Thomas Bronack, President
Data Center Assistance Group, LLC
bronackt@dcag.com | bronackt@gmail.com
(917) 673-6992
https://www.dcag.com

Incident and Problem Management

From Reactive Recovery to Proactive Resilience

1. Executive Summary

In today's threat landscape, speed and clarity are critical when responding to technology disruptions, cyber incidents, or recurring system failures. Data Center Assistance Group, LLC (DCAG) provides comprehensive Incident and Problem Management services designed to minimize downtime, improve root cause visibility, and streamline response and resolution processes. Our approach combines best practices from ITIL, DevSecOps, and Continuous Threat Exposure Management (CTEM) with automation, playbooks, and executive-level visibility—delivering faster recovery and greater operational assurance.
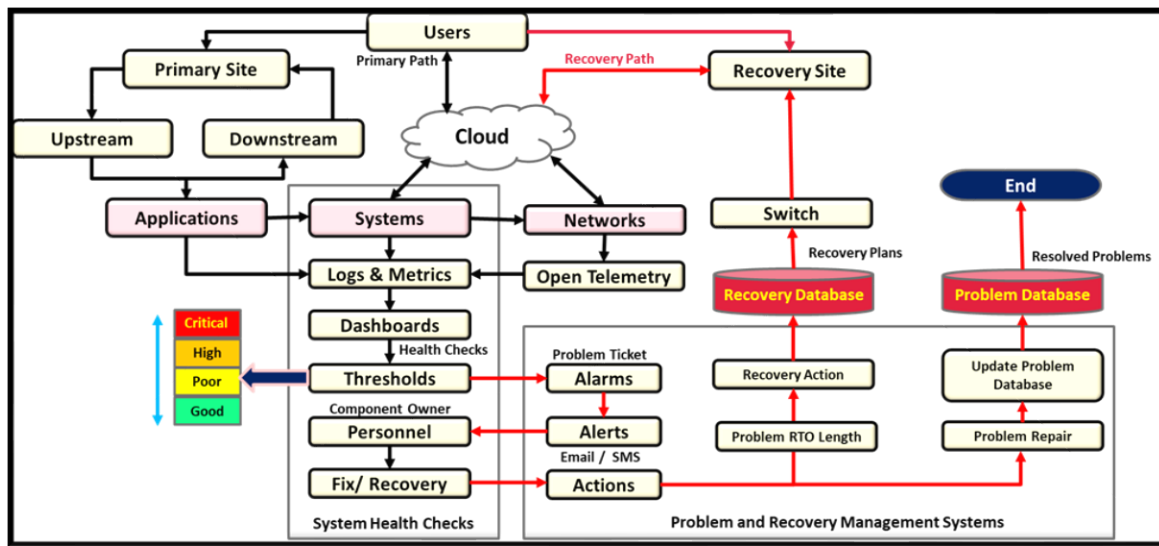

Figure 1: Incident and Problem Management Flow

2. Business Challenge

Organizations struggle with:
- Delayed or inconsistent incident response and root cause resolution
- Inadequate incident logging, escalation, and prioritization processes
- Gaps in post-incident reviews and remediation tracking
- Lack of integration between monitoring, alerting, and resolution workflows
- Disconnected communication across Dev, Sec, Ops, and Recovery teams.

3. Our Solution

DCAG offers Incident and Problem Management solutions tailored to the organizational environment and maturity. We align our services with ITIL, ISO, NIST, and CTEM

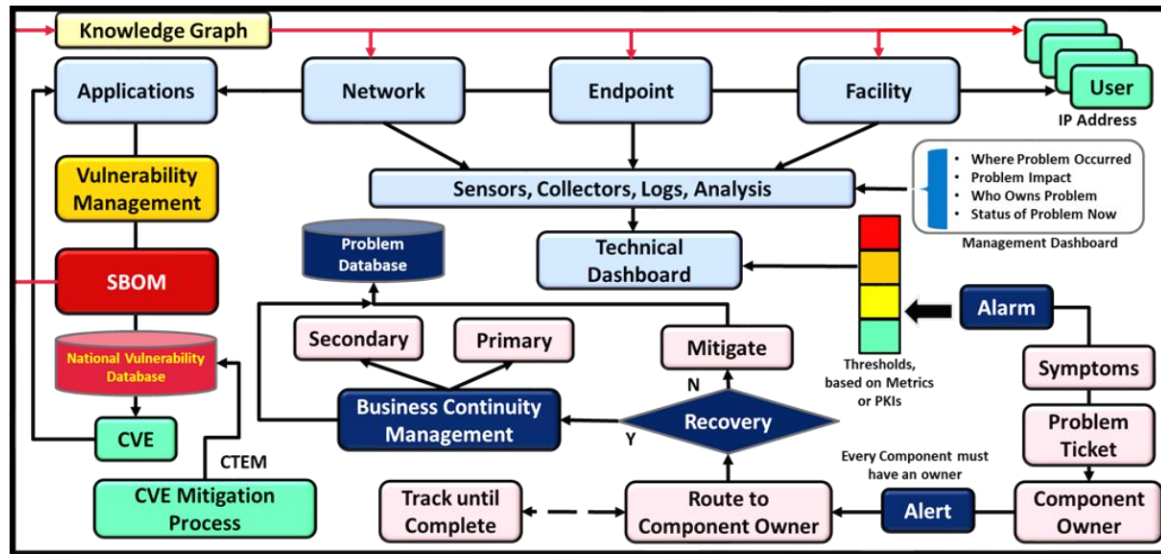practices—bringing structure, automation, and accountability to every phase of incident and problem response.

Figure 2: Tracking Problems and Incidents through a Dashboard

Some problems take longer to repair than others, but if a problem impacts a critical system, product, or service, planning to enact a recovery should be taken into consideration. If the time it takes to repair a problem is longer than the Recovery Time Objective (RTO), then a recovery should be enacted prior to the RTO time limit.

Services include:
- Incident lifecycle process definition, triage model development, and war room playbooks
- Automation of incident alerts and escalations tied to monitoring thresholds
- Root cause analysis, ticket linking, and resolution pathways
- Problem analysis aligned with recovery, change, and vulnerability management
- Post-incident reviews with mitigation tracking and executive summaries

4. Key Service Components
- ☑ ITIL-aligned Incident and Problem Management Frameworks
- ☑ Custom Incident Classification and Prioritization Models
- ☑ Root Cause Analysis Templates and Response Tracking
- ☑ Integration with Monitoring and SIEM Platforms (e.g., CloudWatch, XDR)
- ☑ Problem Management tied to Risk and Vulnerability Systems
- ☑ War Room and Recovery Playbooks for Major Incidents
- ☑ Post-Incident Reviews and Executive Reporting Dashboards
- ☑ Training and Simulation Workshops for Key Stakeholders

5. Outcomes & Business Value

Our Incident and Problem Management services deliver:

- Faster Incident Response Times
- Improved Root Cause Clarity
- Integrated Recovery and Remediation
- Operational Maturity
- Better Communication

6. Engagement Approach

Our offerings support tactical implementations and enterprise-wide maturity models:

Engagement Model	Description	Ideal For
Incident Readiness Assessment	Evaluate current practices and gaps across response lifecycle	New ITSM/IRM adopters or growing orgs
Response Playbook Development	Create documented SOPs, escalation maps, and resolution workflows	Teams with unclear or inconsistent handling
Full Lifecycle Implementation	Design and deploy integrated incident/problem programs	Large enterprises and regulated industries
Simulations and Reviews	Conduct drills, workshops, and postmortems to improve readiness	Cross-functional teams and stakeholders

7. Turn Incidents Into Insights

DCAG transforms reactive chaos into strategic control. Let us help you reduce time-to-resolve, prevent repeat incidents, and restore confidence across your enterprise.
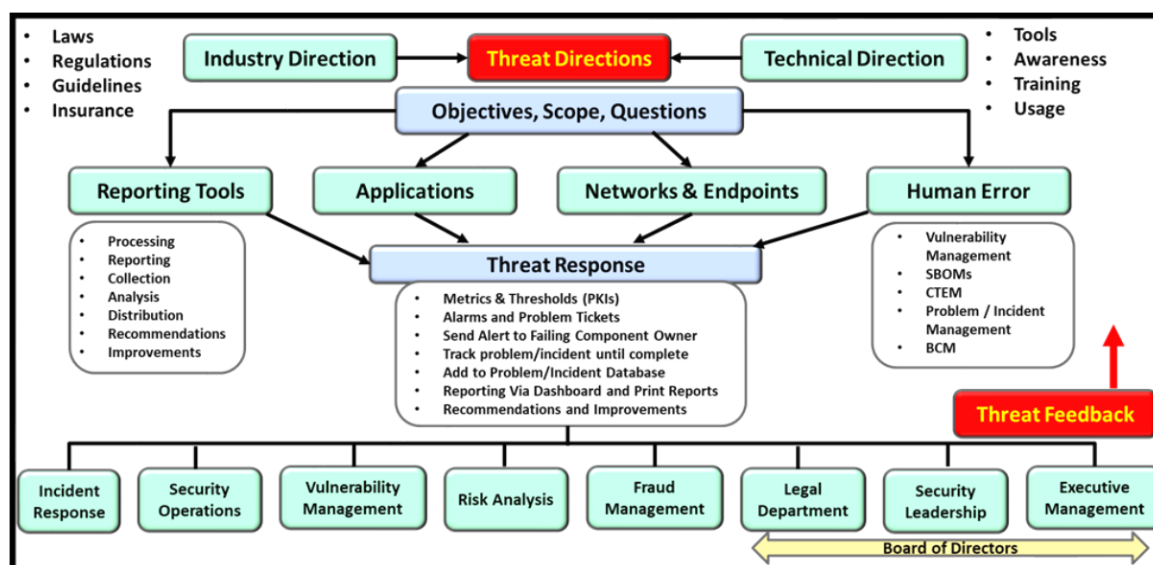
Figure 3: Addressing Threats

Be able to identify and react to encountered threats in the form of cyber incidents, technical problems, and interruptions to business operations.
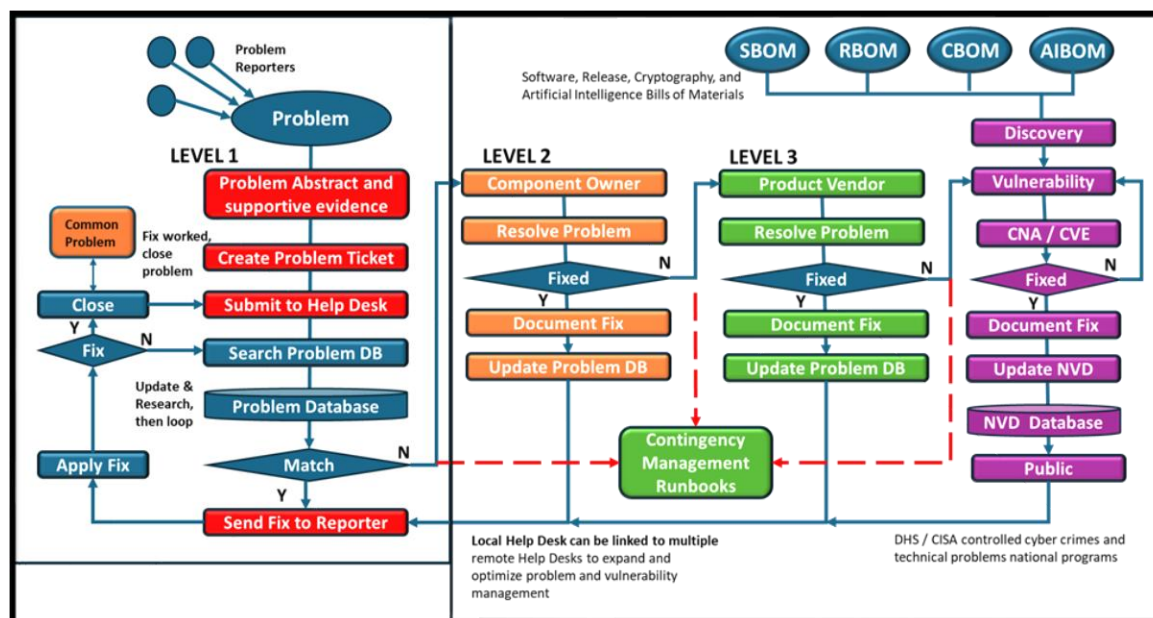

Figure 4: Integrated Problem and Vulnerability Management with BOMs (Bill of Materials)

Identify every component and its owner, in your environment, so that you can route component problems to them for a more rapid mitigation. Component Owners can be reporters (Level 1), subject matter experts (Level 2), or vendors (Level 3), so knowing who to report problems to is very important.
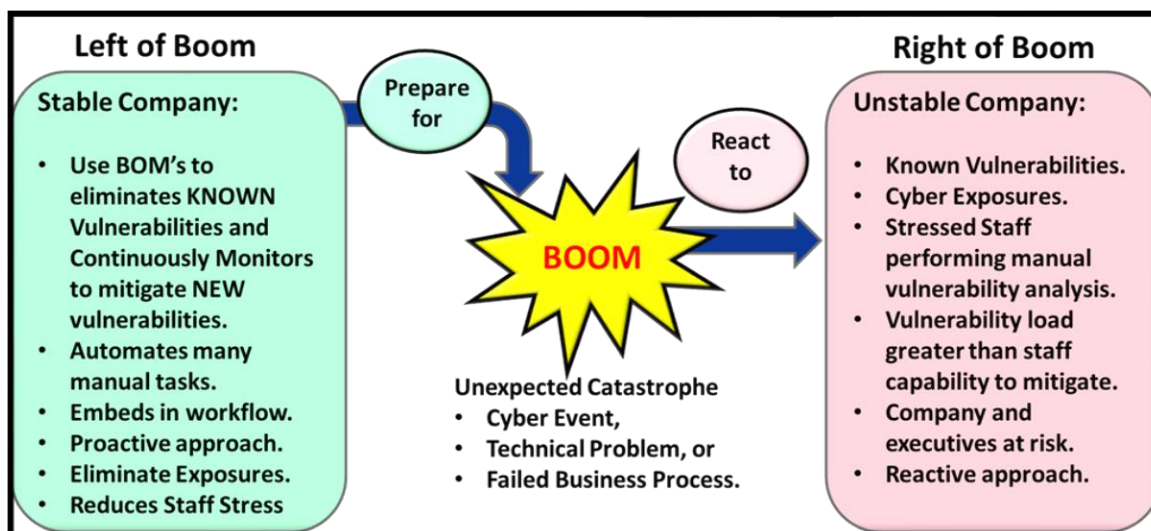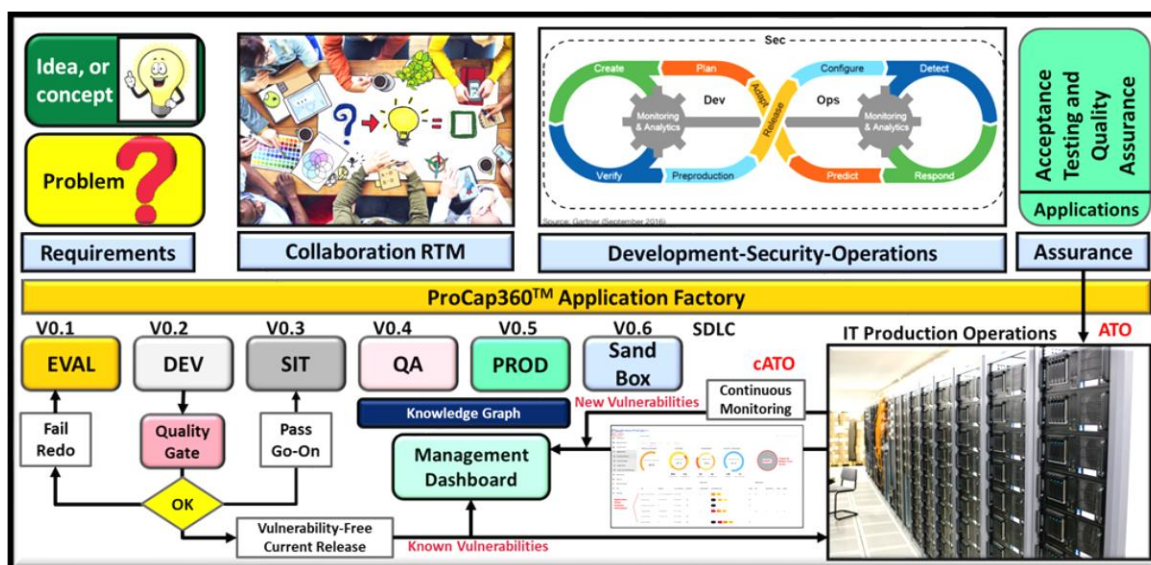
Figure 5: Left of Boom proactive preparation as opposed to reactive responses.

Left of Boom implies that you are planning recoveries or responses to problems that may occur before they happen, rather than being reactive and waiting for a problem to happen before performing a response.

Integrating an Application Factory concept with Control Gates to ensure application phases meet strict quality guidelines before being allowed to leave one phase of development and enter the next phase. This approach will put you on the path of achieving DevSecOps and guaranty that application components will be at current release levels and vulnerability free prior to entering the production environment.

From problem and incident management to an application factory will allow your organization to be more efficient and experience fewer problems, thereby freeing up your

staff to complete their job functions with less stress. We believe this is the future direction of IT Operations Management.

If you would like to discuss these concepts to see how they may help your organization, I can be reached via the contact information below. I look forward to assisting your organization achieve these results.

Contact:

Thomas Bronack, CBCP
Founder & Executive Consultant
✉ bronackt@gmail.com | bronackt@dcag.com | 📞 (917) 673-6992
Data Center Assistance Group, LLC
https://www.dcag.com