Data Center Assistance Group, LLC

Thomas Bronack, President

Website: https://www.dcag.com

Email: bronackt@dgamil.co | or bronackt@gmail.com

Phone: (917) 673-6992

Project Management Functional Responsibilities

Data Center Assistance Group, LLC

Table of Contents

Contents

Table of Figures

1. Introduction

This document outlines the key project management functions and services required to support the successful delivery of application projects from concept through to production deployment. The goal is to ensure all components are delivered at current release levels and free of known vulnerabilities. This includes Waterfall, Kanban, and Agile methodologies, aligning with best practices and drawing from proven experience in enterprise resilience, compliance, and vulnerability management.

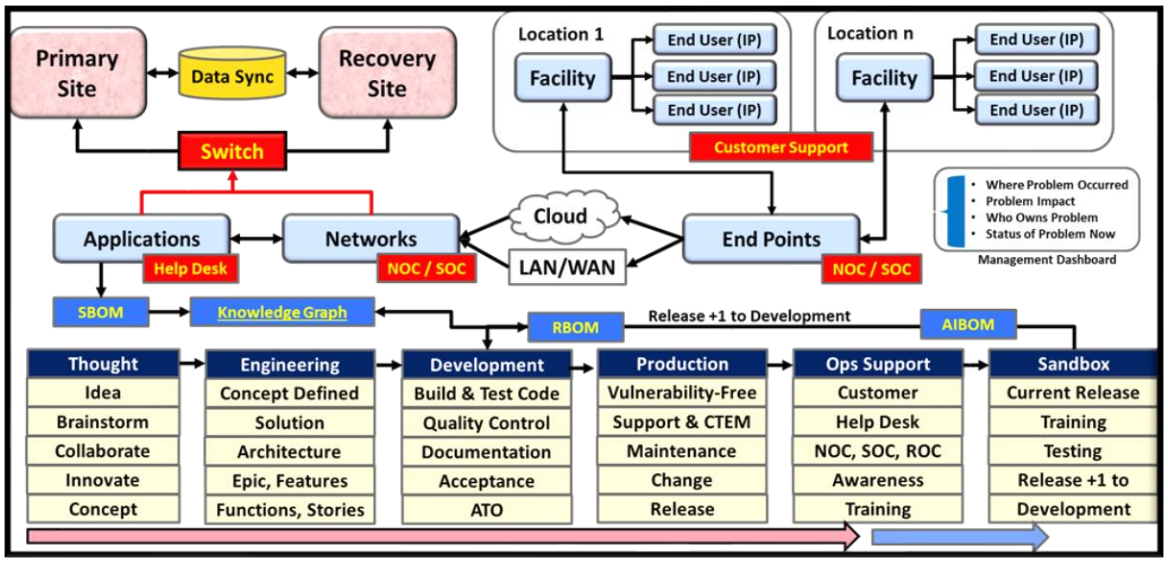

Figure 1: Complete Product / Service development cycle.

Complete Development Cycle and Environment Overview

The complete development cycle for new products, services, and applications includes:

1. **Thought:** From ideas, through brainstorming, collaboration, innovations, and concept finalization. The end goal of this phase is a Requirements Transparency Matrix (RTM) that can be separated into an Epic, Features, and Stories for Agile Development.
2. **Engineering:** Clarifies and defines the concept behind the new product, service, or application, provides solutions that can be architected into a cohesive system that fully defines the Agile Epic, Features, and Stories to be included in the new deployment. TOGAF and other System Architecture products can be used to guide this process in a formalized manner.
3. **Development:** Where the programming and development teams build the product, service, or application based on the defined RTM and Epic, Features, and Stories. Testing is conducted to ensure the correct operation of programs and systems and that they comply with security, vulnerability, risk, user and production acceptance, and audit guidelines and standards. The goal of this stage is to produce a quality product that is accepted by the stakeholders and receives Authorization to Operate (ATO) by production operations.

4. **Production:** Applications entering the production environment must have all their components at current release level and vulnerability free. Support of new deployments must adhere to continuous monitoring in accordance with Continuous Threat Exploit Management (CTEM), so that new threats can be quickly identified and mitigated before hackers can infiltrate your systems. Another recent goal associated with Production Acceptance is the need to incorporate Post-Quantum Cryptography (PQC) to protect data and sensitive information from being hacked.
5. **Ops Support:** Is responsible for supporting all production products, services, and applications by identifying, analyzing, and reporting technical threats and cybercrimes within a problem/incident management system and tracking issues until they are resolved and entered into the Problem Management Database so that they can be quickly recognized by help desk and technical staff during an initial problem analysis (most problems are repeats, so searches my resolve problems quickly).
6. **Sandbox:** Used for full system testing with test data and segregated from the current production environment. Sandbox environments can provide the ability to simulate/reproduce problems to ensure mitigations are accurate. Sandbox environments can be used for hands-on training for new products since they are a replica of the current production environment. Sandboxes can also exercise systems to practice recovery exercises.

Data Processing environment from application to users

1. **Pathway:** Applications support products and services, and they reside in computers, or servers. Users reside in endpoints within a remote Facility (location). Endpoints are connected to computers through Networks (LAN/WAN, Internet, etc.)
2. **Recovery:** A switch is used to transfer operations from a primary site to an alternate site should the entire primary system be disrupted (natural disasters, power outages, technical and cyber problem, etc.). Recovery can be instantaneous if two or more systems are running in parallel, with applications and data processing in sync. Should a transmitted message not be received within a period then a switch can be made to a secondary system and reinitiate the data transfer. If successful, then processing continues from the secondary system, and the outage is transparent to the user.
3. **Support Centers:** Customer support speaks to end users and customers and initiates associated functions related to the purpose of the call. Network Operations Centers (NOC) and Security Operations Centers (SOC) and responsible for monitoring and reacting to network and cyber incidents, and the Help Desk is responsible for accepting problems/incident (Level 1), logging then into the management system, adding problem abstract to the problem ticket, and routing the problem to the owner of the failing component. Problems are tracked and escalated to Subject Matter Experts (Level 2) and Vendors (Level 3) as needed until the issue is resolved, accepted by the reporter, and entered in the problem management database.

4. **BOMs and Knowledge Graphs:** Bill of Materials (Software, Hardware, Release, Cryptography, AI) provide lists of all components within a resource. In the case of SBOMs (Software Bill of Materials), all components are extracted and identified within a Knowledge Graph and programs are researched against public vulnerability management databases to identify existing vulnerabilities (CVE/CWE) and their update path (Patch or New Release). All vulnerabilities must be resolved prior to production acceptance, and continuous monitoring will identify new vulnerabilities that must be quickly resolved to stay ahead of hackers.

2. Functional Responsibilities – Waterfall

The Waterfall model, as a sequential design process, is ideal for well-defined projects with clear requirements. Below are the core project management functions under this methodology:

- **Requirements Gathering:** Collaborate with stakeholders to define comprehensive business and technical requirements.
- **Scope Definition and Business Case:** Document scope, create Work Breakdown Structures (WBS), and develop cost-benefit analysis.
- **Planning and Scheduling:** Build detailed Gantt charts with milestone tracking, dependencies, and critical path analysis.
- **Resource Management:** Allocate technical and functional team members aligned to project phases.
- **Provide Awareness and Training:** Ensure project staff understands work to be done, and the tools and procedures needed to accomplish project goals.
- **Risk and Issue Tracking:** Log, assess, and mitigate project risks and issues using a centralized dashboard.
- **Vulnerability Management:** Ensure all application components are at current release levels and free of known vulnerabilities.
- **Change Control Management:** Establish formal processes to evaluate, approve, and document scope changes.
- **Quality Assurance and Testing:** Plan for unit, integration, system, and user acceptance testing (UAT).
- **Deployment and Transition to Operations:** Coordinate cutover planning, operational readiness, and early life support (ELS).
- **Post-Implementation Review:** Conduct lessons learned sessions and document findings for continuous improvement.
- **Continuous Improvements:** Implement recommendations for improvement obtained through the Post-Implementation Review that have been accepted by technical and executive management. Continuously repeat this process until improvements can no longer be found (excellence through evolution).

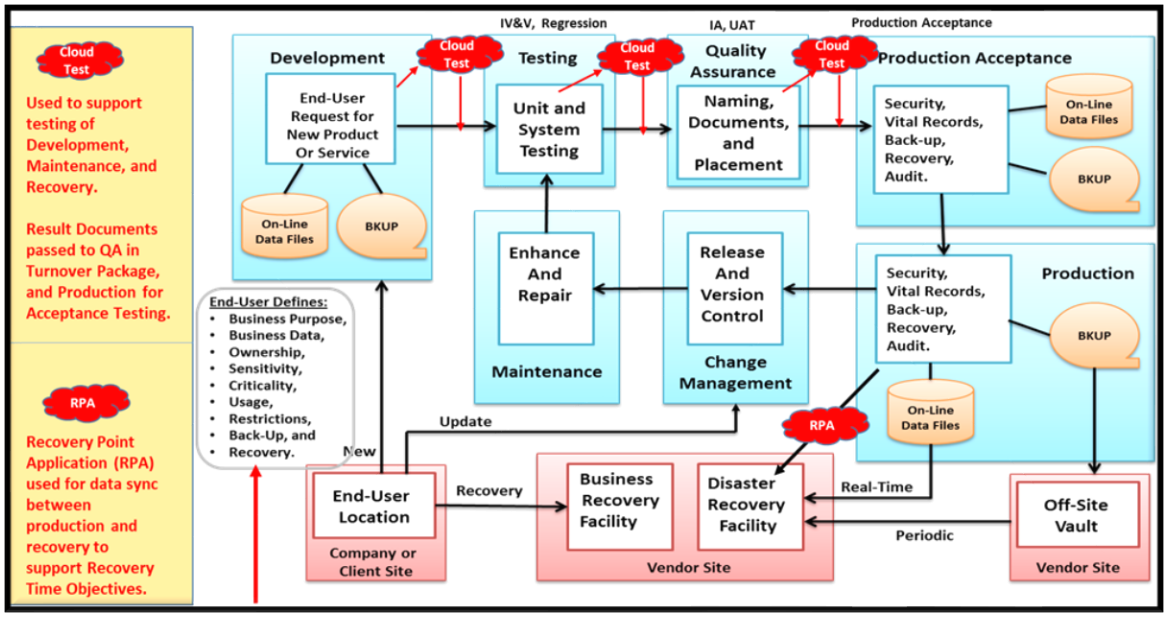

Figure 2: Waterfall Systems Development Lifecycle

Agile Overview for Executives

Agile is a modern approach to software and systems development designed for **speed, adaptability, and customer-focused outcomes**. Rather than long, rigid project plans (often called "Waterfall"), Agile uses **iterative cycles**, typically 2–4 weeks long, called **Sprints**. Each Sprint delivers a small but complete part of the product, allowing for rapid feedback, course correction, and continuous improvement.

Why Agile Matters to Executives:

- **Speed to Value:** Prioritizes delivering business-critical capabilities first.
- **Reduced Risk:** Frequent releases allow earlier detection of problems.
- **Customer Alignment:** Frequent reviews ensure you are building the right product.
- **Team Productivity:** Agile empowers teams to self-manage and continuously improve.

Agile Hierarchy Explained: Epics, Features, and Stories

To manage complexity, Agile breaks work down into layers. Here is how it works—using an **analogy for building a new corporate headquarters**:

1. Epic – The Vision / The Building

- **What it is:** A large business goal or major initiative.
- **Analogy:** "Build a new corporate headquarters."
- **In Agile:** Epics are too big to complete in a single Sprint and are broken into Features.

2. Feature – Major Sections / The Floors

- **What it is:** A meaningful chunk of functionality that delivers value to the business or customer.
- **Analogy:** "Construct the executive floor" or "Build the data center."
- **In Agile:** Each Feature is a tangible output that supports the Epic and consists of smaller, deliverable Stories.

3. Story – Detailed Tasks / The Rooms & Fixtures

- **What it is:** A small, user-focused requirement or task that can be completed in a Sprint.
- **Analogy:** "Install secure Wi-Fi in executive offices" or "Deploy biometric access in data center."
- **In Agile:** Stories are written from a user's perspective (e.g., "As a CIO, I want to receive a real-time dashboard so I can monitor application uptime").

How They Work Together:

You **start with a vision** (Epic), **break it down into large deliverables** (Features), and then **specify exactly what needs to be built** (Stories). Teams implement and deliver incrementally in **Sprints**, continually adjusting based on feedback and business needs.

Agile Roles (Who Does What)

1. Product Owner (PO)

- **Represents the customer/business.**
- Defining priorities and ensuring the team is building the right thing.
- Owns the **Product Backlog**

2. Scrum Master / Agile Facilitator

- Ensures the team follows Agile principles.
- Remove blockers and facilitate communication.
- Coaches the team on continuous improvement

3. Development Team

- Cross-functional (includes developers, testers, designers)
- Self-organizing, delivers potentially shippable products at the end of each Sprint.

4. Stakeholders / Business Executives

- Provide feedback during reviews.
- Prioritizing business goals
- Ensure alignment between Agile outputs and strategic objectives.

Executive Takeaway

Agile is not just a development methodology—it is a **business strategy enabler**. It allows your organization to pivot faster, deliver value sooner, and align better with customer expectations.

Instead of waiting 6–12 months to see results, Agile allows **tangible outcomes in weeks**, ensuring you are investing in **what works**—not just what was planned a year ago.

3. Functional Responsibilities – Agile

Agile project management supports iterative and incremental development, ideal for evolving requirements. Key responsibilities in an Agile context include:

- **Product Backlog Grooming:** Partner with Product Owner to prioritize Epics, Features, and User Stories.
- **Sprint Planning:** Facilitate estimation and task allocation sessions (Scrum Poker, Planning Boards).
- **Daily Standups:** Monitor progress, identify blockers, and keep momentum through servant leadership.
- **Sprint Reviews and Retrospectives:** Capture feedback, track team speed, and incorporate improvements.
- **Agile Metrics and Dashboards:** Use Burndown charts, Cumulative Flow Diagrams, and Velocity tracking tools.
- **DevSecOps Coordination:** Align with CI/CD pipelines, vulnerability scanning, and automated testing teams.
- **Documentation and Knowledge Transfer:** Maintain Confluence, SharePoint, and Wiki-based repositories.

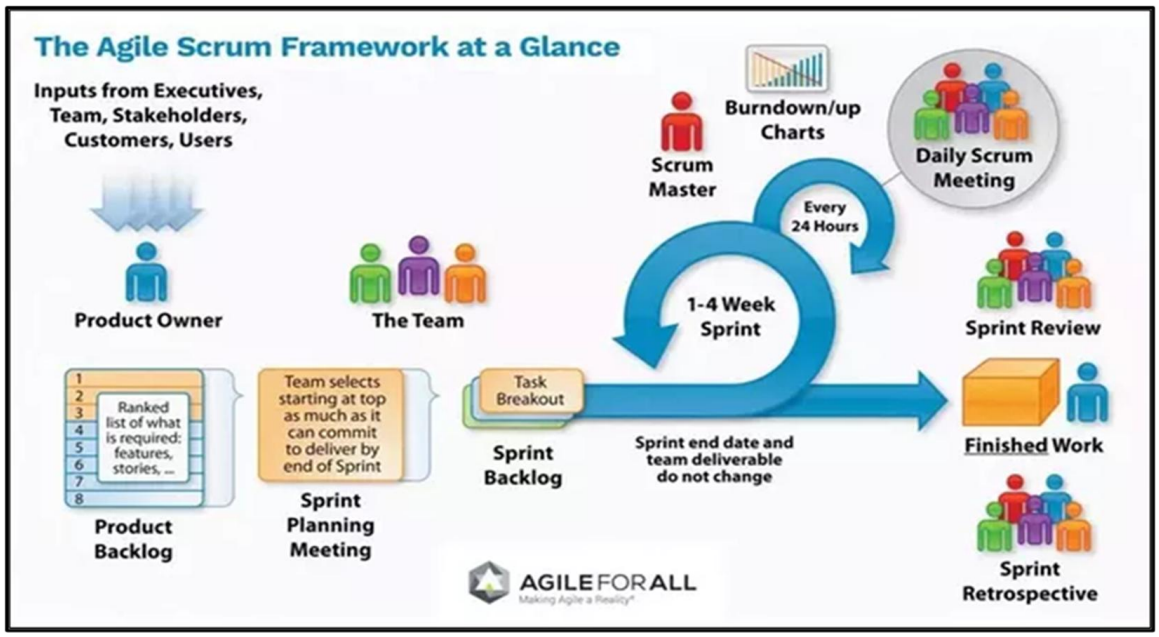

Figure 3: Agile Project Management Overview (using Kanban format)

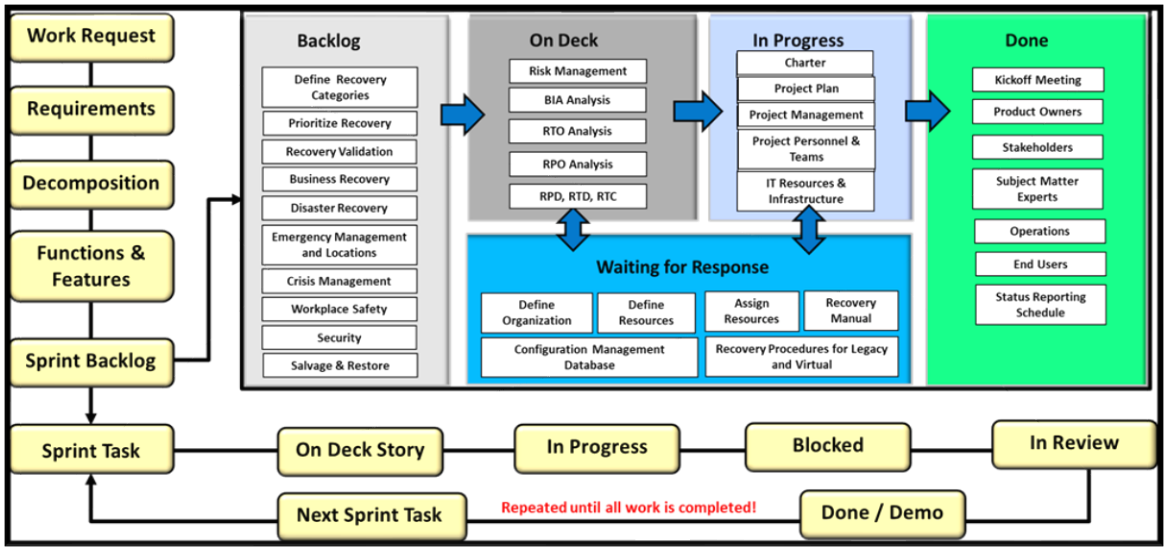

Figure 4: Utilizing the Kankan method to define tasks and their status.

4. Governance and Oversight

Effective governance ensures projects remain aligned with strategic goals, budget, and compliance requirements.

Key responsibilities include building the Project Charter, Project Plan, and maintaining executive communications via Steering Committee and PMO dashboards, issue logs, change requests, and progress status reporting, with Action Items identified, defined, and assigned

with completion dates. Governance provides audit traceability, risk controls, and a foundation for project success.

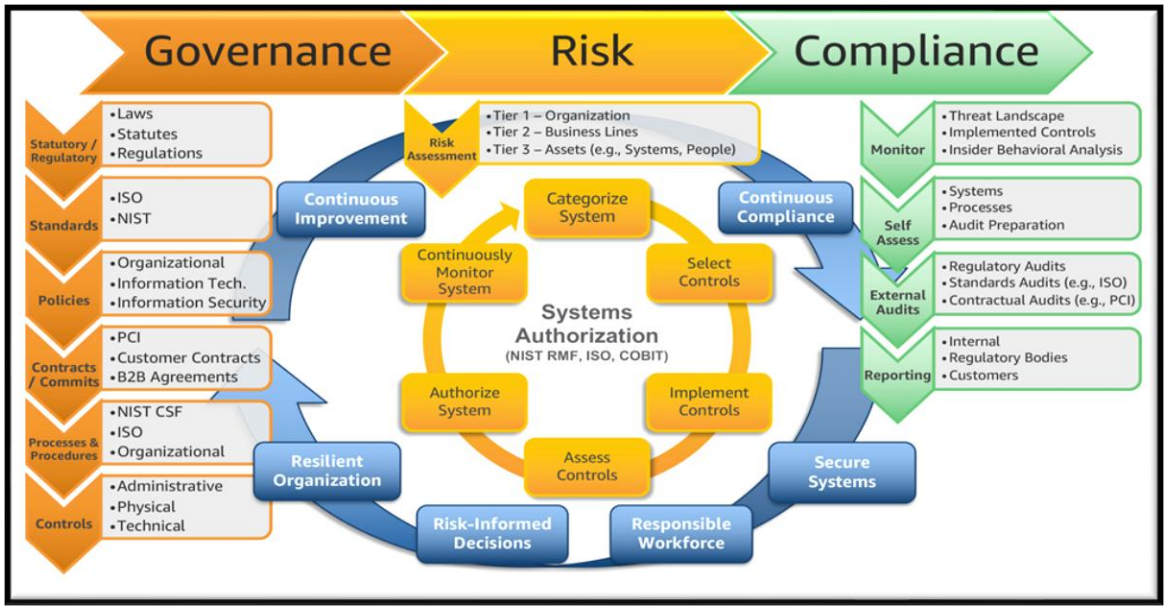

Figure 5: Overview of GRC - Governance, Risk, and Compliance process.

Ensure Governance, Risk, and Compliance is maintained throughout the project and all its phases. Provide Awareness and Training to staff to educate them on how to identify deviations from GRC requirements so that all delivered projects comply with company regulatory guidelines.

Conduct an Audit of compliance requirements if necessary to ensure compliance.

Application Auditing

Follow these guidelines to ensure applications are deployed in accordance with best practices and audit principles.

1. **Audit Universe:** Definition of all domestic and international laws and regulations that the organization must adhere to.
2. **Crosswalk:** Combining similar actions into a single audit question with required supporting artefacts necessary to comply with regulators.
3. **Audit Script:** The list of areas and questions that an auditor must ask when conducting an audit.
4. **Audit Schedule:** The schedule associated with the type of audit (i.e., monthly, quarterly, yearly, etc.).
5. **Audit Results:** Audit results are reported to management and audit regulators as deemed necessary and within the desired format.

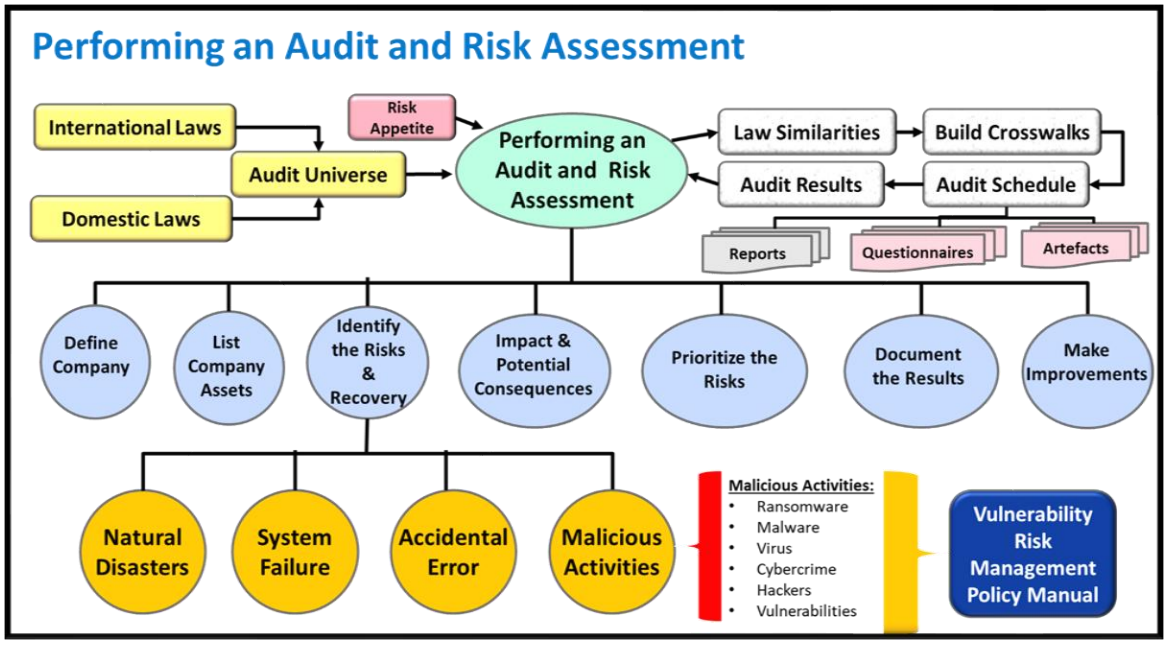

Figure 6: Performing an Audit and Publishing Results

Risk Controls Self-Assessment (RCSA)

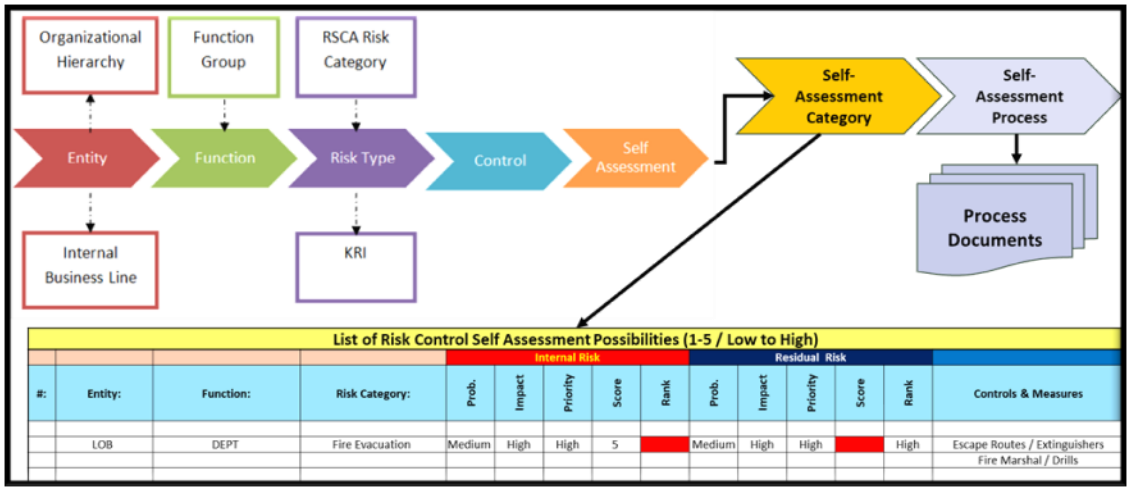

Figure 7: Risk Controls Self-Assessment (RCSA) process.

Each department within a Line of Business will continuously rate and validate established compliance controls to ensure proper protection, raising and incorporating new controls as needed. This process puts audit assistance nearest to the functional area responsible for ensuring controls are proper and in place as needed to protect continuity of business products and services.

Cybersecurity Framework 2.0

1. Provide comprehensive security protection, with Runbooks for Incident & Problem management, Recovery Operations, and Operations personnel.

Figure 8: The three pillars of Governance, Risk, and Compliance

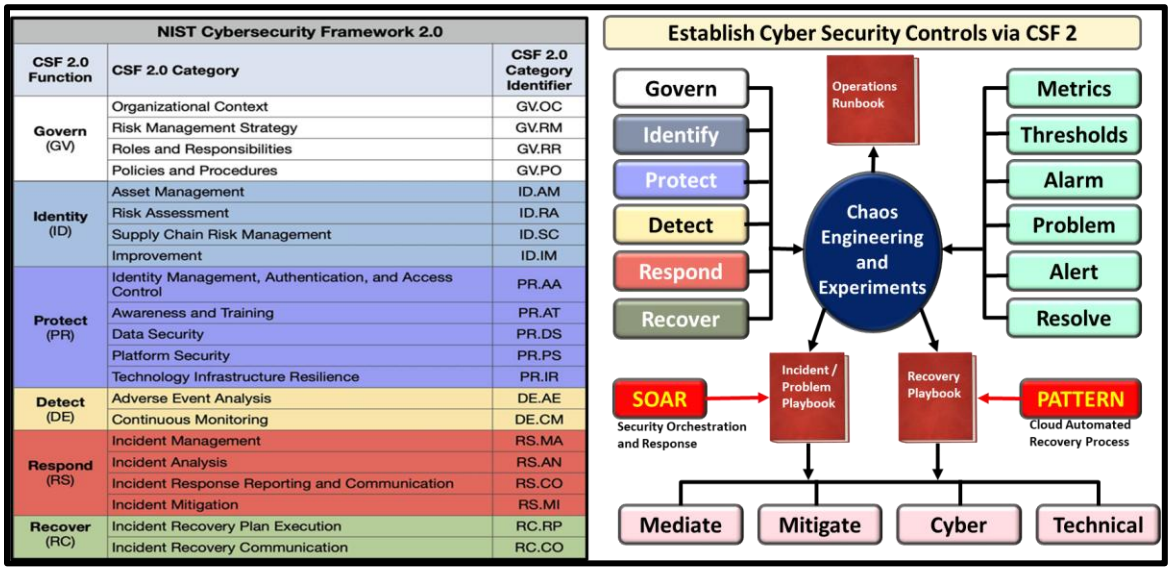

Figure 9: Cyber Security Framework 2.0 and GRC for Applications

Data Sensitivity and Security

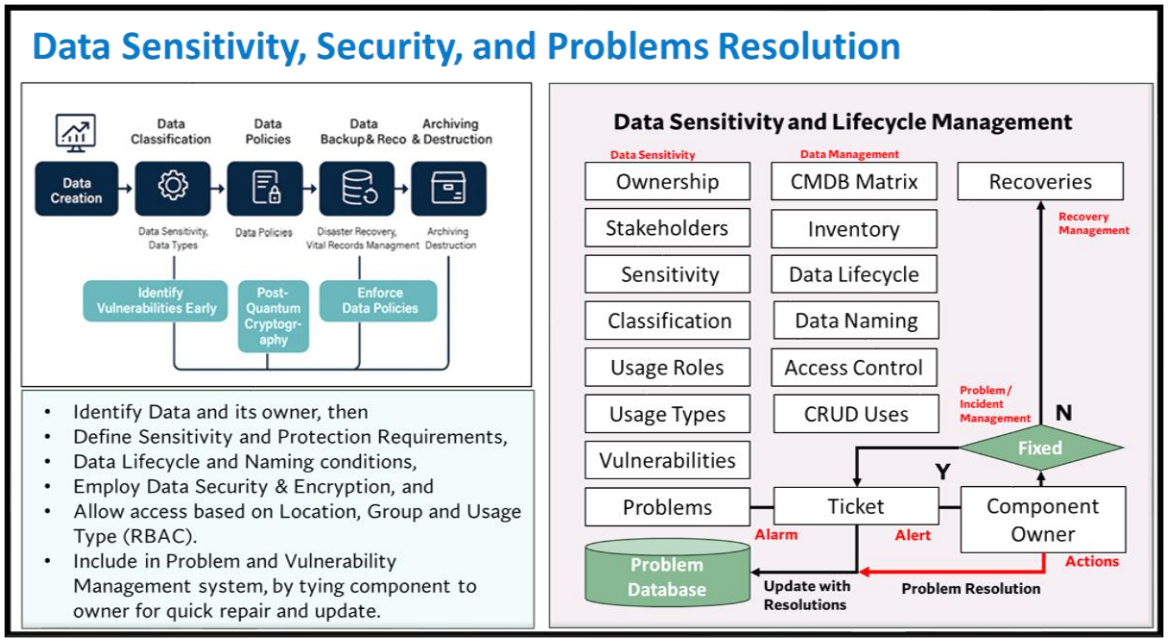

Figure 10: Data Sensitivity, Security, and Problem Management

Ensure Data Sensitivity is performed to properly enact data naming and lifecycle requirements. Also be sure to identify component owners to best know how to route problems.

Identity and Access Management

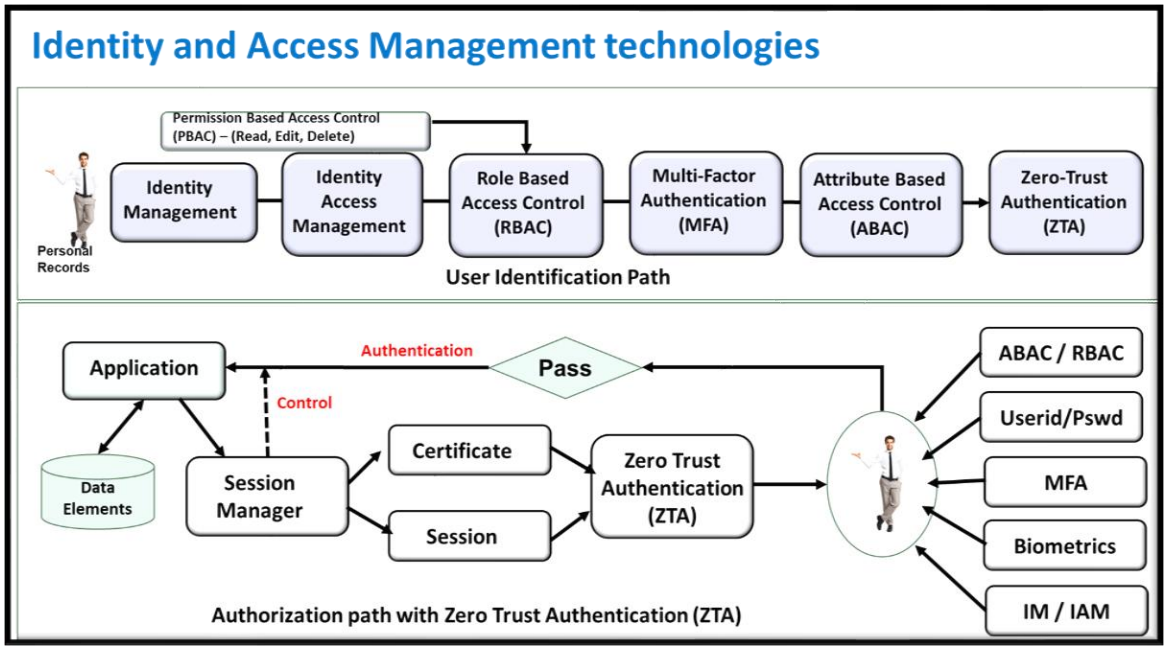

Figure 11: Identity and Access Management Techniques

Once data is defined, then you can establish data access rules that best protect your data in adherence to company data protection guidelines. Utilize Post-Quantum Cryptography (PQC) to protect data going forward because Quantum Computers can defeat today's encryption techniques. Migrate to PQC as soon as possible to protect current critical data from being Harvested Now and Decrypted Later (HNDL) by hackers. Once that data is stolen, it is lost forever and there is no way to get the data back from hackers.

5. Application Quality and Security Assurance

A critical project management function is ensuring the delivered solution is free of known vulnerabilities and supports compliance mandates (e.g., EO 14028, NIST 800-171, SEC Rule 2023-139). Practices include:

- Integrating security testing tools (SAST, DAST, IAST, RASP) into CI/CD pipelines.
- Maintaining SBOM/RBOM compliance with automated discovery and VEX reporting.
- Leveraging CTEM (Continuous Threat Exposure Management) dashboards to track exposure.
- Facilitating secure code reviews and vulnerability remediation with DevSecOps teams.

DevSecOps Environment

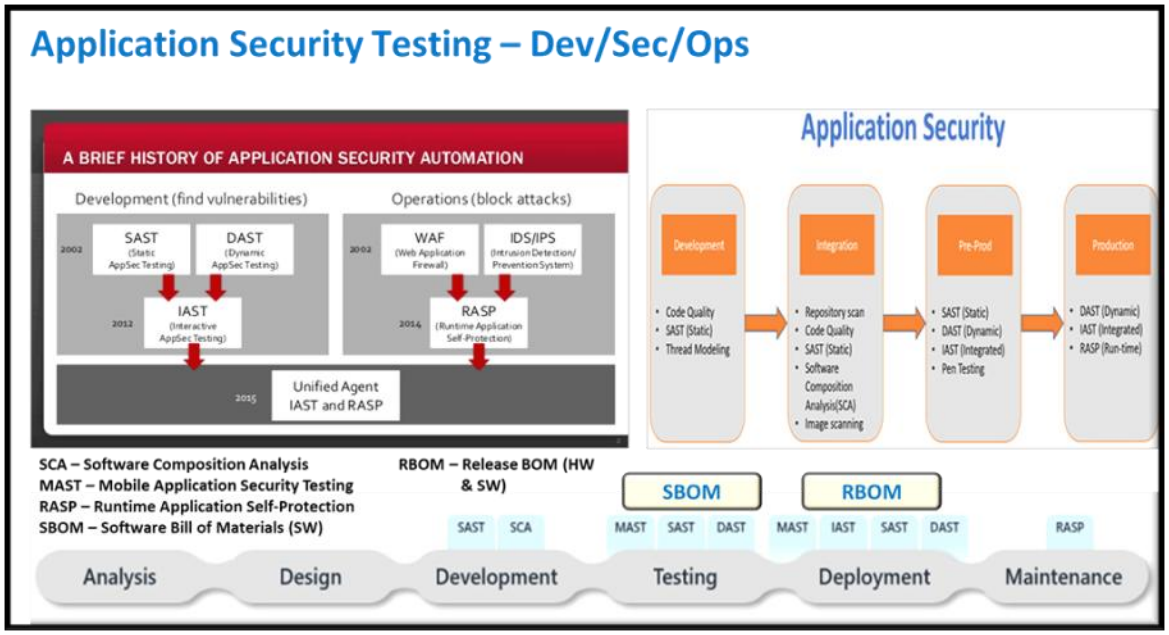

Figure 12: DevSecOps concept and the steps associated with program validation.

Validating application programs throughout the development cycle will reduce security exposures and development times, resulting in more reliable applications at a reduced cost.

Full Development and Testing for SaaS Applications

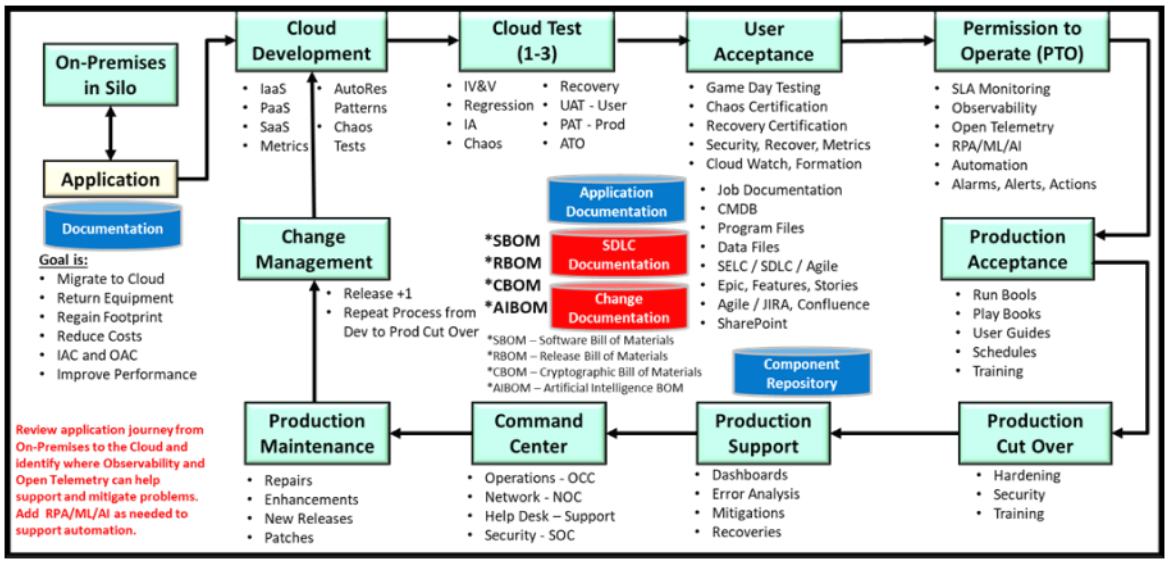

Figure 13: Application Quality through testing and Lifecycle events.

The steps shown in the above illustration will provide you with an in-depth understanding of the process of building, testing, and deploying and application. It further shows how

applications are supported and maintained. Use these steps to help define the actions needed to safeguard applications and to ensure delivery of quality products where all components are at current release levels and free of known vulnerabilities. Utilize Continuous Monitoring to detect any new threats that may arise, so that you can quickly respond to these threats and maintain a consistent supply of business products and services to your clients.

Threat Assessment Process

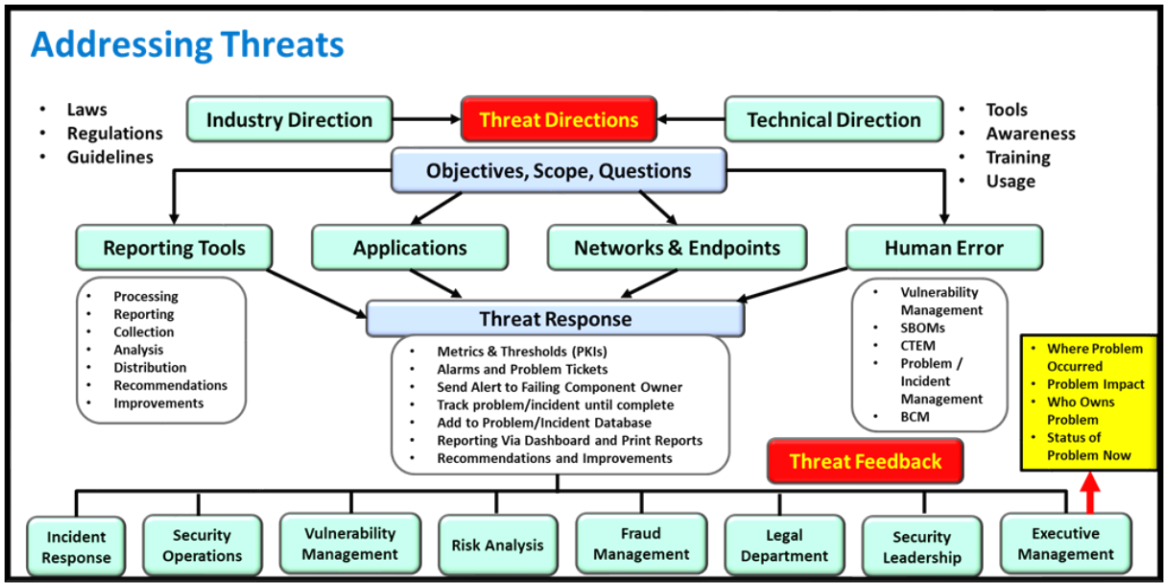

Figure 14: Access threats and reporting for rapid response.

Testing Assessment and Control Arenas

The following concepts should be included in your application's testing process.

- Chaos Management and Experiments for Problem Runbooks.
- Vulnerability Management for component release assurance.
- Information Assurance for Security Management.
- Third-Party Risk Management (TPRM).
- Supply Chain Management.
- Risk Control Asset-Management (RCSA).
- Implement Post-Quantum Cryptography (PQC) to protect sensitive information from Harvest Now, Decrypt Later (HNDL) and potential defeat of presently used encryption.

Problem and Incident Management System Flow

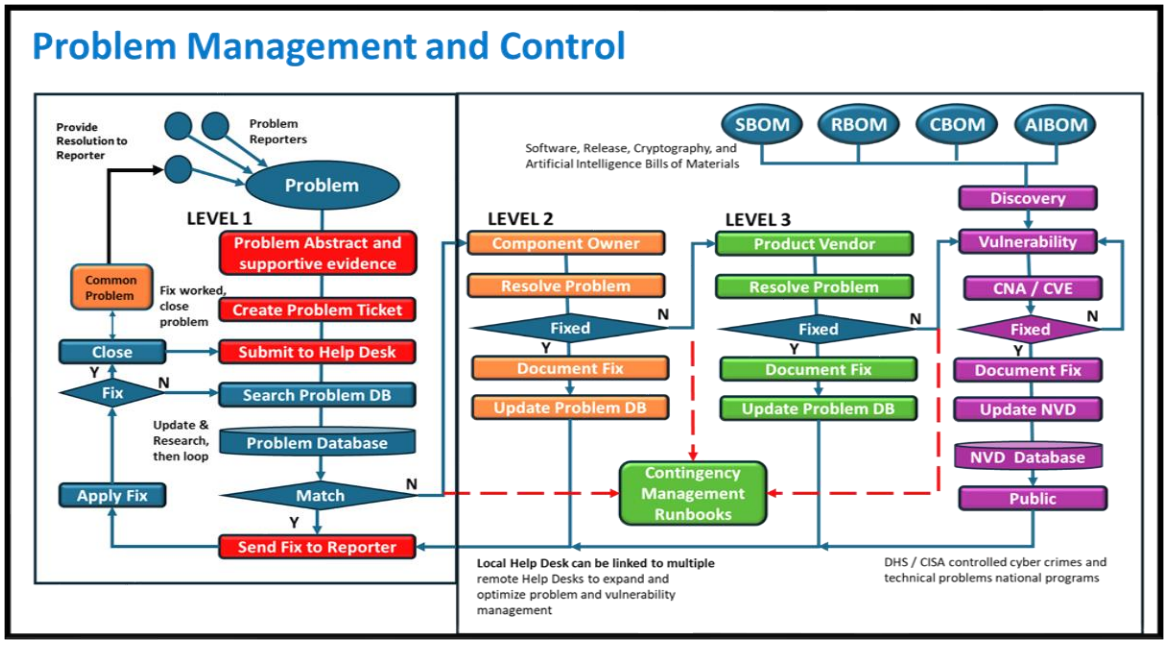

Figure 15: Problem and Incident Management Flow of Events and Controls

Detecting threats and responding to incidents and problems is a concern of every organization. All projects, whether they be for new products or services, or for updates to current products and services should be able to interface with the Incident/Problem Management organization, so that threats can be recognized and routed to the component owner for resolution. If a problem's resolution time is greater than the Recovery Time Objective (RTO), or if the threat is a great magnitude, then a recovery should be initiated immediately.

Initiating Recovery Operations (All Types)

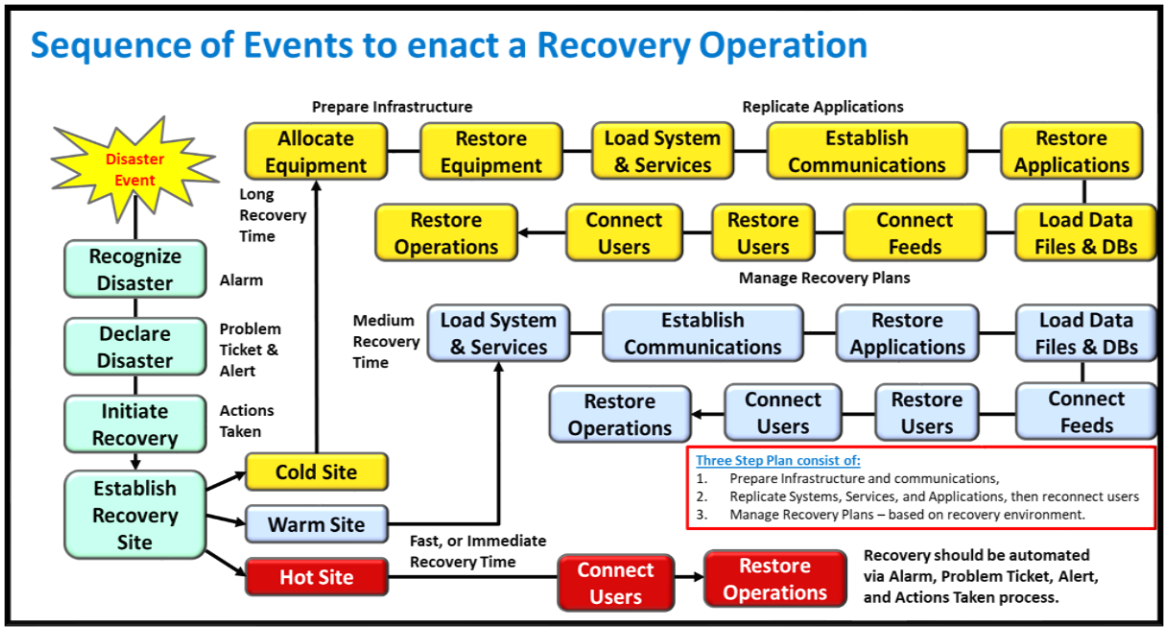

Figure 16: Sequence of events associated with Recovery Management types.

6. Cross-Lifecycle Integration

Project Managers must manage integration points across SDLC, SELC, and Agile delivery models. Activities include:

- **Bridging gaps** between product owners, developers, testers, operations, and security personnel.
- **Driving acceptance** through Production Readiness Reviews (PRRs) and Runbook validation.
- **Mapping project milestones** to Configuration, Change, and Release Management gates.
- **Ensuring production components** meet cATO (continuous Authorization To Operate) criteria.

Global Vulnerability Guidelines and Standards Overview

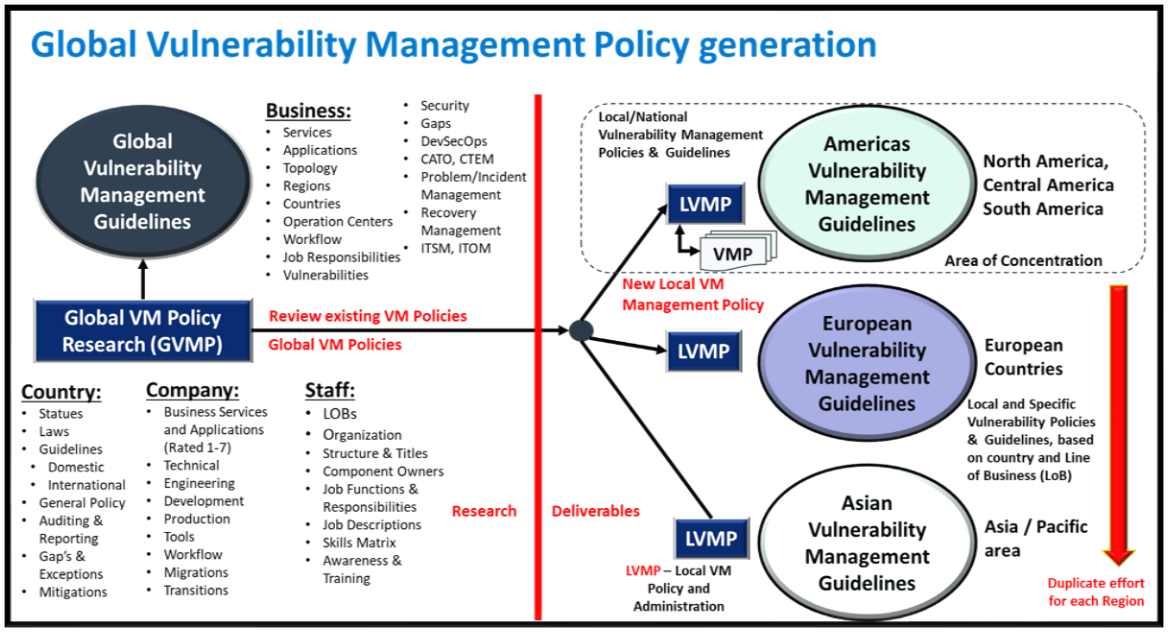

Figure 17: Integrating Standards and Guidelines within Enterprise

7. Migrating Applications to the Cloud

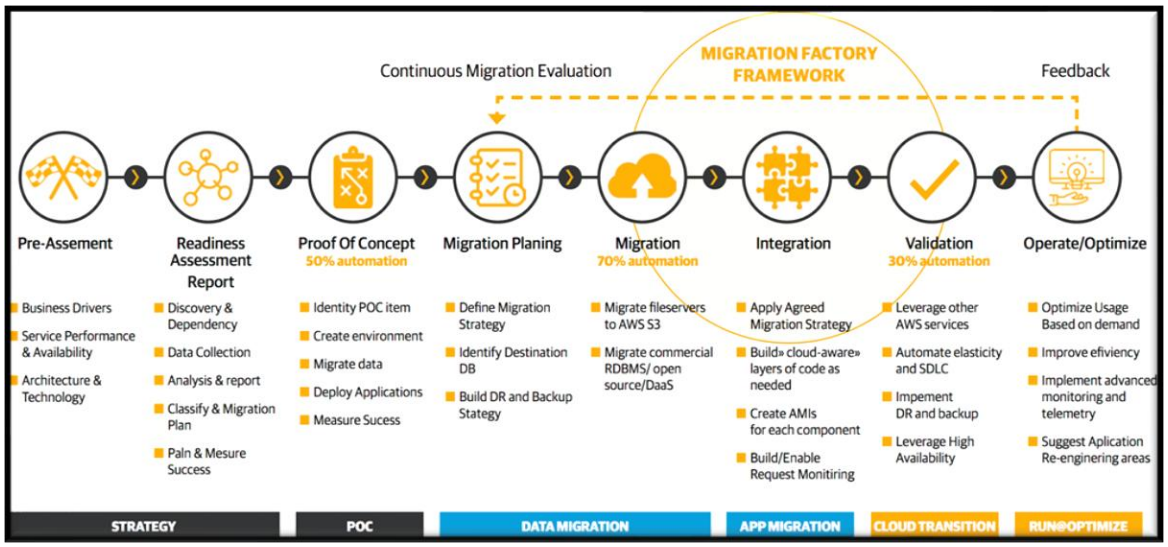

Figure 18: Process for migrating applications to the Cloud.

Migrating an application from on premises silo to the Cloud requires planning and a migration plan. The above illustration outlines how to migrate an application to the cloud, while the next illustration provides an overview of the protection provided by Managed Service Providers (MSPs) and your own responsibilities.

Cloud Security Guidelines for Managed Service Providers (MSPs)

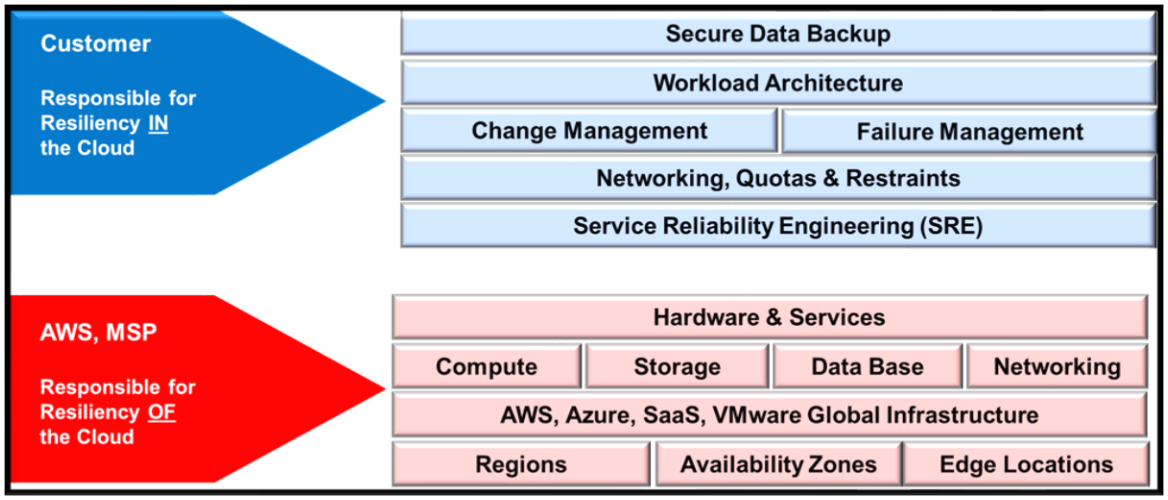

Figure 19: Cloud Provider Protections

8. Summary and Continuous Improvement

A skilled Project Manager enables secure, compliant, and efficient software delivery by aligning people, process, and tools. This document presents functional responsibilities to support delivery from concept through deployment. Leveraging hybrid Waterfall and Agile strategies, security compliance, and lifecycle coordination ensures optimal business outcomes.

Fully Developed DevSecOps and Production Operations System

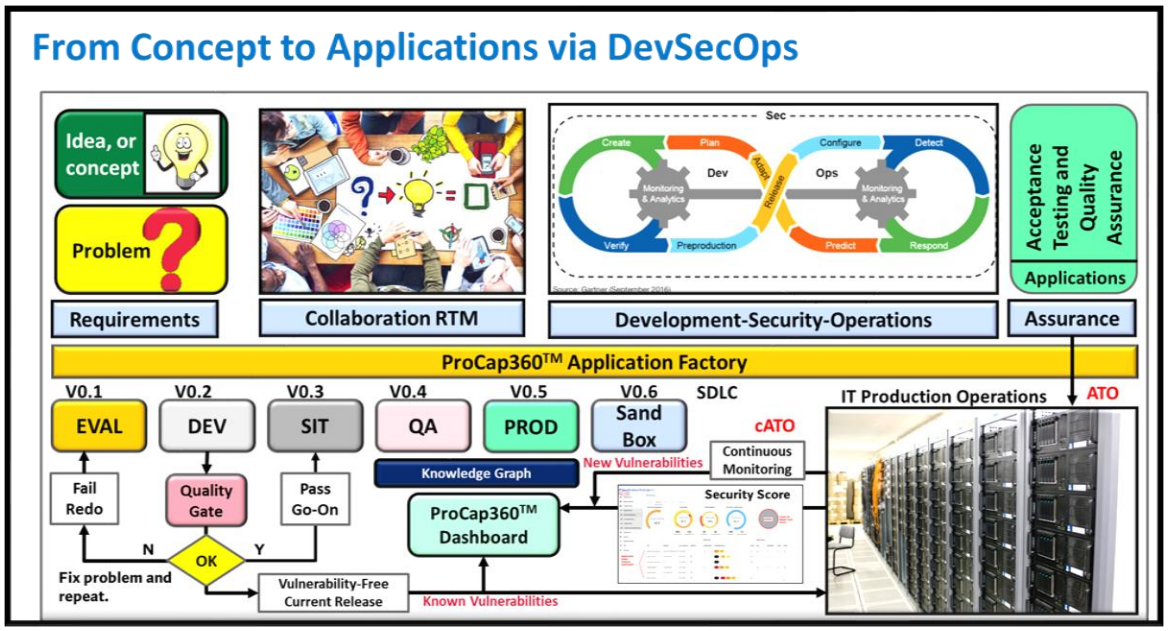

Figure 20: Deploying Secure, Efficient, and Vulnerability-Free Applications

Contacting DCAG for further discussions and contracting

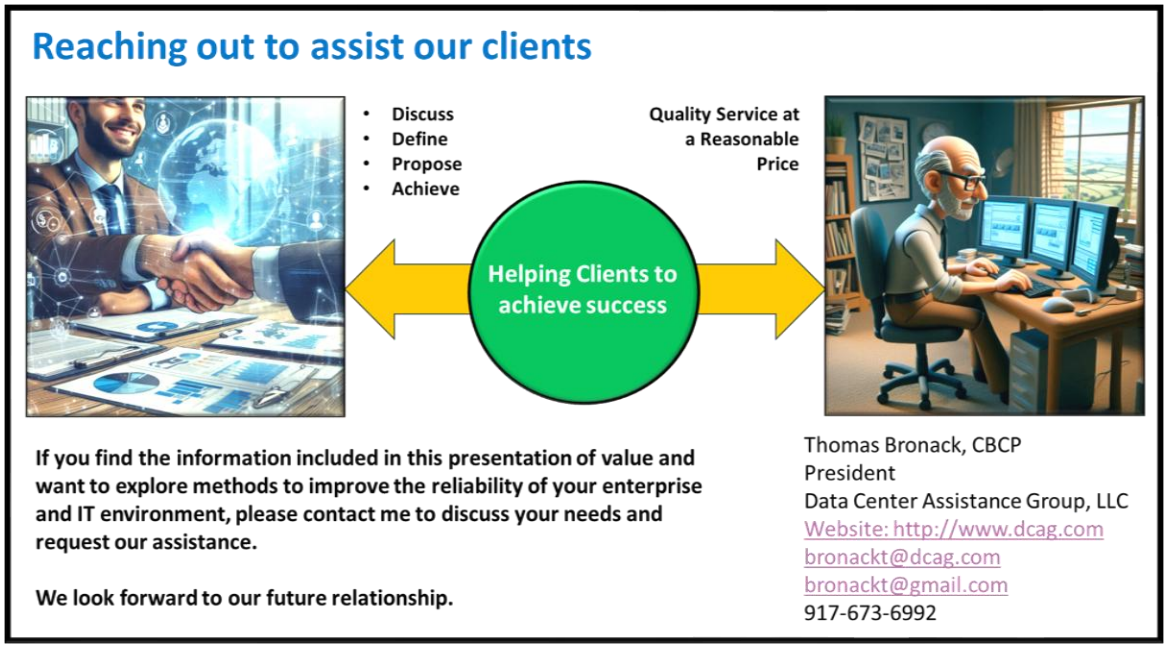

Figure 21: How to contact DCAG. LLC for assistance

