# Disaster Recovery & Business Continuity

10-Step Executive Framework for Government Agencies

Data Center Assistance Group, LLC (DCAG)

Project Initiation and Management

- Governance-backed program aligned with FISMA, COG (Continuity of Government), and COOP mandates.

- Executive charter signed by agency CIO or COO.

- Formation of a Steering Committee with CISO, COOP Manager, and key mission stakeholders.

- Program charter incorporates FISMA and COOP directives.

- Approved project plan with milestones, KPIs, and assigned resources.
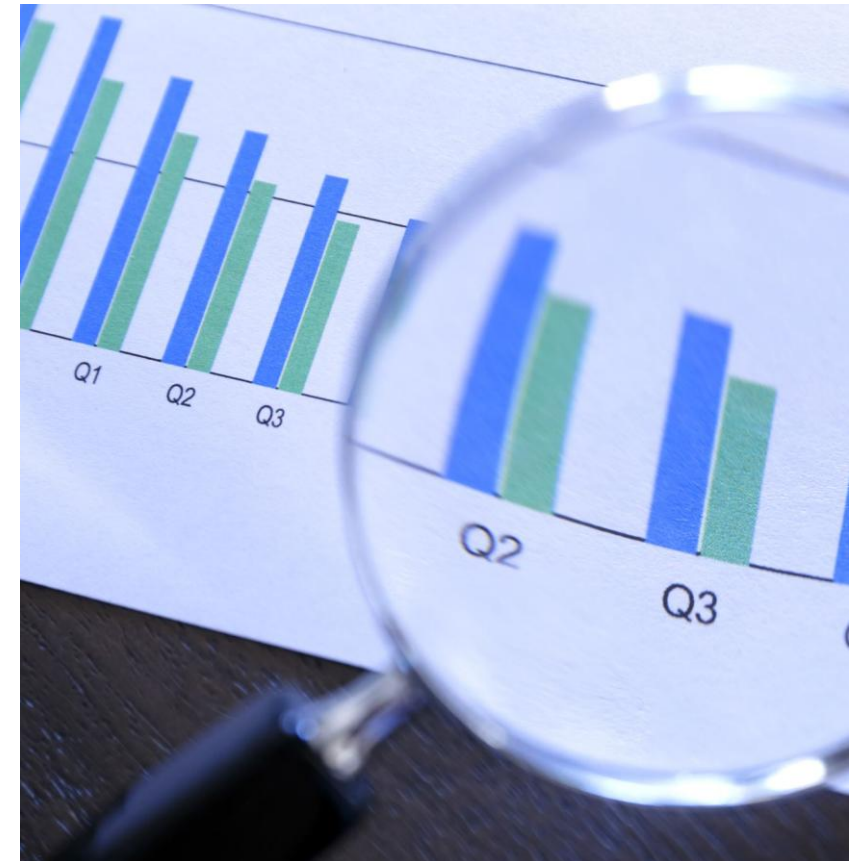
Risk Evaluation and Controls Improvement

- Risk Register per NIST 800-30 and ISO 31000 (Risk Management),
- Mission Essential Functions (MEFs),
- Risk Committee Reviews and Migration Updates,
- FISMA readiness via Audit Logs.

Business Impact Analysis (BIA)

MTPD (Maximum Tolerable Period of Disruption)

MEFs (Mission Essential Functions),

RTO (Recovery Time Objectives),

RPO (Recovery Point Objectives), and dependencies.

Developing Business Continuity Strategies

- Analyze COOP strategies and cost-aligned options.

- Develop cloud-based and alternate site options.

- Create component failure recovery procedures.

- Define Disaster Recovery Initiation Process.

- Evaluate costs vs. federal grant or budget alignment

Emergency Response and Operations Restoration

- Initiate Recovery Plans and exercise types and schedules.
- Activate Contingency Command Center (CCC).
- Activate Emergency Operations Center (EOC).
- coordinate with FEMA/DHS, validate backups.
- Verify continuation of services.

Designing and Implementing Continuity Plans

- **Document** functional plans, control access, maintain updates.

- **Integrate** within Application Development Lifecycle to ensure recovery plans work correctly prior to production acceptance.

- **Include** Recovery Runbooks with application turnover to production.

- **Manage** and protect recovery runbooks and related documentation.

- **Align** with Release Management process.
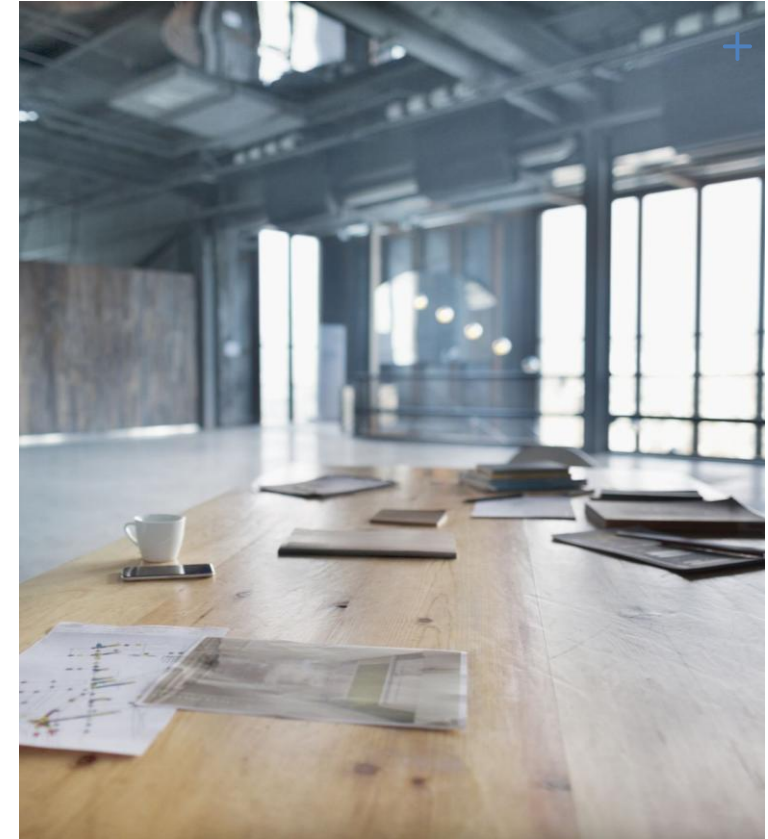
Awareness and Training

Business Continuity and Awareness training.

Role-based training, scenario drills, executive briefings.

Maintaining and Exercising Plans

- Simulations,
- AARs (Award Action Records), and
- FCD-1 (Federal Continuity Directive 1) compliance tracking.

Continuity Program Management Cycle

Public Relations and Crisis Communications

JIC ([Joint Information Center](#) I [Emergency Management Institute](#)) alignment,

Vetted communications,

FOIA preparation,

Single Management Voice from EOC or designated Public Relations coordinator..

Coordinating with Public Authorities

MOUs (Memorandum of Understanding),

Joint Exercises,

Multi-Agency Coordination,
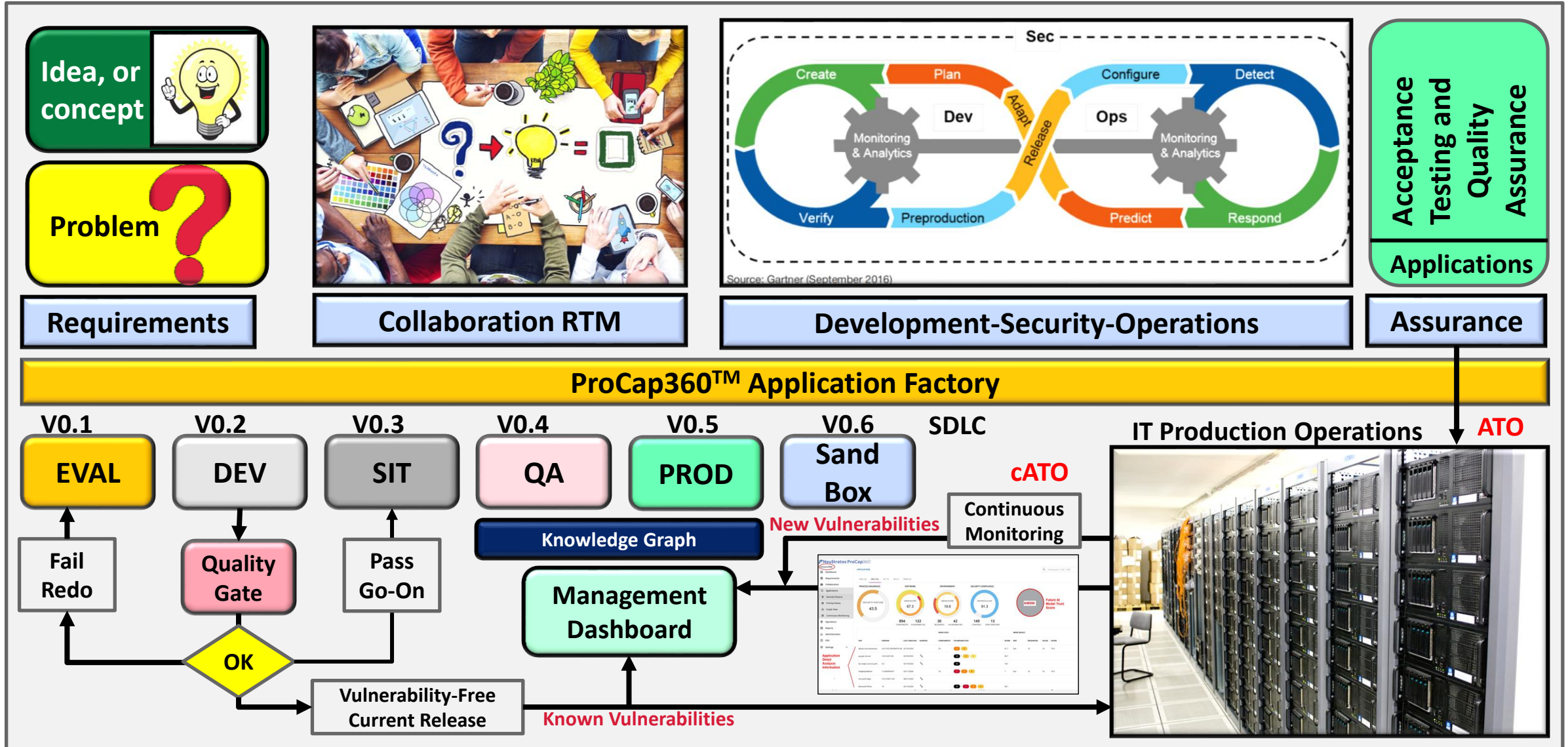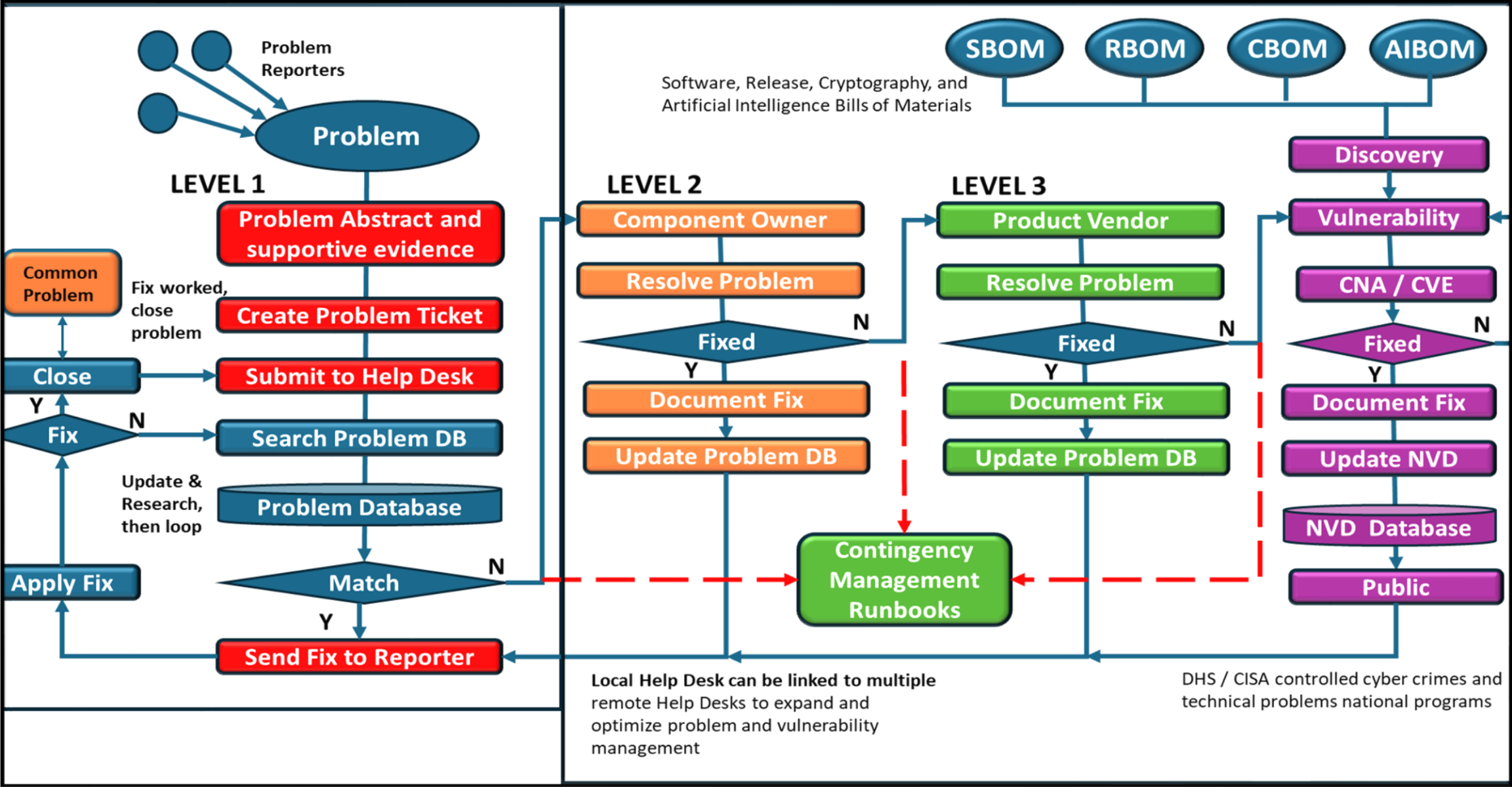
Emergency Responders,

Government Representatives/

Governance and Oversight

- **Oversight:** Steering Committee led by CIO with CISO, CFO, COOP, Legal, and Audit

- **Tools:** MS Project, Asana, ServiceNow ([FedRAMP](#)-authorized via NIST SP 800-37)

- **Reporting:** Weekly status, monthly dashboards, quarterly OMB briefs

- **Compliance:** Annual FISMA, NIST 800-34, COOP/FCD assessments

Application Factory, Vulnerability-Free Applications

Requirements

Collaboration RTM

Development-Security-Operations

Source: Gartner (September 2016)

Acceptance Testing and Quality Assurance — Applications

Assurance

ProCap360™ Application Factory

V0.1	V0.2	V0.3	V0.4	V0.5	V0.6	SDLC
EVAL	DEV	SIT	QA	PROD	Sand Box	

IT Production Operations ATO

cATO

Continuous Monitoring

Fail Redo

Quality Gate

Pass Go-On

Knowledge Graph

New Vulnerabilities

Management Dashboard

OK

Vulnerability-Free Current Release

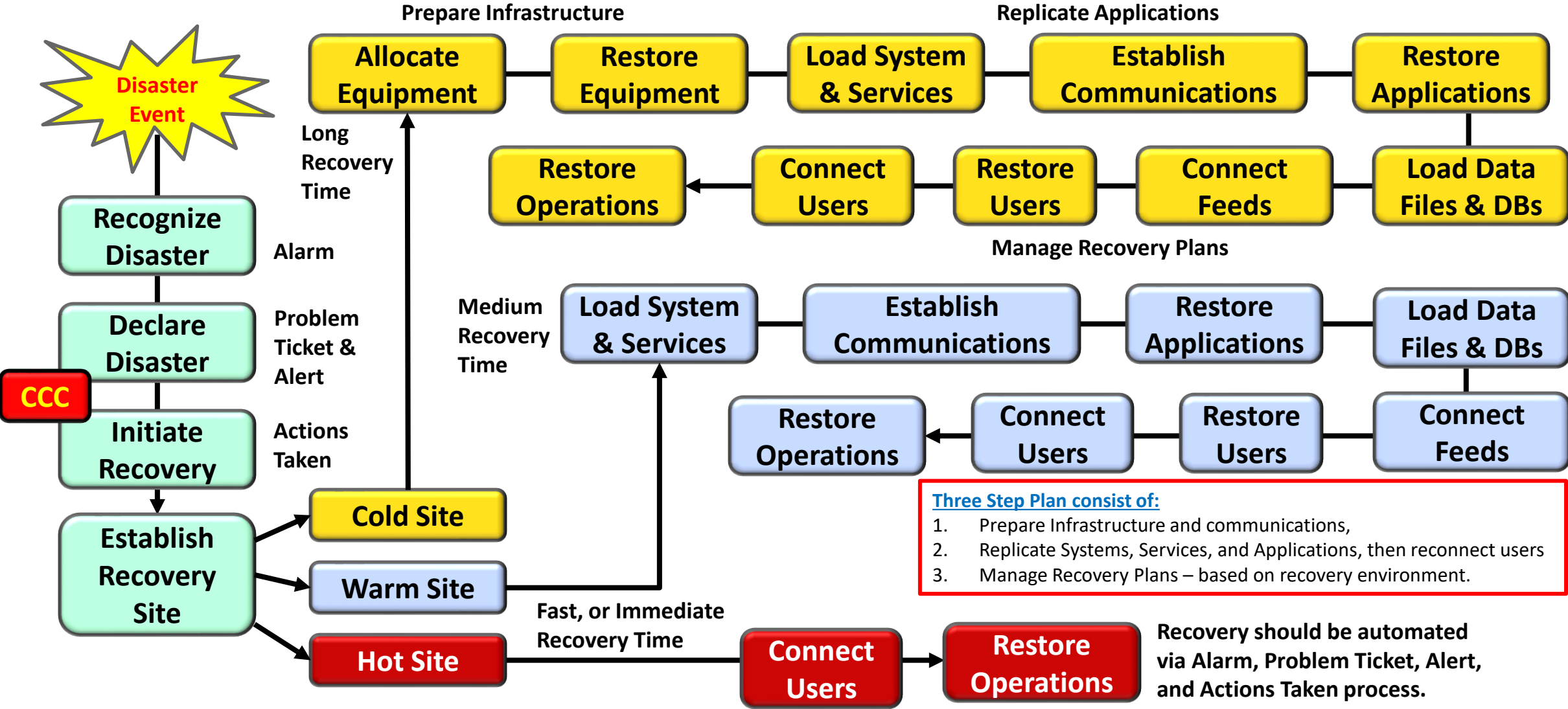Known Vulnerabilities

Incident and Problem Management flow with Contingency Management

Tracking Problems through a Dashboard
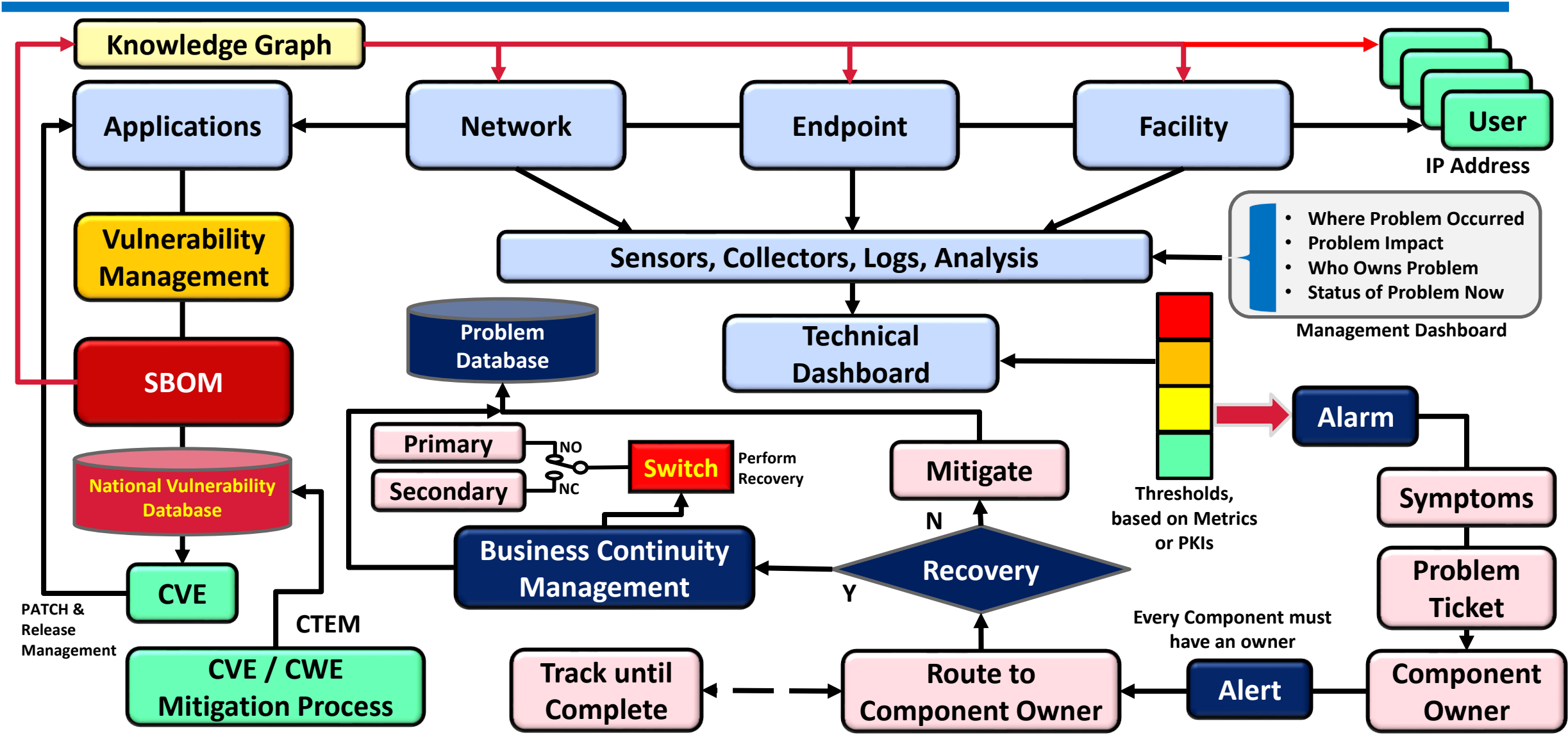
Sequence of Events to enact a Recovery Operation

Disaster Event

Prepare Infrastructure

Replicate Applications

Allocate Equipment — Restore Equipment — Load System & Services — Establish Communications — Restore Applications

Long Recovery Time

Restore Operations ← Connect Users — Restore Users — Connect Feeds — Load Data Files & DBs

Manage Recovery Plans

Recognize Disaster — Alarm

Declare Disaster — Problem Ticket & Alert

CCC

Initiate Recovery — Actions Taken

Medium Recovery Time

Load System & Services — Establish Communications — Restore Applications — Load Data Files & DBs

Restore Operations ← Connect Users — Restore Users — Connect Feeds

Establish Recovery Site

Cold Site

Warm Site

Hot Site

Fast, or Immediate Recovery Time

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.

Connect Users → Restore Operations

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

Contact Information

Thomas Bronack, President

Data Center Assistance Group, LLC

- bronackt@dcag.com
- bronackt@gmail.com
- (917) 673-6992
- www.dcag.com