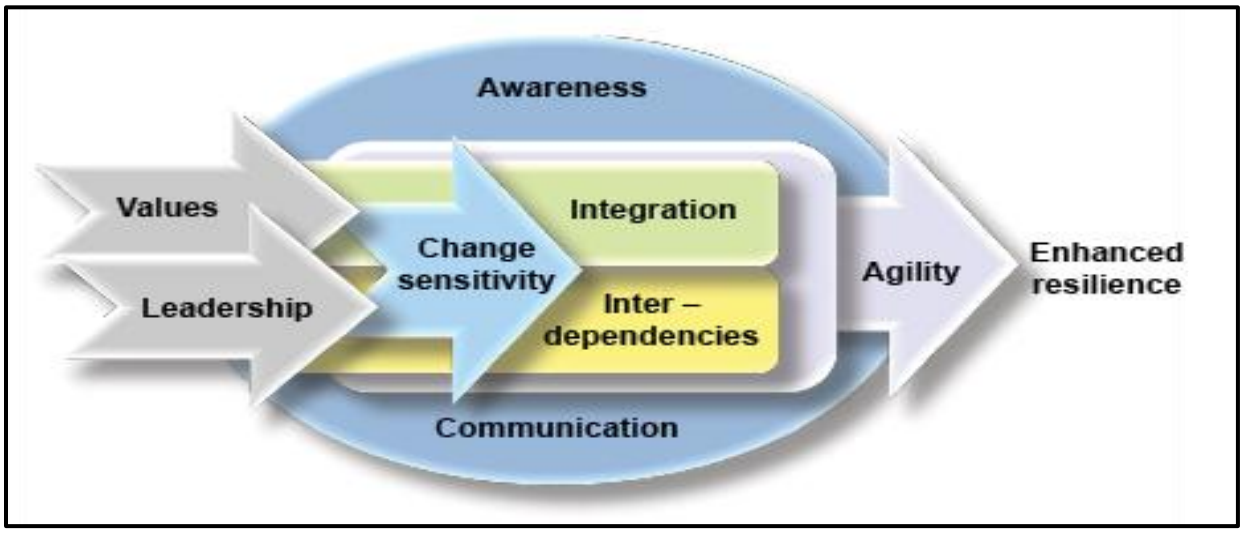
# Protecting the Corporation, through:

## Enterprise Resilience

## Risk Management Foundation (RMF)

## Business Continuity Management (BCM)

## Site Reliability Engineer (SRE)




- **Know your Business.**
- **Relate your business goals to IT Services.**
- **Analyze Risks and Define Controls.**
- **Build your Service Environment and ensure quality.**
- **Provide Service Continuity and Recovery Management**
- **Ongoing Monitoring and improvement**

# Table of Contents:

## Contents

# Table of Figures

## Executive Summary

In today's digital-first and disruption-prone environment, enterprise resilience is no longer optional - it is a competitive differentiator and regulatory necessity. This paper presents a comprehensive approach to embedding resilience into every layer of an organization, from risk management and disaster recovery to agile development and site reliability engineering (SRE).

We explore how integrating leading frameworks - such as COSO, NIST CSF 2.0, ITIL, TOGAF, and ISO - can help organizations proactively anticipate, absorb, and adapt to adverse events. The document outlines practical methods for classifying applications by criticality, implementing recovery strategies based on RTO/RPO/RTC, and using AI-driven planning for rapid response and continuous improvement.

A major emphasis is placed on transforming IT operations through the lens of SRE to reduce toil, automate recovery processes, and improve operational KPIs like MTTR, SLA adherence, and service availability. The paper also introduces Application Security Risk (ASR) scoring, Resilience-as-Code principles, and Chaos Engineering as modern tools for proactive fault tolerance.

Additionally, the paper underscores the importance of integrating **vulnerability management** into the Systems Development Life Cycle (SDLC). This proactive inclusion ensures production applications are deployed with minimal risk, using components that are up-to-date and verified against known vulnerabilities. By integrating **continuous monitoring**, organizations can guard against newly emerging threats and swiftly implement mitigation actions. Leveraging tools such as **Software Bills of Materials (SBOMs)** and automated vulnerability platforms like **ProCap360™ (www.procap360.com)** enable this process by identifying at-risk components and enforcing secure production control gates.

The result is an operational ecosystem that not only protects applications from both known and emerging threats but also delivers measurable **cost savings** through:

- Reduced stress and burnout among technical personnel
- Fewer cybersecurity breaches and incidents
- Improved SLA performance and compliance
- Enhanced customer satisfaction and brand reputation
- Lower costs in emergency response, patch management, and regulatory penalties

Real-world applicability is strengthened through detailed lifecycle models, cloud migration strategies, and DevSecOps integration patterns, offering a blueprint that can be tailored to commercial enterprises, government agencies, and regulated industries alike.

This paper empowers technology leaders to:

- Aligning IT resilience with business outcomes and customer value.
- Measure and mitigate risk using standardized frameworks.
- Build a culture of shared responsibility and operational agility.
- Justify investments with measurable ROI and resilience KPIs.

Whether facing cyber threats, supply chain shocks, or future pandemics, the guidance herein supports building an organization that can not only survive—but thrive - in the face of disruption.

## Key takeaways include:

- **Enterprise Resilience Defined**
  Practical guidance on evolving beyond traditional disaster recovery into a proactive, integrated resilience model that spans business, IT, cybersecurity, and compliance.
- **Framework Integration for Assurance and Agility**
  Clear alignment across NIST CSF 2.0, ISO 27001, RMF, CMMC, TOGAF, COSO, and COBIT frameworks for cross-functional resilience planning.
- **SRE as a Catalyst for Continuous Operations**
  How Site Reliability Engineering accelerates mean time to recovery (MTTR), reduces toil, and enables observability, automation, and operational maturity across cloud-native environments.
- **Real-Time Risk Metrics & ROI Measurement**
  Introduction of quantifiable metrics such as Application Security Risk (ASR), service level objectives (SLOs), recovery time capability (RTC), and actionable dashboards for executive decision-making.

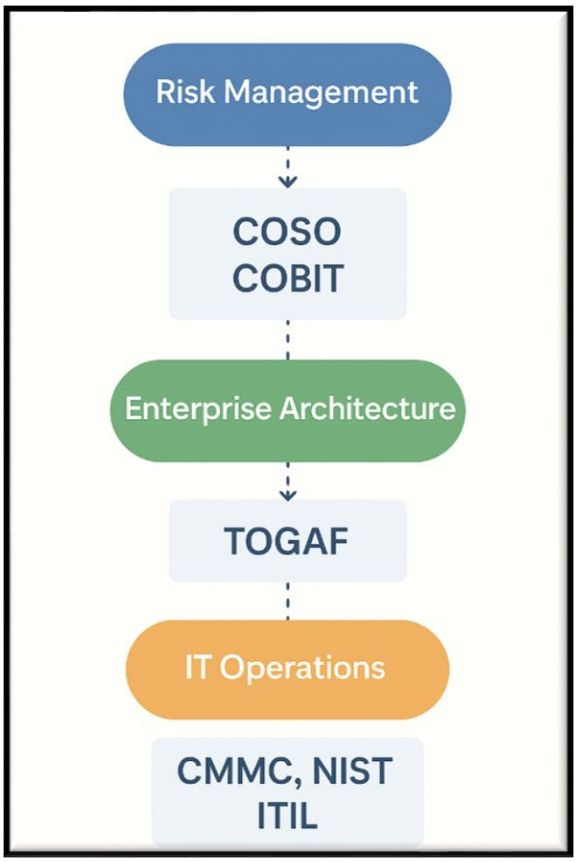



*Figure 1: Unified Framework Map*

- **AI & Automation in Resilience Operations**
  Exploration of how artificial intelligence, GenAI, and machine learning can drive scenario planning, chaos testing, cloud migration optimization, and service continuity.
- **AI Agentic RAG** agents can be developed to interact with personnel to automate and supplement functional operations, reduce stress and costs, and improve efficiency.
- **Cloud-Native Resilience & Zero Trust Readiness**
  Guidance on securing modern, containerized, and hybrid cloud environments through resilience-as-code, Zero Trust Architecture, and infrastructure-as-code recovery planning.
- **Building a Risk-Aware Culture**
  Frameworks and practical steps for embedding resilience into corporate culture, employee behavior, and strategic priorities—ensuring business continuity and regulatory alignment across geographies.

This document serves as a foundational resource for IT leaders, security professionals, and executive decision-makers seeking to transform fragmented legacy recovery strategies into dynamic, resilient ecosystems. Whether preparing for an AWS Marketplace submission, government procurement, or internal transformation, the insights within are designed to accelerate your journey from risk management to business advantage.

# Defined Audience & Purpose

## Audience

This document is intended for a diverse group of organizational leaders and technical professionals responsible for enterprise risk, continuity, and IT operations. The target audience includes:

- **Chief Information Officers** (CIOs) and Chief Information Security Officers (CISOs) to implement resilient IT strategies.
- **DevSecOps, SRE, and Platform Engineering** teams responsible for service uptime, automation, and application lifecycle management.
- **Risk Managers and Governance, Risk & Compliance** (GRC) professionals tasked with regulatory adherence and mitigation planning.
- **IT Operations Managers and Enterprise Architects** focused on aligning IT architecture with business continuity.
- **Program Managers**, Project Leads, and Business Continuity Planners supporting continuity of operations and disaster recovery initiatives.
- **Procurement Officers** and Compliance Auditors evaluate secure, efficient, and compliant vendor solutions.

## Purpose

The purpose of this white paper is to provide a unified and actionable roadmap for building enterprise resilience through the integration of risk management frameworks, secure systems development practices, cloud-native technologies, and modern operational methodologies like Site Reliability Engineering (SRE). It aims to:

- Equip decision-makers with a cross-domain understanding of how resilience frameworks intersect with cybersecurity, compliance, and IT performance.
- Provide practical guidance for implementing scalable and secure IT infrastructure capable of adapting to modern disruptions.
- Highlight how tools such as SBOMs and platforms like ProCap360 enable vulnerability-aware operations and proactive risk mitigation.
- Demonstrate measurable business value through resilience—including reduced breach incidents, improved team efficiency, and better customer experiences.
- Introduce the importance of Post-Quantum Cryptography (PQC) and how to migrate from current encryption practices to quantum resilient cryptography to best protect the organization's most essential information and comply with current laws and mandates.

By clarifying how strategic foresight, continuous monitoring, and secure automation converge to create resilient enterprises, this paper supports IT and executive leaders in future-proofing their mission-critical systems.

## Cybersecurity Resilience: NIST CSF 2.0

In an era of escalating cyber threats and increased regulatory scrutiny, the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) provides a vital foundation for achieving cybersecurity resilience. The 2024 release of NIST CSF 2.0 expands upon the original five core functions—Identify, Protect, Detect, Respond, and Recover—by offering enhanced guidance and integration options with industry-specific standards and Governance models.

### CSF 2.0 Core Functions

| Function | Category | Category Identifier |
|---|---|---|
| **Govern (GV)** | Organizational Context | GV.OC |
| | Risk Management Strategy | GV.RM |
| | Cybersecurity Supply Chain Risk Management | GV.SC |
| | Roles, Responsibilities, and Authorities | GV.RR |
| | Policies, Processes, and Procedures | GV.PO |
| | Oversight | GV.OV |
| **Identify (ID)** | Asset Management | ID.AM |
| | Risk Assessment | ID.RA |
| | 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)** | Continuous Monitoring | DE.CM |
| | Adverse Event Analysis | DE.AE |
| **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 |

*Figure 2: CSF 2.0 Structure and categories.*

- **Govern:** Organizational Structure, Risk Management Strategy, Cybersecurity Supply Risk Supply Chain (all components), Roles, Responsibilities, Authorities, and Oversight.

- **Identify:** Understand organizational assets, risks, and exposures. Includes asset management, governance, risk management, and supply chain protection.
- **Protect:** Develop safeguards to ensure service delivery. Includes access control, awareness training, data security, and secure development practices.
- **Detect:** Implement capabilities to discover anomalies, events, and potential security incidents in real time.
- **Respond:** Define effective incident response protocols, including containment, communication, and root cause analysis.
- **Recover:** Develop and implement recovery processes to maintain business resilience, including backup strategies, restoration procedures, and continuous improvement.

## New Enhancements in CSF 2.0

- Expanded emphasis on governance and supply chain risk management.
- Enhanced mappings to frameworks such as ISO 27001, COBIT, and COSO ERM.
- Improved cross-functional integration with enterprise architecture and GRC systems.
- Support for profile customization to meet sector-specific needs.

## Integration with Enterprise Resilience Strategies

NIST CSF 2.0 serves as a bridge between operational security controls and executive-level risk management. When integrated with other frameworks such as COSO (for enterprise risk oversight) and TOGAF (for architectural alignment), it ensures cybersecurity efforts are:


*Figure 3: Implementing CSF2.0 Cybersecurity Process*

- Implement Govern and controls section as foundation for CSF2.0 implementation.
- Identify critical business products, services, and compliance requirements.
- Establish teams and assign functional responsibilities.

- Establish Plan of Action and Milestones (POA&M) and start project actions.
- Scalable across cloud and hybrid environments
- Measurable use compliance metrics and KPIs.
- Mapped to business priorities and customer-facing outcomes.

## Zero Trust Architecture (ZTA)

To address advanced persistent threats and lateral movement within systems, organizations are adopting Zero Trust principles. ZTA complements CSF 2.0 by enforcing:


- Continuous identity verification (IAM, MFA, RBAC/ABAC)
- Least privilege access enforcement
- Micro-segmentation and strong endpoint monitoring

Together, CSF 2.0 and ZTA create a robust, adaptive, and continuously monitored security posture that aligns with broader enterprise resilience initiatives.

# What is Enterprise Resilience

Resilience is an organization's capacity to anticipate and react to problems and changes, not only to survive, but also to evolve and thrive.

## Definition of a Resilient System:

A system is resilient if it continues to provide services and conducts its mission in the face of adversity (i.e., if it provides the required capabilities despite excessive stress that can cause disruptions). This document includes both Enterprise Resilience and Corporate Compliance Certification, to address all forms of recovery, risk management and optimizing production operations through best practices, continuous monitoring, and continuous improvements.

Being resilient is important because no matter how well a system is engineered, reality will eventually conspire to disrupt the system. Resilience includes all forms of Recovery Management, Risk Management, and Contingency Planning. Corporate Compliance Certification includes adhering to domestic and internationals laws and regulations for the countries where the company conducts business.

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

### An overview of Enterprise Resilience and Corporate Compliance Certification

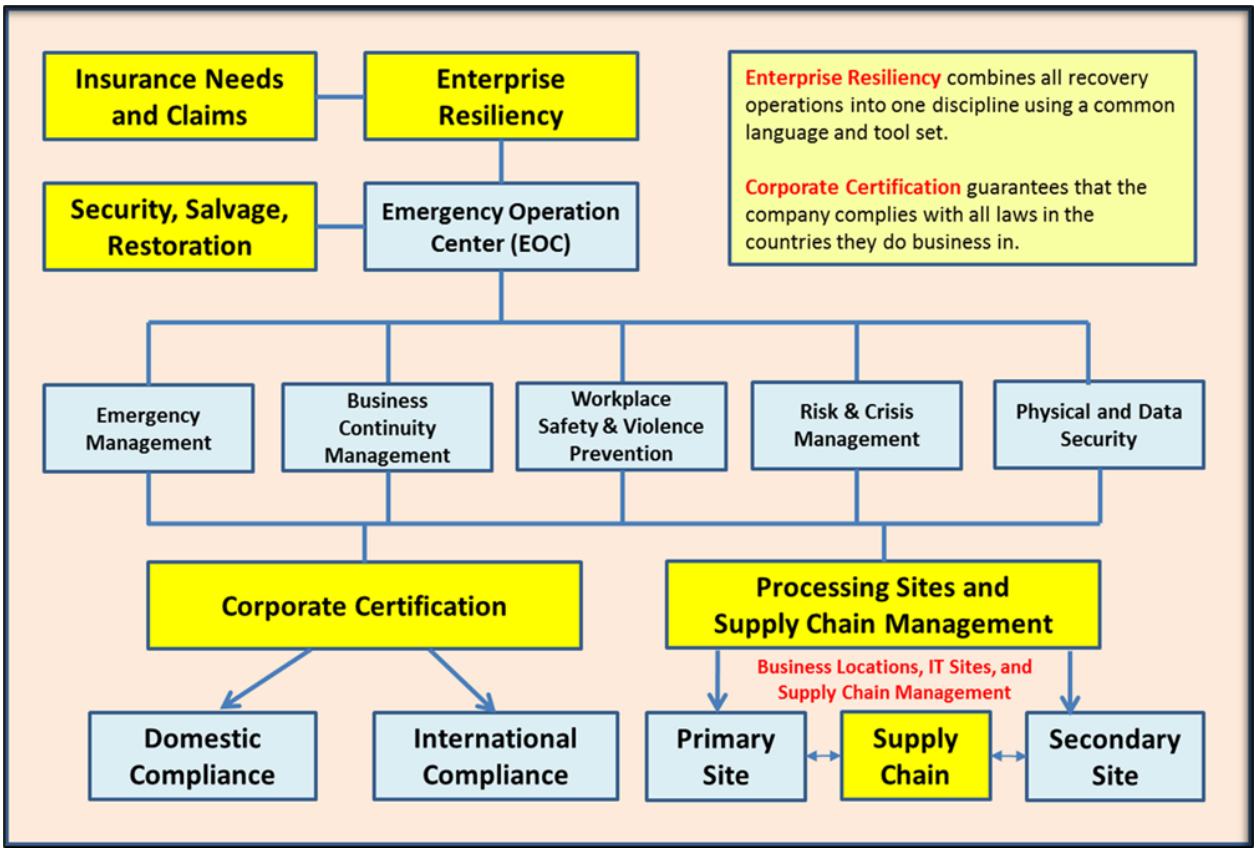



*Figure 4: Enterprise Resilience and Corporate Certification*

Recovery practices are vastly different for recovering applications in Silos (Monolithic Systems) than when applications reside in the Cloud (Microservices), but they both start by knowing your business and exposures that must be addressed in a priority order.

*Over time, the concept of operational resilience matured into consideration much more than just keeping the lights on. It has evolved to include the effects of a business disruption on employees, customers, suppliers, stakeholders – the operating ecosystem of an enterprise. Today's successful resilience programs are found in organizations with a strong teamwork culture, cooperation, self-awareness, and shared values. Figure 5: Zero Trust Architecture*

## What comprises Enterprise Resilience?

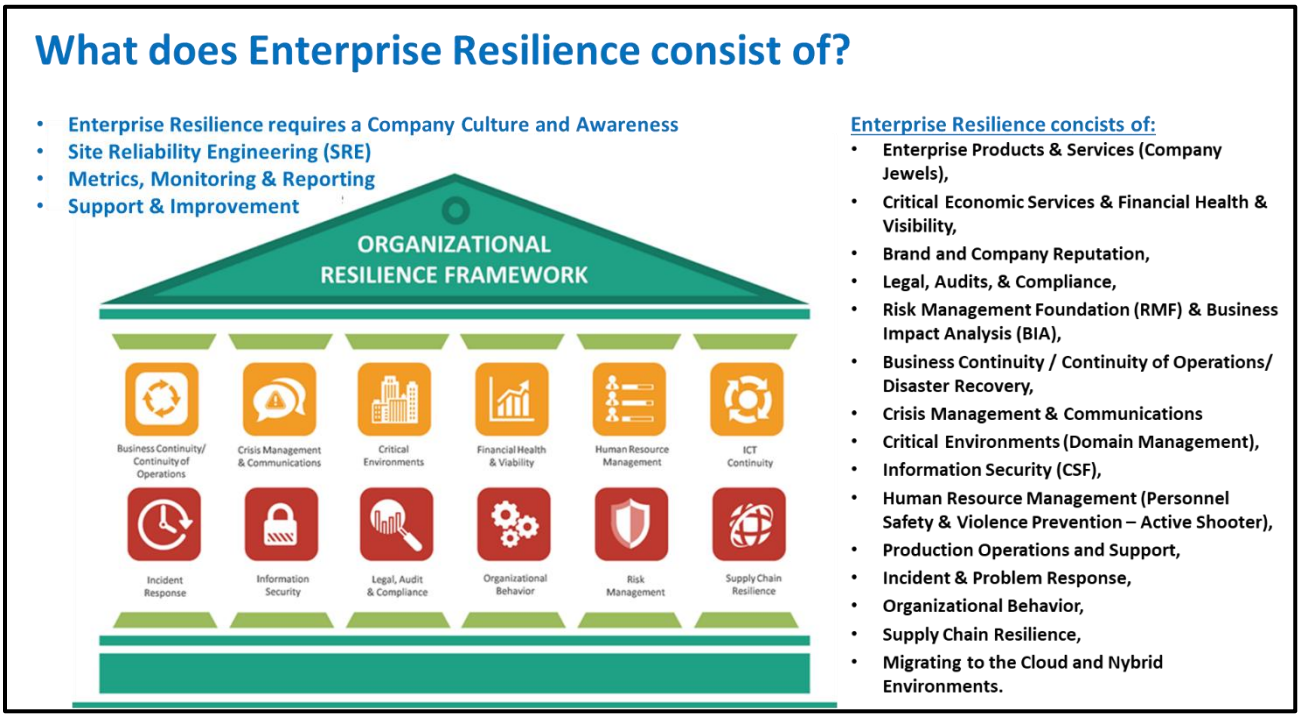



*Figure 6: Overview of Enterprise Resilience and its components.*

Operational resilience is an organization's ability to deliver on its promise to its customers, no matter what. It is a connected understanding of your organization's operations that unlocks the ability to deliver on current commitments to customers and evolve with them as circumstances and needs change. It creates an interactive understanding of the day-to-day operating environment that makes business work and identifies where it is prone to breaking. And if it breaks, resilience allows it to be reassembled in new, innovative ways that incorporate lessons learned, resulting in better forward service for the customer and community.

Enterprise risk management (ERM) is a methodology that looks at risk management strategically from the perspective of the entire firm or organization. It is a top-down strategy that aims to identify, assess, and prepare for potential losses, dangers, hazards, and other probable causes of harm that may interfere with an organization's operations and objectives and/or lead to losses.

- Enterprise risk management (ERM) is a firm-wide strategy to identify and prepare for hazards with a company's finances, operations, and objectives.

- ERM allows managers to shape the firm's overall risk position by mandating certain business segments engage with or disengage from activities.
- Traditional risk management, which leaves decision-making in the hands of division heads, can lead to siloed evaluations that do not account for other divisions.
- The COSO framework for enterprise risk management identifies eight core components of developing ERM practices.
- Successful ERM strategies can mitigate operational, financial, security, compliance, legal, and multiple other types of risks.

## Process followed when performing Enterprise Resilience and Recovery Management

### 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 with Best Practices.
d) **Recovery Planning -** Time Objective (RTO), Recovery Point Objective (RTO), Recovery Time Capability (RTC), and Recovery Group (service continuity, time to recover, time sensitive applications and services).
e) **Application Recovery Capabilities -** Backup, Recovery, Vaulting, Recovery Time Capability (RTC), current recovery plans, current Risk Analysis, current Business Impact Analysis.

### 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), Governance (GRC), 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.
c) **Implement required Controls** over identified 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 provide a Letter of Attestation to Regulators.
b) **Ensure security** is optimized and in place with awareness and staff 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.
f) **Utilize Bill of Materials** like Software (SBOM), Release (RBOM), Cybersecurity (CBOM), and Artificial Intelligence (AIBOM) to detect KNOWN vulnerabilities and component failures that can be resolved prior to production acceptance in support of Authorization to Operate (ATO).
g) **Continuous Improvement –** for monitoring NEW vulnerabilities, results, enhancements, releases, and patches.

### Process to follow when determining how best to protect your business.

The following illustration will help you develop a methodology to follow when defining your organization's need for Enterprise Resilience and Corporate Compliance Certification.

### The process for protecting your Enterprise.

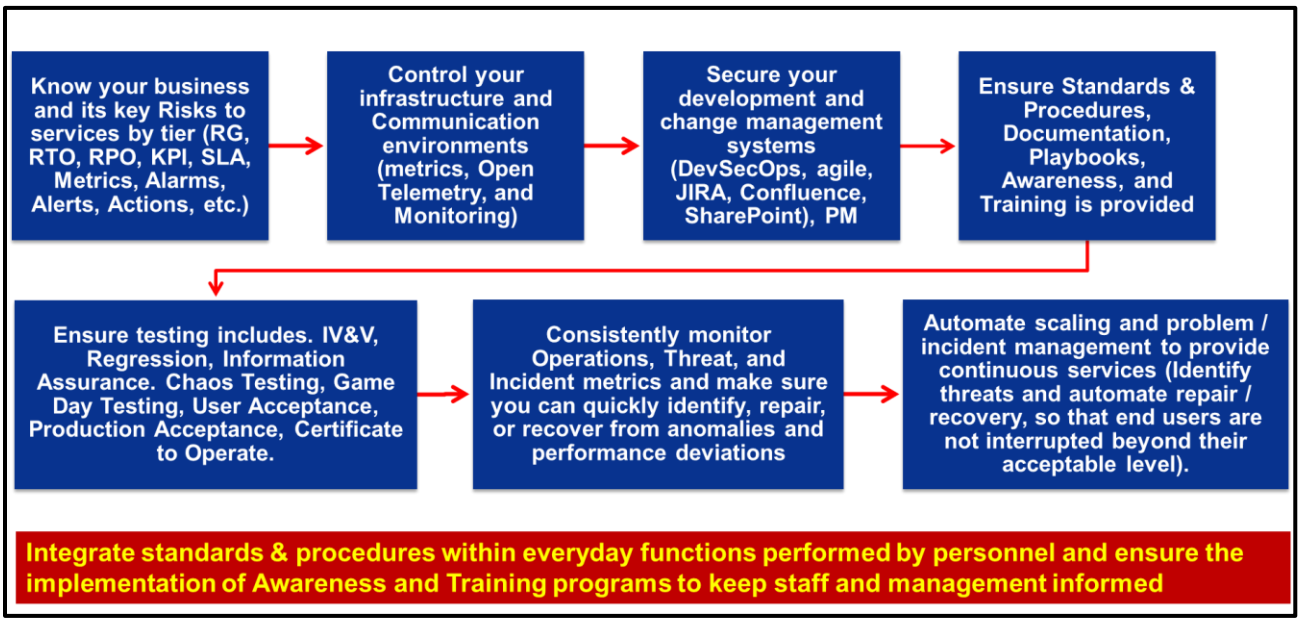



*Figure 7: Process to consider when planning to protect your company.*

## Rating your applications and services by their security metric

Why are breaches continuing despite deploying innovative solutions supported by compliance to thwart the attacks? Are applications more secure relative to current threats or less secure? How much more security is required? What is the current level of risk posed by application security? Can the security budget be decreased, or should it be increased? If increased, to what extent is risk reduced? What are the applications' changes in the risk level before and after the deployment of innovative security measures?

No definitive answer exists for these questions because there is no standard metric to know the exact status of application security. Unanswered questions have paved the way for attackers to continue exploiting applications. Therefore, a security metric that can quantify the risk posed by applications is essential to make decisions in security management and thwart attacks.

Currently, a generic risk assessment metric is used to assess application security risk (**ASR**). This does not encompass the basic factors of application security such as compliance, countermeasure efficiency and application priority. Obviously, the results are not commensurate with the actual risk posed by

application security. Real application security risk is perceived and not measured. Hence, organizations are not able to implement the required security controls. The business is unaware of its applications' susceptibility to attack. This is the main reason for continued attacks on applications despite deploying robust security measures. ASR measurement requires a specifically designed metric that involves all the factors of application security. This article aims to define the standard for security in applications by designing a metric.

The entire process of metric design allows the business to find the optimum answer for the following questions:

- What path could an attacker take to get inside the application?
- What tools are required to defeat the existing security measures?
- What are the possible signs of an attack particular to each category of application?
- Can existing security measures detect the attack?

Answering these questions ensures that the organization has considered potential attacks and helps toward the implementation of required controls if existing measures are inadequate.

Application security (see document) is made up of four factors:

**Governance (GV) Organizational Structure and Oversight.**

- Vulnerability (Vulnerability density - Vd)
- Countermeasure (Countermeasure efficiency – Ce),
- breach impact (Breach cost – Bc) and
- compliance (Compliance index – CI).

Analyzing these key factors, four prime terms on which ASR depends emerge. The four key terms are breach cost (Bc), vulnerability density (Vd), countermeasure efficiency (Ce) and compliance index (CI).

**CI** is the ratio of the number of compliance requirements met (CRM) to a total number of compliance requirements (CRT) in the application (i.e., CRM / CRT – ¼, or 25%).

**Vd** is the ratio of number of vulnerabilities to the size of software (SST), or Vd / SST = 5/25 = 20%.

**Ce** is the measure of implementation efficiency of countermeasures (i.e., Ce = 30 out of 50, or 30/50 = 60%).

**Bc** is the assessment of the likelihood of cost that would be incurred in case of attack.

The following illustrations may better explain the relationships involved in Application Security Risk (ASR) evaluations.

## Building your Enterprise Resilience environment

How does an organization build a culture of resilience? How does it create a culture that is embraced by its directors, executives, workforce, and customers?

It starts with building relationships and speaking the same language. This is a brand-defining moment for an organization, requiring agility that empowers an organization to adapt quickly in changing times. It looks to break down the departmental "silos" that impede communication and cooperation within the organization.

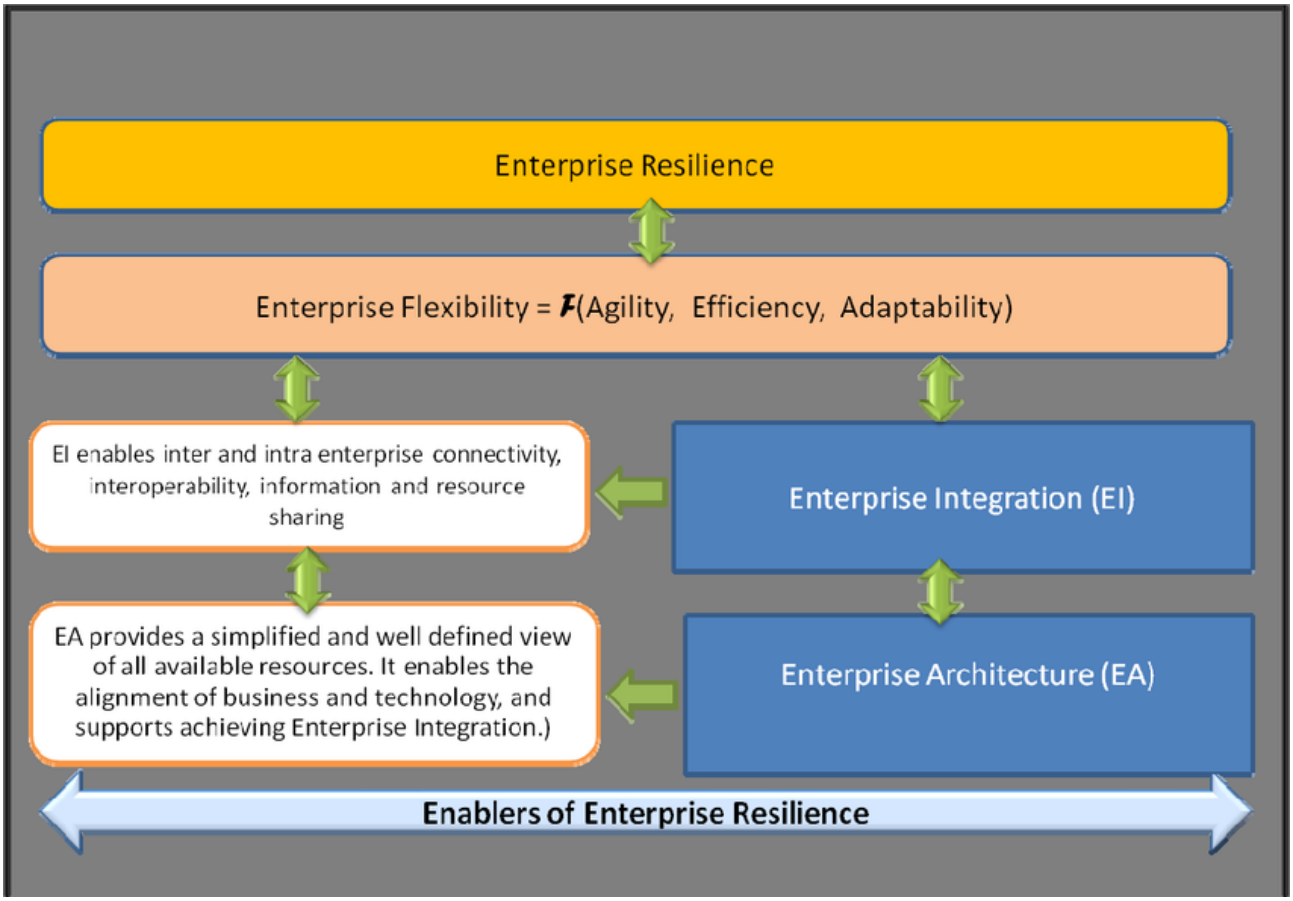



*Figure 8: Enterprise Integration (SI) and Enterprise Architecture (EA) overview.*

Organizational resilience is more than just checking the box for regulatory/compliance. It is a culture that does more than just respond to disruptions. Resilience helps organizations make informed decisions, in the face of events both anticipated and novel. It is initiative-taking, not reactive. It is planning for the severe, but plausible events – a health crisis, a catastrophic supply chain disruption, a large-scale climate emergency – but also the layering of every day events.

Applying a "Left of Boom" philosophy will allow you to take a proactive role in predicting, and planning for, business interruptions. Put an 'X' in every box and ask what would happen if this failed. Then construct a response to best protect the organization.

## How to protect your Company by implementing Enterprise Resilience

Starting by rating your applications and services by revenue generation and client facing into a Recovery Group (RG) based on Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) is your first step, then you must decide on the best practices used to integrate applications and services into your IT System and Recovery environments.

Enterprise resilience and IT systems integration are critical components of IT production operations. Here are a sample of the best practices that can help organizations achieve resilience and optimize their IT production operations:

1. **Understand the criticality of a given process:** To achieve resilience, an organization needs to understand the criticality of a given process, evaluate the underlying technology, recognize the corresponding business impact, and know the risk tolerance of the organization and external stakeholders [1].
2. **Incorporate technology resilience into enterprise design and architecture**: Mature organizations incorporate technology resilience into enterprise design and architecture. Resilient designs incorporate elements of redundancy, scalability, flexibility, recoverability, and interoperability [1].
3. **Develop management systems based on best practices**: Enterprises that develop management systems based on best practices, such as Information Technology Infrastructure Library (ITIL), create an effective operation [2].
4. **Orchestrate asynchronous calls to enterprise back-end systems by using queues and events**: This approach is useful for enterprise integration using message broker and events [3].
5. **Move data from an on-premises SQL Server database into Azure Synapse Analytics and transform the data for analysis**: This approach is useful for enterprise business intelligence [3].

It is important to note that these best practices are not exhaustive but can serve as a starting point for organizations looking to improve their IT production operations.

# Best Practices - tools and guidelines

## COSO – Committee of Sponsoring Organizations

**COSO** – Enterprise Risk Management – integrated framework developed by COSO (Committee of Sponsoring Organization of the Treadway Commission) is an organization that develops guidelines for businesses to evaluate internal controls, risk management, and fraud deterrence. In 1992 (and subsequently re-released in 2013), COSO published the *Internal Control - Integrated Framework*, commonly used by businesses in the United States to design, implement, and conduct systems of internal control over financial reporting and assessing their effectiveness.

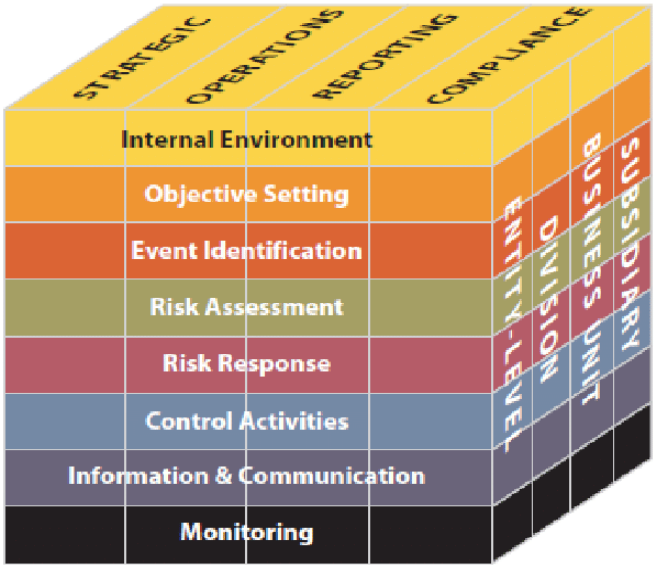



*Figure 9: COSO Overview Diagram*

Internal control is a process, affected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance.

## COBIT - Control Objectives for Information and Related Technology

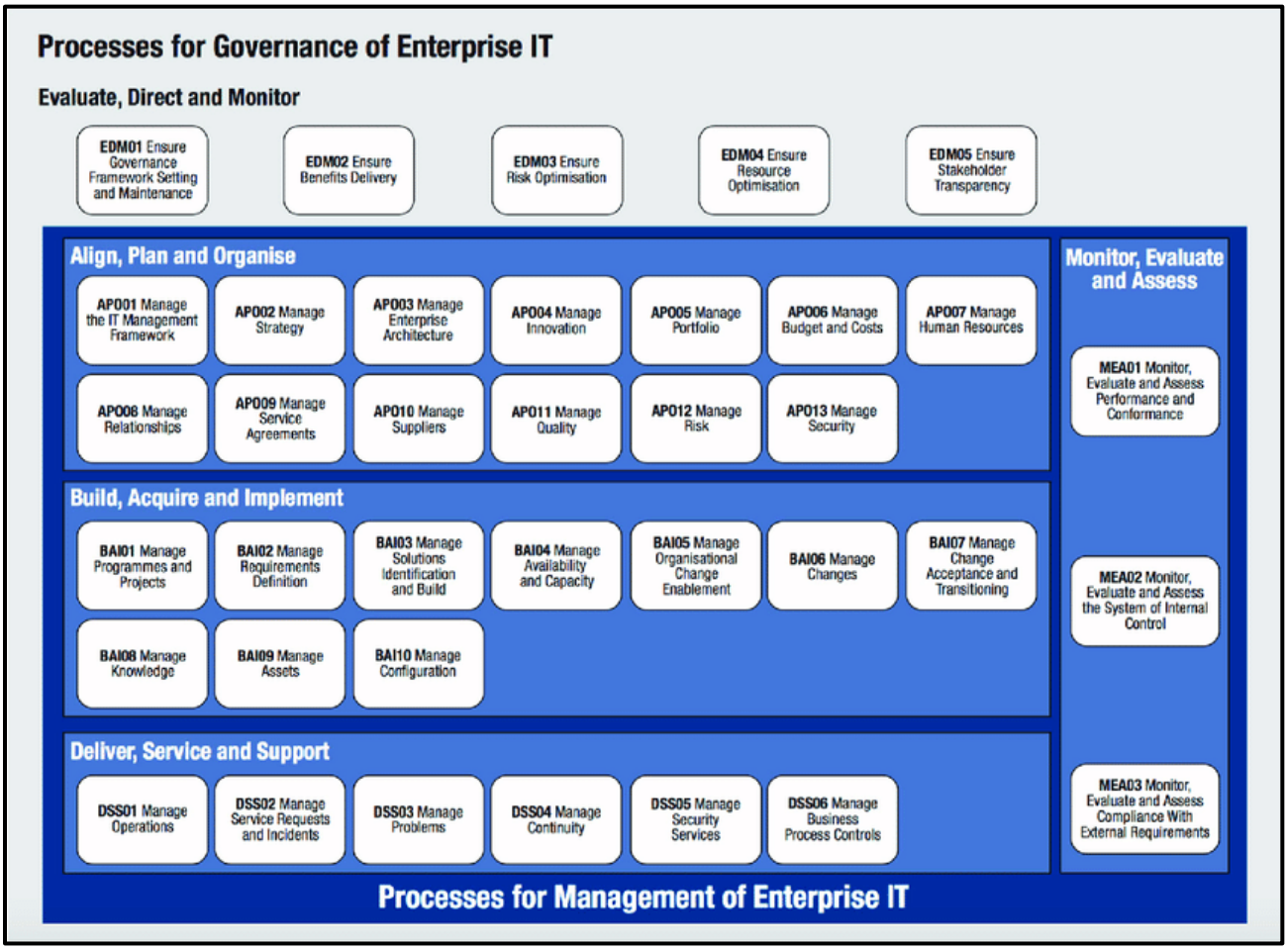



*Figure 10: COBIT process model.*

**COBIT** (**Control Objectives for Information and Related Technologies**) is a framework created by ISACA for information technology (IT) management and IT governance.

The framework is business focused and defines a set of generic processes for the management of IT, with each process defined together with inputs and outputs, key process-activities, process objectives, performance measures and an elementary maturity model.

Again, in this integrated form, the key elements identified by COBIT 5 are viewed as one system and include:

- Integrating quality management into solutions for development and service delivery,
- Collecting and analyzing risk data,
- Developing and maintaining a project plan,
- Defining and maintaining business and technical requirements,
- Designing, building and testing solution components, and
- Documenting, tracking, performing and reporting on change.

## CMMC - Cybersecurity Maturity Model Certification

CMMC is a U.S. Department of Defense (DoD) program that applies to Defense Industrial Base (DIB) contractors. It is a unifying standard and new certification model to ensure that DoD contractors properly protect sensitive information.

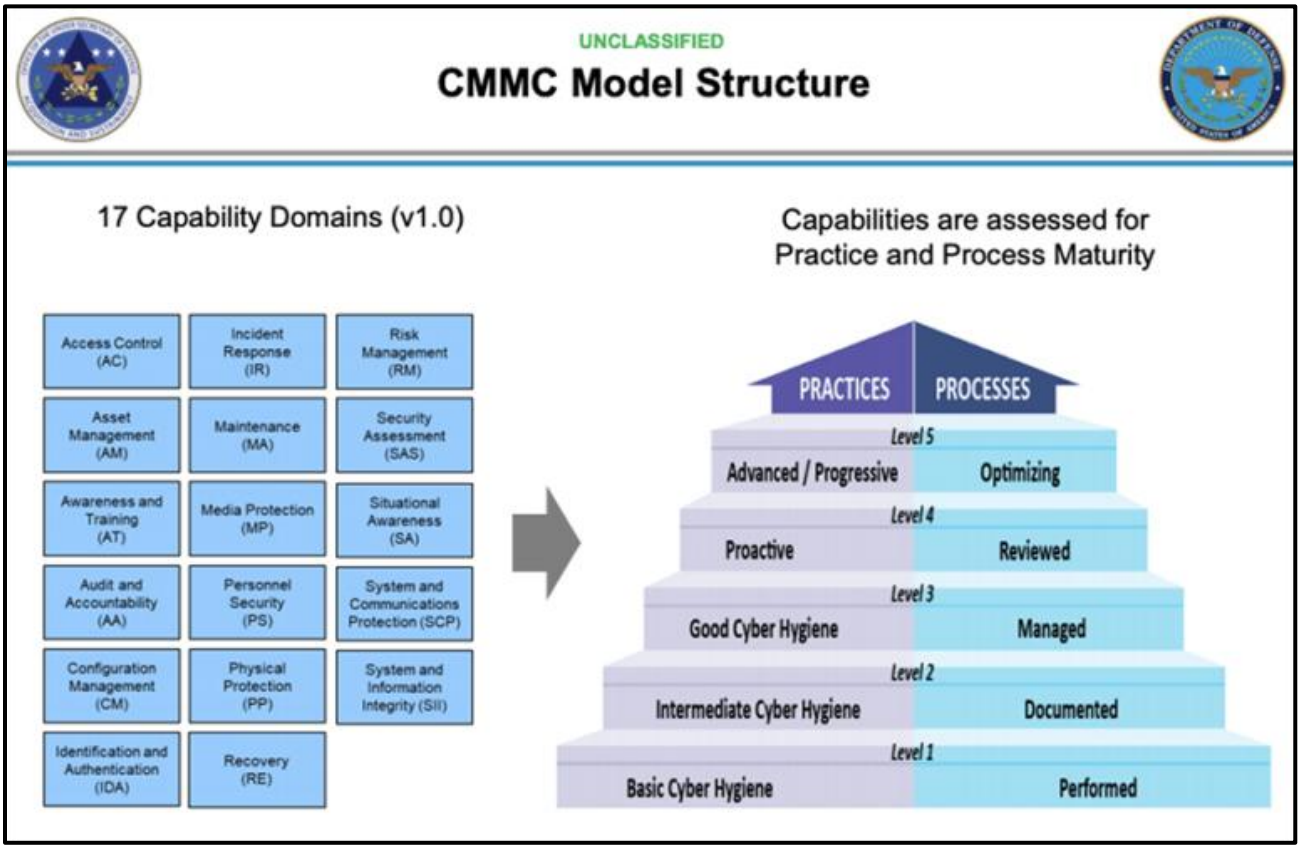



*Figure 11: CMMC Framework Model*

The framework (see Link) provides a model for contractors in the Defense Industrial Base to meet the security requirements from NIST SP 800-171 Rev 2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. Some contracts will also include a subset of requirements from NIST SP 800–172, Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication. 800–171.

CMM was originally developed for Software Development and Maintenance but later it was developed for:

- Systems Engineering
- Supplier Sourcing,
- Integrated Product and Process Development,
- People CMM, and
- Software Acquisition.

After CMMC, the DoD discovered that some vendors and suppliers could not prove their support of CMMC standards, even when they said they complied, so DoD create the CMMI (Capability Maturity Model Integration) standards and required vendors and suppliers to adhere to these standards by a dateline or forfeit their ability to work with the US Government.

## CMMI - Cybersecurity Maturity Model Integration

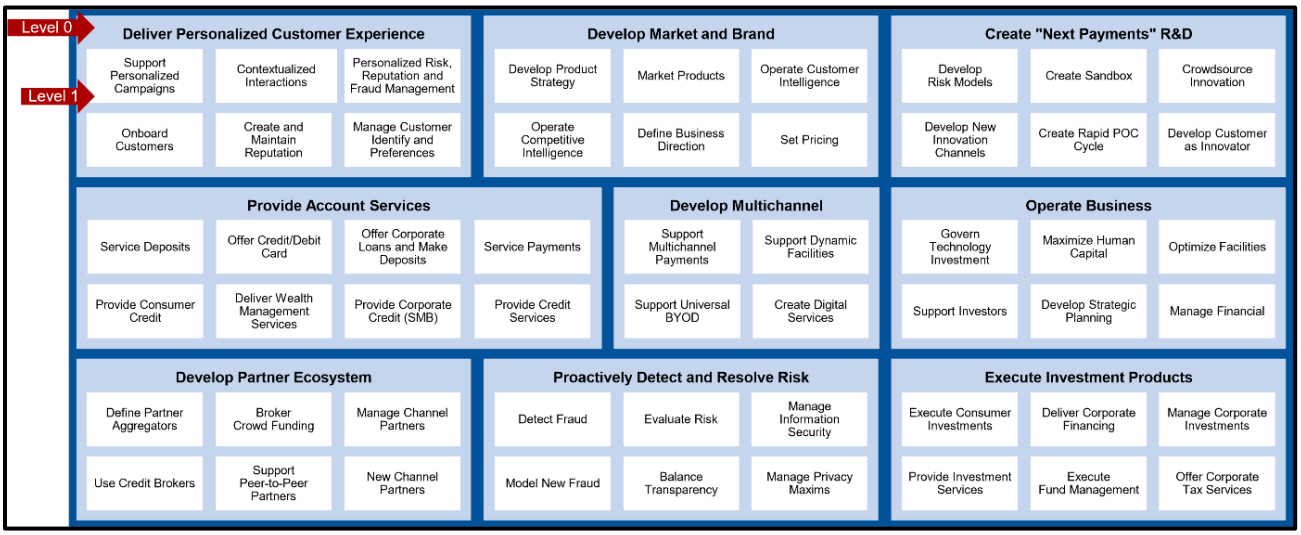



*Figure 12: CMMI (Capability Maturity Model Integration) process diagram.*

Mandated by the Under Secretary of Defense for Acquisition and Sustainment (OUSC(A&S)) for all Defense Industry Base (DIB) organizations to enhance the protection of Controlled Unclassified Information (CUI) and Federal Controlled Information (FCI) within the Supply Chain. (December 2021)

The Cybersecurity Maturity Model Capabilities (CMMC) was developed to judge your organization's ability to adhere to these new protection standards for obtaining and continuing business with the United States Government.

- The CMMC will review and combine various cybersecurity standards, best practices, and map these controls and processes across maturity levels that range from basic cyber hygiene to advanced. For a given CMMC level, the associated controls and processes, when implemented, will reduce risk against a specific set of cyber threats.
- The CMMC effort builds upon existing regulation (DFARS 252.204-7012), that are based on trust, by adding a verification component with respect to cybersecurity requirements.
- The goal is for CMMC to be cost-effective and affordable for small businesses to implement, at the lower CMMC levels.
- Authorized and accredited CMMC Third Party Assessment Organizations (C3PAOs) will conduct assessments and issue CMMC certificates to Defense Industrial Base (DIB) companies at the appropriate level.

## Information Assurance

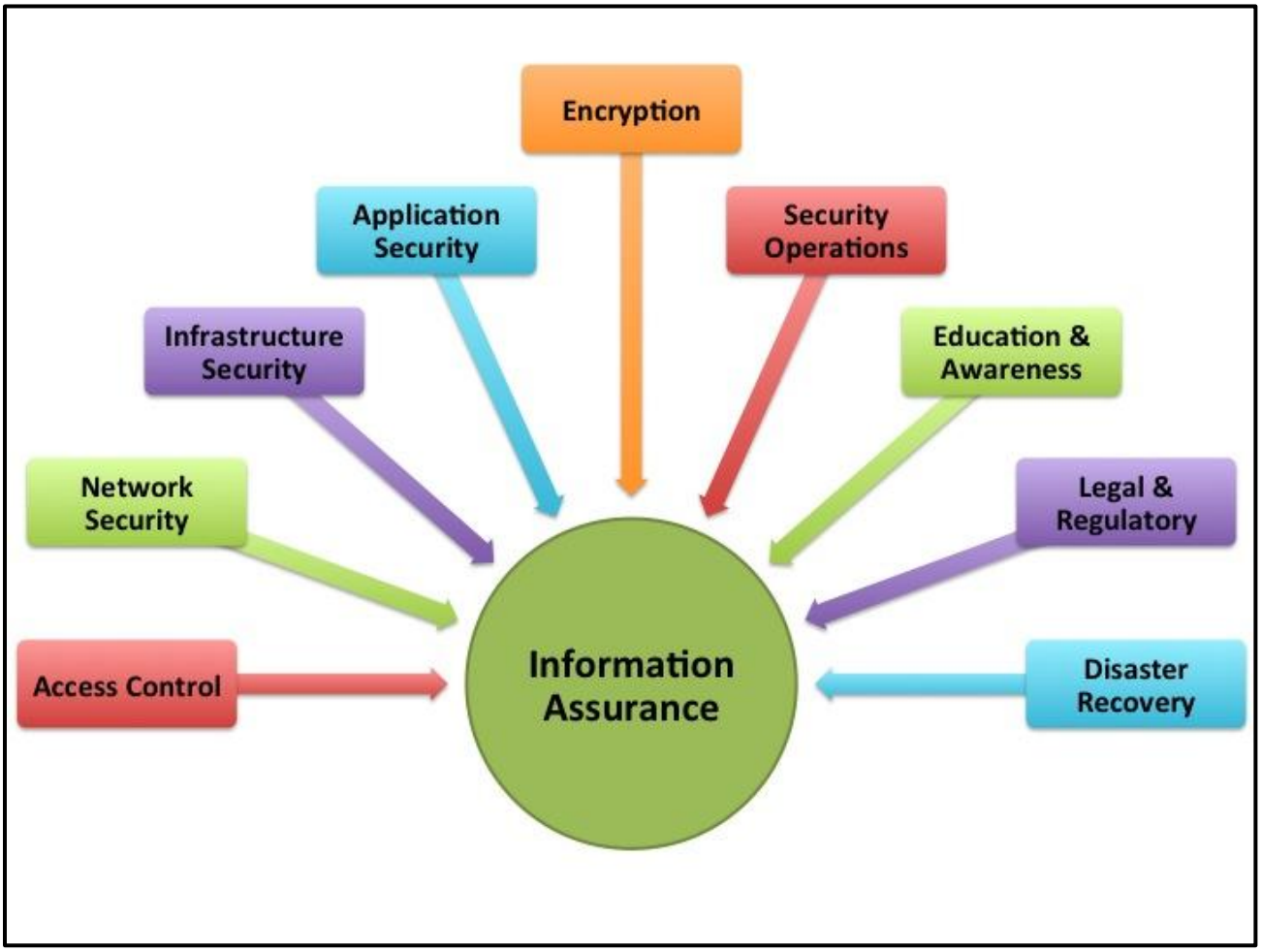



*Figure 13: Information Assurance validations and requirements.*

Information assurance (IA) is the process of processing, storing, and transmitting the right information to the right people at the right time.[1] IA relates to the business level and strategic risk management of information and related systems, rather than the creation and application of security controls. IA is used to benefit business through the use of information risk management, trust management, resilience, appropriate architecture, system safety, and security, which increases the utility of information to only their authorized users.

Besides defending against malicious hackers and code (e.g., viruses), IA practitioners consider corporate governance issues such as privacy, regulatory and standards compliance, auditing, business continuity, and disaster recovery as they relate to information systems. Further, IA is an interdisciplinary field requiring expertise in business, accounting, user experience, fraud examination, forensic science, management science, systems engineering, security engineering, and criminology, in addition to computer science.

## RMF – Risk Management Foundation


*Figure 14: RMF - Risk Management Foundation overview.*

A risk management framework is **a set of references and tools that decision-makers rely on to make decisions about how to manage risk**. It could include, for example, policies, strategies, plans, processes and models, and statements of your organization's position on risk.

What you have in your framework depends on two things:

- the risks, threats and challenges in your internal and external context.
- your organization's risk maturity.

## RMM - Risk Maturity Model

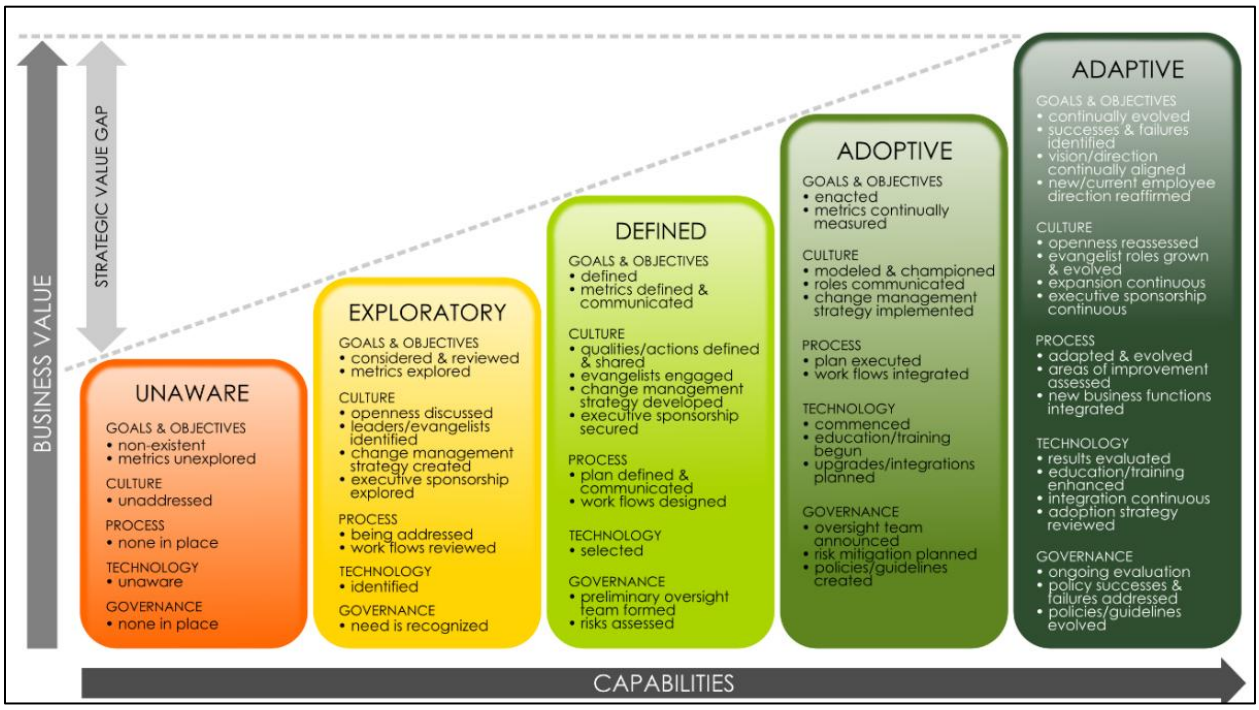
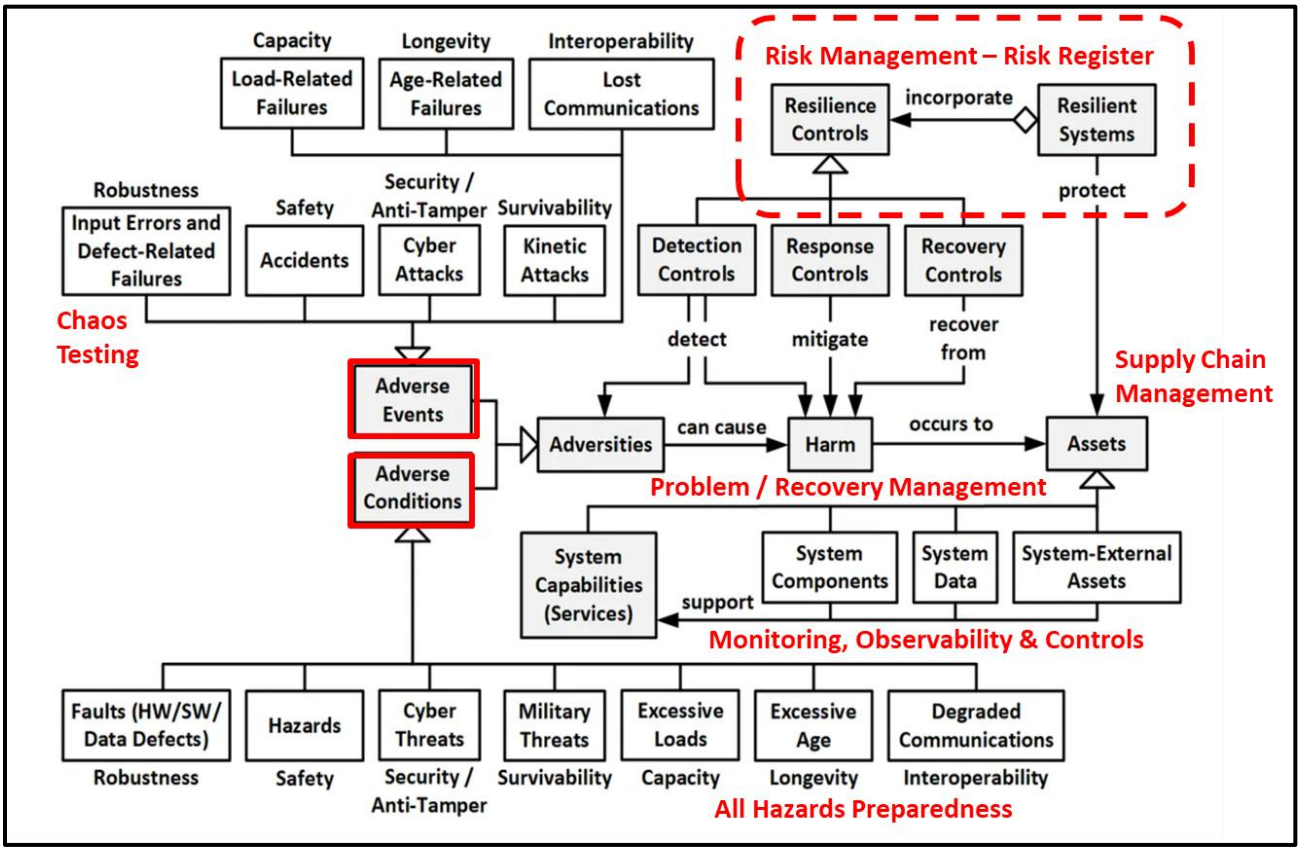



*Figure 15: Risk Maturity Model (RMM) phases.*

Review this Risk Maturity Model to determine where you presently are, then decide where you want to be and when. After discussion and agreement, set your goals and objectives within a clearly scoped project. Have management and stakeholders select a leader and assign a team. The leader and team will scope the work and define the phases and tasks to be performed, then define a project plan with devoted resources for time periods that have defined costs. Have project plans approved by management and allocate the budget required to conduct and support the project.

Every company should strive to achieve the best Risk Maturity Model deemed necessary to properly support customer and regulatory needs, while reducing the toil on staff and management alike.

## What is Risk and why is it so important to eliminate?




## ITIL – Information Technology Infrastructure Library

The IT Infrastructure Library (ITIL) is sometimes referred to as the ITIL foundation or the ITIL framework. Regardless of the language used to describe it, ITIL refers to the set of guiding principles IT service professionals use to standardize their processes. The article below answers the question “What is ITIL?” before examining its processes and why they are important to the IT industry.

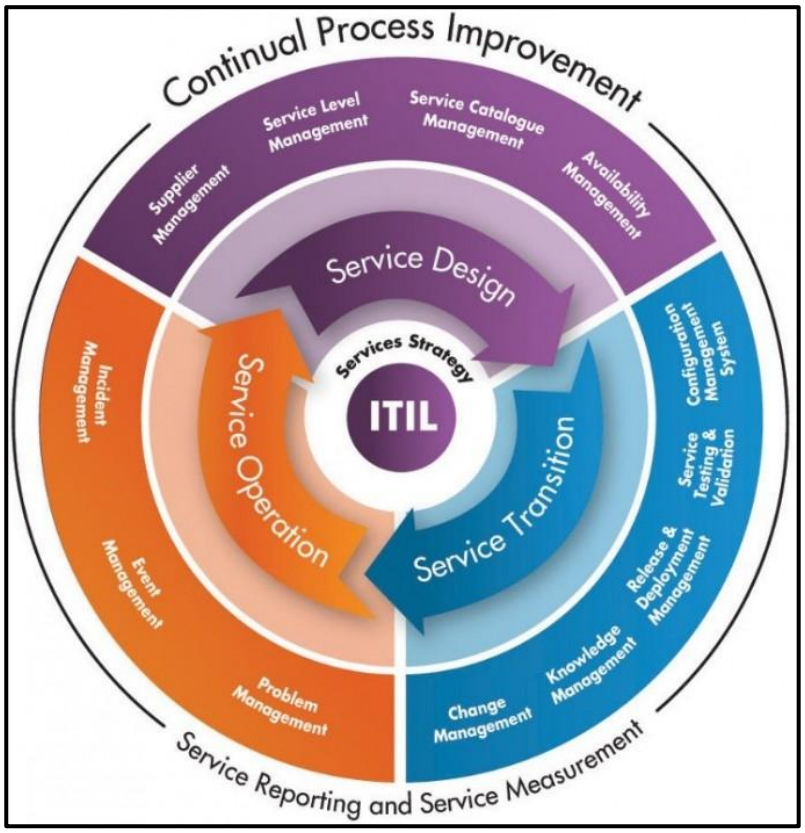
**What is ITIL?**

ITIL is a set of practices. Its primary purpose is to provide a systematic approach to IT service management (ITSM). Since its 1989 inception by the UK Central Computer and Telecommunications Agency, the ITIL framework has undergone revisions. Today, these revisions span four versions and five books. Each book contains guidelines surrounding the various processes and phases of the IT service lifecycle.

**ITIL benefits and use cases.**

Any organization can use ITIL, from small businesses in the US to large-scale enterprises abroad. It provides a flexible roadmap for organizations to follow when undertaking a digital transformation. There are more reasons a company may align their IT processes with the ITIL framework including:

- **Standardization**. As mentioned above, standardization is one of the primary goals of the ITIL foundation. ITIL helps create predictable IT environments, making it easier to manage risks, solve problems, and streamline processes.
- **Transparency.** Establishing a set of standards helps improve visibility in IT costs and operations. ITIL helps bridge the gap between departments by enabling IT admin to be front-end business service partners in addition to back-end support.
- **Cost-effectiveness.** The ITIL framework is designed to help organizations use their hardware and software resources as efficiently as possible.
- **Strategic alignment**. Like the DevOps methodology, the ITIL framework seeks to unite business operations and IT departments. Enhanced communication helps organizations better translate business strategies and goals into technical requirements.
- **Organizational change management.** The ITIL foundation includes the best practices for change management. With these guidelines, IT professionals can release changes without interrupting service.




See Link for more information.

*Figure 16: ITIL - Information Technology Infrastructure Library overview.*

## ServiceNow

ServiceNow is a **platform-as-a-service**, which allows for the operation of enterprise and technical management support systems, such as IT service management and help desk functionality. The company's core business revolves around management of "incident, problem, and change" IT operational events.

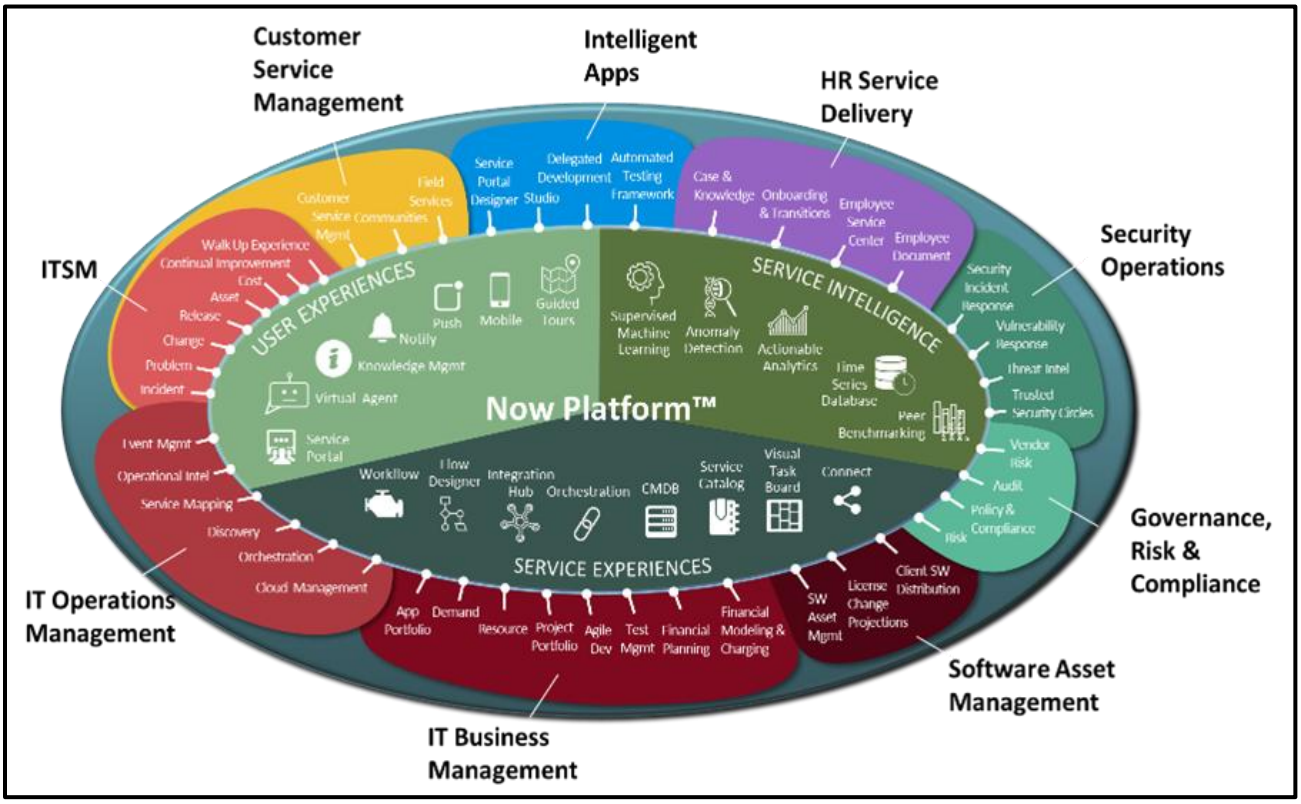



*Figure 17: ServiceNow Platform and Capabilities*

Businesses who are looking to reduce costs - and drive growth - **work with ServiceNow**, the intelligent platform for digital transformation. ServiceNow is not a system of record - but rather a system of action - a platform that sits atop organizations' existing data and systems, preventing the need to rip and replace those existing systems. With simple, easy-to-use interfaces that empower employees and customers, the ability to purposefully orchestrate and automate tasks and processes across their enterprise—that also extends to their ecosystems—to drive efficiency and optimization, using customizable, low-code tools that allow organizations to quickly scale and adapt to any force, ServiceNow is the only intelligent platform that empowers organizations to grow the top line while protecting the bottom line. ServiceNow helps companies take a platform and digital-first approach that creates a better organizational posture for today and drives efficiency and growth for the future. See Link for additional information.

You can consider ServiceNow as a Forms Management and Control System, which was previously the greatest loss of productivity in IT operations. Find the right form, learn what it means, complete it,

validate the fields, route the form for approval, forward to designated person, and have the work completed, communicate with worker, and track activity until completed and stored in an activity repository.

**Question:**

What would happen if the government declared another Covid Shut-Down, what would the staff do – Work from home? Do they have the connections and equipment to support ideation, collaboration, and innovative responses to emerging events and challenges? Should this be considered in our proposal?

## TOGAF – The Open Group for Architecture Framework

A proven approach to Enterprise Resilience is The Open Group Architectural Framework (TOGAF), which provides a roadmap to follow when looking to improve the operations of a company to better support the business.

Starting with an understanding of the business from a purely business perspective, TOGAF guides the practitioner through various evaluations and delivery pathways to develop and implement the most efficient environment achievable. Consistent monitoring and evaluation will result in continued excellence as new and improved technologies and business are incorporated.

An overview of TOGAF, and its phases, is provided in the following illustration. **Link to Details.** The TOGAF® standard is an open, industry consensus framework for Enterprise Architecture.

It is a foundational framework, which means that it is applicable to the development of any kind of architecture in any context. This foundational framework is supplemented by The Open Group TOGAF Library,[1] an extensive and growing portfolio of guidance material, providing practical guidance in the application of the TOGAF framework in specific contexts.

The TOGAF Standard, Version 9.2 is an update to the TOGAF 9.1 standard to provide additional guidance, correct errors, address structural challenges, and remove obsolete content. All of these changes will make the TOGAF framework easier to use and maintain.[2]

### The TOGAF documentation consists of a set of documents:

- The TOGAF standard which describes the applicable approach to Enterprise and IT Architecture
- The TOGAF Library, a portfolio of guidance material to support the practical application of the TOGAF approach.

There are six parts to this document:

- **PART I** - (Introduction) This part provides a high-level introduction to the key concepts of Enterprise Architecture, and particularly the TOGAF approach. It contains the definitions of terms used throughout the TOGAF documentation.

- **PART II** - (Architecture Development Method) This part is the core of the TOGAF framework. It describes the TOGAF Architecture Development Method (ADM) - a step-by-step approach to developing Enterprise Architecture.
- **PART III** - (ADM Guidelines & Techniques) This part contains a collection of guidelines and techniques available for use in applying the TOGAF approach and the TOGAF ADM.
- **PART IV** - (Architecture Content Framework) This part describes the TOGAF content framework, including a structured metamodel for architectural artifacts, the use of re-usable Architecture Building Blocks (ABBs), and an overview of typical architecture deliverables.
- **PART V** - (Enterprise Continuum & Tools) This part discusses appropriate taxonomies and tools to categorize and store the outputs of architecture activity within an enterprise.
- **PART VI** - (Architecture Capability Framework) This part discusses the organization, processes, skills, roles, and responsibilities required to establish and operate an architecture function within an enterprise.

## Utilizing Enterprise Architectural Techniques

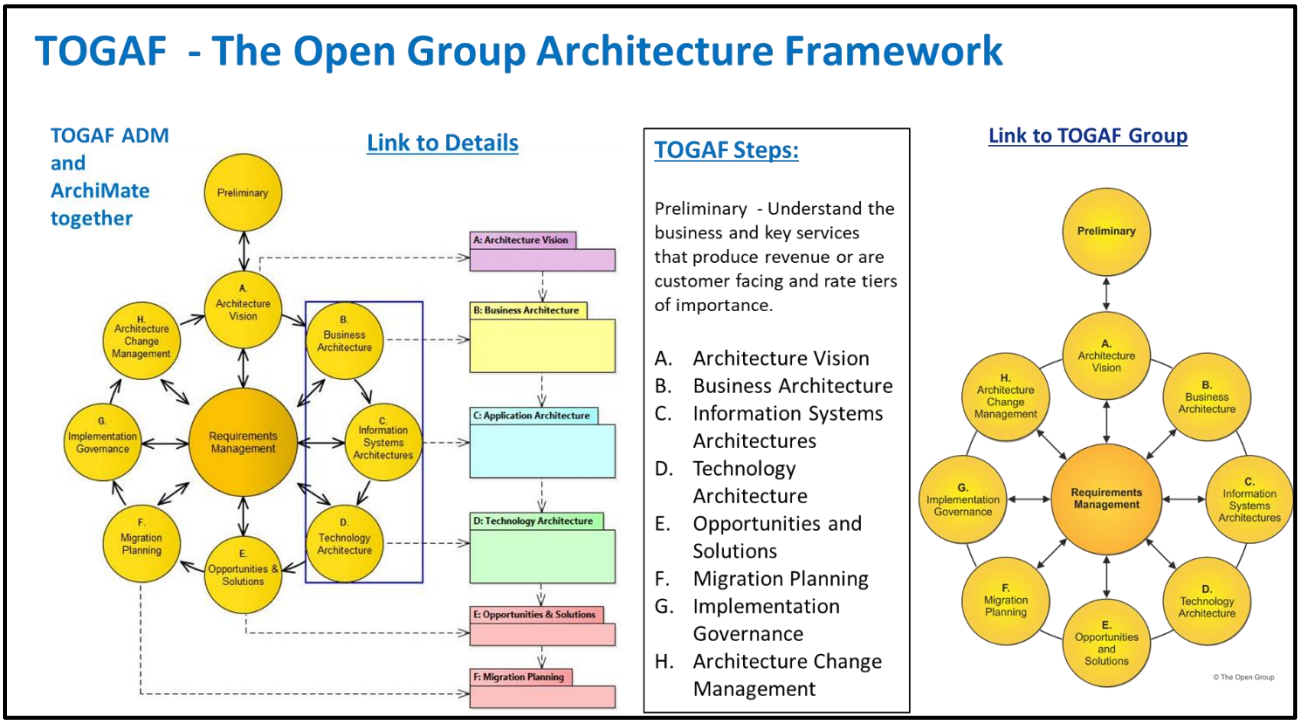



*Figure 18: Overview of The Open Group on Architecture Framework (TOGAF) process.*

### Phases within the TOGAF ADM (Applications Development Methodology) are as follows:

1. The **Preliminary Phase** describes the preparation and initiation activities required to create an Architecture Capability including customization of the TOGAF framework and definition of Architecture Principles.
2. **Phase A: Architecture Vision** describes the initial phase of an architecture development cycle. It includes information about defining the scope of the architecture development initiative,

identifying the stakeholders, creating the Architecture Vision, and obtaining approval to proceed with the architecture development.

3. **Phase B: Business Architecture** describes the development of Business Architecture to support the agreed Architecture Vision.
4. **Phase C: Information Systems Architectures** describes the development of Information Systems Architectures to support the agreed Architecture Vision.
5. **Phase D: Technology Architecture** describes the development of Technology Architecture to support the agreed Architecture Vision.
6. **Phase E: Opportunities & Solutions** conducts initial implementation planning and the identification of delivery vehicles for the architecture defined in the previous phases.
7. **Phase F: Migration Planning** addresses how to move from the Baseline to the Target Architectures by finalizing a detailed Implementation and Migration Plan.
8. **Phase G: Implementation Governance** provides an architectural oversight of the implementation.
9. **Phase H: Architecture Change Management** establishes procedures for managing change to the new architecture.
10. **Requirements Management** operates the process of managing architecture requirements throughout the ADM.

There are four architecture domains that are commonly accepted as subsets of an overall Enterprise Architecture, all of which the TOGAF Standard is designed to support:

1. **Business Architecture** defines business strategy, governance, organization, and key business processes,
2. The **Data Architecture** describes the structure of an organization's logical and physical data assets and data management resources,
3. The **Application Architecture** provides a blueprint for the individual applications to be deployed, their interactions, and their relationships to the core business processes of the organization, and
4. **Technology Architecture** describes the digital architecture and the logical software and hardware infrastructure capabilities and standards that are required to support the deployment of business, data, and applications services. This includes digital services, Internet of Things (IoT), social media infrastructure, cloud services, IT infrastructure, middleware, networks, communications, processing, standards, etc.

There are other domains that could be defined by combining appropriate views of the Business, Data, Application, and Technology domains. For example:

1. Information Architecture
2. Risk and Security Architectures
3. Encryption and Post-Quantum Cryptography
4. Digital Architecture

The TOGAF framework enables the creation of these multi-dimensional views and categorizes them to create specific domains that enable an enterprise to consider the wider scope of their enterprise and capabilities.

## TOGAF Capabilities Framework

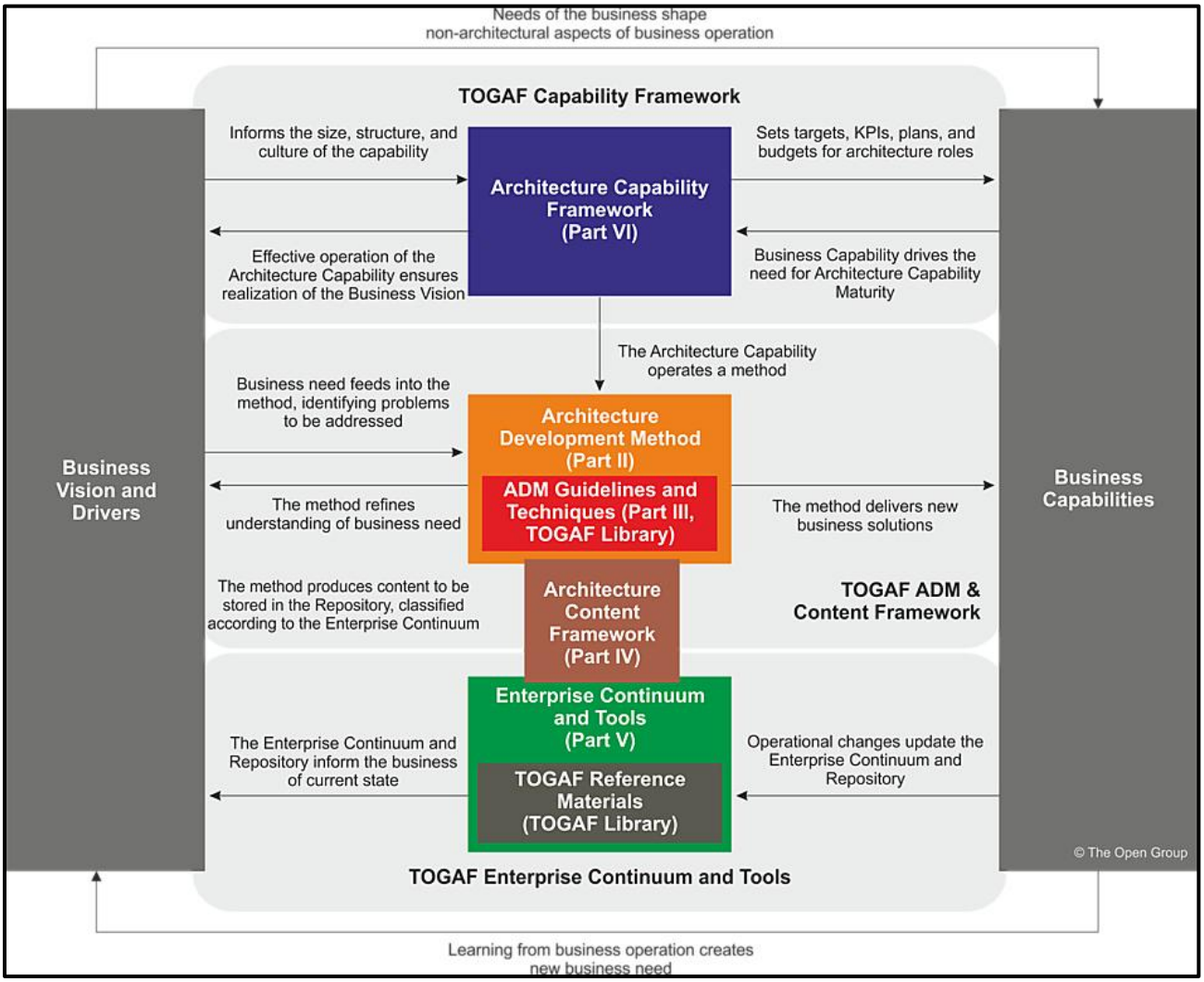



*Figure 19: TOGAF Capabilities Framework diagram.*

Click this link to review the detailed articles about the TOGAF Standard, Version 9.2.

The needs of the business feed this process (see COSO, and COBIT), then TOGAF Enterprise Continuum Tools and procedures are used to develop the right systems architecture to presently support the business. Continuous monitoring and improvement recommendations from Production Operations feed updates to TOGAF that build a new optimized, secure, and compliant environment.

## TOGAF Capabilities Planning and Usage

Working with TOGAF incorporates Business Planning with Enterprise Architecture, Operations Management, and Portfolio / Program / Project Management in the Development / Maintenance

environment, with Architecture Governance and Project Management Guidelines to provide input to the Solutions Development group.

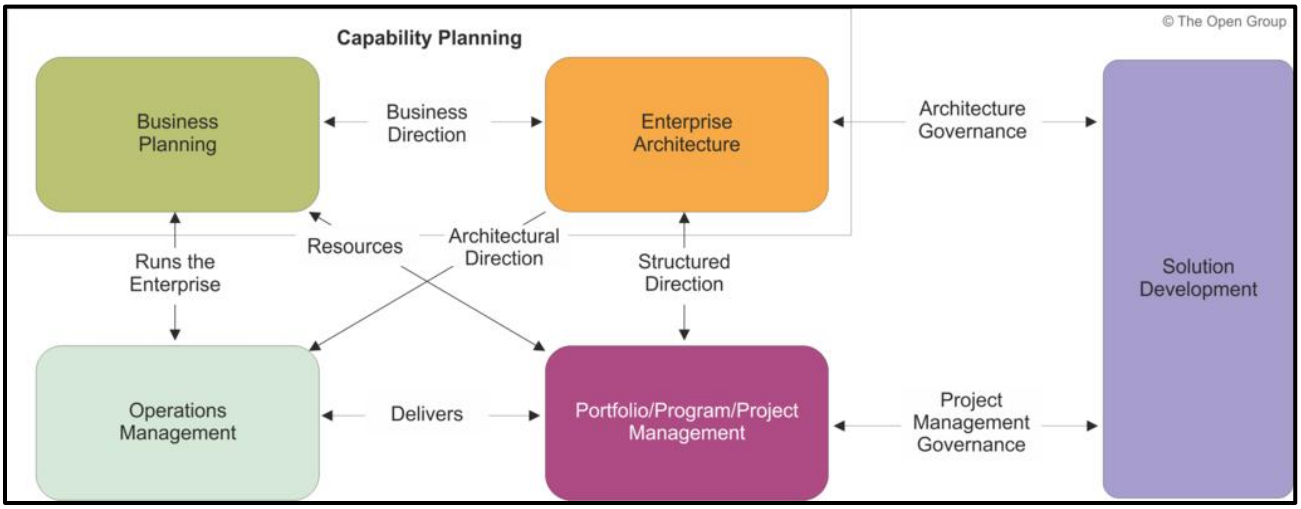



*Figure 20: Enterprise Capability Management via TOGAF*

## ArchiMate 3.0 Specification

ArchiMate is a programming product that assists in creating TOGAF sources and modeling. It provides high-level language design and modeling tools that can display architectural views of applications and simplifies the application architecture process. The open-source modelling toolkit for creating ArchiMate models and sketches. Used by Enterprise Architects everywhere.

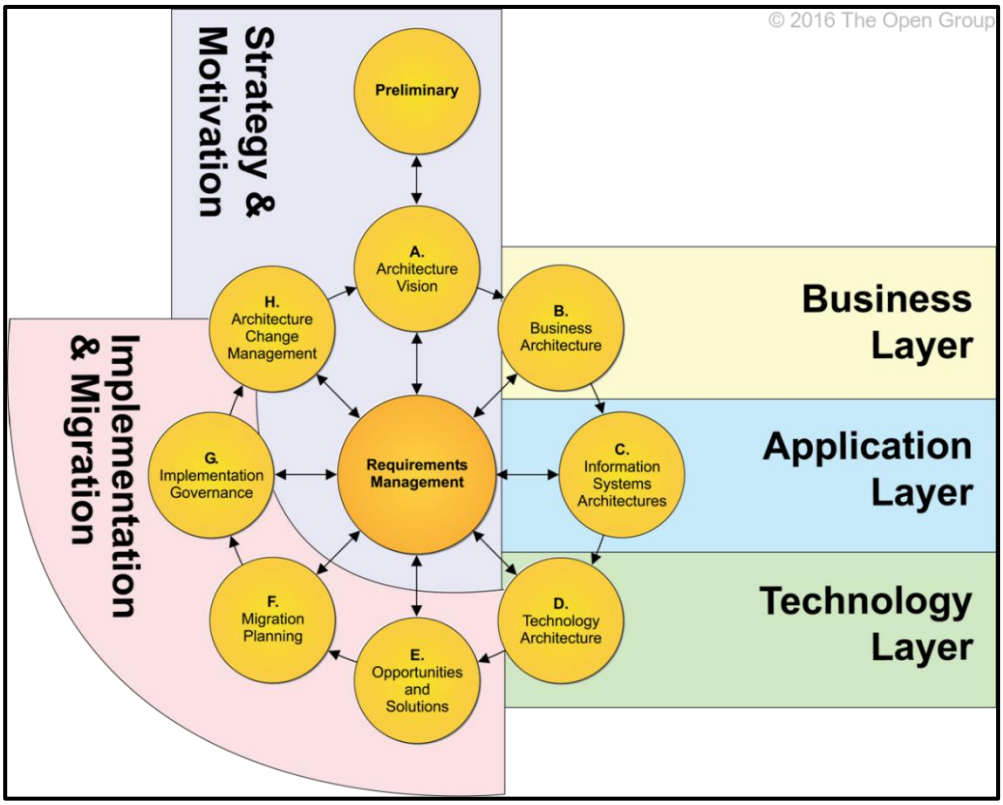
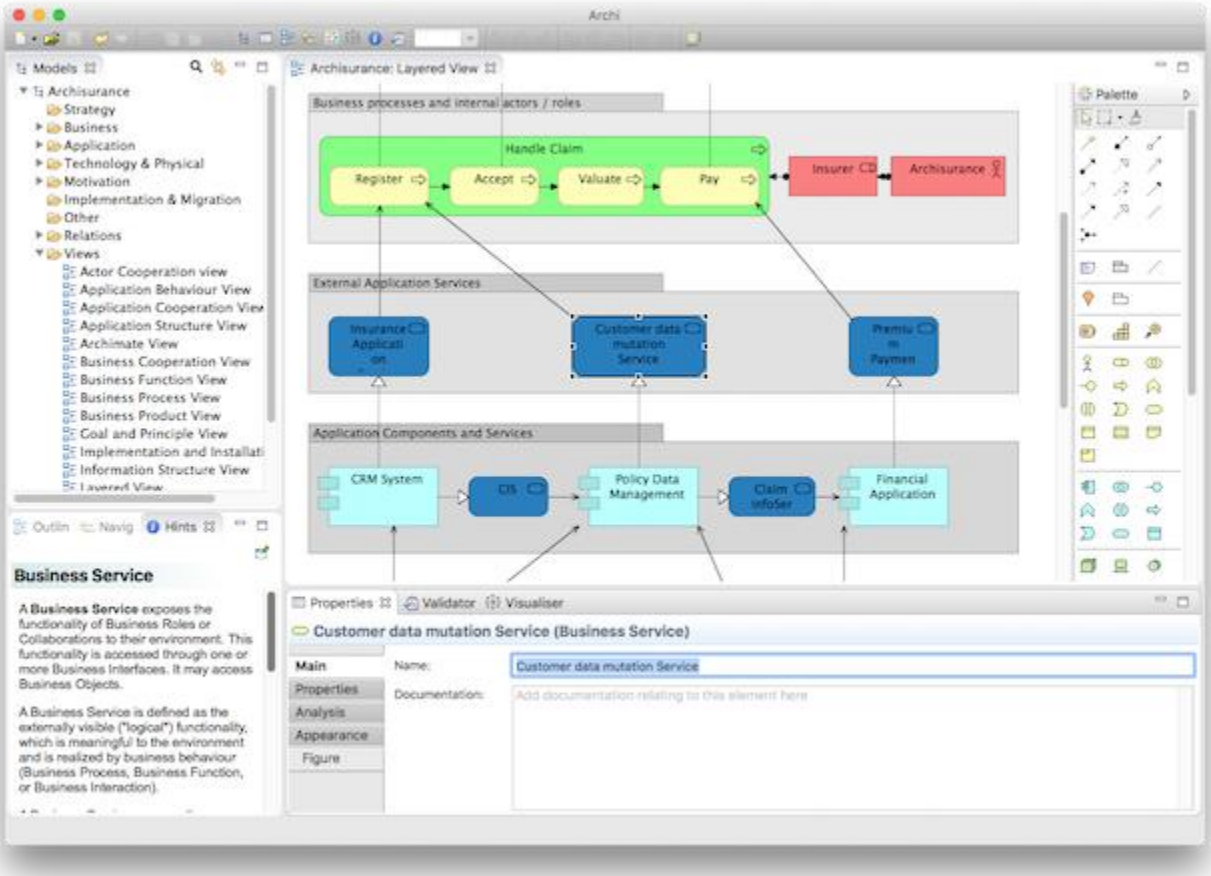



*Figure 21: ArchiMate 3.0 Overview diagram!*

Easily and intuitively create all ArchiMate elements and relations in all the ArchiMate views. Use the magic connector to create the correct connections between ArchiMate concepts. Refine your model with user-defined properties and colorize your diagram with your own color scheme.

## ArchiMate Layer view




The ArchiMate tool assists TOGAF engineers gather and control the information they use to develop systems architectures based on business needs. It can simplify the process and reduce costs, while maintaining a repository of Architecture Development information that can be maintained and improved over time.

## Creating an IT Operations environment from Development through Production

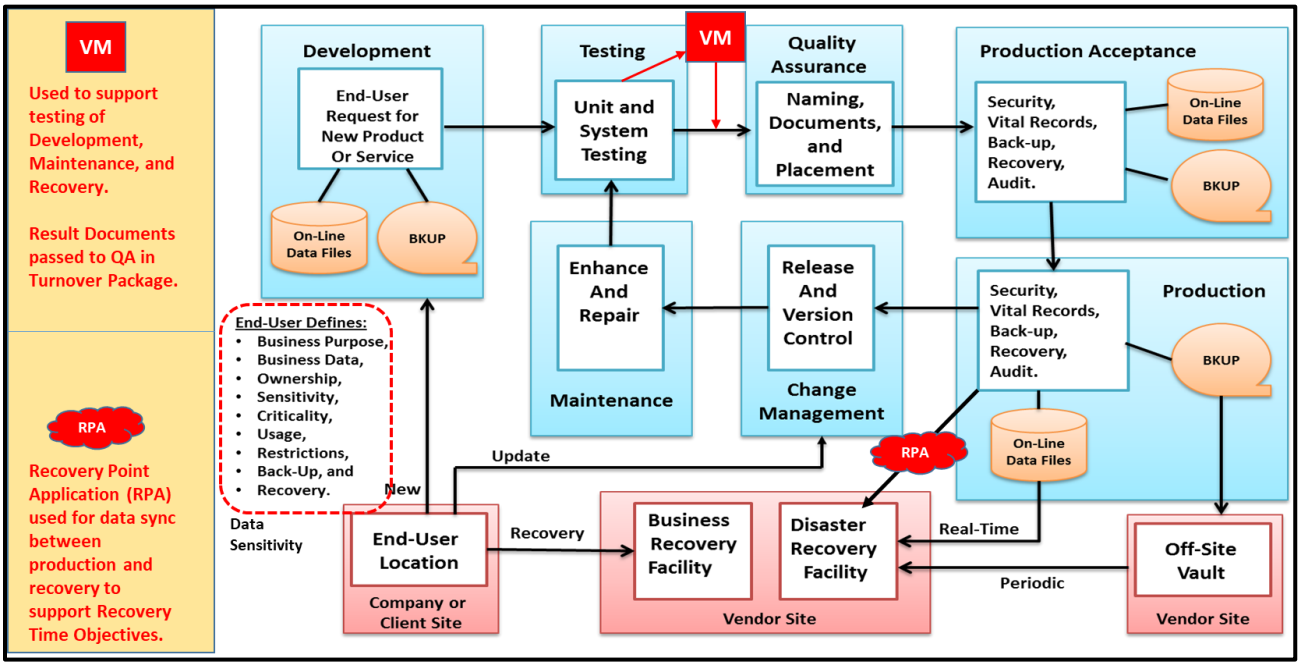



*Figure 22: Systems Development Life Cycle between Development and Production*

When a new application is being entered into the Development process, the initial steps to be performed consist of:

**Application and Data Sensitivity** – To define the criticality of the application and its data, a Sensitivity Analysis is performed to define.

- **What** is the Business Process associated with this application?
- **How important** is the application to the company's success?
- **What is the data** used by the application?
    - how is data named and classified (data credentials),
    - who owns the data and what is their contact information,
    - who can use the date (Group) and under what conditions (Create, Read, Update, Delete – CRUD),
    - when should the data be backed up (Continuously Available, High Availability, Incremental Availability, etc.),
    - how long does it take to restore (Recovery Time Capability – RTC),
    - does the data require encryption (at Rest and in Transit) and vaulting,
- **does the application support** a remote location, and will the application be required at the recovery site as well as the production site, and
    - should the data be copied to the application recovery environment?
    - How do you synchronize the data between sites (Production and Recovery)

**Development** – When the application is built. Initially the process will include a:

- **Business Review** to define operation, ownership, criticality, and effort to construct.
- Then a **technical review** is performed to define the tasks needed to build the application, the resources needed, and the time and costs for developing the application.
- **A meeting** is then conducted to determine if the product should be developed in-house or purchased as a Commercial Off-The-Shelf (COTS) application and
- **a Go/No-Go** decision is made.

After Development, the product must go through rigorous testing, which includes:

- **IV&V** – Installation Validation and Verification (all necessary components are included)
- **Regression** – the application can still perform past functions.
- **IA** (Information Assurance) – to validate the security and compliance of the application.
- **Chaos Testing** – related to cloud-based applications and used to run problem simulations and exercise the application under stressful conditions. Train the application team on distinct types of problems and develop a problem recovery manual with a list of problem experiments and their results (Problem Symptoms, Possible Causes, Root Cause Analysis techniques, Steps followed to solve the Problem or Incident).
- **User Acceptance Testing (UAT)** – to prove to the user that the applications perform as expected with all features and functions requested.
- **Production Acceptance Testing (PAT)** – to prove to Production Operations that the product functions as desired and meets all IT Operations requirements, including Vital Records Management and Version and Release Management.
- **Game Day Testing** – Full shake-out test of application by users and the operations team to validate operation, instructions, and documentation.
- **Production Operations** – Running of the application in the production environment.
- **Production Support** – responsible for repairing all technical problems and cybersecurity incidents that may be encountered, usually divided into a Help Desk for technical problems and a Security Operations Center (SOC) for cybersecurity incidents.
- **Change Management** – occurs when new releases and enhancements are introduced, but also to correct encountered error conditions that may require a software / hardware update (Patch, Engineering Change, etc.). When Changes are introduced, they will go through a Version and Release Management change to update the version or release associated with the product. All material related to the change must be of the same Version and Release level.
- **Vulnerability Management** – for release and patch management to remove CVEs and CWEs.
- **Vital Records Management** – is responsible for handling vital data files and safeguarding the data contents of these files, including data backup / recovery and vaulting (air gaps between vault and system to eliminate virus and malware introductions).
- **Recovery Operations** – Should a site experience a disaster event, or an application have a disaster event requiring a recovery operation at an alternate site. Recovery Management is performed in the cloud differently than in Silo. Cloud recovery is faster and more flexible because assets are readily available through the cloud provider and the staff does not have to travel to a recovery facility, load data onto allocated assets (if available) and start applications.

## Integrating Business Continuity and Disaster Recovery into the Development and Maintenance cycles

To best safeguard a company from encountering disaster events and to ensure the continuity of business that executives are responsible for. To achieve this it is important to develop a comprehensive Business Continuity Management organization that will examine potential disaster events, cybercrimes, problem events, cyber incidents, and risk exposures to determine best practices to protect the organization. Once these decisions have been made by defining the most important services, functions, and applications, that produce revenue to keep the business running or are customers facing that need to be protected to safeguard the company brand, a rating of applications and services can be created.

One of the most essential steps in developing a Business Continuity Plan is to first protect data, so that it can be backed up and recovered should a disaster occur. There are static data files (like programs, and training manuals, or standards & procedures) and dynamic files (like data received from upstream jobs or feeds and data produced for downstream usage). Both file types are categorized, labeled, and must adhere to a predefined life cycle and retention period. This process is called Vital Records Management.

Data recovery is asynchronous for Continuously Available Application that require immediate recovery, or synchronous for “highly available” applications that require incremental data backups to adhere to their RTO and RPO objectives. Applications should be evaluated to determine their Recovery Time Objective (RTO) and current Recovery Time Capability (RTC) and then improved if RTC is not capable of meeting RTO objectives. Vaulting of Vital Records should include an Air Gap between the vaulted data and the IT Systems to eliminate potential malware and virus infections and guaranty data integrity.

Utilize Immutable Data techniques to further protect vaulted data, where immutable data is safeguarded against changes or hacker attacks.

## Resiliency Patterns and Groups

### Resilience Patterns and Recovery Groups

| 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<br>2. No multi-region **INFRASTRUCTURE**<br>3. **APPLICATION** code only available in single region<br>4. Multi-region **RECOVERY** not supported | 1. **TRANSACTIONAL TRAFFIC** - handled by primary region only<br>2. **INFRASTRUCTURE available on stand-by**<br>3. **APPLICATION** provisioned, but in shutdown state | 1. **TRANSACTIONAL TRAFFIC** - handled by primary region only<br>2. **INFRASTRUCTURE available on standby**<br>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<br>2. **INFRASTRUCTURE always available in both regions**<br>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<br>2. **APPLICATION CODE** maintaned for currency in **BOTH REGIONS**<br>3. Operate Production from stand-by region periodically | 1. Maintain **PERSISTENT DATA REPLICATION** infrastructure<br>2. **APPLICATION CODE** maintaned for currency in **BOTH REGIONS**<br>3. Operate Production from stand-by region periodically | 1. Maintain **2-WAY PERSISTENT DATA REPLICATION**<br>2. **APPLICATION CODE** maintaned for currency in **BOTH REGIONS**<br>3. Operate Production from stand-by region periodically |
| Recovery Steps | 1. **ACQUIRE INFRASTRUCTURE**<br>2. **BUILD OU**T infrastructure<br>3. **DEPLOY** application<br>4. **RECOVER / RECREATE DATA**<br>5. **REDIRECT TRAFFIC** to region 2 | 1. **SCALE INFRASTRUCTURE**<br>2. **STARTUP** application<br>3. **FAILOVER TRAFFIC** | 1. **AUTO- SCALE INFRASTRUCTURE**<br>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) |
| | | Preferred Patterns | | |

*Figure 23: Separating Applications into Resilience Group by Importance, RTO, and RPO*

Classifying applications into Recovery Groups (RG) based on their relative importance and their Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO).

Since we are proposing a solution to a government facility, we should be aware of the “Whole of Government” approach to recovery management as shown in the next illustration. I am not sure If we are required to provide a “Whole of Government” recovery approach, so it should be asked as a question to the RFP provider.

## Continuity of Government guidelines


| Acronym | Definition |
|---|---|
| CGC | Continuity Guidance Circular |
| COG | Continuity of Government |
| COOP | Continuity of Operations |
| CWG | Continuity Working Group |
| DHS | Department of Homeland Security |
| ECG | Enduring Constitutional Government |
| EMAC | Emergency Management Assistance Compact |
| EO | Executive Order |
| FCD | Federal Continuity Directive |
| HSEEP | Homeland Security Exercise and Evaluation Program |
| MOA/MOU | Memoranda of Agreement/Memoranda of Understanding |
| NEF | National Essential Function |
| PPD | Presidential Policy Directive |
| SLTT | State, Local, Tribal and Territorial |

*Figure 24: Whole Government recovery groups and guidelines.*

Government guidelines for protecting the Whole of Government. We may have to consider these points when submitting our proposal.

## Eight Practical Steps to Building a More Risk-Aware and Resilient Culture

The following are eight steps that executives and managers tasked with leading organizational resilience should take to create cultural excellence:

1. **Learn what is critical** to your customer and how your organization can best deliver services that respond to the critical needs of the client.
2. **Connect resilience** to your strategic priorities as a response to the RFP.
3. **Readjust priorities** best match the clients' needs and ensure adaptability to changing customer needs when challenges arise that were not previously planned for.
4. **Expand and deliver** the value perception, so the customer has confidence that we can deliver today and in the future no matter what crisis may occur, or unforeseen event arise.
5. **Integrate into the strategic decision process** to eliminate potential liabilities and provide genuine business value.
6. **Make resilience everybody's role**. Integrate resiliency within the everyday functions performed by personnel through better products, procedures, guidelines, training, and automated standards and procedures.

7. **Measure your progress.** Start with a benchmark on current performance and track trends when changes and improvements are made to ensure our efforts have a positive impact on business value.
8. **Communicate** to all levels of the organization by defining the information, format, and frequency of reports to be distributed to Executive, Senior, and Direct Line Management, as well as project managers, team members, and stakeholders.

**Measurement of ROI**

**Customer Impact:**

- Customer satisfaction
- Issue response and resolution times.
- Reduced number of escalations
- Bolstered brand perception/equity.

**Operational and Executive Engagement**

- Board and executive engagement.
- Team engagement
- Decision outcomes
- Market / competitive awareness

**Efficiency**

- Reduced cost of distribution.
- Reduced regulatory penalties.
- Reduced legal, audit, and insurance costs.
- Decreased customer restitution (SLA adherence).
- Frequency of Issues.
- Productivity improvements.
- Cost maintaining legacy systems eliminated or reduced.

Building a more risk-aware and resilient culture helps you more closely monitor signals in your operating environment – market, regulatory, competitive, third party, finance, operations – enabling you to take a proactive approach in resolving issues before they become a crisis The development of a resilience culture can be today's boon of productivity for organizations – delivering continuity of business operation, business expansion, and operational optimization. A resilience culture will produce a tangible return on investment, including:

**Real-Time Risk-Based Decisions**

When you free insights that were stuck in siloed systems, spreadsheets, and documents, that data can now be leveraged to create a single operating view of the entire organization.

**Improved Prioritization**

Better understanding of what matters eliminates redundancy, streamlines your business, and simplifies your operations by understanding the dependencies and critical elements of every process.

**Improved Risk Mitigation**

Building a more risk-aware and resilient culture helps you more closely monitor signals in your operating environment – market, regulatory, competitive, third party, finance, operations – enabling you to take an initiative-taking approach in resolving issues before they become a crisis.

**More efficient and Effective Teams**

Through more risk-aware and resilient operations, you gain an understanding of the current level of utilization, where teams are bogged down, processes that need more investment, or where approaches can be consolidated. Your team benefits from clarity on single points of failure and course correction before it is too late.

The pandemic has taught us much about the importance of operational resilience. Technology is an essential tool in your culture transformation efforts. Organizations that were caught unprepared by the recent global crisis are newly focused on the importance of building risk-aware and resilient operations.

## Safeguarding the Environment via ISO and NIST Standards

The ISO (International Standards Organization) is a world-wide standards organization that provides internationally approved guidelines, while the NIST (National Institute of Standards and Technology) provides nationally approved standards. Combining the two provides a global approach to safeguarding the enterprise with the best practices accepted globally. Countries, or industries, may have their standards that must be adhered to as well. Be sure to check if applicable.

An ISO Integration model is provided, along with an overview of the Risk Management Framework using NIST guidelines for your review. These models will provide a road map for achieving an optimized, safeguarded, and compliant environment for your enterprise to thrive.

## Integrating ISO Safeguards within the IT Environment

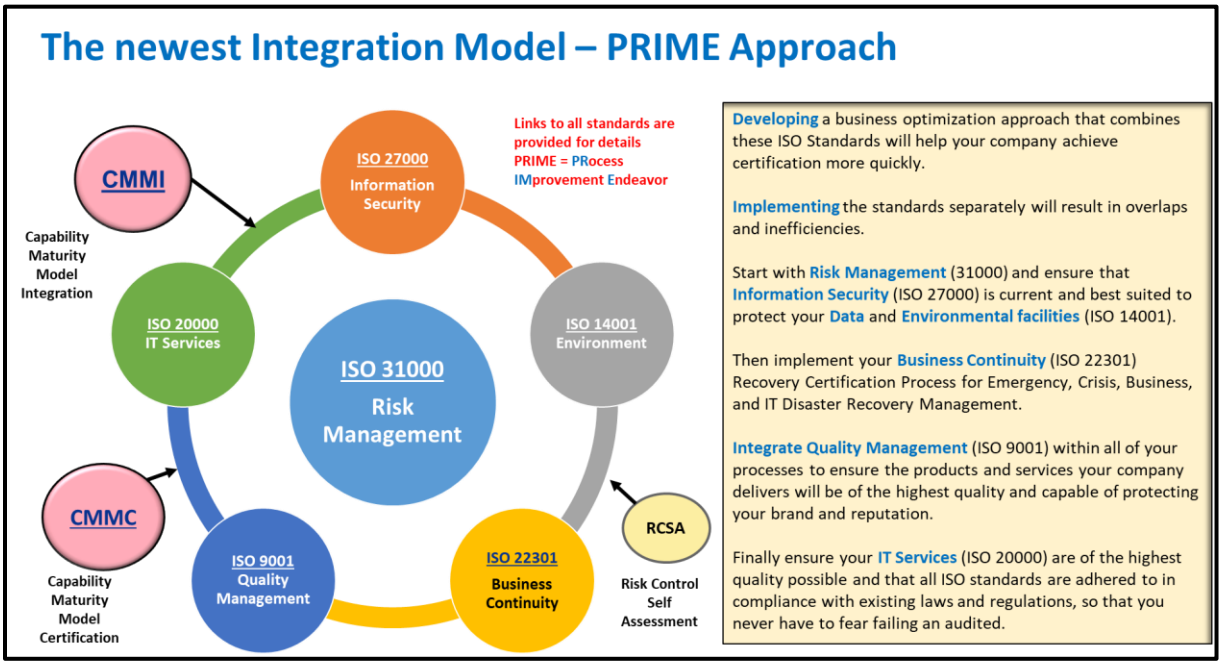



*Figure 25: Integrating ISO Guidelines via PRIME Process Improvement Endeavor*

## NIST Risk Management Framework

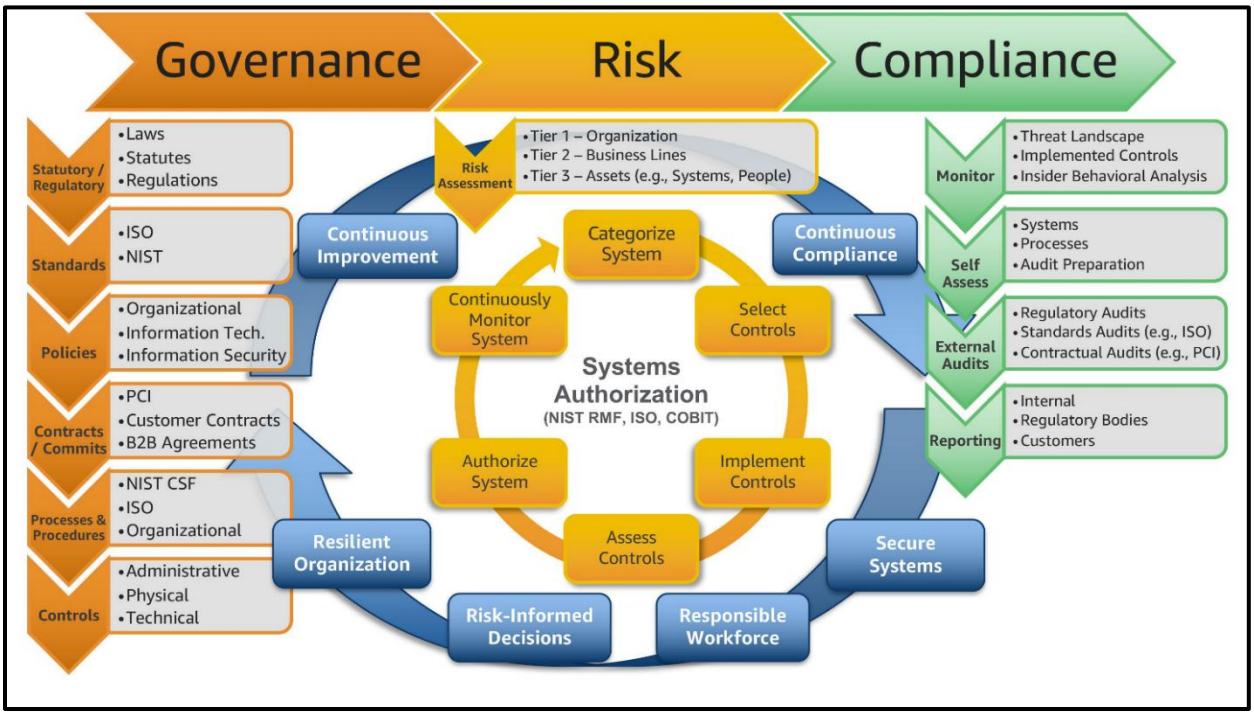



*Figure 26: NIST - Risk Management Framework overview.*

A complete list of NIST Standards provided by the National Institute of Standards and Technology can be found via this link. It is searchable by category of specific NIST Standard.

## CSE – Controlled Service Environment

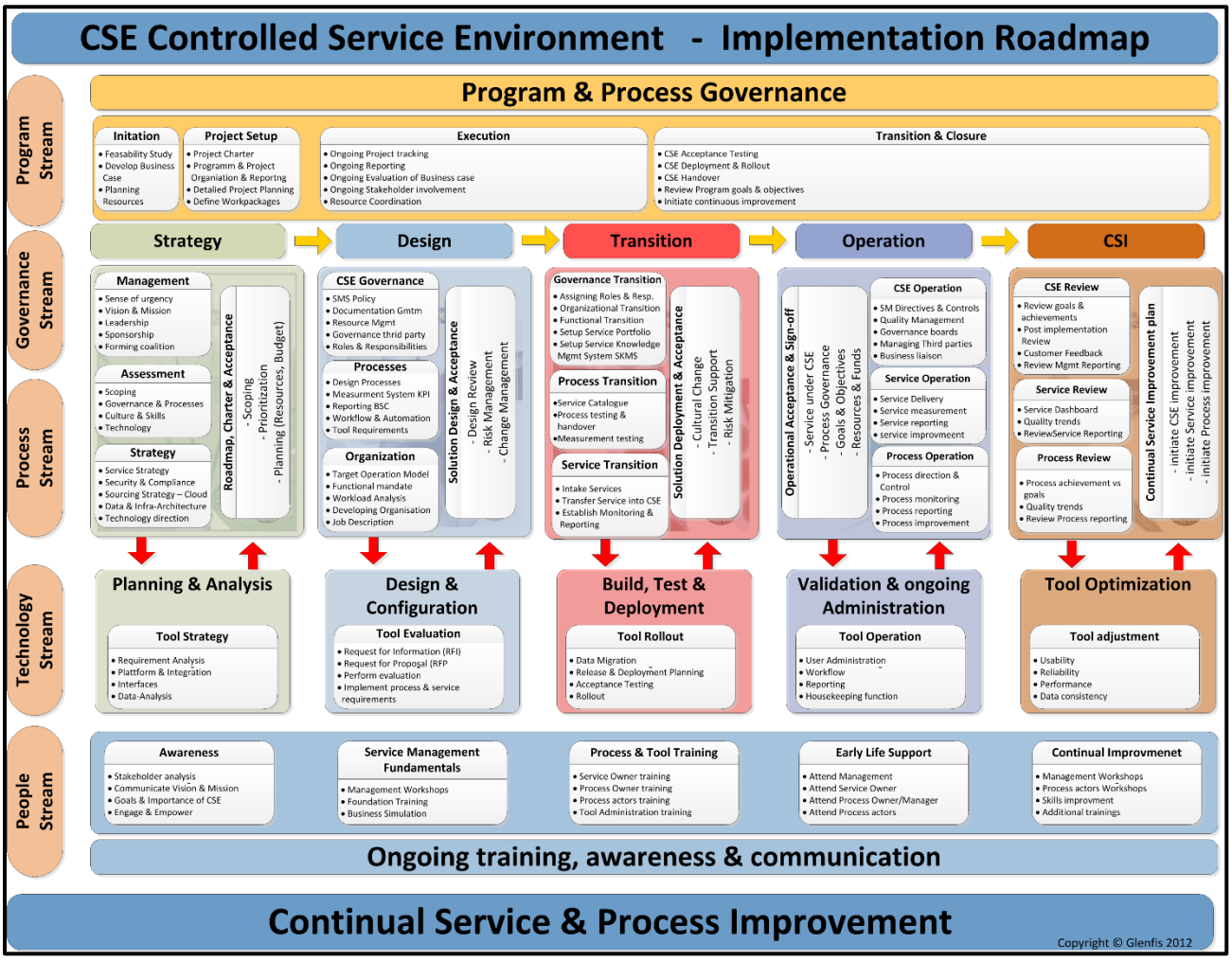



*Figure 27: CSE - Controlled Service Environment overview.*

Process improvement is a methodology within project management (See PMBOK – Project Management Book of Knowledge) that helps you take in and evaluate feedback about your processes to ensure continual improvement. It is a temporary or short-term endeavor designed to improve the process and result in improved performance in a key performance indicator of the business. There are five key actions that, when implemented correctly, can increase the odds of a smoothly run process improvement project that ends with breakthrough results. These are:

1. developing stakeholder relationships,
2. establishing sound ground rules,
3. applying proper facilitation skills,

4. incorporating improvement methodologies within the project, and
5. utilizing powerful testing procedures within every project

## Incorporating Disaster Recovery into the JIRA/Agile Life Cycle

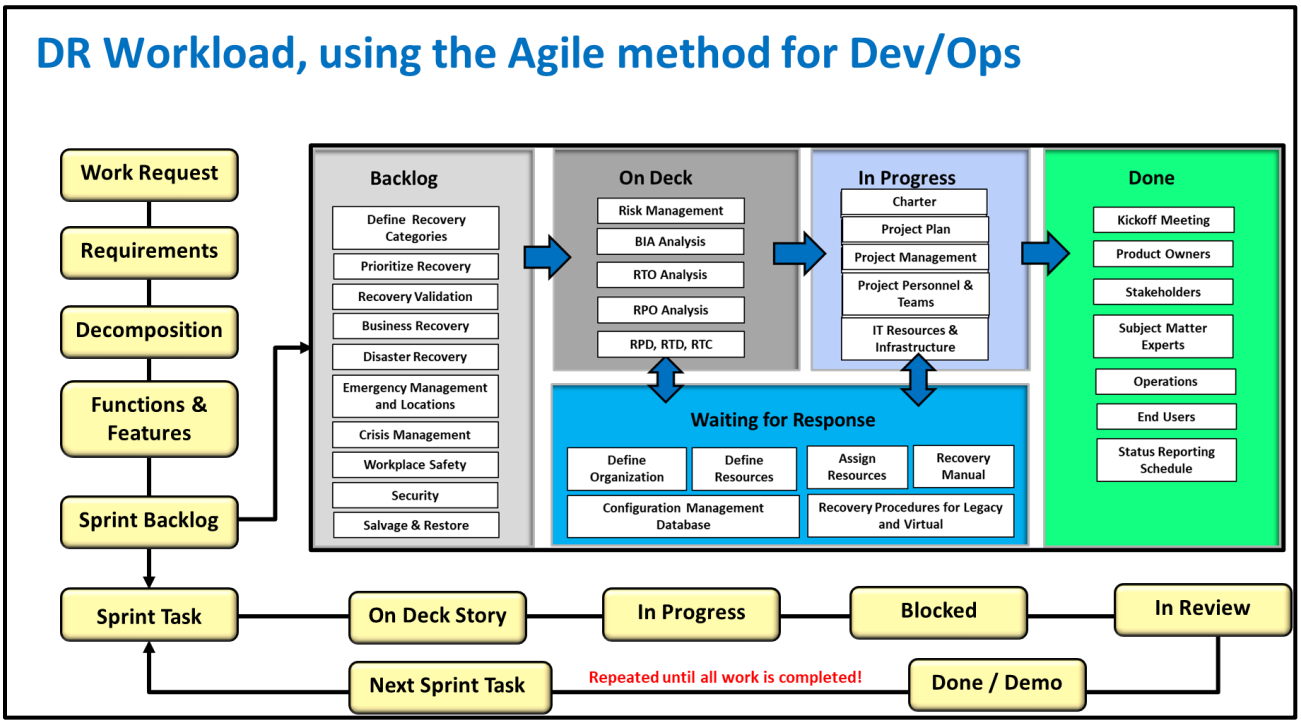



*Figure 28: DR Stories and JIRA / Agile for Dev/Ops*

The above diagram illustrates the Business Continuity Management (BCM) steps necessary to provide Application Recovery Certification through the KANBAN process within the JIRA / Agile SCRUM methodology.

## Jira / Agile SCRUM Methodology

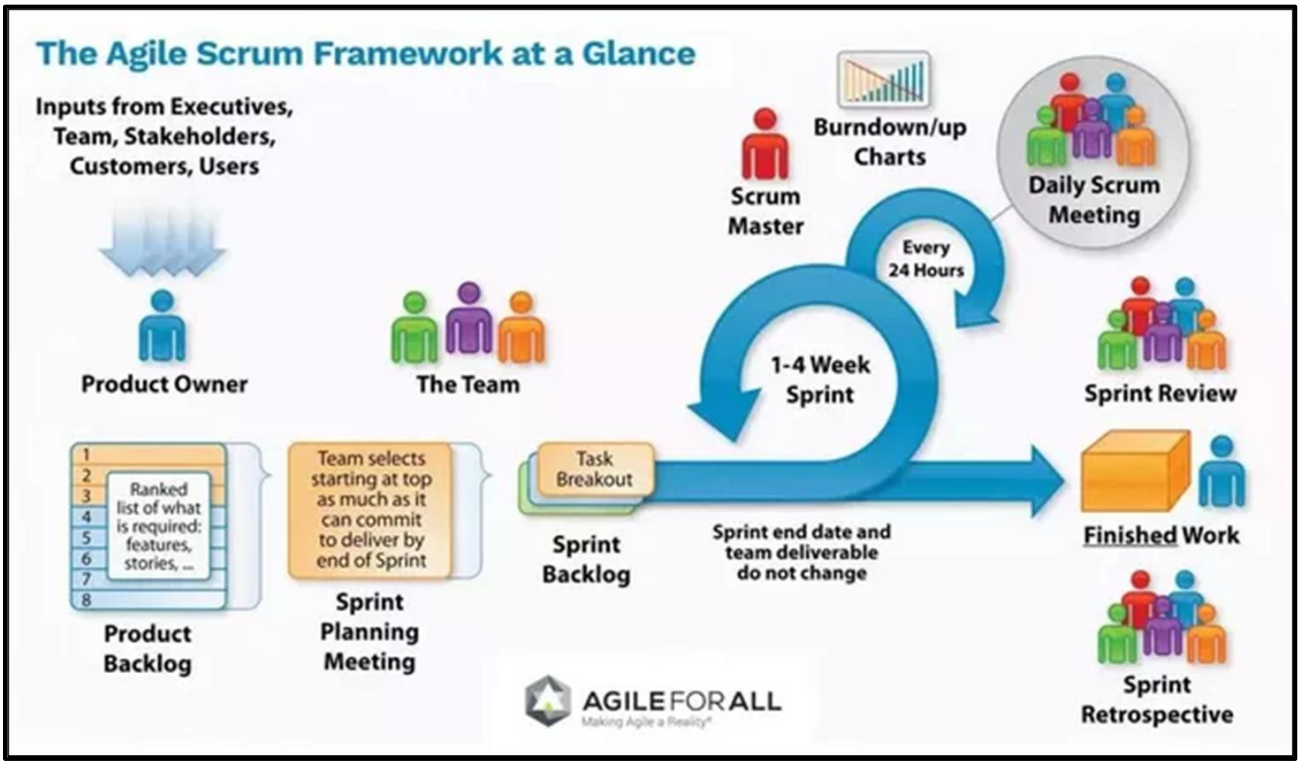



*Figure 29: JIRA, Agile, SCRUM Methodology overview.*

## Building and Implementing an Application

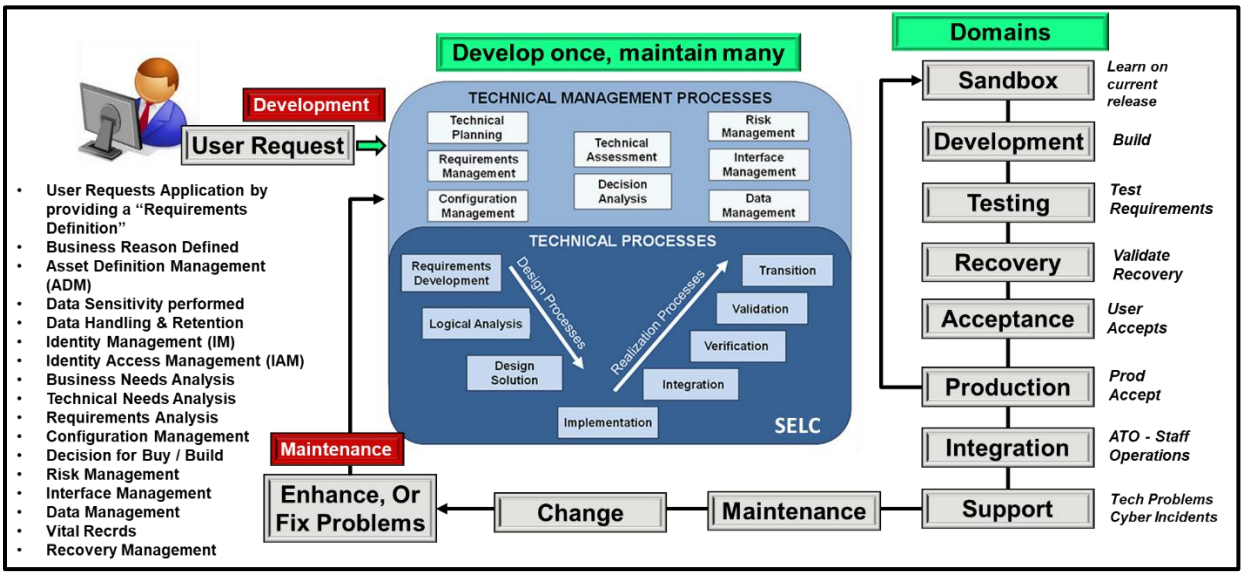



*Figure 30: Building and Implementing Applications using SELC and SDLC*

## Cybersecurity Framework

The illustrations below will help you understand the Cybersecurity Framework used to integrate the five-step cyber incident response process of:

1. Governance
2. Identify (ID)
3. Protect (PR)
4. Detect (DE)
5. Respond (RS), and
6. Recover (RC)

| Function | Category | Category Identifier |
|---|---|---|
| Govern (GV) | Organizational Context | GV.OC |
| | Risk Management Strategy | GV.RM |
| | Roles, Responsibilities, and Authorities | GV.RR |
| | Policy | GV.PO |
| | Oversight | GV.OV |
| | Cybersecurity Supply Chain Risk Management | GV.SC |
| Identify (ID) | Asset Management | ID.AM |
| | Risk Assessment | ID.RA |
| | 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) | Continuous Monitoring | DE.CM |
| | Adverse Event Analysis | DE.AE |
| 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 |

*Figure 32: Cybersecurity Framework Operation*


*Figure 31: Cybersecurity Framework integration*

The process of reviewing and implementing a Cybersecurity Framework is shown above. Refer to the NIST publication regarding Cybersecurity Framework for detailed information via this Link.

This NIST Cybersecurity Framework (CSF) 2.0 Reference Tool allows users to explore the **Draft** CSF 2.0 Core (Functions, Categories, Subcategories, Implementation Examples). The Tool offers human and machine-readable versions of the draft Core (in JSON and Excel). It also allows users to view and export portions of the Core using key search terms.

Aspects related to the presentation and functionality of this Tool are still under development. Informative References will be added once CSF 2.0 is finalized in early 2024, which will help to show the connection between the CSF and other cybersecurity frameworks, standards, guidelines, and resources. Since CSF 2.0 and Informative References will be updated more frequently than the rest of the Core, they will be published and maintained online only.

Future versions will enable users to create their own version of the CSF 2.0 Core with selected Informative References. As the CSF is designed to be used with other cybersecurity resources, this

planned functionality to down select Informative References will help organizations in building Profiles to implement the CSF. NIST encourages feedback on this tool to be sent to cprt@nist.gov.

Note: This tool leverages the NIST Cybersecurity and Privacy Reference Tool (CPRT) where users can view information across many of NIST's cybersecurity and privacy resources.

## COSO to Cybersecurity Foundation 2.0 Relationships

| COSO ERM Principles | NIST CSF Categories |
|---|---|
| **Governance & Culture Component** | |
| 1 Exercises Board Risk Oversight | Identify |
| 2 Establishes Operating Structures | Identify, Protect |
| 3 Defines Desired Culture | Identify, Protect |
| 4 Demonstrates Commitment to Core Values | Identify, Protect |
| 5 Attracts, Develops, & Retains Capable Individuals | Identify |
| **Strategy & Objective Setting Component** | |
| 6 Analyzes Business Context | Identify, Protect |
| 7 Defines Risk Appetite | Identify, Protect |
| 8 Evaluates Alternative Strategies | Identify, Protect |
| 9 Formulates Business Objectives | Identify |
| **Risk Performance Component** | |
| 10 Identifies Risk | Identify, Protect, Detect, Respond, Recover |
| 11 Assesses Severity of Risk | Identify, Protect, Detect, Respond, Recover |
| 12 Prioritizes Risks | Identify, Protect, Detect, Respond, Recover |
| 13 Implements Risk Responses | Identify, Protect, Detect, Respond, Recover |
| 14 Develops Portfolio View | Identify, Protect |
| **Review & Revision Component** | |
| 15 Assesses Substantial Change | Identify, Protect |
| 16 Reviews Risk and Performance | Identify, Protect, Detect, Respond, Recover |
| 17 Pursues Improvement in ERM | Identify, Protect, Detect, Respond, Recover |
| **Info, Communication & Reporting Component** | |
| 18 Leverages Information Systems | Identify, Protect, Detect, Respond, Recover |
| 19 Communicates Risk Information | Identify, Protect, Detect, Respond, Recover |
| 20 Reports on Risk, Culture, and Performance | Identify, Protect, Detect, Respond, Recover |

*Figure 33: COSO to SCF 2,0 Relationship*

## Sample Recovery Management Life Cycle and Deliverables

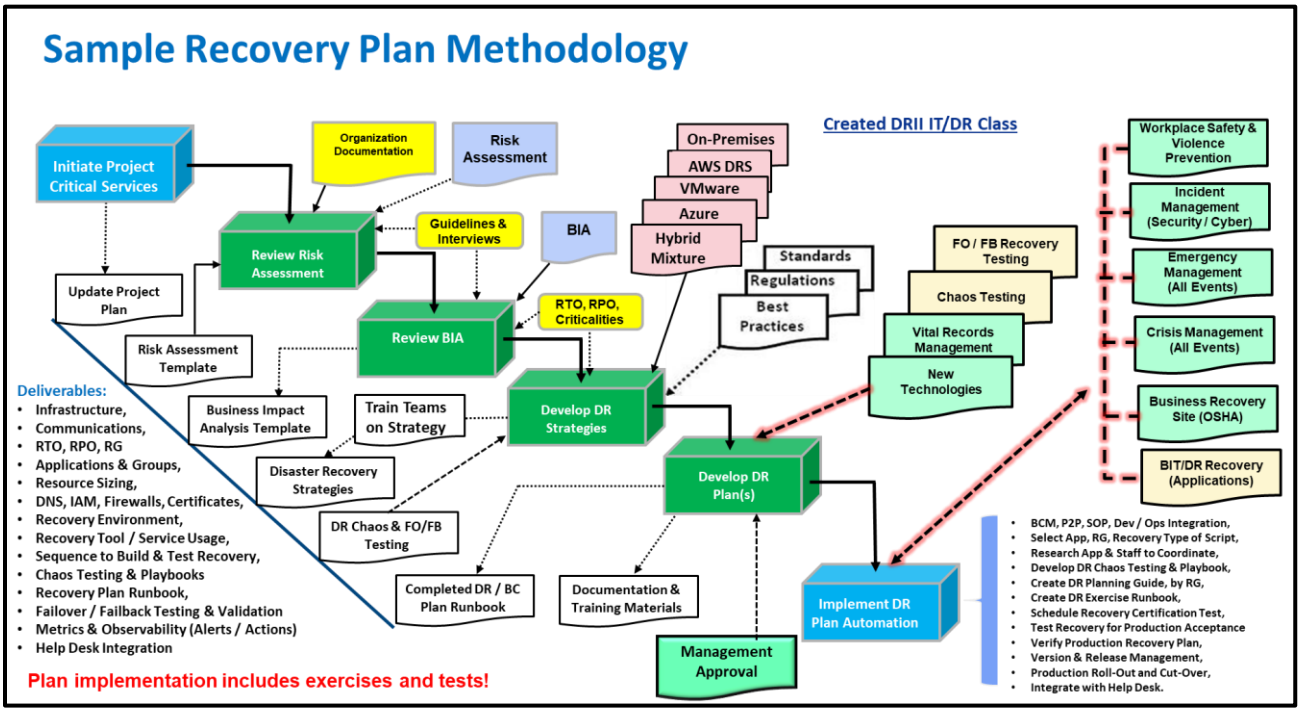



*Figure 34: The Business Continuity Management Process overview.*

The above diagram illustrates the steps needed to implement Business Continuity Management in an organization. A list of deliverables is provided, and the steps needed to build Recovery Playbooks are shown.

## DRII Ten Step Professional Practices for Business Continuity:

1. **Program Initiation and Management**
    a. Establish the need for a business continuity program.
    b. Obtain support and funding for the business continuity program.
    c. Build an organizational framework to support the business continuity program.
    d. Introduce key concepts, such as program management, risk awareness, identification of critical functions/processes, recovery strategies, training and awareness, and exercising/testing.
2. **Risk Assessment**
    a. Identify risks that can adversely affect an entity's resources or image.
    b. Assess risks to determine the potential impacts to the entity, enabling the entity to determine the most effective use of resources to reduce these potential impacts.
3. **Business Impact Analysis**
    a. Identify and prioritize the entity's functions and processes to ascertain which ones will have the greatest impact should they not be available.

   b. Assess the resources required to support the business impact analysis process.
   c. Analyze the findings to ascertain any gaps between the entity's requirements and its ability to deliver those requirements.
4. **Business Continuity Strategies**
   a. Select cost-effective strategies to reduce deficiencies as identified during the risk assessment and business impact analysis processes.
5. **Incident Response**
   a. Develop and assist with the implementation of an incident management system that defines organizational roles, lines of authority and succession of authority.
   b. Define requirements to develop and implement the entity's incident response plan.
   c. Ensure that incident response is coordinated with outside organizations in a timely and effective manner when appropriate.
6. **Plan Development and Implementation**
   a. Document plans to be used during an incident that will enable the entity to continue to function.
7. **Awareness and Training Programs**
   a. Establish and maintain training and awareness programs that result in personnel being able to respond to incidents in a calm and efficient manner.
8. **Business Continuity Plan Exercise, Assessment, and Maintenance**
   a. Establish an exercise, assessment and maintenance program to maintain a state of readiness.
9. **Crisis Communications**
   a. Provide a framework for developing a crisis communications plan.
   b. Ensure that the crisis communications plan will provide timely, effective communication with internal and external parties.
10. **Coordination with External Agencies**
   a. Establish policies and procedures to coordinate incident response activities with public entities.

## Disaster Recovery Planning

Implementing disaster recovery with data backup and recovery involves multiple tasks to ensure that an organization's critical data and systems can be restored in case of a disaster. Diverse groups within an organization play various roles in this process. Here is an overview of the tasks and the groups involved:

1. **Risk Assessment and Business Impact Analysis:**

   **Group:** Risk Management, Business Continuity, IT Management

   Identify potential risks and threats that could lead to a disaster and assess their potential impact on the business. This step helps prioritize resources and efforts.

2. **Define Recovery Objectives:**

   **Group:** IT Management, Business Continuity

Determine recovery time objectives (RTOs) and recovery point objectives (RPOs) for different systems and data. RTO is the maximum acceptable downtime, and RPO is the maximum data loss allowed.

**3. Develop Disaster Recovery Plan (DRP):**

**Group:** IT Management, Business Continuity, IT Team

Create a detailed plan that outlines the steps to be taken during and after a disaster. This includes procedures for data backup, system recovery, communication, and resource allocation.

**4. Data Backup:**

**Group:** IT Team, Database Administrators

Regularly back up critical data following the defined RPO. Implement strategies such as full backups, incremental backups, and differential backups based on the needs of the organization.

**5. Choose Backup Solutions:**

**Group:** IT Management, IT Team

Select and implement appropriate backup solutions, which could include on-premises backup systems, cloud-based backup services, and off-site storage.

**6. Implement Redundancy and Replication:**

**Group:** IT Team, Network Administrators

Set up redundant systems and data replication to ensure that data is available even if one location or system fails.

**7. Test Recovery Procedures:**

**Group:** IT Team, Business Continuity

Regularly evaluate the disaster recovery plan and backup systems through simulated disaster scenarios. This helps identify weaknesses and refine the plan.

**8. Training and Documentation:**

**Group:** IT Team, Business Continuity

Train personnel in their roles during a disaster and the steps to follow for recovery. Maintain clear and up-to-date documentation of the recovery procedures.

**9. Communication Plan:**

**Group:** Communication Team, IT Team

Develop a communication plan to inform stakeholders, employees, and customers about the disaster and the recovery process.

**10. Incident Response:**

**Group:** IT Team, Incident Response Team

In case of an actual disaster, follow the predefined steps in the disaster recovery plan to initiate recovery procedures and minimize downtime.

**11. Continuous Improvement:**

**Group:** IT Management, Business Continuity

Regularly review and update the disaster recovery plan based on changes in technology, business needs, and lessons learned from testing and incidents.

It is important to note that the specific roles and groups involved can vary based on the organization's size, industry, and structure. Effective disaster recovery requires collaboration and coordination among various teams to ensure a smooth recovery process in case of emergencies.

## The Disaster Recovery Life Cycle

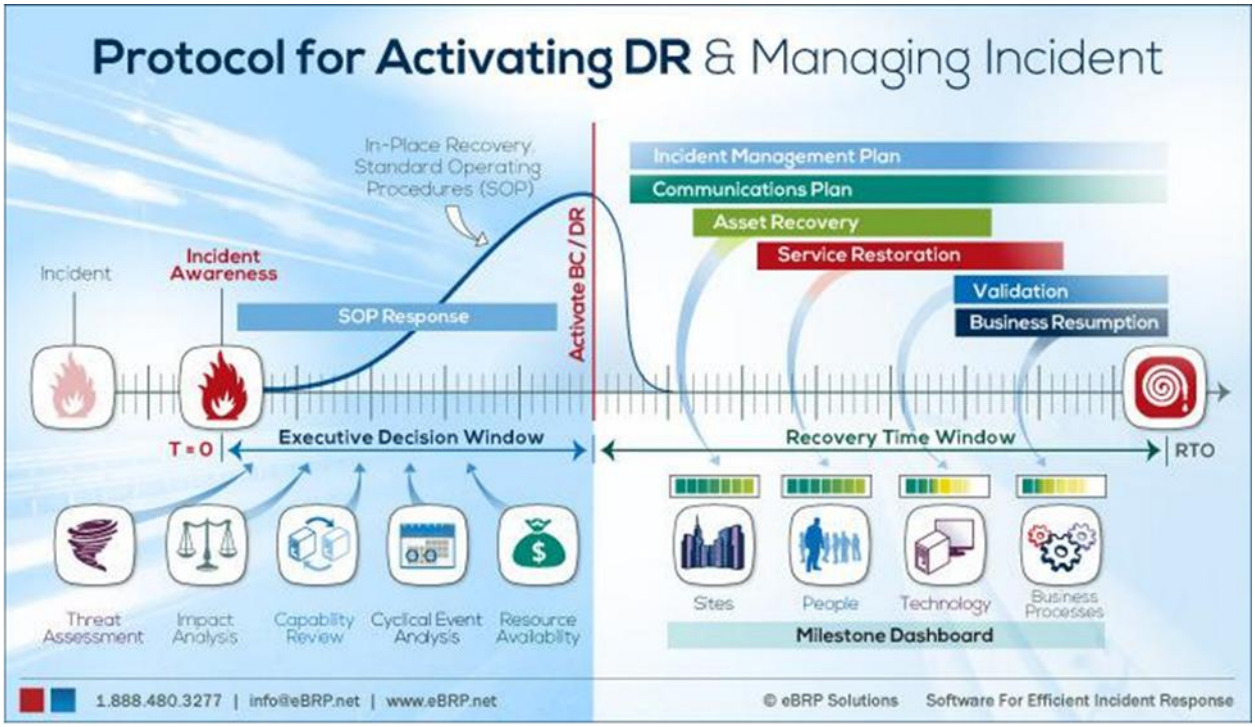



*Figure 35: Disaster Recovery Life Cycle - Actions to be Taken.*

It may take time between when a disaster event occurs and when it is recognized. For that reason, it is important to make personnel aware of what disasters are and how to respond to them in accordance with their job functional responsibilities. Let us examine the above example to better understand personnel's needs relating to disaster events.

1. **Incident** - an incident occurs. Who knows how to recognize the incident? Who can declare a Disaster?
    a. **Threat Awareness** – Executive Decision Window – Executive Operations Center (EOC) – people become aware of the threat and notify executive management, help desk, and recovery operations.
    b. **Impact Analysis** – the extent of the disaster event's impact is evaluated and reported, so the appropriate response can be formulated and enacted.
    c. **Capacity Review** – Any loss of capacity is determined, and the remaining capacity is determined and reported.
    d. **Cyclical Event Analysis** – is this an event that repeats every cycle, or is it a unique event?
    e. **Resource Availability** – what resources have become unavailable and which resources remain.
    f. **Site Protection Plan** – if the site is damaged and first responders called, the police will initially secure the site, but you are responsible for site security when the police leave. For that reason, you should dispatch company security to the site to protect your resources after the First Responders leave.
    g. **Site Salvage Plan** – any salvageable equipment, papers, or other assets that have survived the disaster event must be salvaged and protected against loss or theft.
    h. **Site Restoration Plan** – the damaged site must be recovered and restored to its original operating status, at a minimum.
2. **Threat Awareness** – awareness of the defined disaster event is provided to appropriate pre-defined individuals and job functions.
3. **Standard Operating Procedures (SOP)** Response – any pre-developed recovery plans are selected based on Threat Awareness and executed.
4. Activate BC/DR Plan
    a. Disaster Recovery Plan for loss of IT Services.
    b. Business Recovery Plan for loss of a location, including:
        i. Site Evacuation and Personnel Safety Plan.
        ii. Movement to Recovery Site or Working From Home (WFH) personnel plan.
        iii. Work restoration via remote site or WFH.
        iv. Site Protection, Salvage, and Restoration Plans.
        v. Site Validation Plan to ensure ability to return to original site.
        vi. Return to original site plan.
    c. **Emergency Management Plan** – for natural disasters.
    d. **Crisis Management Plans** – for unique events impacting personnel or the business.
    e. **Personnel Safety and Violence Prevention** – for active shooter or other events that may result in injury to personnel, visitors, or customers.
5. **Incident Management Plan** – Recovery Time Window
    a. **Milestone Dashboard –** Contingency Command Center (CCC) for multiple recoveries
    b. **Plan and Steps** – which plans are activated, their teams and actions.
    c. **People** – the disaster and the recovery team members impact which people.
    d. **Technology** – what technology is impacted and needs to be replaced or repaired.
    e. **Business Process** – what business processes are impacted and to what extent.

6. **Communications Plan** – from executive management, to company personnel and their families, the media, community, and anyone else identified. Separate communications plans should be drafted, and representatives assigned to speak for the company in a single voice (usually Executive Management, or their Communications Representative).
7. **Asset Recovery Plan** – what assets were damaged and need to be repaired or replaced.
8. **Service Recovery Plan** – recovery plans should be developed for the loss of a single service or multiple services.
9. **Validation Plan** – plans should be developed to validate the successful restoration of services after the recovery plan has been executed.
10. **Service Restoration Plan** – a plan to evaluate that all company services have been fully restored should be created and executed at this time and then announced through company communications representatives.

### Using Artificial Intelligence Planning can assist in Enterprise Resilience.

Artificial Intelligence (AI) is available for providing planning assistance for projects, phases, and individual tasks.

The following illustration provides a pathway for defining how best to migrate applications to the cloud. Click on this link to learn more details about the subject.

## AI Planning for Migrating Application to the Cloud

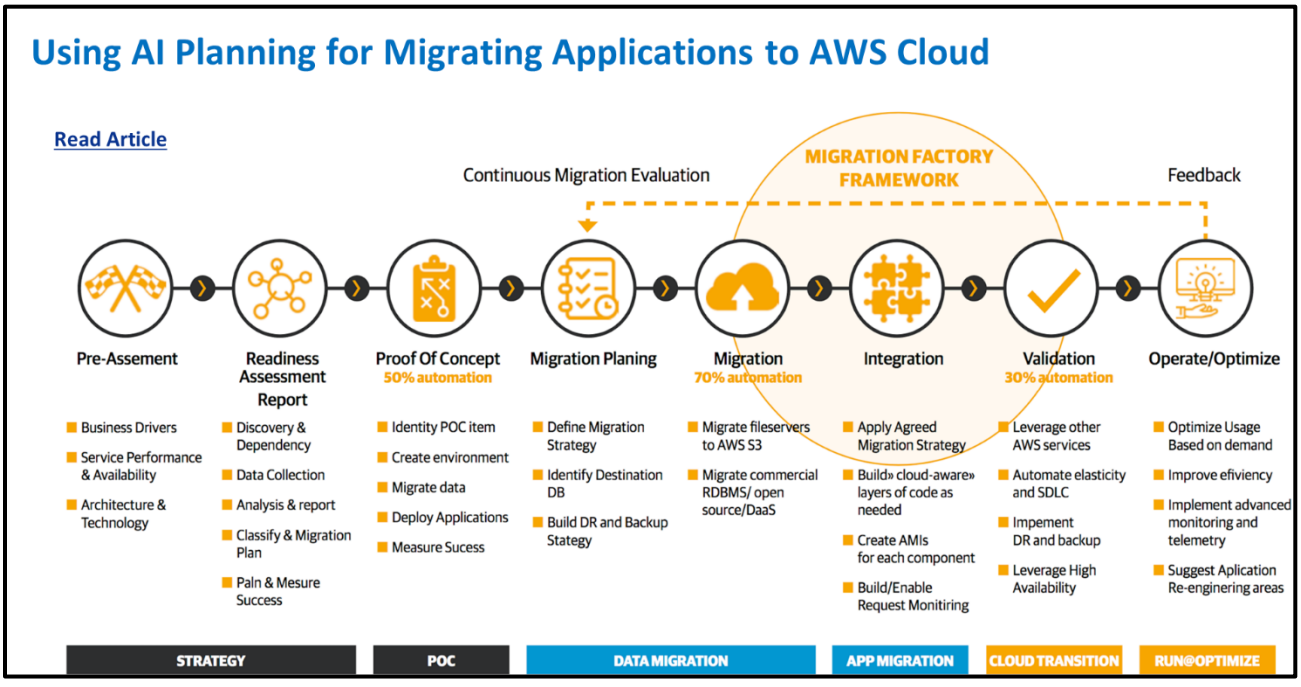



*Figure 36: Using AI Planning for Migrating Applications to the AWS Cloud*

The phases and steps used for migrating an application to the cloud are illustrated above, while the next illustration shows the specifics used for migrating an application to the cloud.

Phases include:

1. Strategy
2. Proof of Concept
3. Data Migration
4. Application Migration
5. Cloud Transition, and
6. Run@ Optimized

## Migrating Applications to the Cloud

The specific steps used to migrate an application to the cloud as shown below.

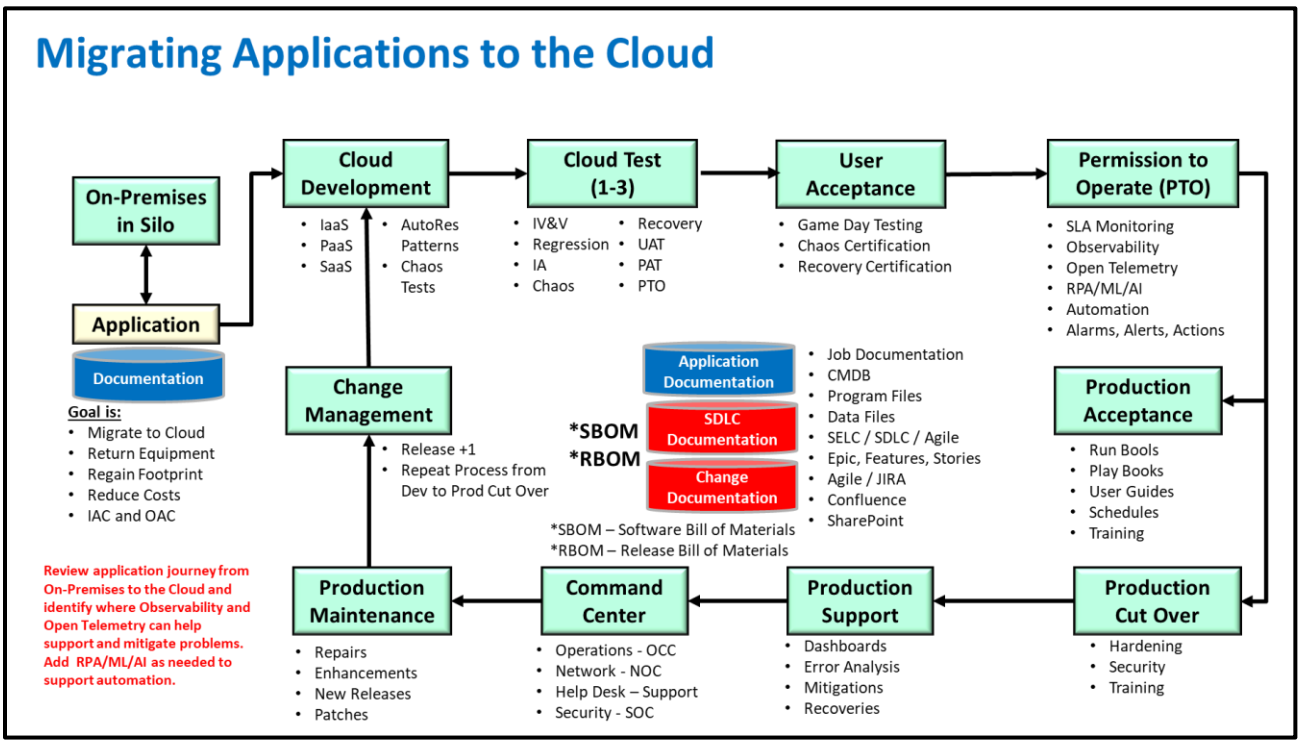



*Figure 37: Overview of the process of Cloud Application Certification*

The above illustration provides an overview of every step required to validate an applications migration from a Silo as Monolithic Application to the Cloud using Microservices and APIs. As you see, there are required steps needed to successfully accomplish this task.

## Chaos Testing

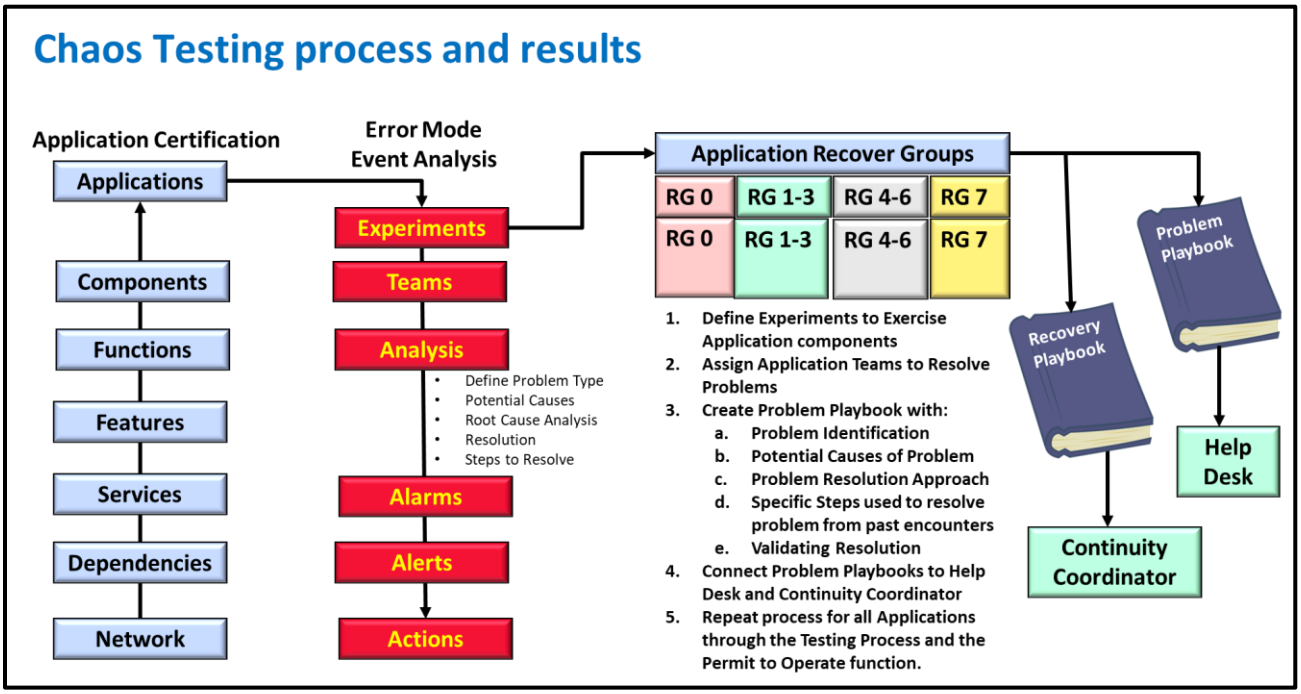



*Figure 38: Chaos Testing process and Runbooks produced.*

Playbooks produced through Chaos Testing are essential to Problem Resolution and Recovery.

# Incorporating Site Reliability Engineering into IT Operations

**Functions provided by the Site Reliability Engineer**

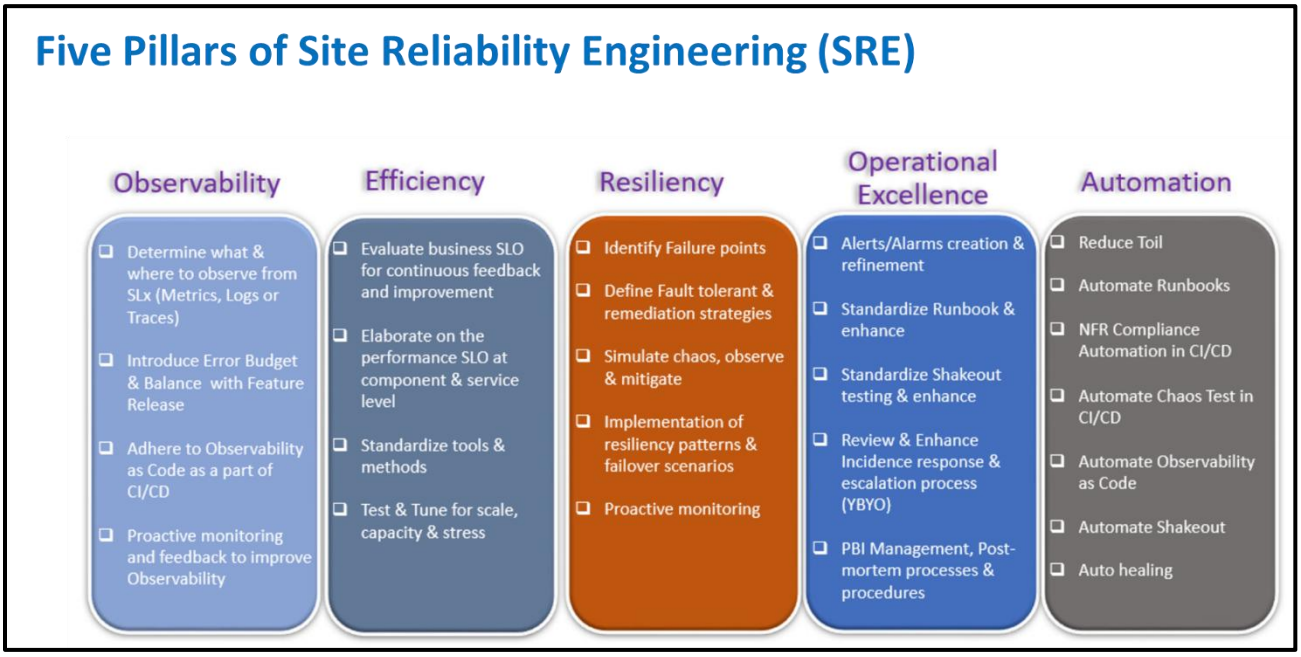



*Figure 39: The Five Pillars of Site Reliability Engineering*

Utilizing an SRE approach to optimize IT Operation has proven to improve efficiency, reduce costs, and result in improved development, testing, and maintenance of systems. The six phases of an SRE's service are shown above, but their main goal is to continuously improve IT Operations through automation that reduces toil and staffing requirements, resulting in lower costs and fewer mistakes.

[SRE Handbook Table of Contents]

## Optimizing the efficiency of IT Operations through the SRE Maturity Model

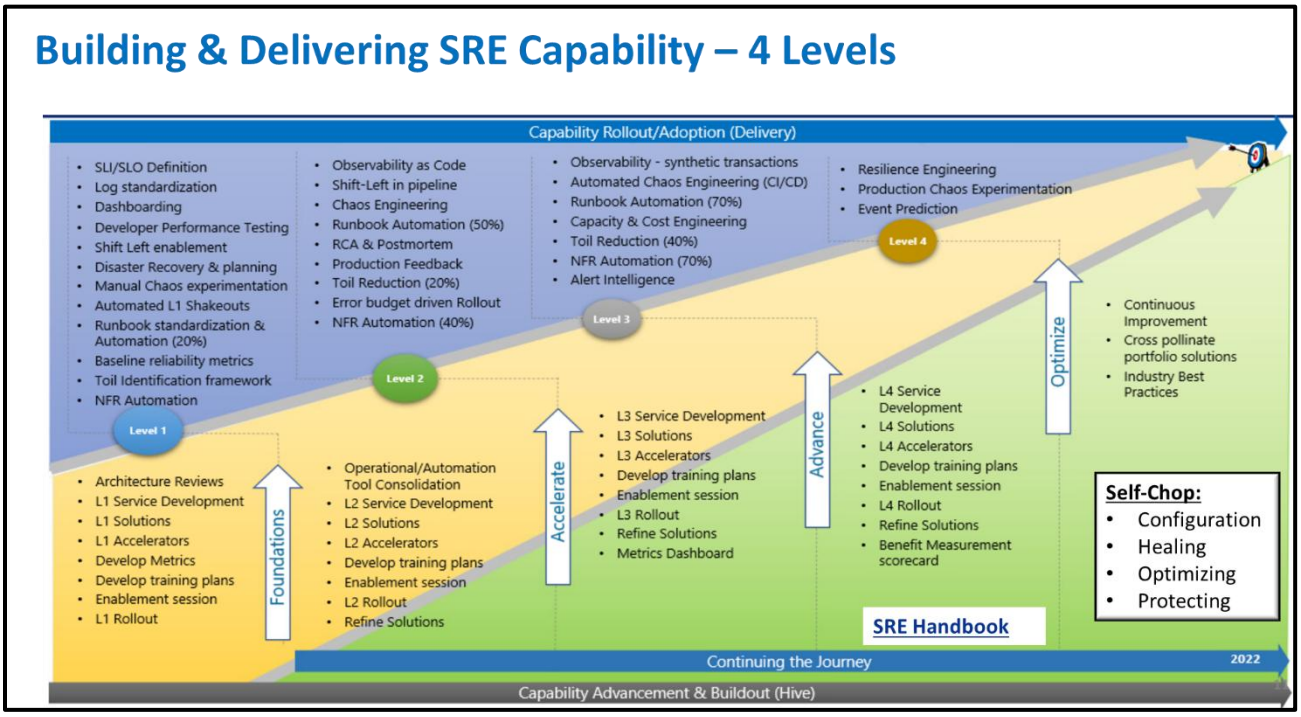



*Figure 40: Building and Delivering SRE Capabilities - 4 Levels of Optimization*

Following the SRE maturity model will result in an optimized IT Operational environment, reduced risks, improved efficiency and performance, and cost savings due to automation improvements that can supplement or reduce staff requirements.

# Secure SDLC and Vulnerability Management

A secure Systems Development Life Cycle (SDLC) is fundamental to reducing enterprise risk and achieving operational resilience. Traditional approaches to application development often delay security considerations until the final phases, leaving critical vulnerabilities unaddressed. Modern resilient organizations embed vulnerability management throughout the SDLC to ensure secure, compliant, and robust production systems.

## Key Components of a Secure SDLC

- **Threat Modeling & Secure Design:** Start with security architecture reviews and threat modeling during the planning phase.
- **Component Validation:** Ensure all libraries, APIs, and third-party services are scanned and verified for vulnerabilities prior to integration.

- **Static and Dynamic Analysis:** Implement automated static (SAST) and dynamic (DAST) security testing as part of the CI/CD pipeline.
- **Production Control Gates:** Use control gates to prevent deployments of applications or services containing known vulnerabilities.
- **Developer Training & Awareness:** Empower developers with secure coding best practices, IDE-integrated scanning tools, and secure development policies.

## Continuous Monitoring in Production

Once deployed, applications must remain protected against evolving threats. Continuous monitoring is essential for:

- Detecting newly disclosed CVEs that affect application components.
- Identifying changes in compliance posture or system behavior
- Automating mitigation actions such as hotfixes, patches, or service isolation

Tools like **Software Bills of Materials (SBOMs)** allow organizations to track the composition of their software assets and correlate vulnerabilities with affected components. Platforms like **ProCap360** extend this capability by integrating SBOM analysis with control gates, continuous scanning, alerting, and risk scoring.

## ProCap360 Use Case

ProCap360 automates:

- Detection of vulnerable components via integrated SBOM scans
- Blocking deployment of applications that include high severity vulnerabilities.
- Continuous risk scoring prioritizes remediation efforts.
- Documentation and reporting for audit and compliance teams.

By incorporating ProCap360 into both development and production environments, organizations achieve a seamless vulnerability management lifecycle that supports:

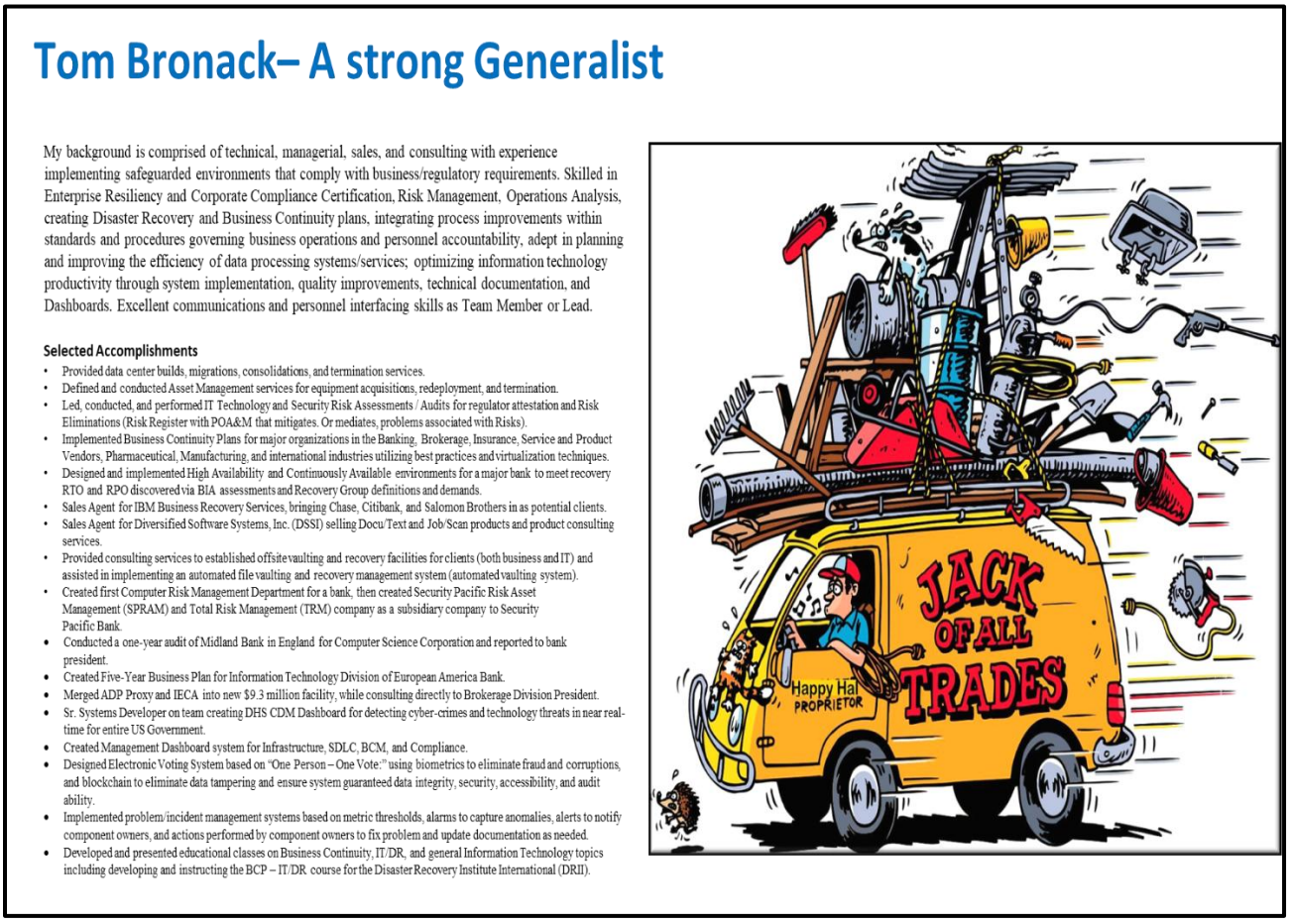
- Rapid identification and mitigation of application-level risks
- Improved collaboration between security and engineering teams
- Enhanced compliance with NIST, CMMC, and ISO frameworks

## Quantifiable Benefits

- **Fewer Breaches:** Early detection and elimination of vulnerabilities before production.
- **Reduced Toil:** Automation reduces the burden on security and operations personnel.
- **Faster Incident Response:** Continuous monitoring shortens time to detect and remediate issues.
- **Improved Compliance:** Real-time alignment with regulatory requirements.
- **Increased Customer Trust:** Consistently secure applications enhance reputation and retention.

Embedding vulnerability management into the SDLC and operational environment turns resilience from a static goal into a dynamic, measurable, and continuously improving discipline.

## About the author



# Tom Bronack– A strong Generalist

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 and demands.
- 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 product consulting services.
- 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 Security Pacific Risk Asset Management (SPRAM) and Total Risk Management (TRM) company as a subsidiary company 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.
- 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).



*Figure 41: Tom Bronack - A Strong Generalist*

**Contact Information**

Thomas Bronack, CBCP

President, Data Center Assistance Group, LLC

Email: bronackt@dcag.com

Website: www.dcag.com

Phone: (917) 673-6992