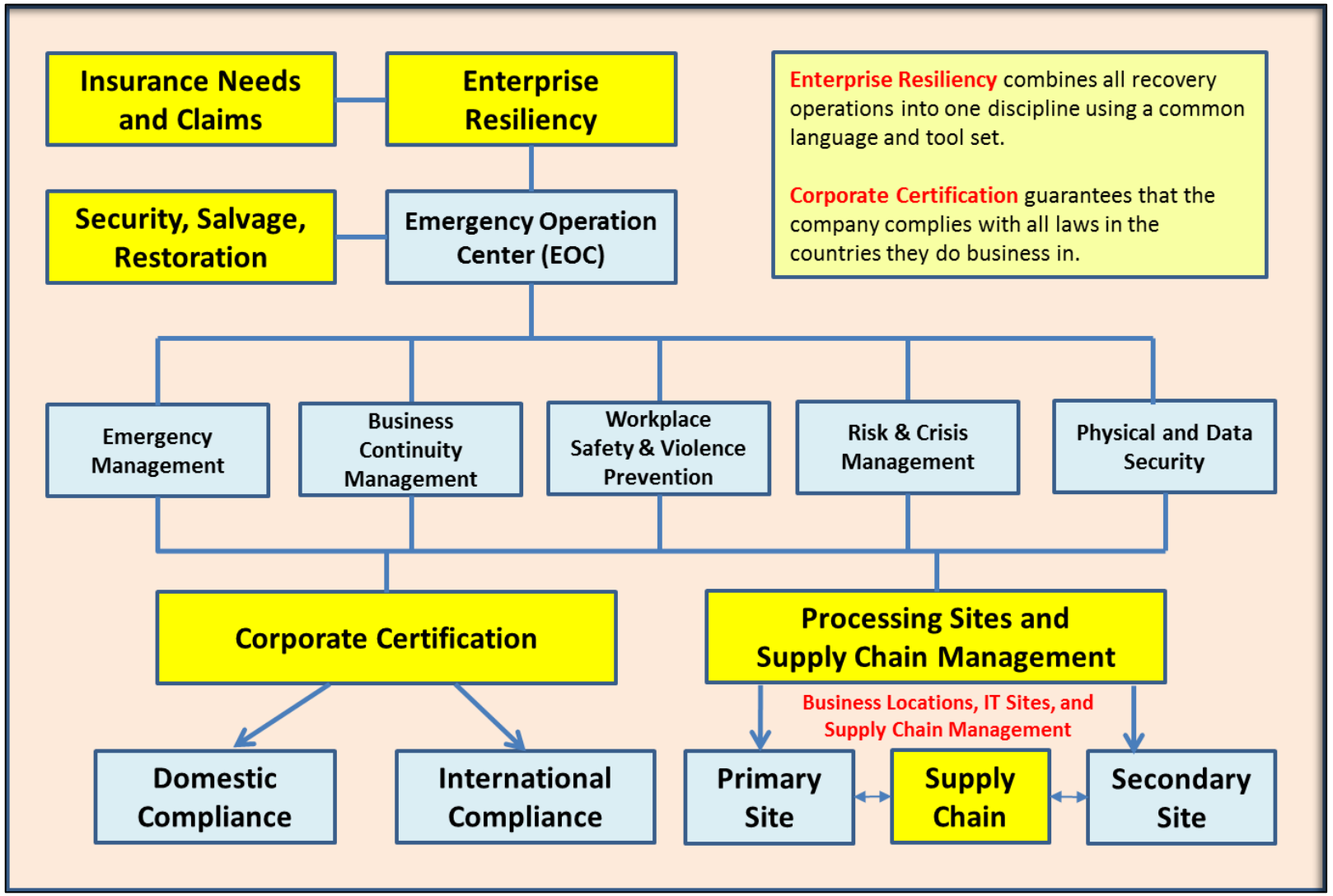
Enterprise Resiliency and Corporate Certification

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

Enterprise Resiliency is the combining of all Recovery Disciplines under one umbrella, utilizing a common language and common set of tools so that the combined knowledge of recovery personnel can be best used.

Corporate Certification is responsible for adhering to all required laws and regulations of the countries where the company conducts business.

Risk Management, Insurance, Claims, Security, Salvage, and Restoration of sites that have experienced a disaster is included along with Supply Chain Management and Workplace Safety and Violence Prevention.



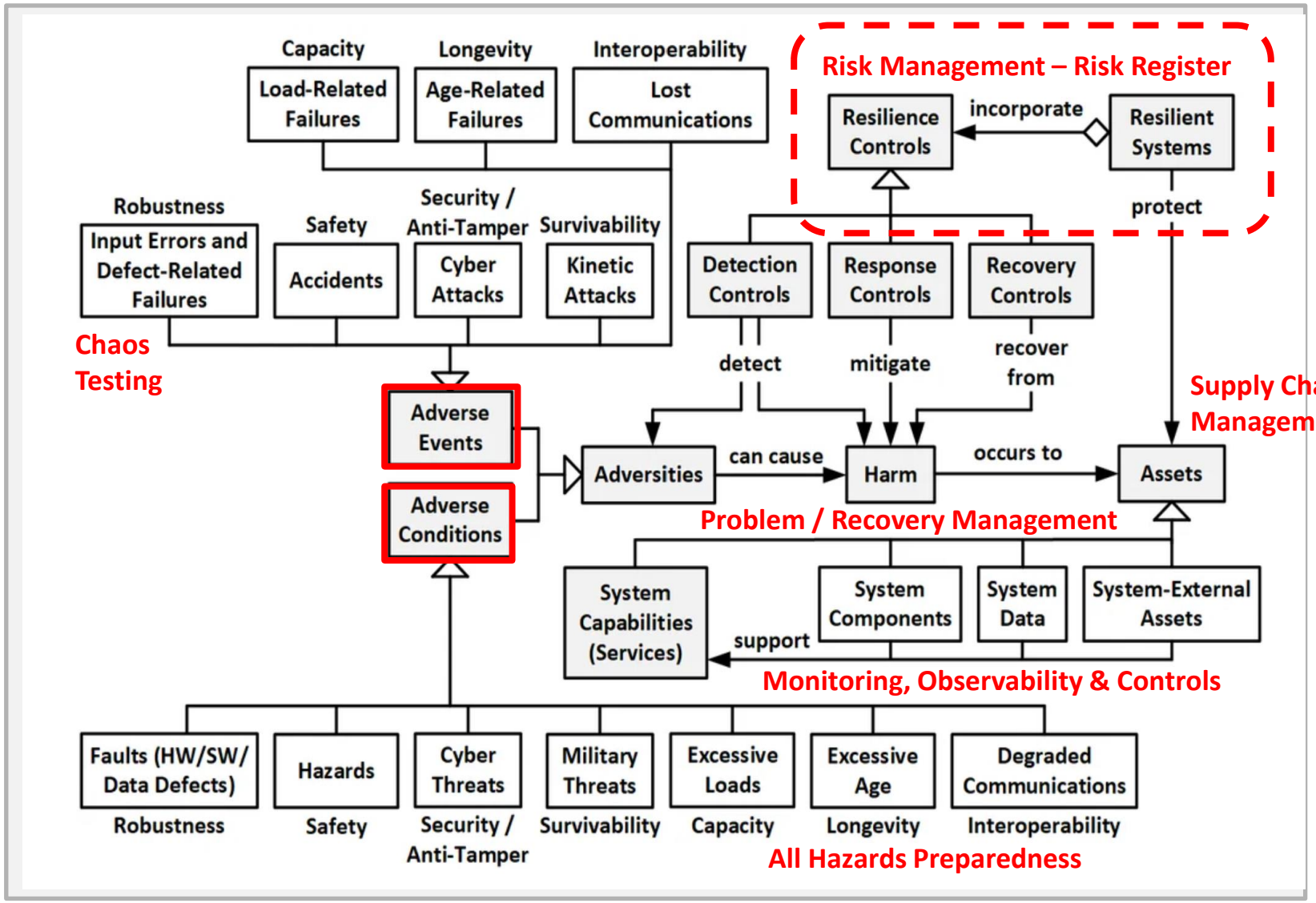
What is Resilience and why is it important

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

Definition:

Basically, a system is resilient if it continues to carry out its mission in the face of adversity (i.e., if it provides required capabilities despite excessive stresses that can cause disruptions). Being resilient is important because no matter how well a system is engineered, reality will sooner or later conspire to disrupt the system.

Achieving resilience when so many components can cause a disruption if a difficult task indeed. It requires the full understanding and cooperation of the entire organization, its vendors, and suppliers.



Process followed in performing Enterprise Resilience

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

1. Rating your company's sensitive applications

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

2. Locate weaknesses to be overcome

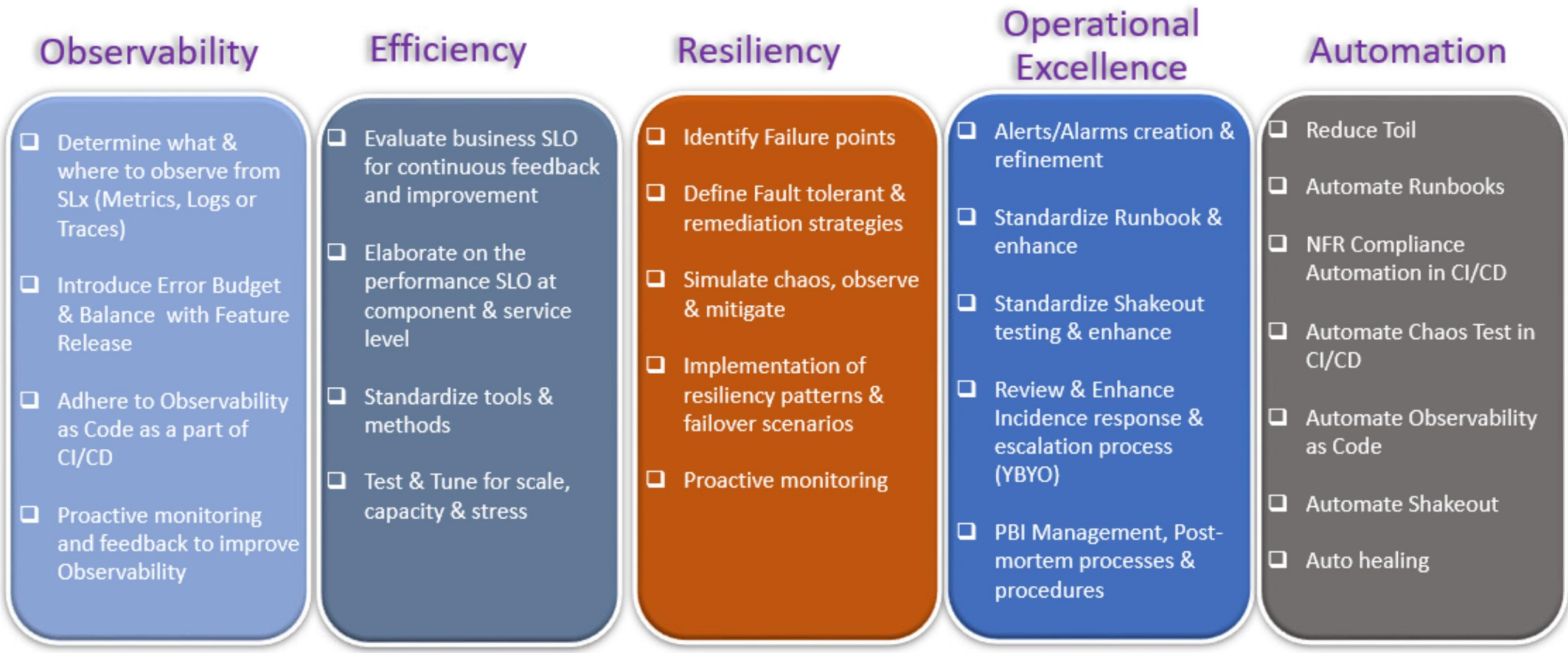
a. **Analyze** exposures and how you can best protect the business going forward (Risk Assessment, BIA, Security (Physical / Data / CSF / CIA), Compliance (Laws, Regulations, Attestation, Auditing), Development (Systems Engineering Life Cycle – SELC), Operations (Systems Development Life Cycle – SDLC),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

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

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

Five Pillars of Site Reliability Engineering (SRE)

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

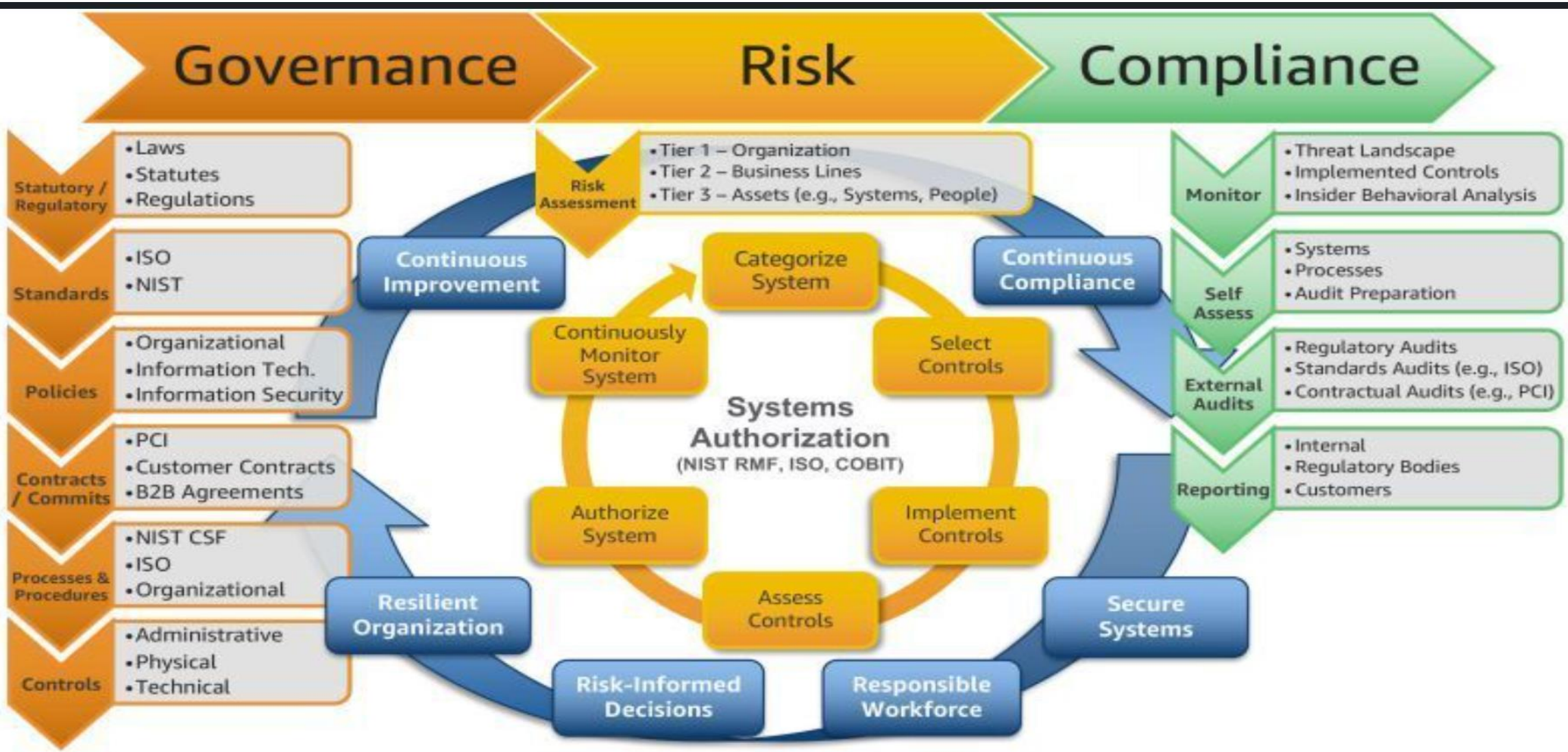


[Google – Site Reliability Engineer Handbook]

NFR – Non-Financial Reporting

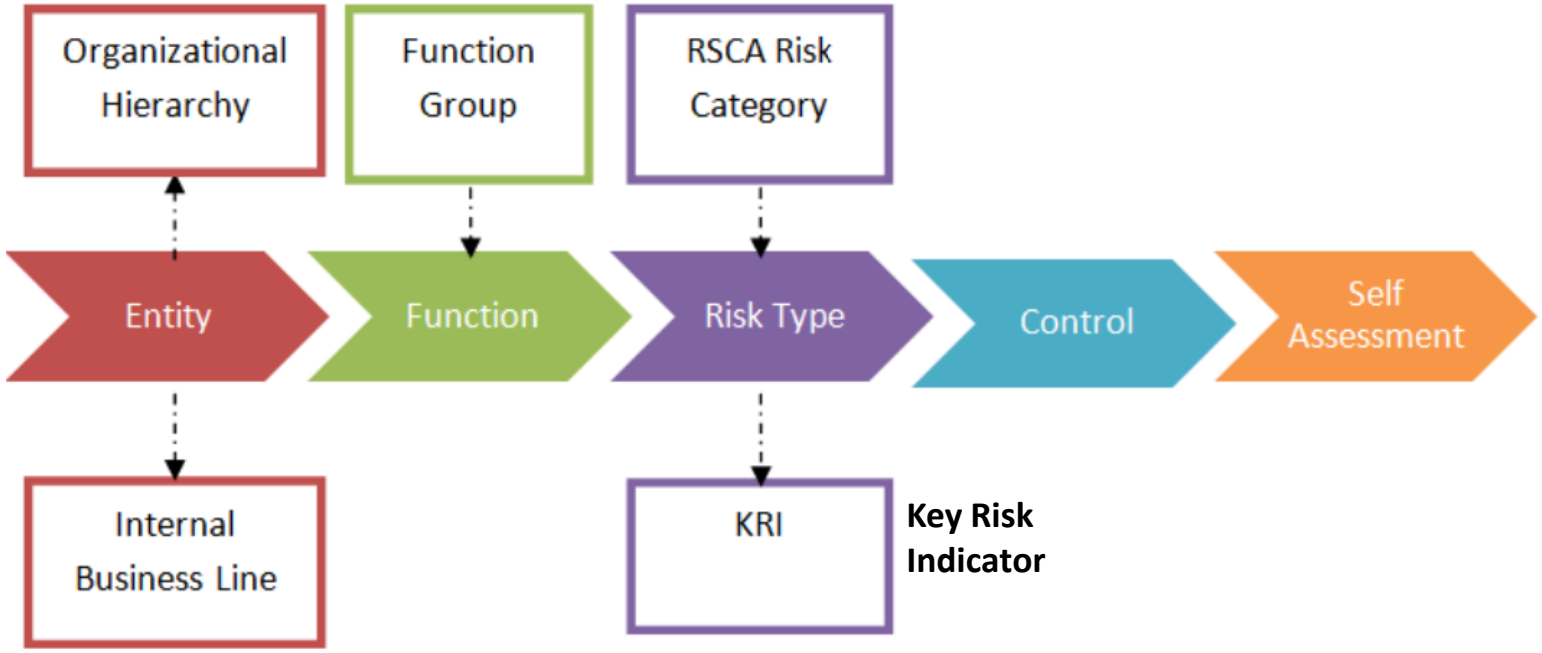
GRC and Risk Management to ensure compliance

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



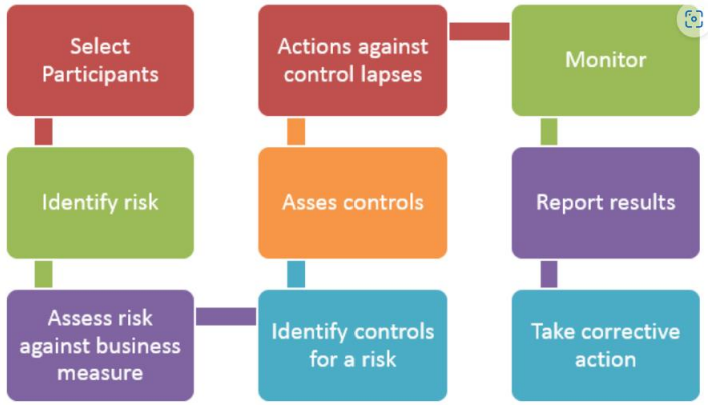
Risk Control Self Assessment (RCSA)

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



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

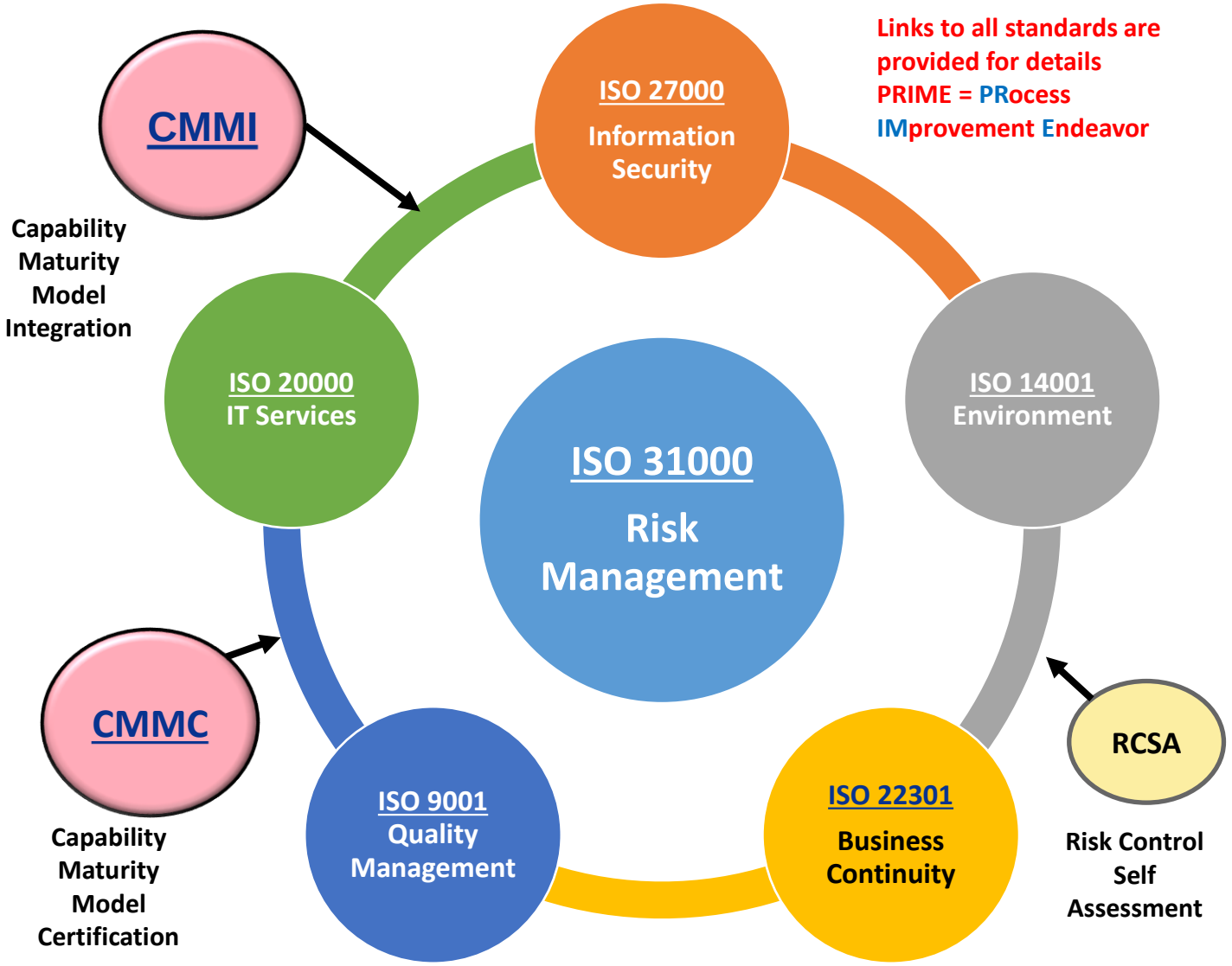


RCSA (Risk Control Self Assessment) is an empowering method/process by which management and staff of all levels collectively identify and evaluate risks and associated controls. It adds value by increasing an operating unit's involvement in designing and maintaining control and risk systems, identifying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

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 will help your company 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).

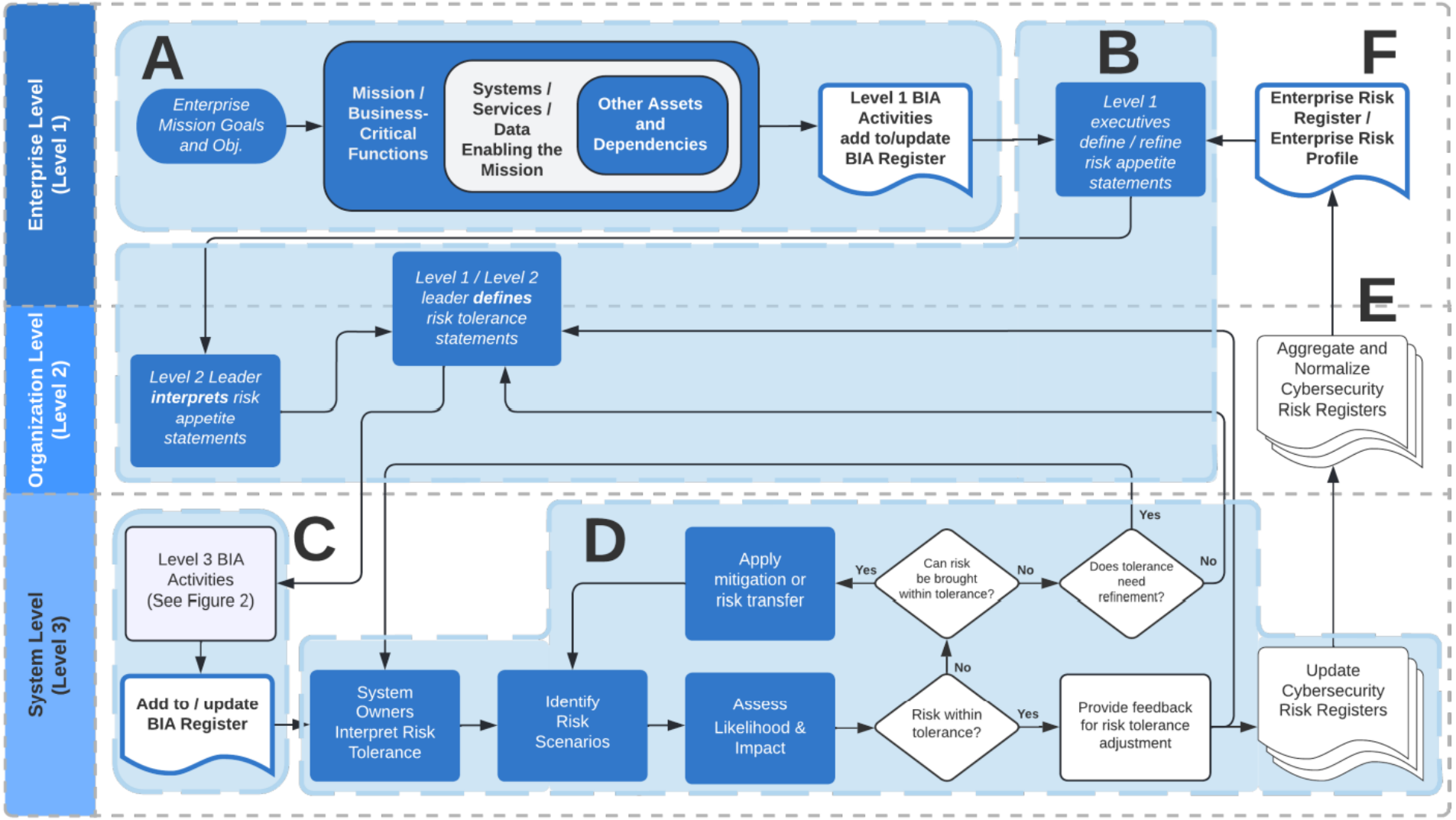
Then implement your **Business Continuity** (ISO 22301) Recovery Certification Process for Emergency, Crisis, Business, and IT Disaster Recovery Management.

Integrate Quality Management (ISO 9001) within all of 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.

Business Impact Analysis - BIA

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

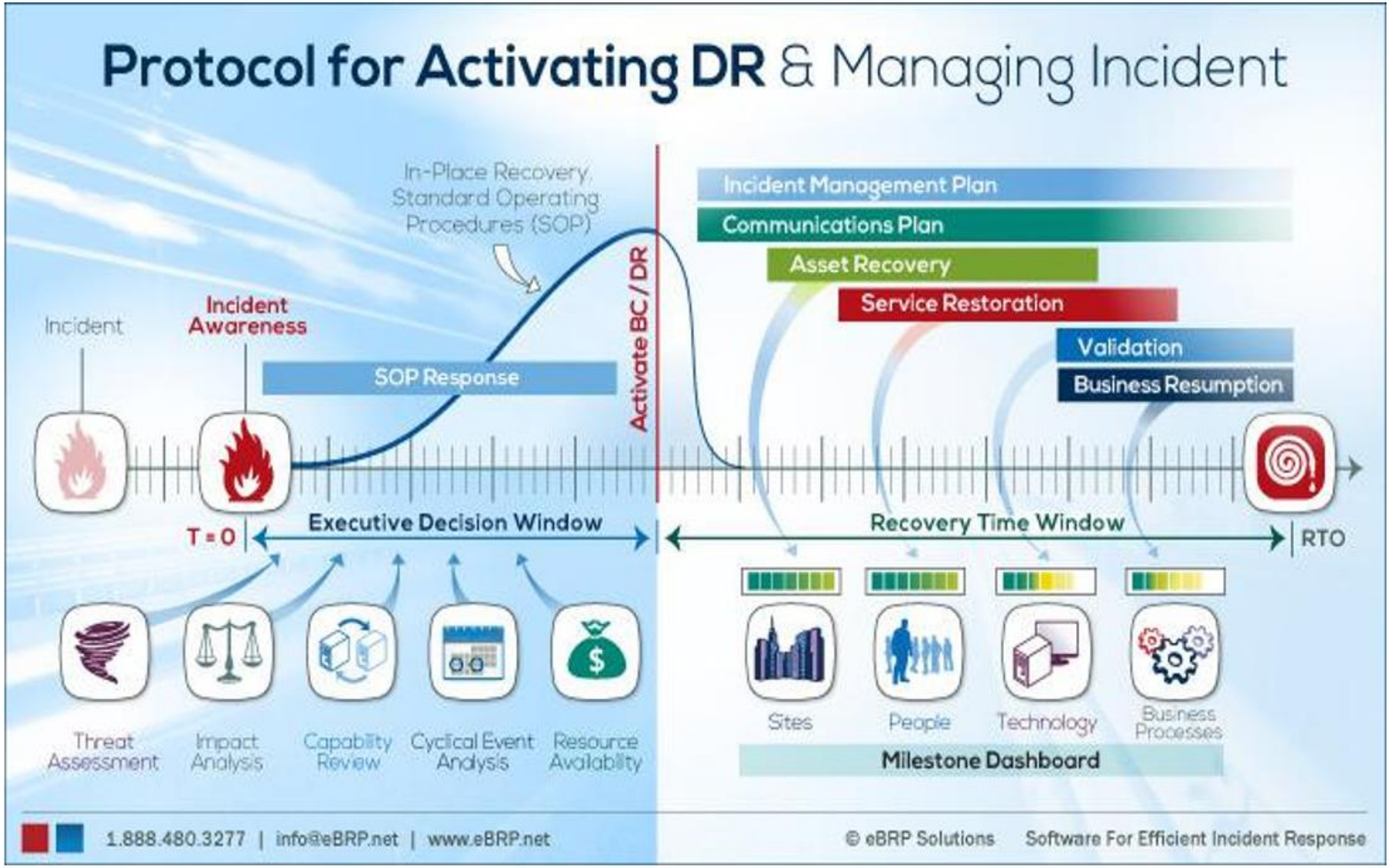


Link to Document

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

The Disaster Recovery Life Cycle

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

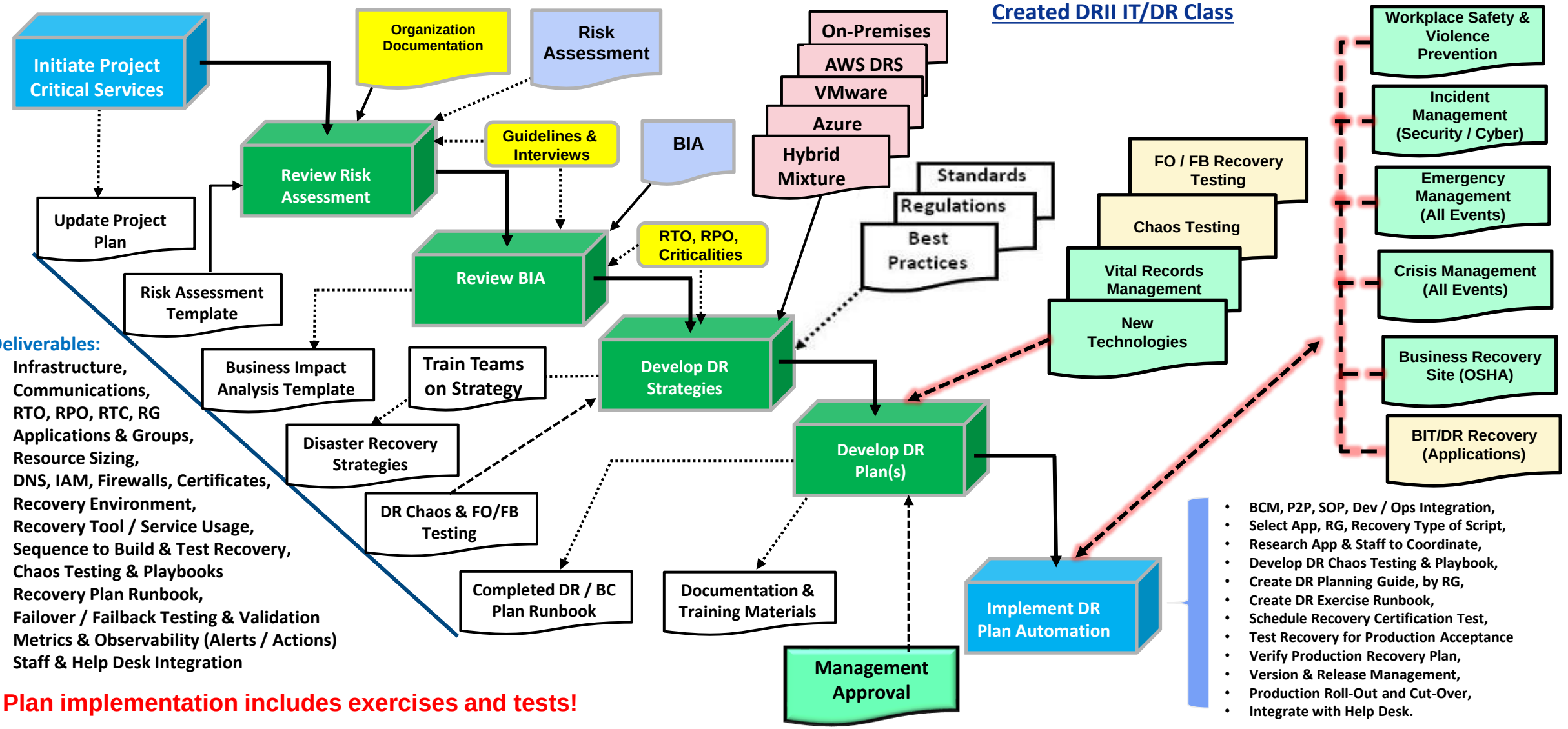


DR Life Cycle:

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. Servce Restoration
   e. Validation
   f. Business Resumption (RTO)
3. **Milestones Dashboard**
   a. Sites
   b. People
   c. Technology
   d. Business Processes

Sample Recovery Plan Methodology

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



Deliverables:

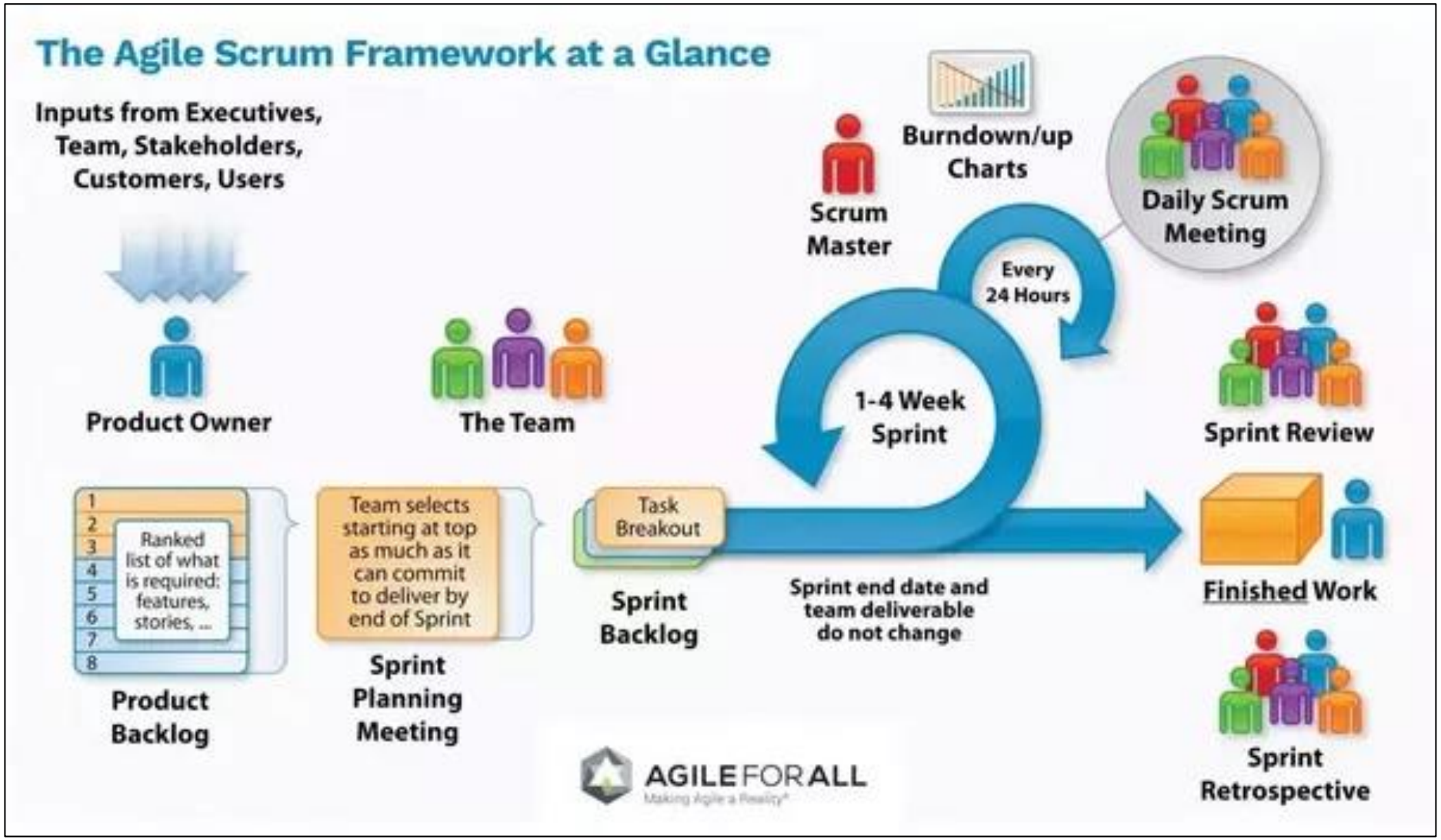
- Infrastructure,
- Communications,
- RTO, RPO, RTC, RG
- Applications & Groups,
- Resource Sizing,
- DNS, IAM, Firewalls, Certificates,
- Recovery Environment,
- Recovery Tool / Service Usage,
- Sequence to Build & Test Recovery,
- Chaos Testing & Playbooks
- Recovery Plan Runbook,
- Failover / Failback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

Agile vs Waterfall Systems Development

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

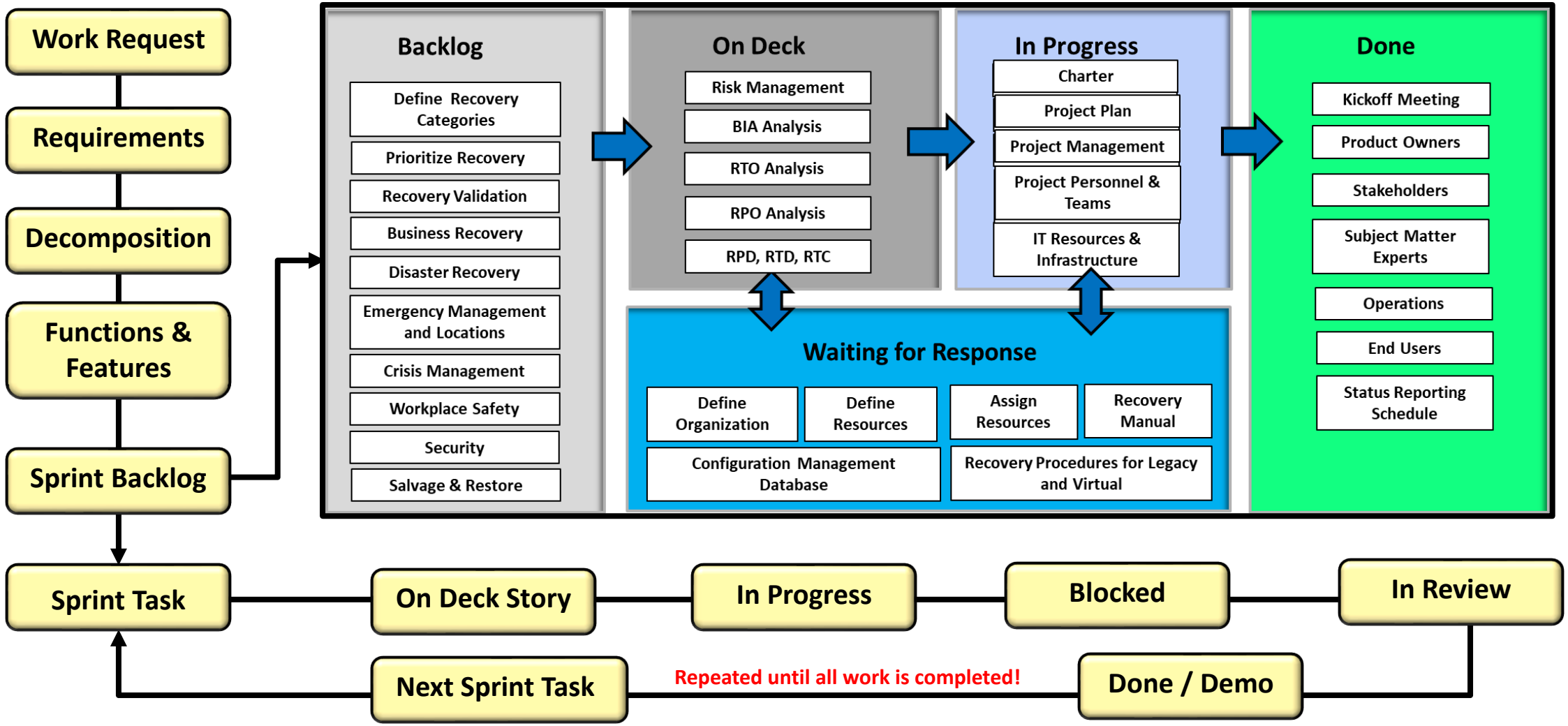


- Conception
- Initiation
- Analysis
- Design
- Construction
- Testing
- Deployment

Waterfall Model

DR Workload, using the Agile method for Dev/Ops

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



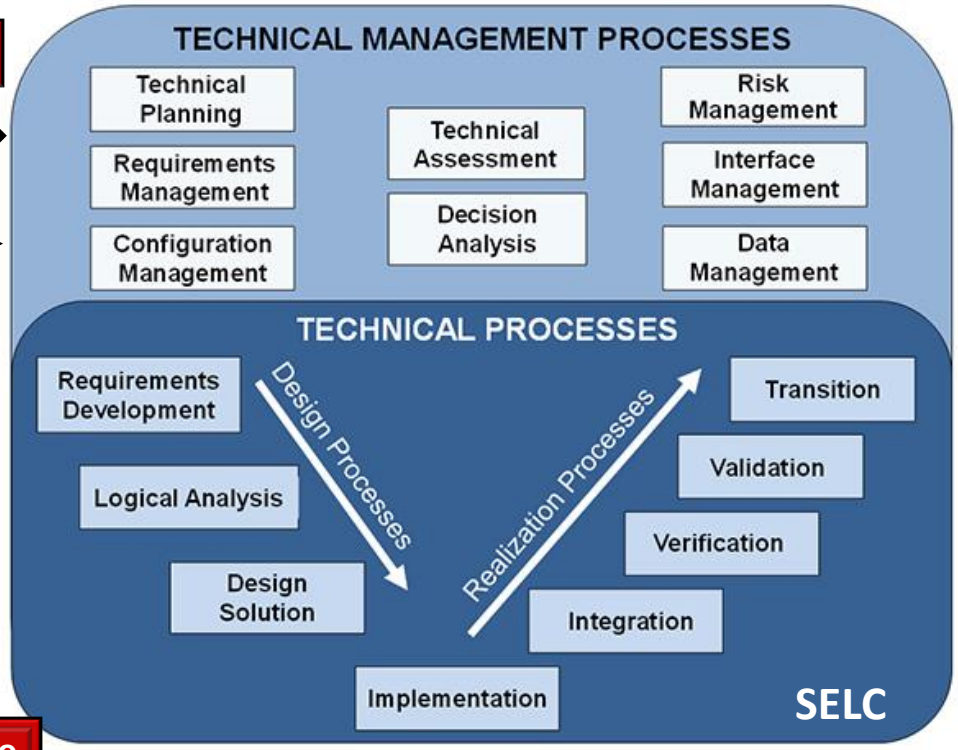
Building and Implementing an Application

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

Development

User Request

Develop once, maintain many



Domains

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

- 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 Recrds
- Recovery Management

Maintenance

Enhance, Or Fix Problems

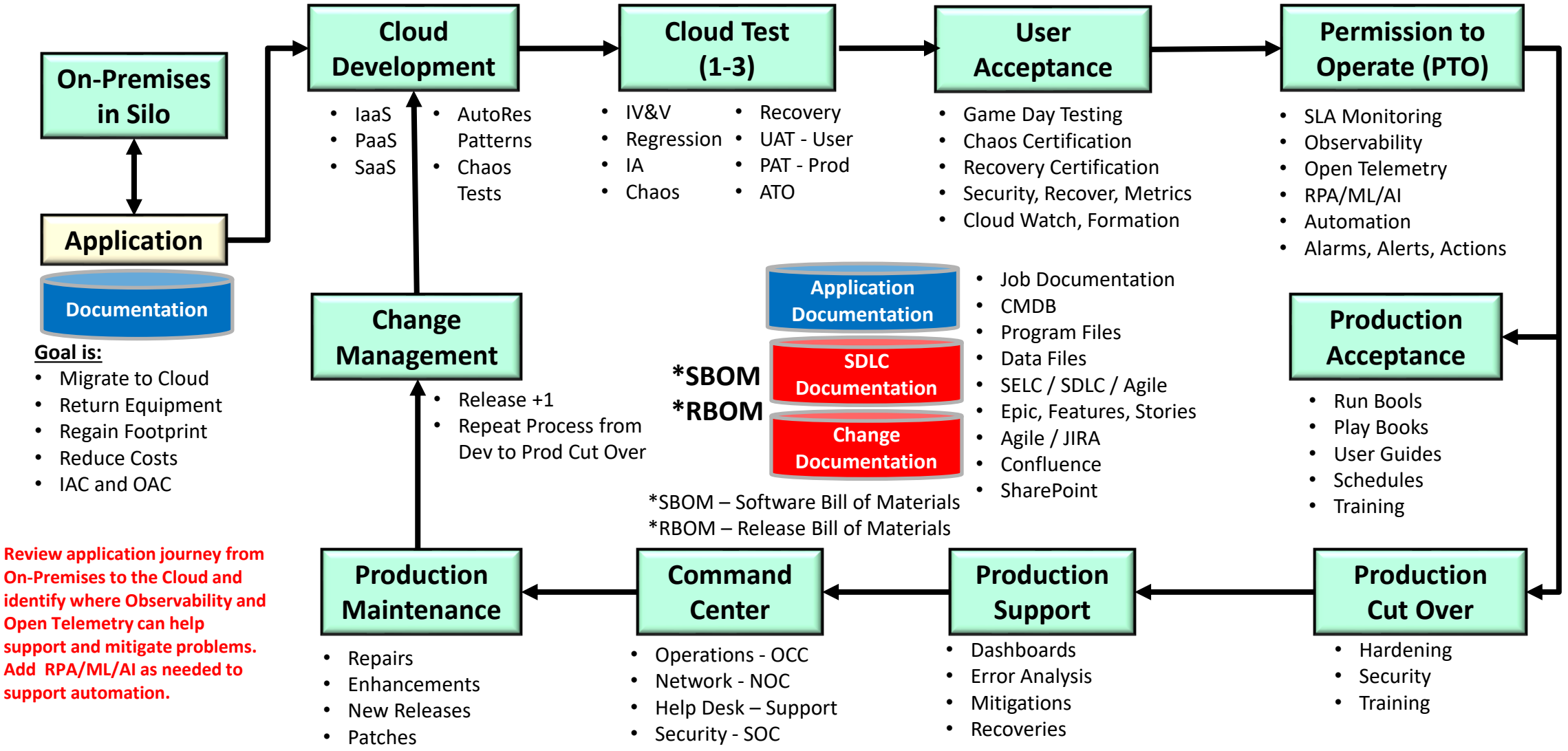
Change

Maintenance

Fix Problems, Update Releases, Enhancements

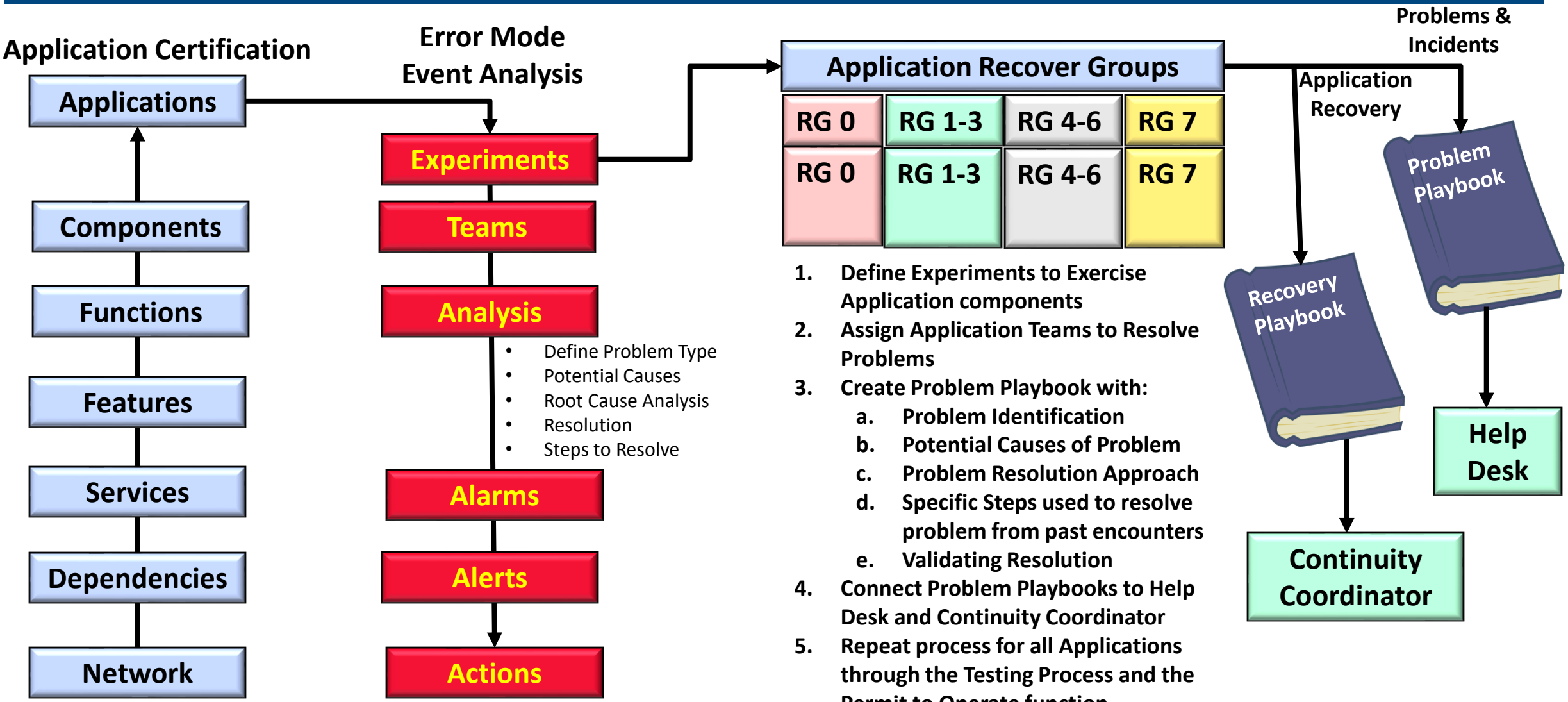
Migrating Applications to the Cloud

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



Chaos Testing process and results

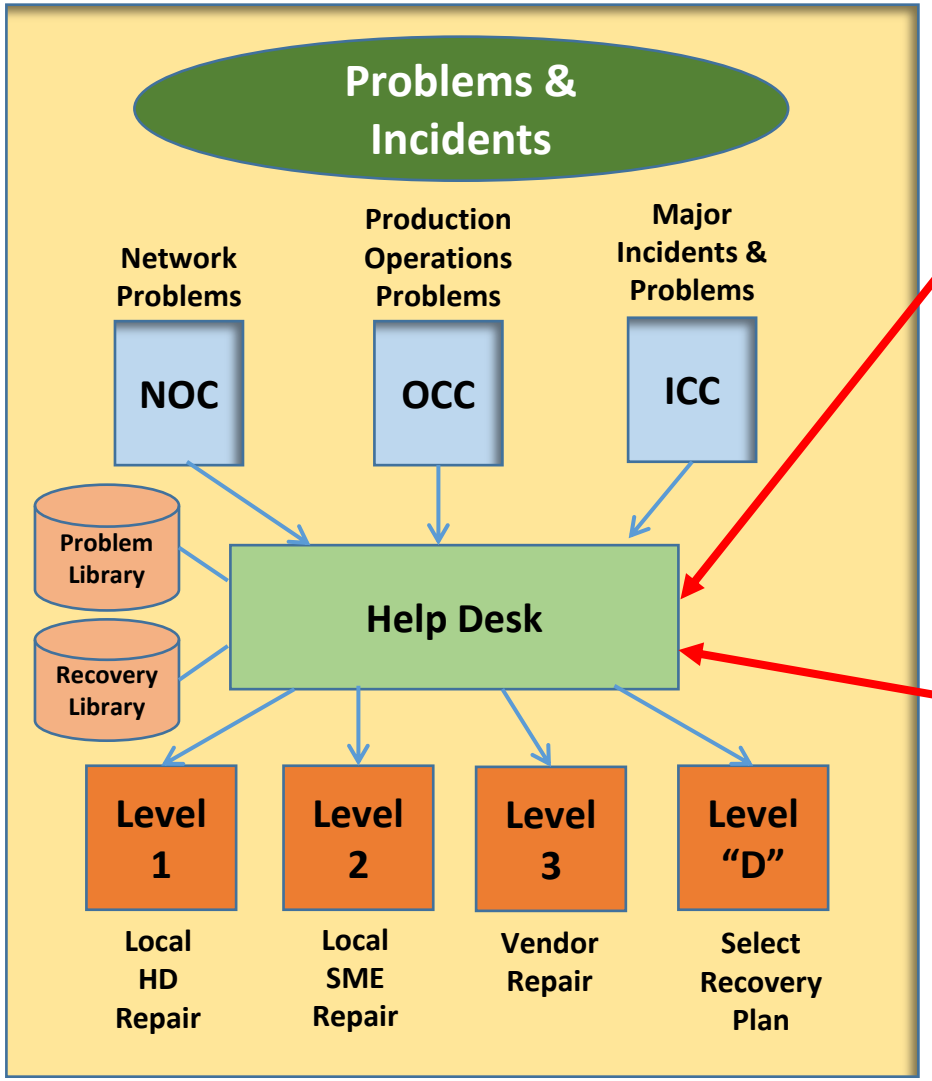
Thomas Bronack
Email: bronackt@dcag.com
Phone: (917) 673-6992



1. Define Experiments to Exercise Application components
2. Assign Application Teams to Resolve Problems
3. Create Problem Playbook with:
   a. Problem Identification
   b. Potential Causes of Problem
   c. Problem Resolution Approach
   d. Specific Steps used to resolve problem from past encounters
   e. Validating Resolution
4. Connect Problem Playbooks to Help Desk and Continuity Coordinator
5. Repeat process for all Applications through the Testing Process and the Permit to Operate function.

Activating and Coordinating Disaster Recovery Plans

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



Site Protection, Salvage, & Restoration

Contingency Command Center

Coordinate Recovery Teams

Notified by Help Desk of Recovery Need:

- Verify Problem and Match to Recovery Plan;
- Notify Contingency Plan Coordinator;
- Activate Plan and Perform Tasks;
- Operate at Contingency Site;
- Coordinate Production Site Protection, Salvage and Restoration;
- Return to Production Site; and,
- Continue Production Operations.

Emergency Operations Center

Coordinate Company Operations

Communicate Recovery Operations with:

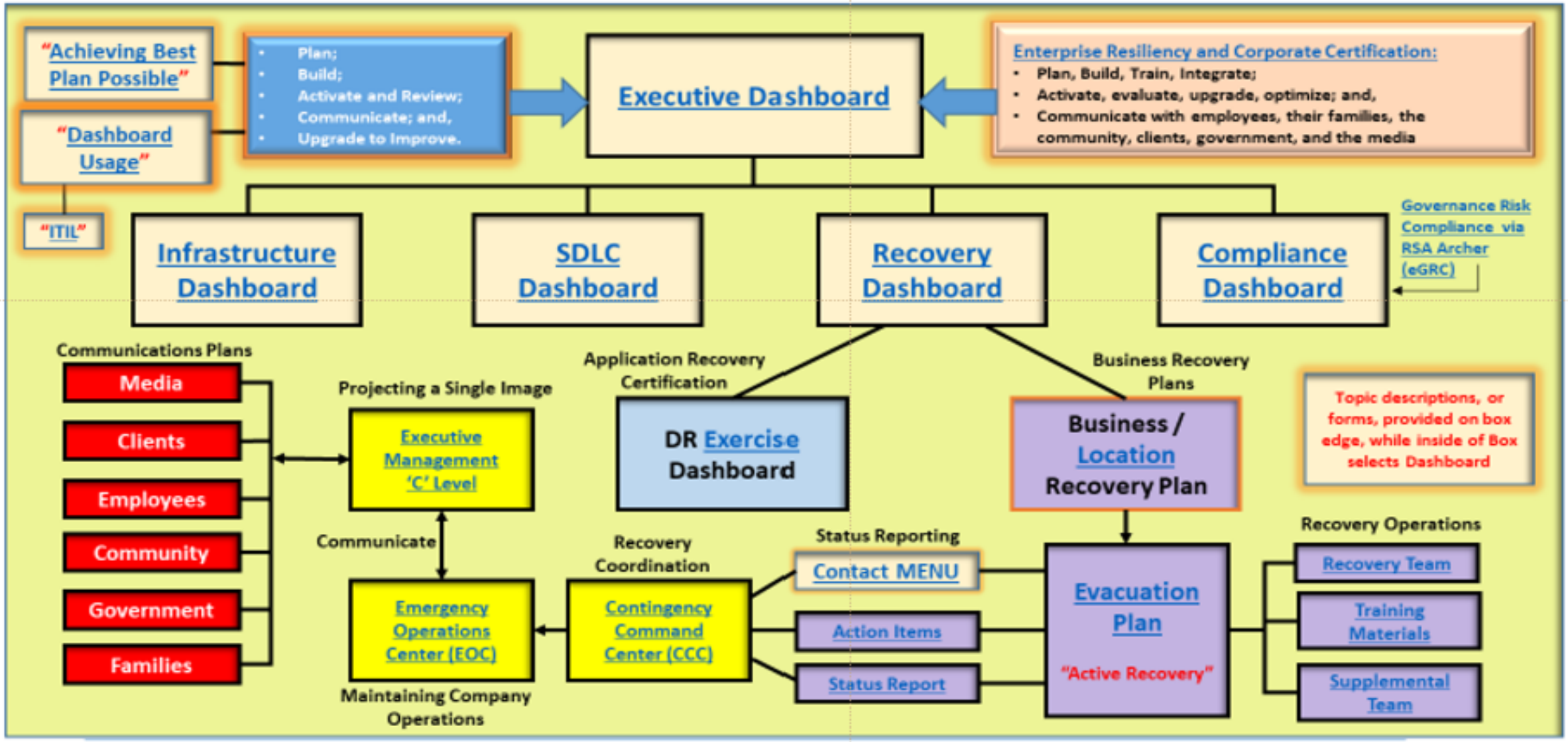
- Executive Management;
- Lines of Business, Personnel, Clients, Vendors, Supply Chain, and Workplaces;
- Command Centers;
- First Responders and Community Agencies;
- Companies close-by and the News.

Reporting Disaster Events:

- **Command Centers** May Recognize problems that can become disaster events (Operations, Network, Help Desk via User Reporting, Incident Control Center, etc.);
- **Contingency Command Center** (CCC) is notified and Recovery Operations starts;
- The **Emergency Operations Center** (EOC) responds to business interruptions in order to maintain the highest level of operations possible; and,
- EOC communicates to outside world with a **single voice**.

Dashboard System used for Enterprise Resilience

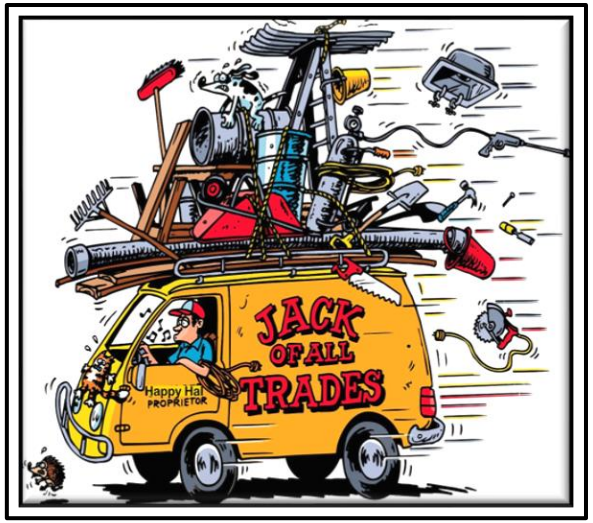
Thomas Bronack
Email: bronackt@dcag.com
Phone: (917) 673-6992



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