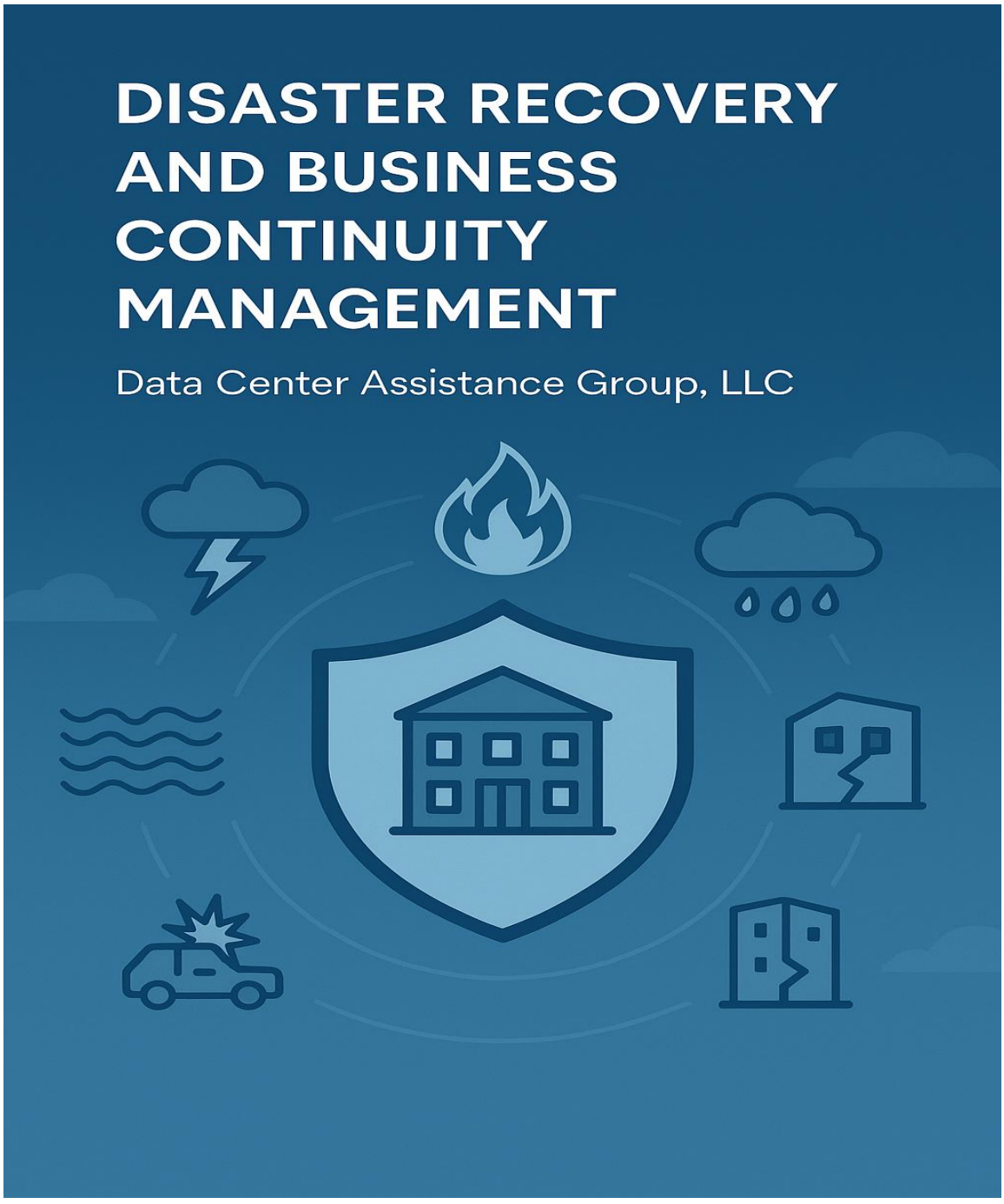


By Thomas Bronack, President
Data Center Assistance Group, LLC
bronackt@dcag.co or
bronackt@gmail.com
(917) 673-6992
Website: https://www.dcag.com

Executive Framework: 10-Step Disaster Recovery and Business Continuity **Program**

By: Data Center Assistance Group, LLC (DCAG)

Email: bronackt@dcag.co | bronackt@gmail.com
Phone: (917) 673-6992
Website: https://www.dcag.com

Table of Contents

Contents

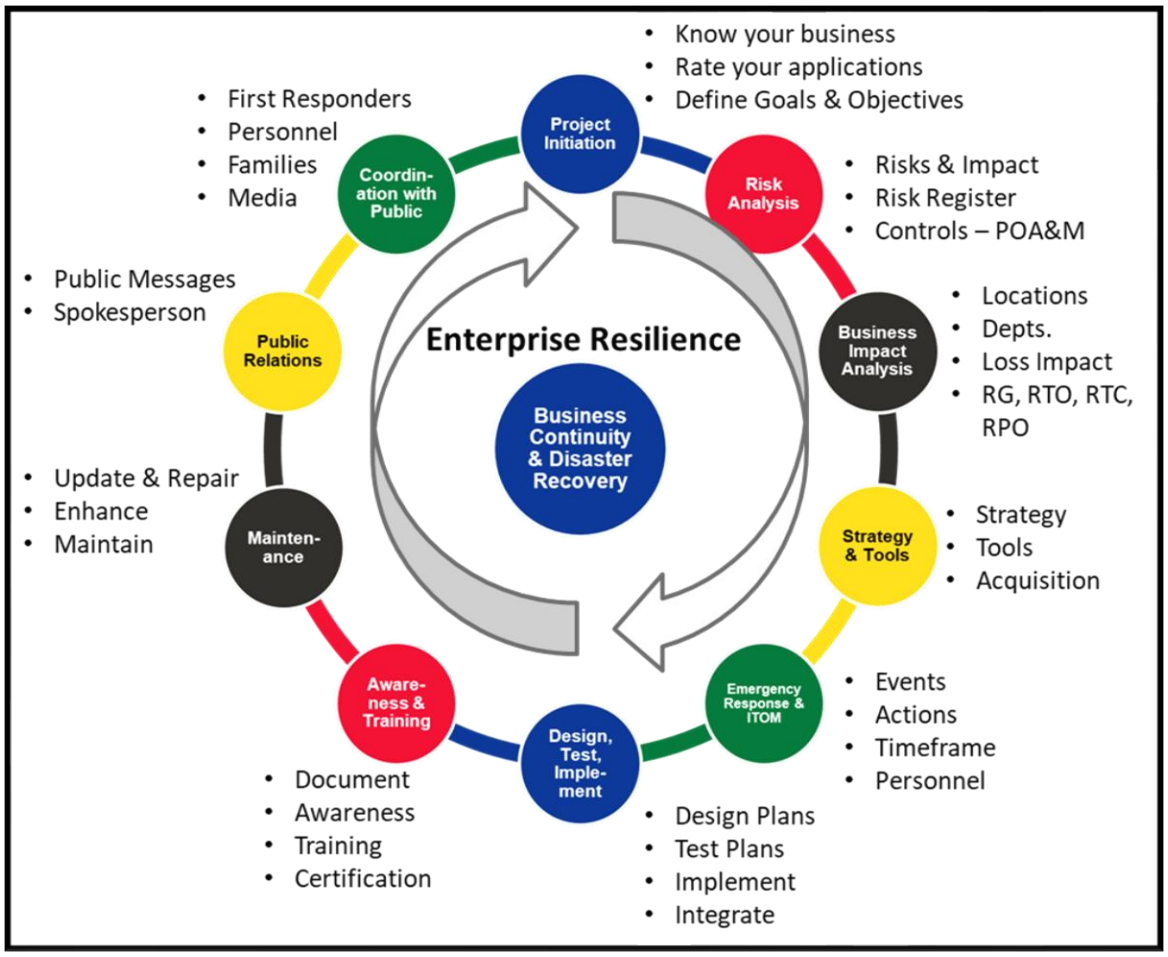
Objective:

Establish a comprehensive, sustainable, and measurable program tailored to government agency operations, ensuring mission continuity, regulatory compliance, and public trust through proactive disaster recovery and business continuity planning.

Federal Compliance References Integrated:

- NIST SP 800-34 Rev. 1 (Contingency Planning for Federal Information Systems)
- NIST SP 800-30 Rev. 5 (Risk Assessment)
- FISMA, FedRAMP, PPD-40 (National Continuity of Government)
- FCD-1, FCD-2 (COOP Planning)
- FIPS 199 impact Levels and Mission Essential Functions (MEFs)
- ISO 31000 (Descriptive video links)
- OMB A-130 standards (Managing Information as a Strategic Resource)
- Secure by Design guidelines (QWASP guidelines)
- PCI DSS – Payment Card Industry Date Security Standard
- Executive Order 14028 – Improving Nation's Software Security Supply Chain with SBOMS
- OBM M-22-18 and M-13-16 – Improving the defense and Resilience of Government Networks.
- **FDA** – Control over medical device supply chain and cybersecurity problems
- **CRA** – European Cyber Resilience Act – Hardware and Software Components cyber requirements
- **DORA** – Digital Operational Resilience Act – Strengthen the financial sectors resilience.
- **GDPR** – EU Digital Rights of their Citizens

The Disaster Recovery Ten-Step Process.



1. Project Initiation and Management

Goal: Gain management approval and funding for Business Continuity function.

- Launch a governance-backed program aligned with agency mandates and mission objectives.

Key Actions:

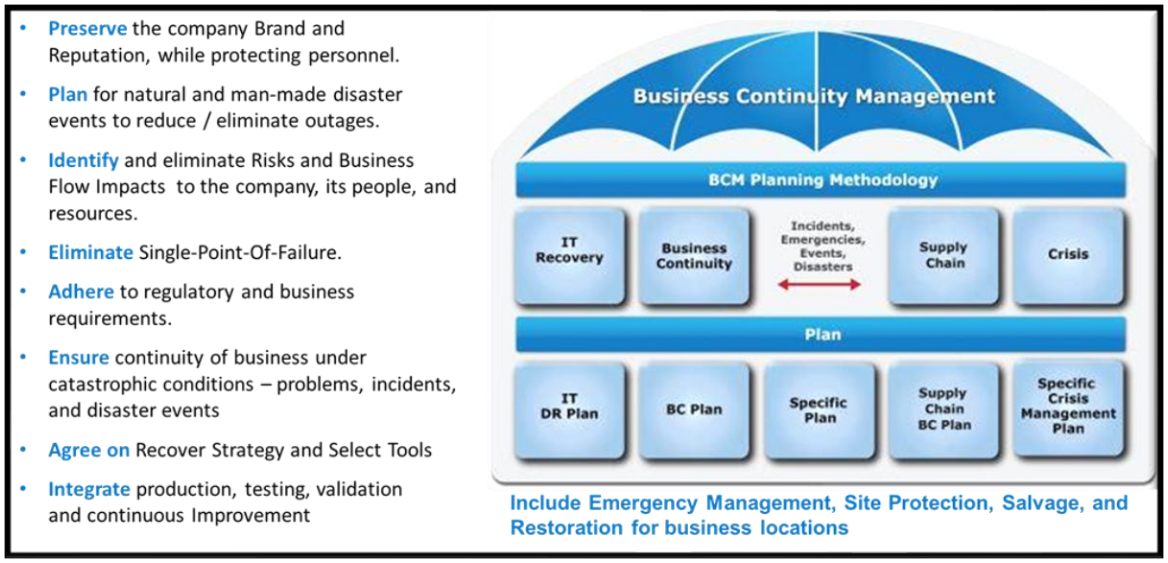
- Executive charter signed by agency CIO or COO.
- Formation of a Steering Committee with CISO, COOP Manager, and key mission stakeholders.
- Program charter incorporates FISMA and COOP directives.
- Approved project plan with milestones, KPIs, and assigned resources.

Results Tracking:

- MS Project, Asana, or ServiceNow dashboards (PM Tools).

- Bi-weekly progress reports to the Steering Committee.
- RACI matrix for federal accountability (Responsible, Accountable, Consulted, and Informed).

Components contained within Business Continuity and Disaster Recovery



Enterprise Resilience & Business Continuity Management (BCM)

Definition:

- **Enterprise Resilience** is the organization's ability to anticipate, absorb, adapt to, and rapidly recover from disruptions—whether from cyber incidents, natural disasters, supply chain failures, or operational crises.
- **Business Continuity Management (BCM)** is the structured framework and set of processes that ensure critical business functions can continue or be quickly restored following a disruption.

How they are created:

- **Risk and Impact Analysis** – Identify threats, vulnerabilities, and mission-critical functions.
- **Strategy Development** – Define recovery and continuity strategies for essential operations, systems, and services.
- **Plan Design** – Document recovery procedures, escalation paths, communication protocols, and responsibilities.
- **Training & Exercises** – Build organizational awareness through drills, simulations, and continuous improvement.
- **Ongoing Maintenance** – Update and validate plans regularly to adapt to new risks, technologies, and regulations.

Why they are important:

- **Minimize Downtime** – Protect revenue streams, mission delivery, and service levels.
- **Maintain Public & Stakeholder Trust** – Demonstrate operational readiness and transparency during crises.
- **Ensure Compliance** – Align with regulations (e.g., NIST, ISO, FISMA) and contractual obligations.
- **Protect People & Assets** – Safeguard employees, facilities, and information assets.
- **Enable Competitive Advantage** – Organizations that recover faster and maintain service continuity can outperform less-prepared peers.

Bottom Line: Enterprise Resilience and BCM are not just risk management tools—they are strategic imperatives that safeguard your ability to operate under any circumstances.

Get to know the company and establish a direction.

Know your company:

1. Most Important Applications & Services (Family Jewels).
2. BIA to Define the damage caused if lost and maximum duration of survival without the application or service.
3. Define Requirements, Scope, Risk, Security, DevSecOps, Testing, Recovery, Acceptance, Deployment, and ITSM, ITOM.
4. Define Audit Universe implement legal & auditing functions.
5. Define Ideation, Brainstorming, Collaboration, to Concept cycle.
6. Implement Systems Engineering Life Cycle (SELC) to respond to new ideas or business opportunities.
7. Implement Systems Development Life Cycle (SDLC) to deploy new products and services.
8. Define Company Organization to respond to cybersecurity and technology problems in a timely manner to the appropriate authorities (i.e., SEC Rule 2023-139)

Know your Environment:

1. Physical and Data Security (Data Sensitivity & Data Flow).
2. Architecture and engineering process.
3. Asset Inventory and Configuration Management.
4. Identify and Access Management.
5. GRC based compliance and attestation, CIA based cybersecurity and elimination of viruses and malware.
6. Development and implementation of DevSecOps.
7. Personnel Titles, Job Functions and Responsibilities, and the integration of sensitive and required services within their everyday work tasks.
8. Staff training and development.
9. Continuous Monitoring and Improvement, along with the adoption of new technologies and processes (i.e., SRE).
10. Deploying error-free products and services (see EO 14028 and OBM M-22-18) and utilize the latest technologies to respond to encountered anomalies and verify compliance.

Set you direction:

1. Most efficient, compliant, and secure production environment, capable of recovering from disaster events and providing continuous vulnerability-free products and services to customers. **Continuity of Succession / Delegation of Authority** must be included along with definition of duties.
2. Integrate guidelines, standard Operating Procedures, skill development, and awareness throughout the organization.

2. Risk Evaluation and Controls Improvement

Goal: Detect risks that must have controls established to better comply to laws and regulations or to eliminate hazards.

- Evaluate operational, information, and supply chain risks based on federal frameworks.

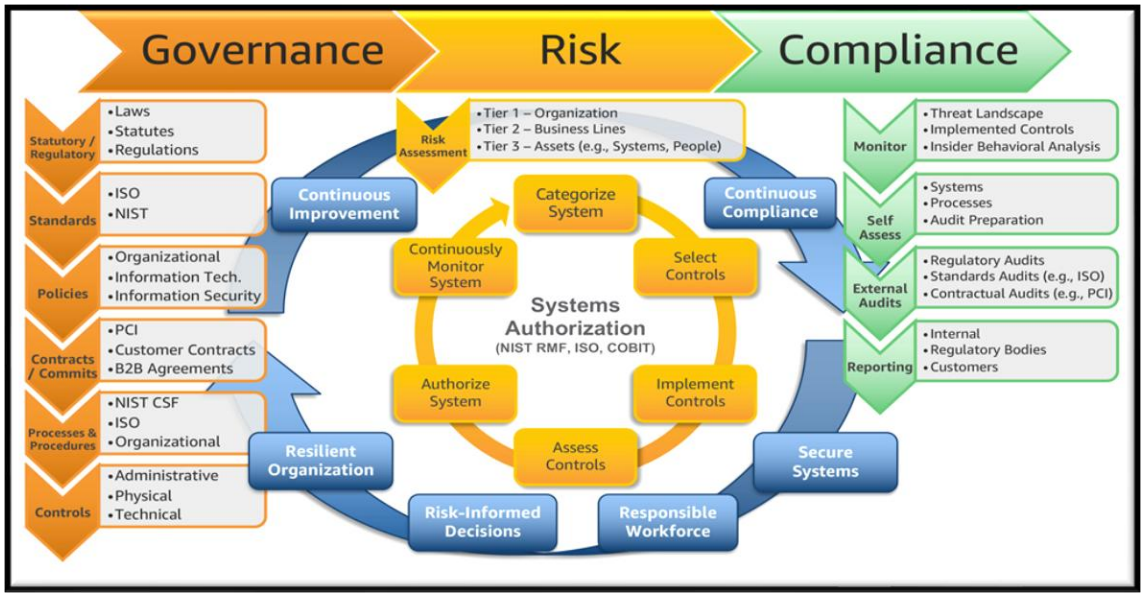
Key Actions:

- Develop a Risk Register using NIST 800-30 scoring methodology.
- Map risks to FIPS 199 impact levels and mission-essential functions (MEFs).
- Prioritize control improvements using ISO 31000 and OMB A-130 standards.

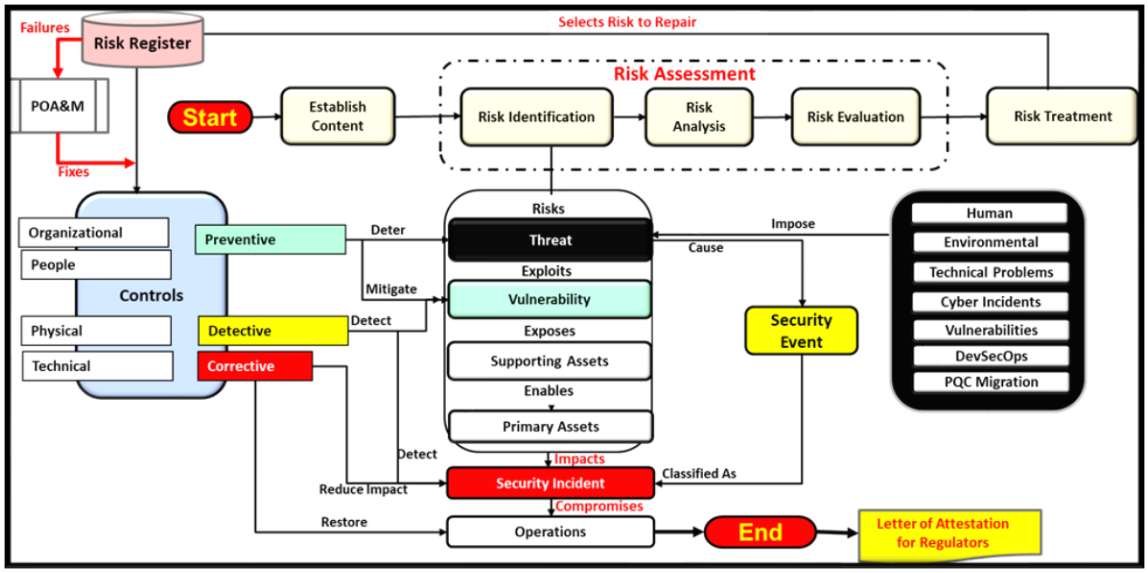
Results Tracking:

- Heat map dashboards updated monthly.
- Risk Committee reviews and mitigation updates.
- Audit logs maintained for FISMA readiness.

GRC – Governance, Risk, and Compliance framework

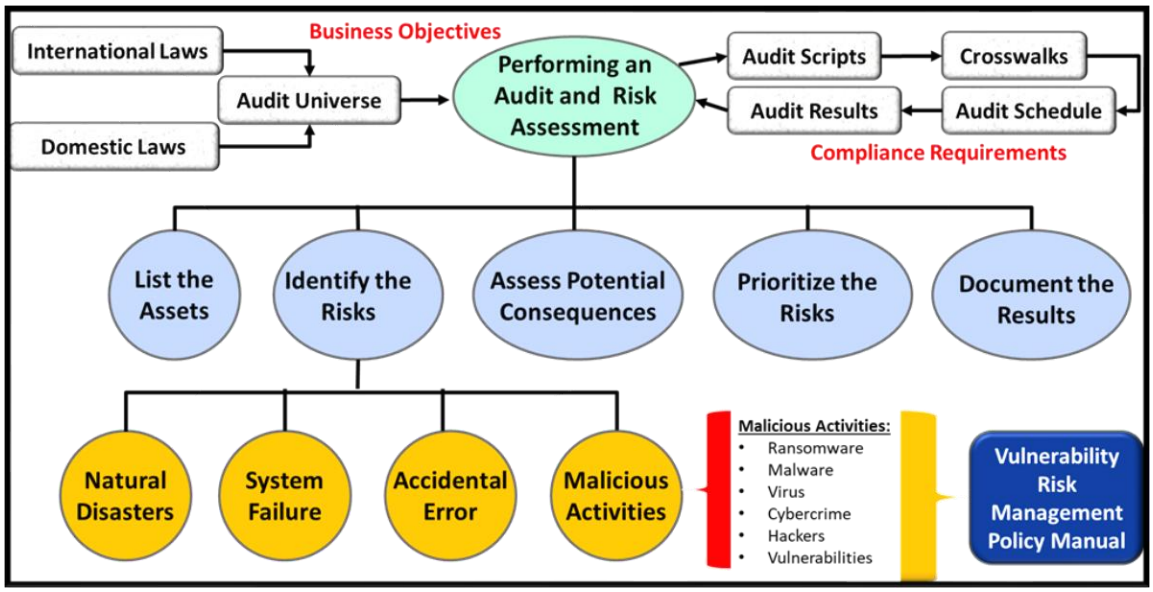


Risk evaluation process and results.



Discovering Risks and taking corrective actions, including initiating recovery plans and actions.

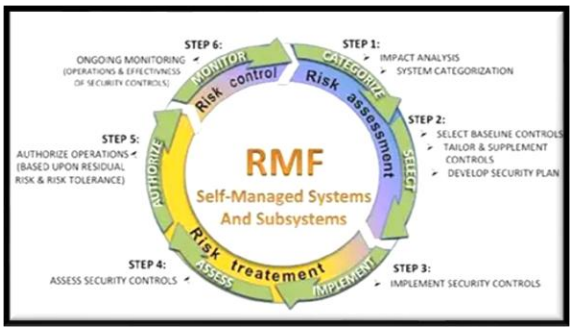
Performing a Risk Assessment and Audit.



Defining your Audit Universe, create crosswalk documents, generate audit scripts with required artefacts, produce an audit schedule, conduct audits, and report results to management and regulators. Located risks are placed in Risk Register with a corresponding Plan of Action with Milestones (POA&M).

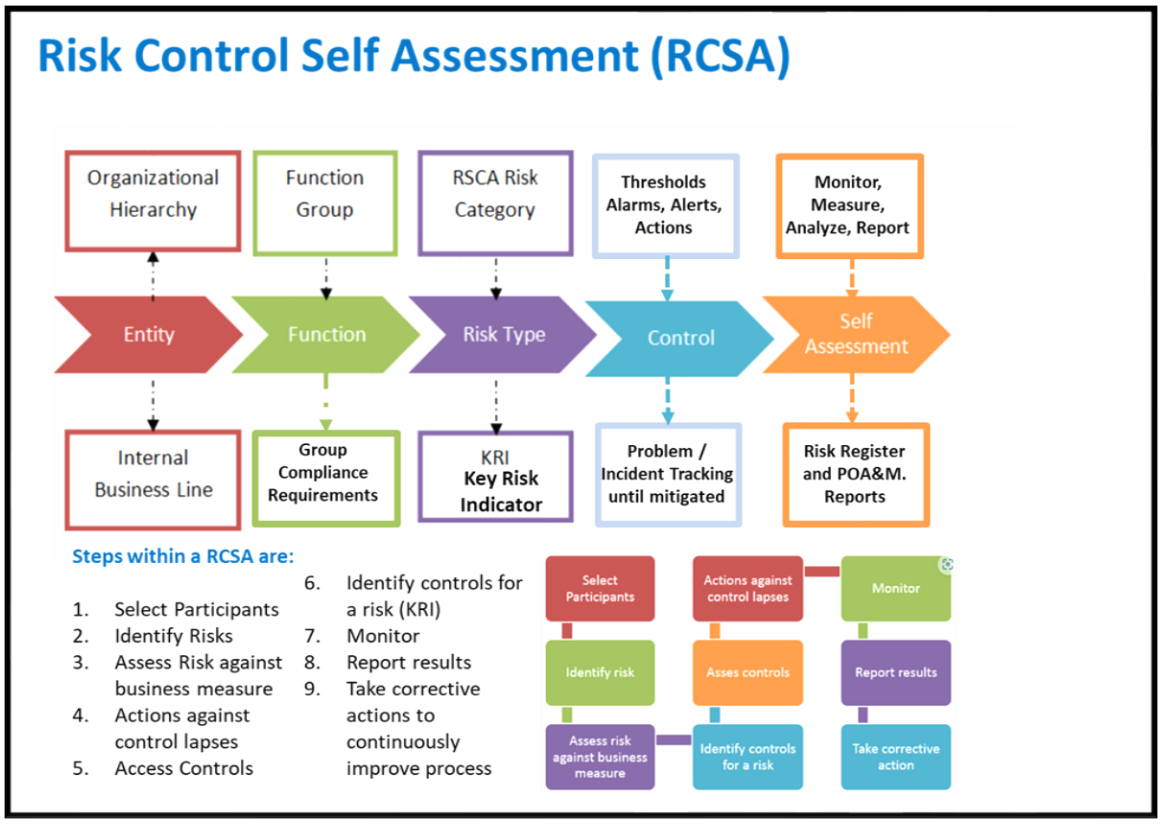
Risk Management Framework

The six-step process associated with Risk Management Framework is illustrated here, including:



1. Categorize Risk Impacts.
2. Select Baseline Controls.
3. Implement Security Controls.
4. Assess Security Controls.
5. Authorize Operations.
6. Monitor, analysis, and report. Implement improvements until optimized.

Risk Control Self-Assessment (RCSA)



RCSA (Risk Control Self-Assessment) is an empowering method/process by which management and staff of all levels collectively identify and evaluate risks and associated controls. It adds value by increasing an operating unit's involvement in designing and maintaining control and risk systems, identifying risk exposures and determining corrective action. The aim of RCSA is to integrate risk management practices and culture into the way staff undertake their jobs, and business units achieve their objectives. It provides a framework and tools for management and employees to:

- Identify and prioritize their business objectives.
- Assess and manage substantial risk areas of business processes.
- Self-evaluate the adequacy of control.
- Develop risk treatment action plans.
- Ensure that the identification, recognition and evaluation of business objectives and risks are consistent across all levels of the organization.

3. Business Impact Analysis (BIA)

Goal: Review facilities and locations to identify weaknesses and define recovery requirements and procedures should a disaster event occur.

- Quantify mission disruption and recovery needs by function.

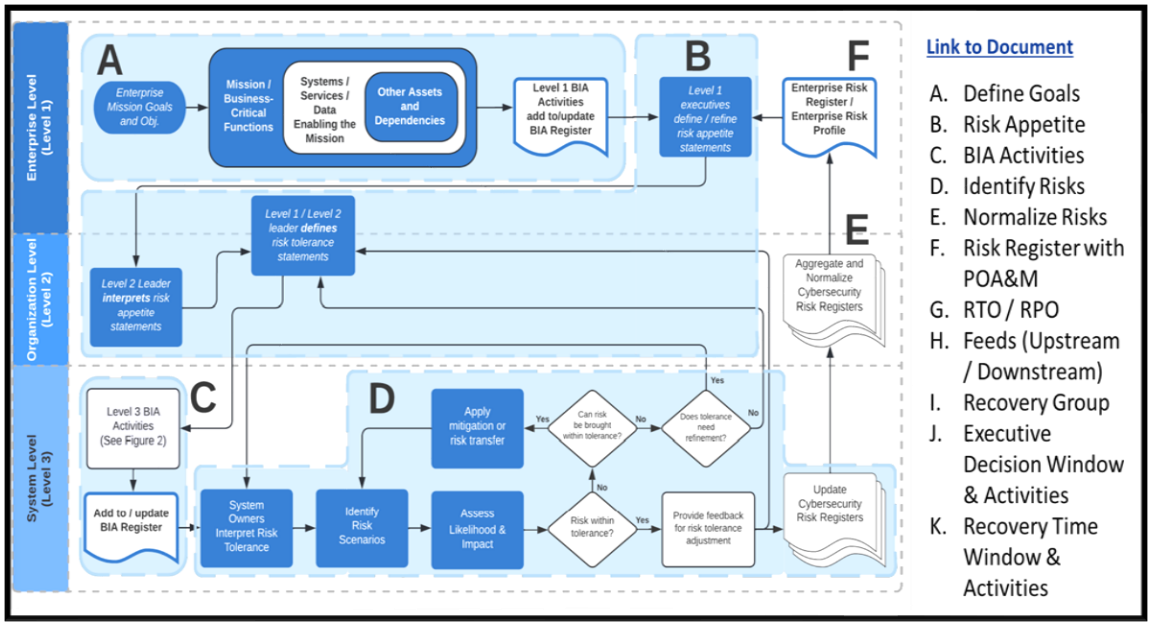
Key Actions:

- Conduct interviews/workshops with MEF owners.
- Define RTO, RPO, and MTPD.
- Identify dependencies, shared services, and cloud vs. on-prem workloads.

Results Tracking:

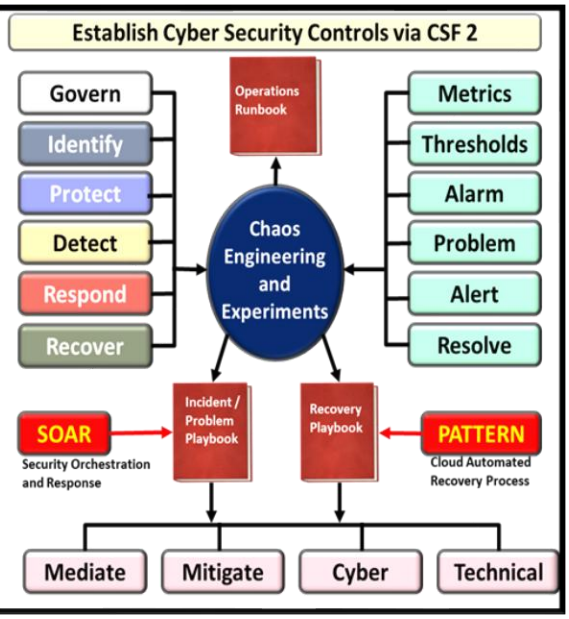
- Executive BIA Summary Reports.
- Dependency matrix across agency components.
- Approval by executive sponsor.

Performing a Business Impact Analysis (BIA)



NIST CFS 2.0 Categories and Applications.

NIST Cybersecurity Framework 2.0		
CSF 2.0 Function	CSF 2.0 Category	CSF 2.0 Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles and Responsibilities	GV.RR
	Policies and Procedures	GV.PO
Identity (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Supply Chain Risk Management	ID.SC
	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)	Adverse Event Analysis	DE.AE
	Continuous Monitoring	DE.CM
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



4. Developing Business Continuity Strategies

Goal: Analyze information obtained through Organization Review of Products and Services, Rating Recovery requirements and their importance, Risk Assessment, and the Business Impact Analysis to determine which tool(s) would best support the complexity of implementing a Business Continuity program within the organization.

- Define and evaluate continuity strategies in alignment with federal and company guidelines.

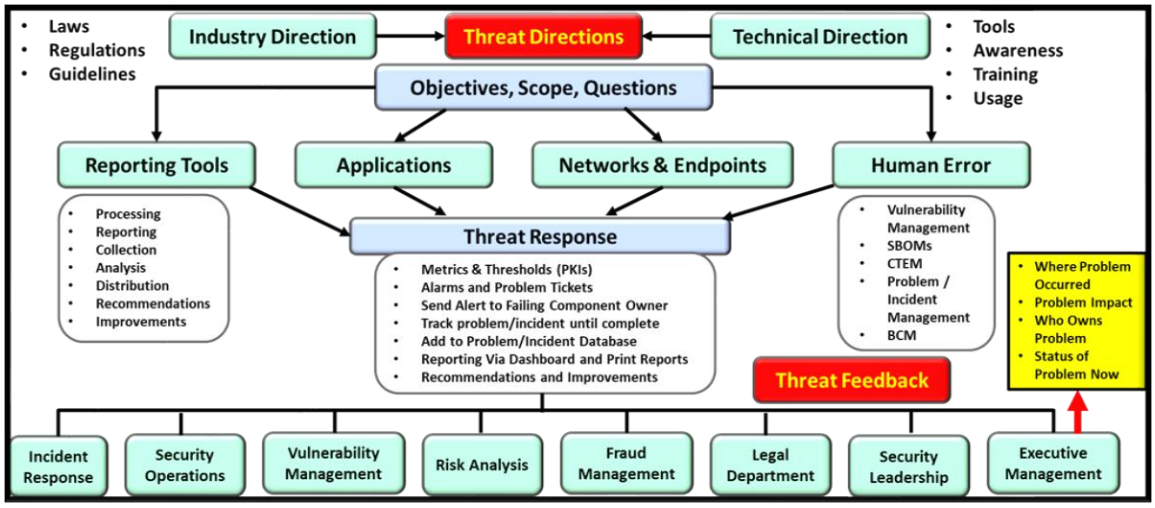
Key Actions:

- Analyze COOP and alternate site options.
- Develop cloud-based and mutual-aid recovery scenarios.
- Evaluate costs vs. federal grant or budget alignment.
- Select product(s)/tool(s) needed to support effort going forward.

Results Tracking:

- Strategy Decision Matrix.
- ROI and OMB A-11 Exhibit 300 compliance.
- COOP Strategy approval.

Understanding Threats and taking corrective actions.



5. Emergency Response and Operations Restoration

Goal: Identifying disaster events and responding to them within Service Level Agreement (SLA) times and metrics is essential and responded to through recovery plans, training, and testing procedures.

- Ensure rapid response capabilities, life safety, and infrastructure protection.

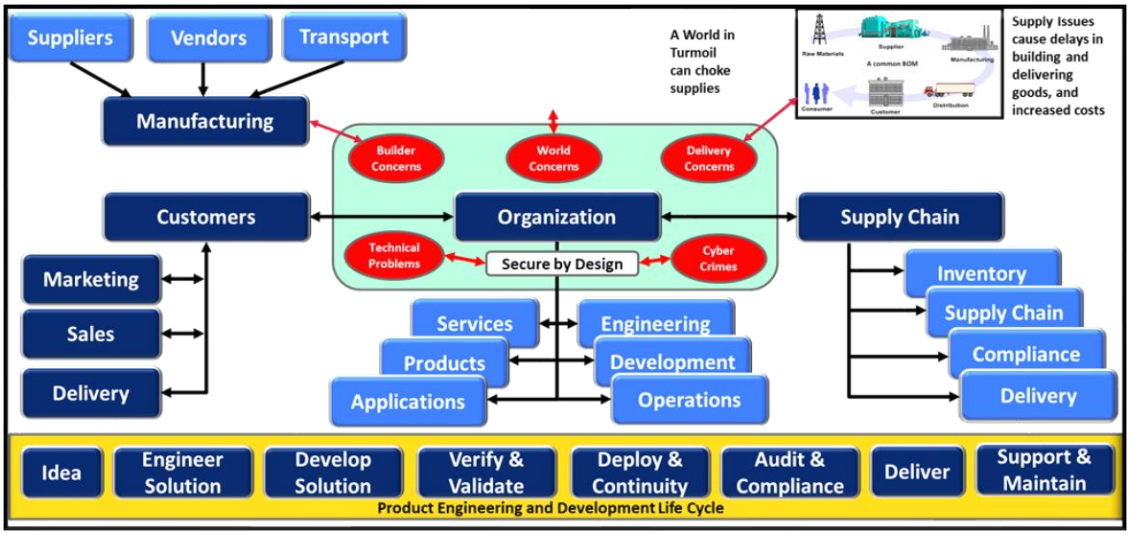
Key Actions:

- Activate Emergency Operations Center (EOC) with ICS structure.
- Contingency Control Center (CCC) to coordinate recovery efforts.
- Validate data vaulting and off-site backups.
- Coordinate with FEMA, DHS, and local responders.

Results Tracking:

- Response drill metrics.
- After-action reviews (AARs).
- FEMA grant and compliance checklists.

Protecting your organization is becoming more difficult.



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

6. Designing and Implementing Business Continuity Plans

Goal: Recovery Plan content requirements are defined and recovery plans created during this step of the project. Teams are trained in recovery plan requirements and plans are evaluated to both train teams and assure accuracy of plans.

- Document and maintain functional plans for recovery and compliance.

Key Actions:

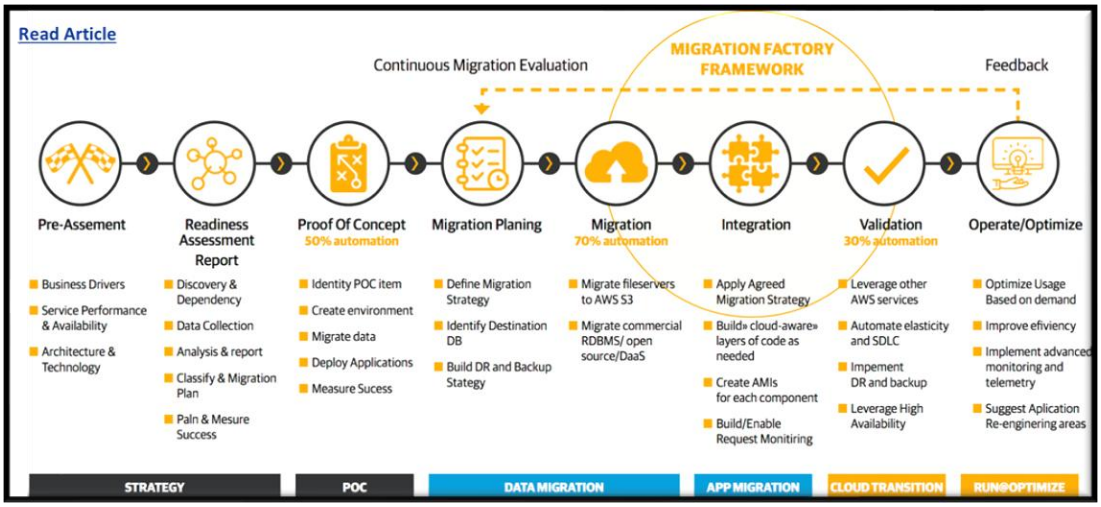
- Use standardized templates for each department.

- Incorporate access control, escalation, and contact rosters.
- Maintain version control and audit logs.

Results Tracking:

- Plan completeness scoring.
- Annual FISMA reporting integration.
- Plan updates approved by division leads.

Designing and Implementing Disaster Recovery Plans

- 

7. Awareness and Training

Goal: Personnel and management must be made aware of the Business Continuity Management process and how it works. Awareness sessions should be conducted and video presentations made available to define the BCM process. Training classes should be conducted for team members and stakeholders responsible for defining and declaring a disaster event.

- Embed continuity culture agency wide.

Key Actions:

- Deliver training tied to federal role-based guidelines.
- Integrate into onboarding and annual ethics/compliance programs.
- Conduct tabletop and Red Team exercises.

Results Tracking:

- Completion reports.
- Training dashboard for executive review.
- Semi-annual executive awareness sessions.

Disaster Recovery Awareness and Training outline

Business resilience refers to an organization's ability to adapt, recover, and thrive in the face of disruptions or unexpected changes that could impact its operations, people, assets, brand, or reputation. It positions organizations to prepare for anything that might come their way[1].

Here's a plan on how to achieve business resilience within a major organization:

1.Risk Assessment and Identification:
1. Conduct a comprehensive risk assessment to identify potential threats and vulnerabilities. Consider both internal (e.g., supply chain disruptions, cyber attacks) and external (e.g., natural disasters, economic downturns) risks.
2. Engage stakeholders from various departments to ensure a holistic view of risks.

2.Business Continuity Planning:
1. Develop a robust business continuity plan (BCP) that outlines procedures for maintaining essential functions during disruptions.
2. Define roles, responsibilities, and communication channels during crises.
3. Regularly review and update the BCP to align with changing circumstances.

3.Diversify Supply Chains:
1. Relying on a single supplier or geographic region can be risky. Diversify suppliers and build redundancy.
2. Establish alternative sourcing options to mitigate supply chain disruptions.

4.Invest in IT Infrastructure and Security:
1. Strengthen IT systems and cybersecurity protocols.
2. Implement data backup and recovery mechanisms.
3. Train employees on security best practices.

5. Establish Strategic Direction and select supportive tools
1. Recovery Management Tool
2. Awareness and training

6.Employee Safety and Well-being:
1. Prioritize employee safety during disruptions.
2. Establish protocols for tracking remote and onsite workers' health and availability.
3. Provide mental health support and resources.

7.Scenario Testing and Drills:
1. Regularly conduct scenario-based testing and drills to validate the effectiveness of your resilience strategies.
2. Simulate disruptions and evaluate the organization's response.

8.Agility and Adaptability:
1. Foster an organizational culture that embraces change and agility.
2. Encourage cross-functional collaboration and innovation.
3. Be prepared to pivot swiftly when necessary.

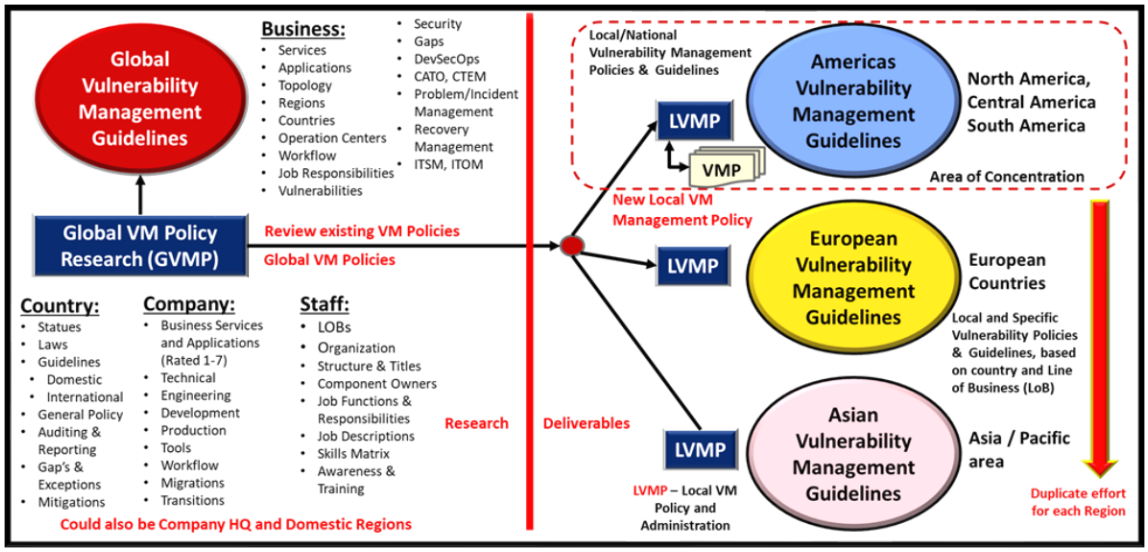
9.Communication and Stakeholder Engagement:
1. Maintain transparent communication with employees, customers, suppliers, and other stakeholders.
2. Establish crisis communication protocols.
3. Address concerns promptly and proactively.

10.Learn from Past Disruptions:
1. Analyze previous disruptions and learn from them.
2. Identify areas for improvement and implement corrective actions.

11.Leadership Commitment:
1. Ensure that senior leadership actively supports and champions business resilience initiatives.
2. Allocate resources and budget for resilience planning and implementation.

Remember that business resilience is an ongoing process. Regularly assess, adapt, and refine your strategies to stay prepared for the unexpected[123].

Implementing Risk & Vulnerability Management with Continuity Services



Formalize guidelines for the entire enterprise and ensure they are integrated into the everyday functions provided by the staff.

8. Maintaining and Exercising Business Continuity Plans

Goal: Recovery Plans must be periodically updated as changes are made. Testing and awareness training must be continuous along with in-depth training sessions as newer employees are assigned recovery functions.

- Verify effectiveness and improve through continuous testing.

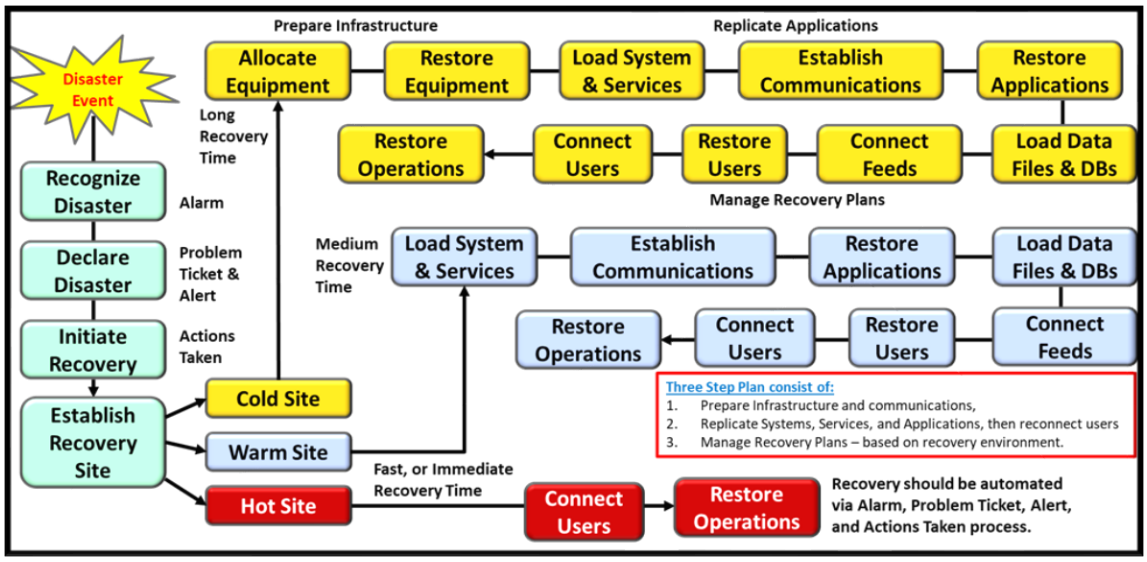
Key Actions:

- Tabletop, simulation, and full-scale exercises.
- Incorporate COOP activation and relocation testing.
- Annual FCD-2 (Federal Continuity Directive) compliance assessments.

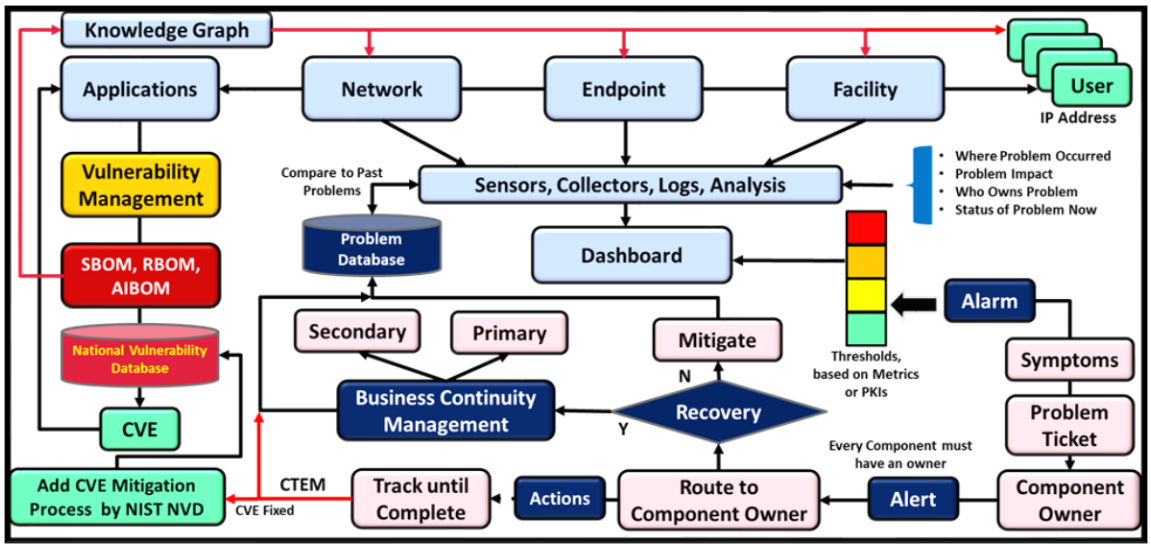
Results Tracking:

- Evaluate success metrics.
- CAP logs and resolution tracking.
- Plan to refresh schedule compliance.

Planning and executing recovery plans.



Tracking problems and initiating recovery operations



9. Public Relations and Crisis Communications

Goal: when disaster events occur, the company should have a single voice to speak with the public and the media. Teams should be formed to speak with impacted families and to address a wide array of questions from the public and family members. Communications from the Contingency Command Center to EOC Management provides status reports, while executive management represents the company to the public.

- Maintain public trust and transparency.

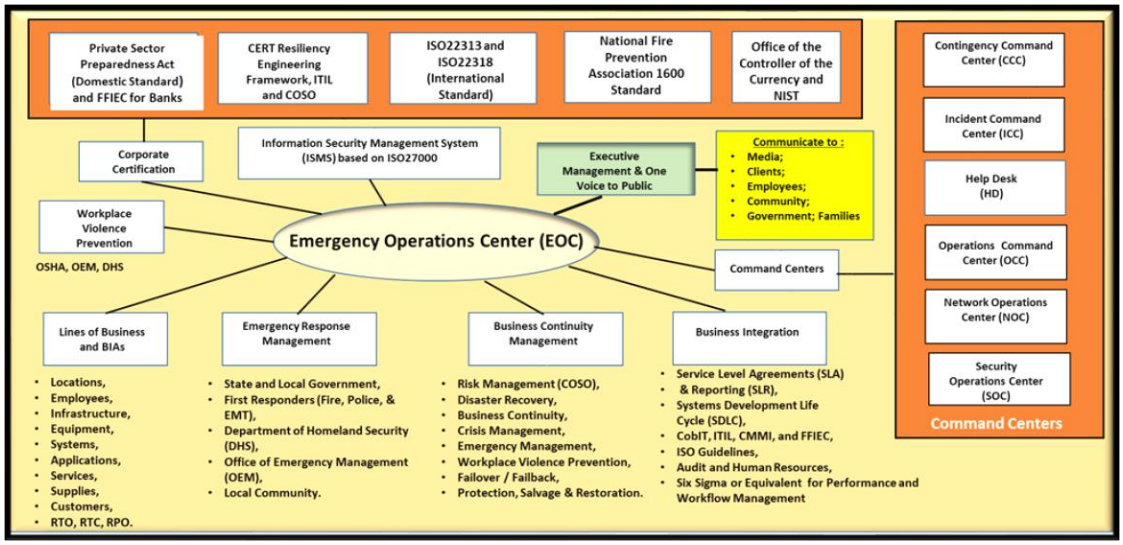
Key Actions:

- Crisis Communications Plan aligned with JIC protocols.
- Pre-approved statements were vetted through General Counsel.
- Coordination with Agency PIO and DHS.

Results Tracking:

- Message impact analytics.
- JIC participation logs.
- FOIA-compliance recordkeeping.

Emergency Operations Center



- Used to provide rapid response to disaster events by having major decision makers within the EOC. CCC provide recovery status reports and any problems that are experiences, executive management coordinated rapid responses to support recovery needs.

10. Coordinating with Public Authorities

Goal: Communications must be conducted with media, first responders, government officials, staff family members and others. Planning responses and defining public relations communications will help coordinate outside communications and safeguard the company's reputation.

- Ensure response and recovery align with multi-agency and federal expectations.

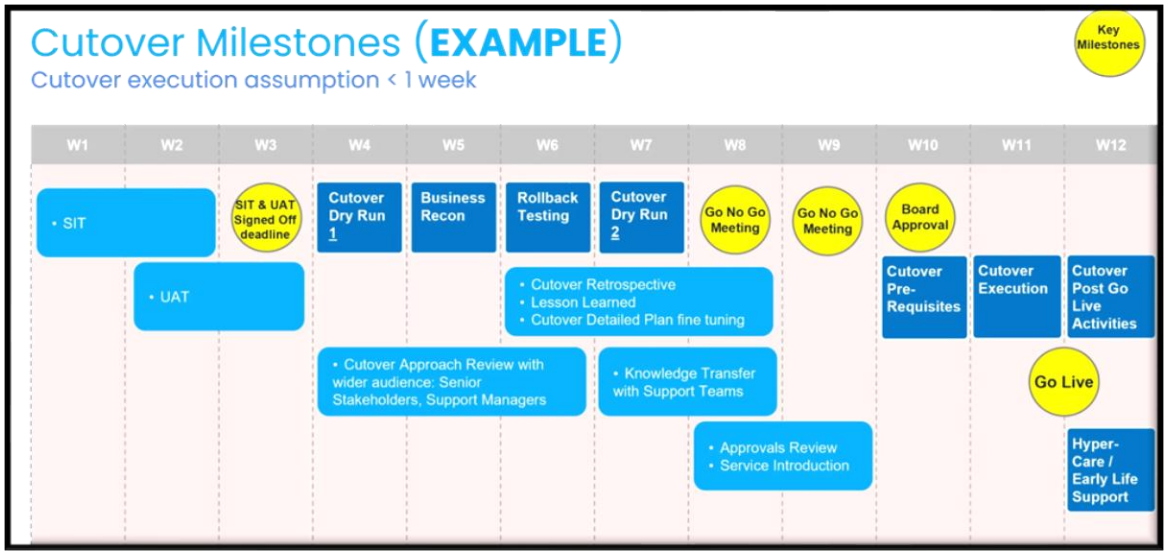
Key Actions:

- Register with FEMA, DHS, state and regional emergency agencies.
- Sign MOUs with peer agencies.
- Participate in joint exercises and continuity calls.

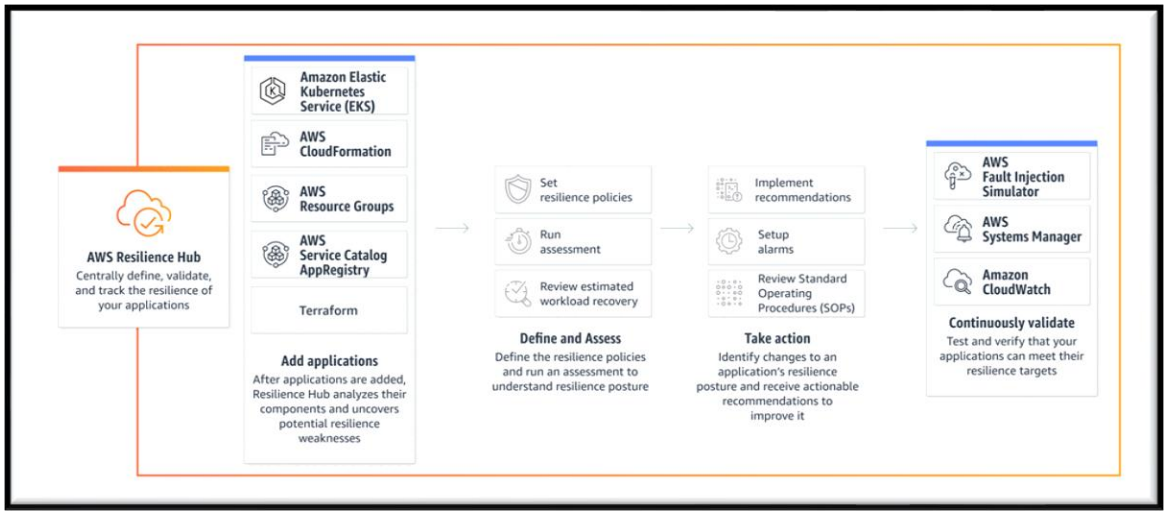
Results Tracking:

- MOU repository and contact directory.
- FEMA and DHS exercise certification.
- Multi-agency incident AARs.

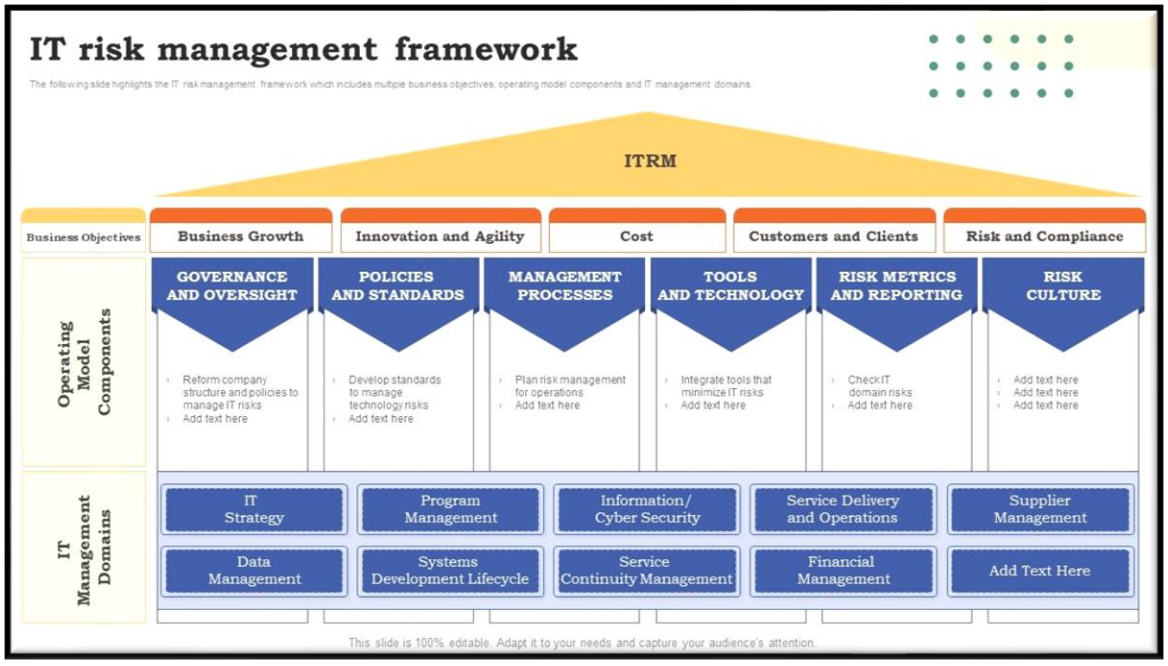
Cutover Product



AWS Resilience Hub



Fusion Risk Management



Governance and Oversight

Steering Committee: Chaired by CIO, with participation from CISO, COOP Coordinator, Legal, and Ops.

Tools Used: MS Project, Asana, ServiceNow, FedRAMP-authorized PM tools.

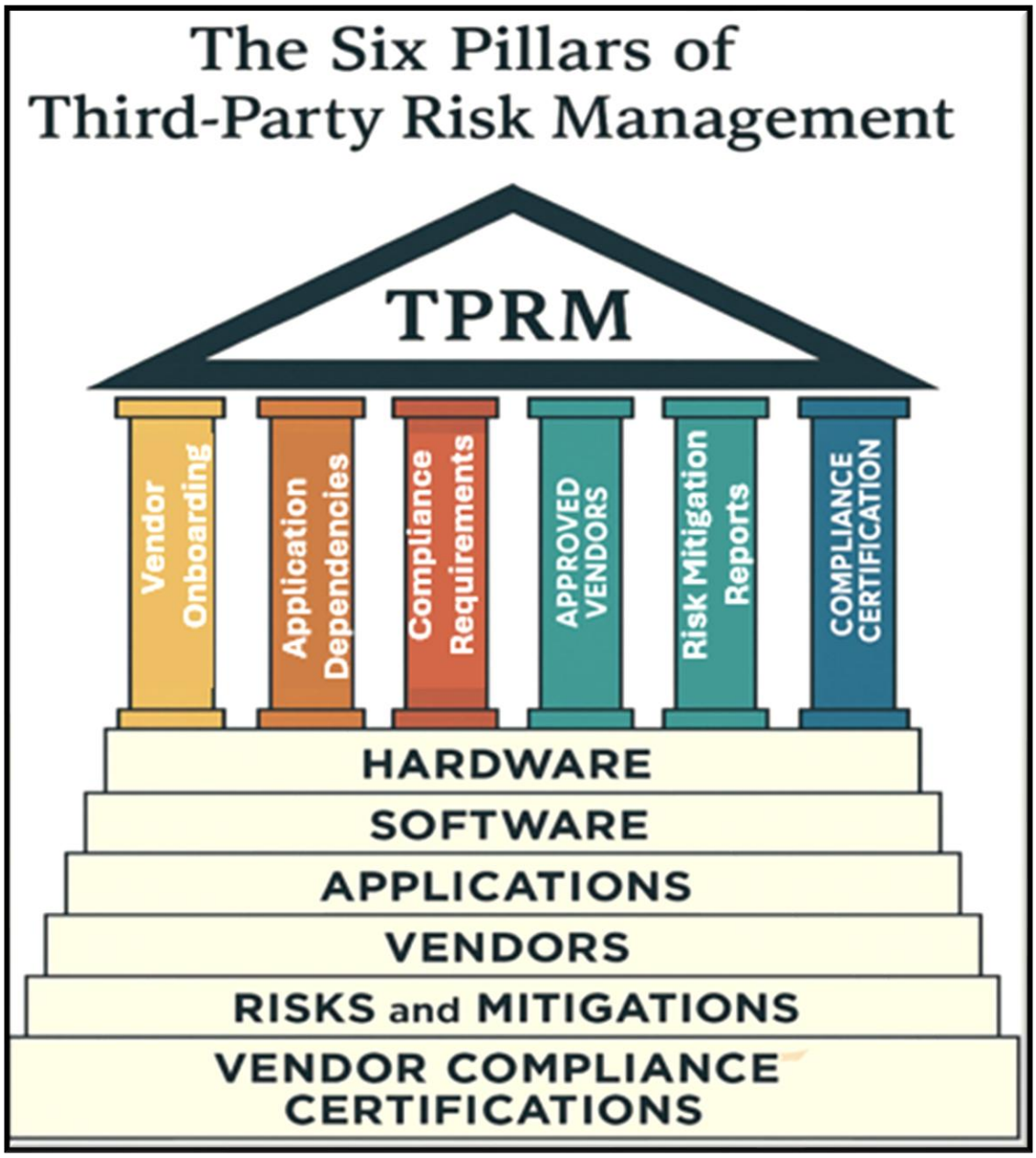
Reporting Cadence:

- Weekly project status reports (WBS, risks, metrics)
- Monthly executive dashboards
- Quarterly board and OMB briefings

Compliance Checks:

- Annual FISMA control assessments
- NIST 800-34 testing documentation
- COOP/FCD readiness scoring.

Third-Party Risk Management



Third-Party Risk Management (TPRM) is the structured process an organization uses to identify, assess, monitor, and mitigate risks that come from its relationships with external vendors, suppliers, or service providers.

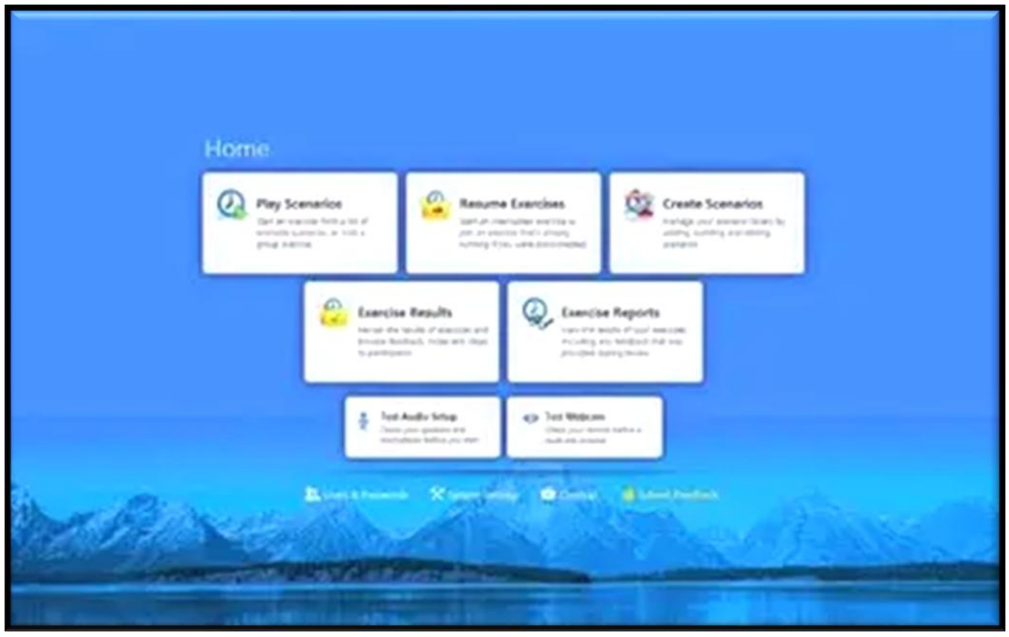
It is accomplished by:

1. **Identifying and Classifying Vendors** – Creating a complete inventory of third parties, their products, and the criticality of the services they provide.

2. **Assessing Risk** – Evaluating vendors for cybersecurity, compliance, operational, and reputational risks using questionnaires, audits, and performance metrics.
3. **Establishing Controls** – Embedding contractual safeguards, security requirements, and service level agreements (SLAs) into vendor relationships.
4. **Ongoing Monitoring** – Continuously tracking vendor performance, regulatory compliance, and emerging risks through dashboards, reports, and periodic reviews.
5. **Remediation and Offboarding** – Implementing Plans of Action & Milestones (POA&Ms) to address issues and ensuring secure, compliant disengagement when a relationship ends.

In practice, TPRM integrates governance, procurement, compliance, and IT security teams to ensure vendors meet organizational standards, protect sensitive data, maintain operational resilience, and comply with applicable laws and regulations.

Avalanche TTX



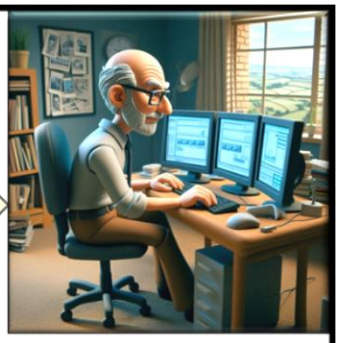
This tool allows you to quickly develop recovery procedures and enables the quick creation of Awareness and Training sessions based on actual product performance and screens.

For additional information, or to discuss your needs, please contact us.

- Discuss
- Define
- Propose
- Achieve

Quality Service at a Reasonable Price

Helping Clients to achieve success



If you find the information included in this presentation of value and want to explore methods to improve the reliability of your enterprise and IT environment, please contact me to discuss your needs and request our assistance.

We look forward to our future relationship.

Thomas Bronack, CBCP
President
Data Center Assistance Group, LLC

bronackt@dcag.com
bronackt@gmail.com
917-673-6992

