Thomas Bronack, CBCP

Presentation Topics

- Hazards faced by Companies
- Know Your Enterprise
- Governance.
- Risk Management,
- Compliance,
- Business Continuity Management,
- Vulnerability Management,
- Full Systems Development Life Cycle,
- ATO / cATO Production Services,
- Business Continuity

Tom Specializes in:

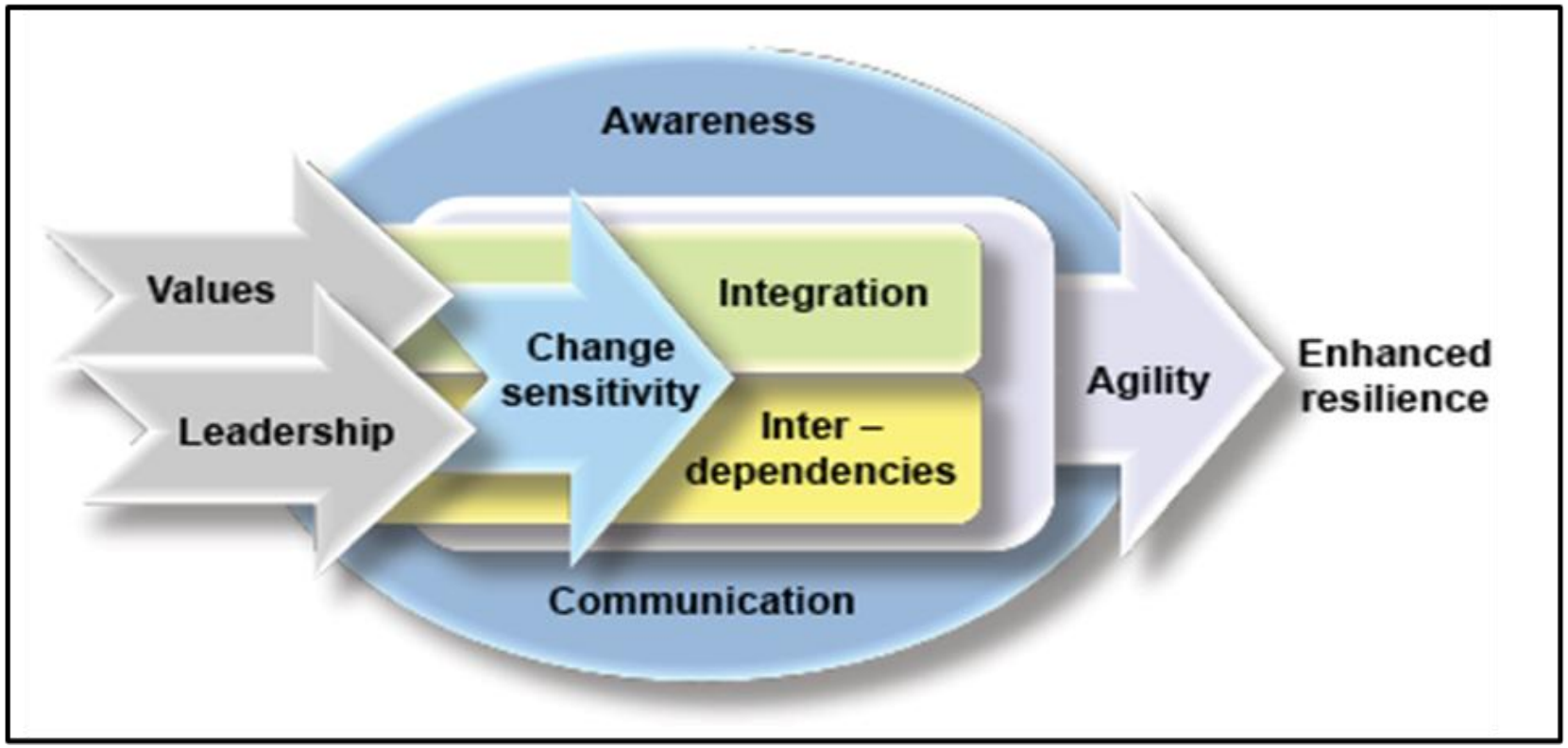
- Enterprise Resilience,
- Corporate Certification,
- Vulnerability Management,
- Cyber Security,
- Post Quantum Cryptography (PQC),
- Inventory, Configuration & Asset Management,
- Strategic and Tactical Planning,
- Project and Team Management
- Awareness and Training

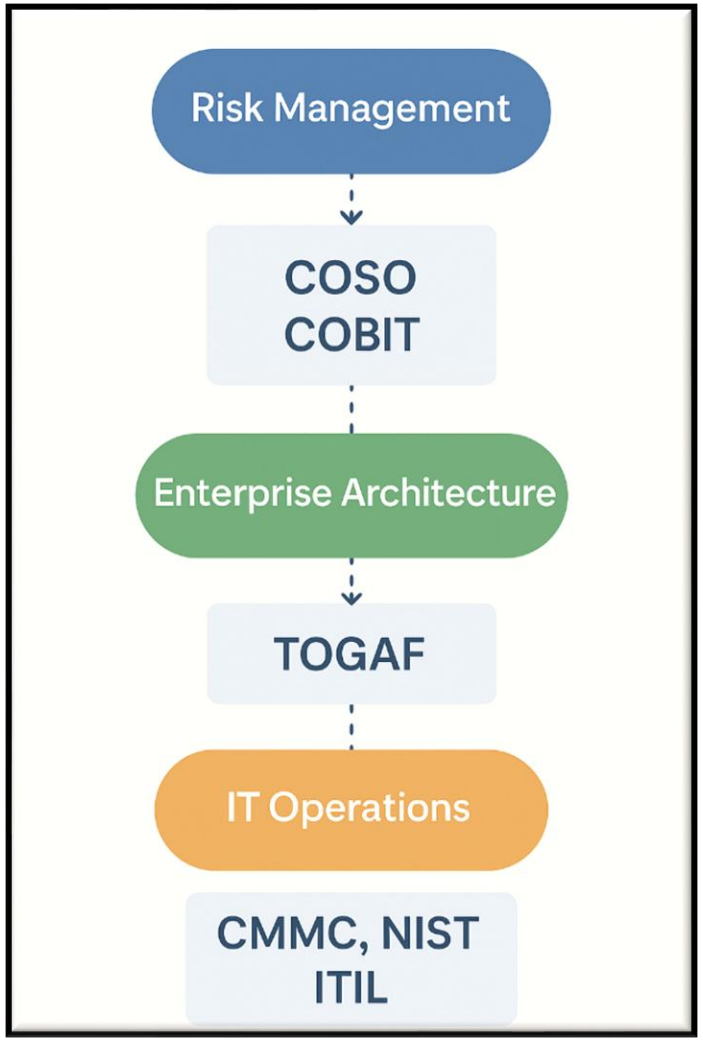
Governance, Risk Management, and Compliance - GRC

Contact Information:

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

The Pathway to a Resilient Business

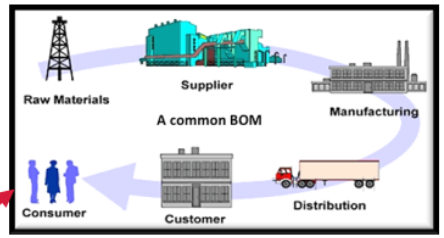




- **Know your Business.**
- **Relate your business goals to IT Services.**
- **Analyze Risks and Define Controls.**
- **Build your Service Environment and ensure quality.**
- **Provide Service Continuity and Recovery Management**
- **Ongoing Monitoring and improvement**

Protecting your organization is difficult

A World in Turmoil can choke supplies



Supply Issues cause delays in building and delivering goods, and increased costs

Suppliers
Vendors
Transport
Manufacturing
Builder Concerns
World Concerns
Delivery Concerns
Customers
Organization
Supply Chain
Technical Problems
Secure by Design
Cyber Crimes
Sales
Marketing
Services
Products
Applications
Engineering
Development
Operations
Inventory
Supply Chain
Delivery

Idea
Engineer Solution
Develop Solution
Verify & Validate
Deploy & Continuity
Audit & Compliance
Deliver
Support & Maintain

Product Engineering and Development Life Cycle

Getting started with facts and a defined direction

Know your company:

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

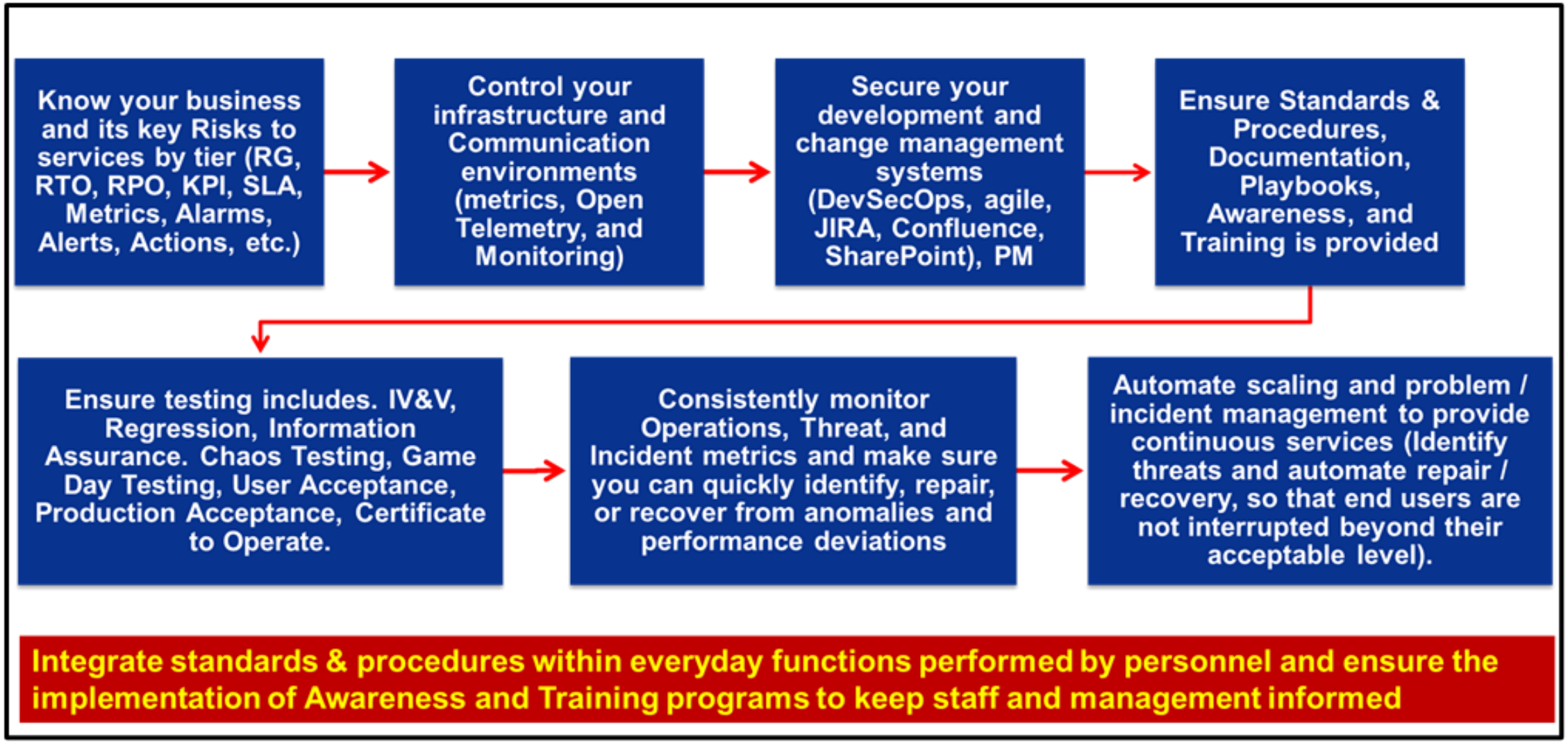
Know your Environment:

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.

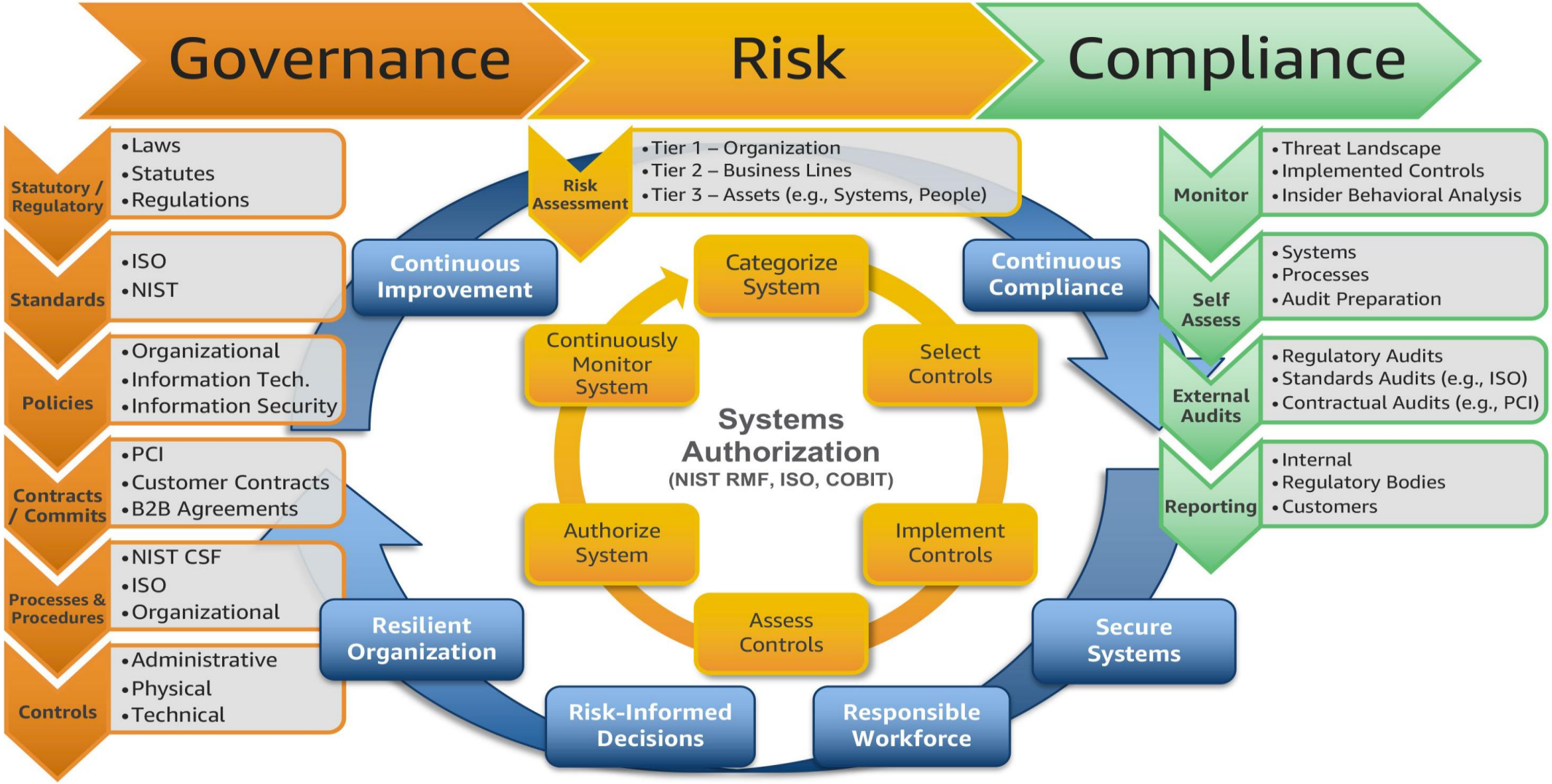
Set you direction:

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.

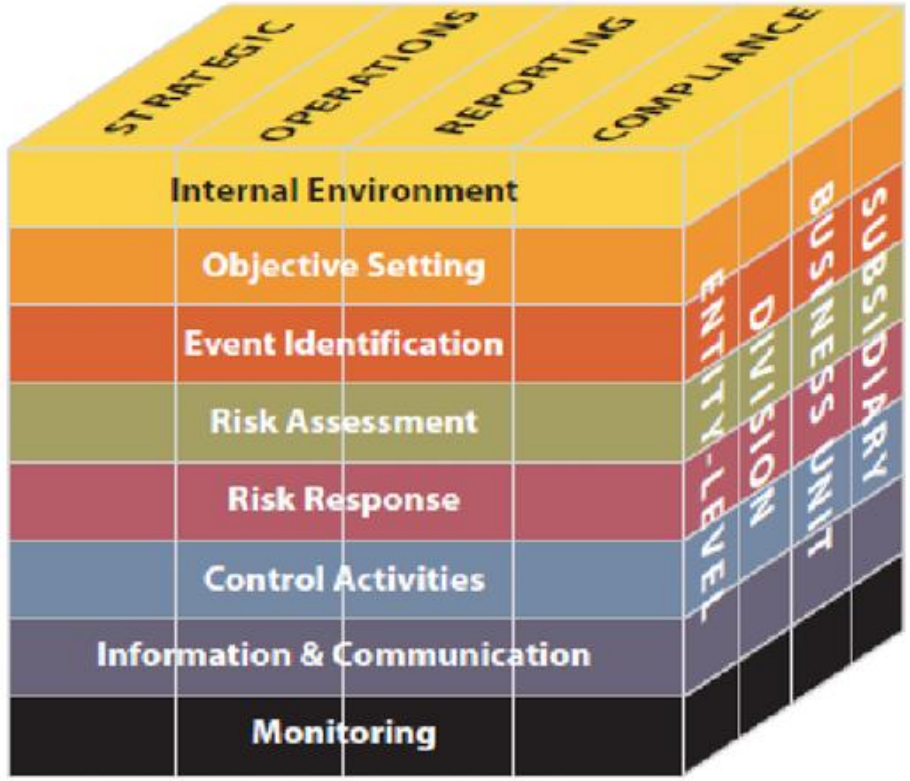
Understanding your Business for better protection



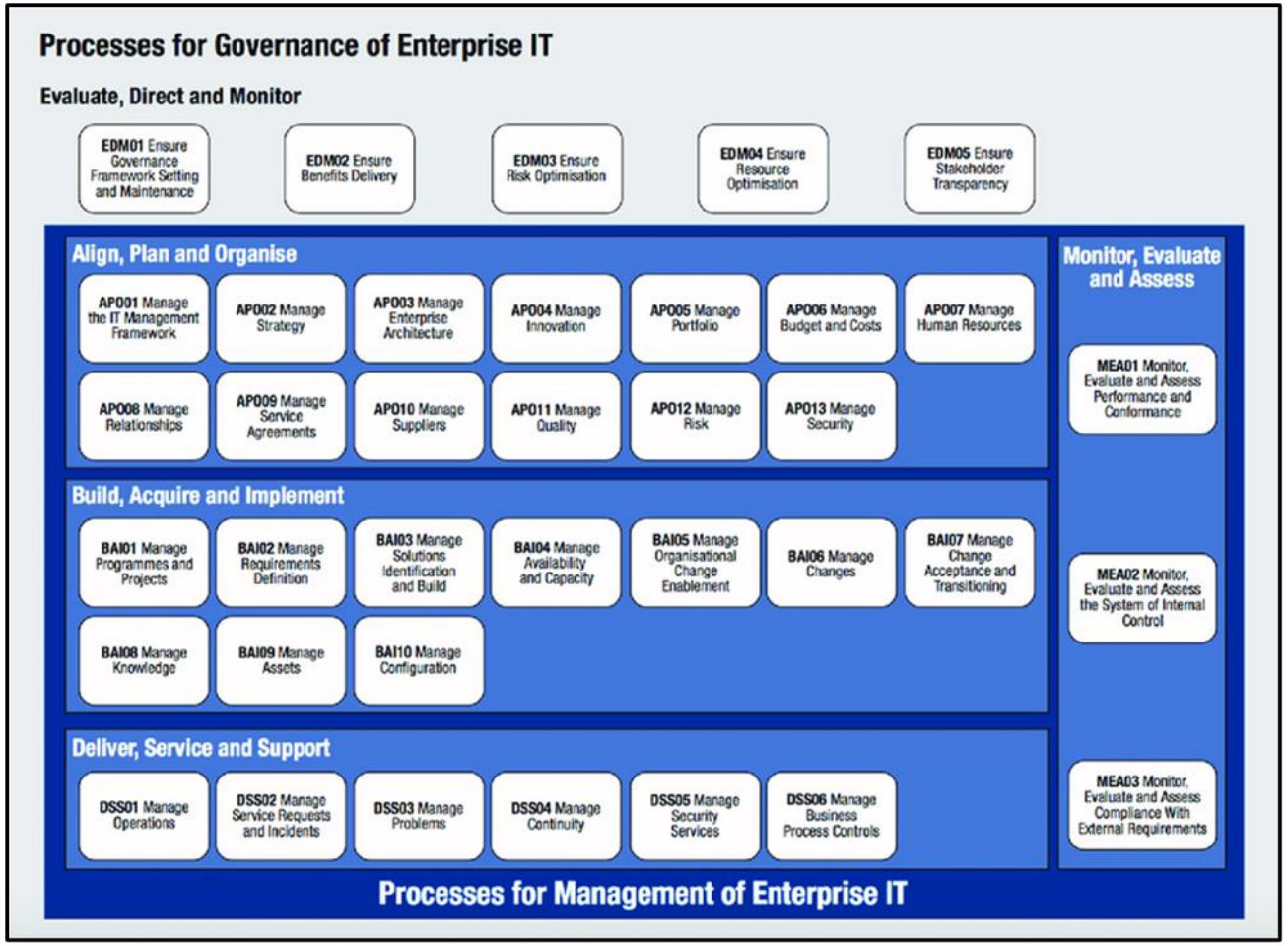
The three pillars of GRC – Governance, Risk, and Compliance



COSO and COBIT Analysis Frameworks

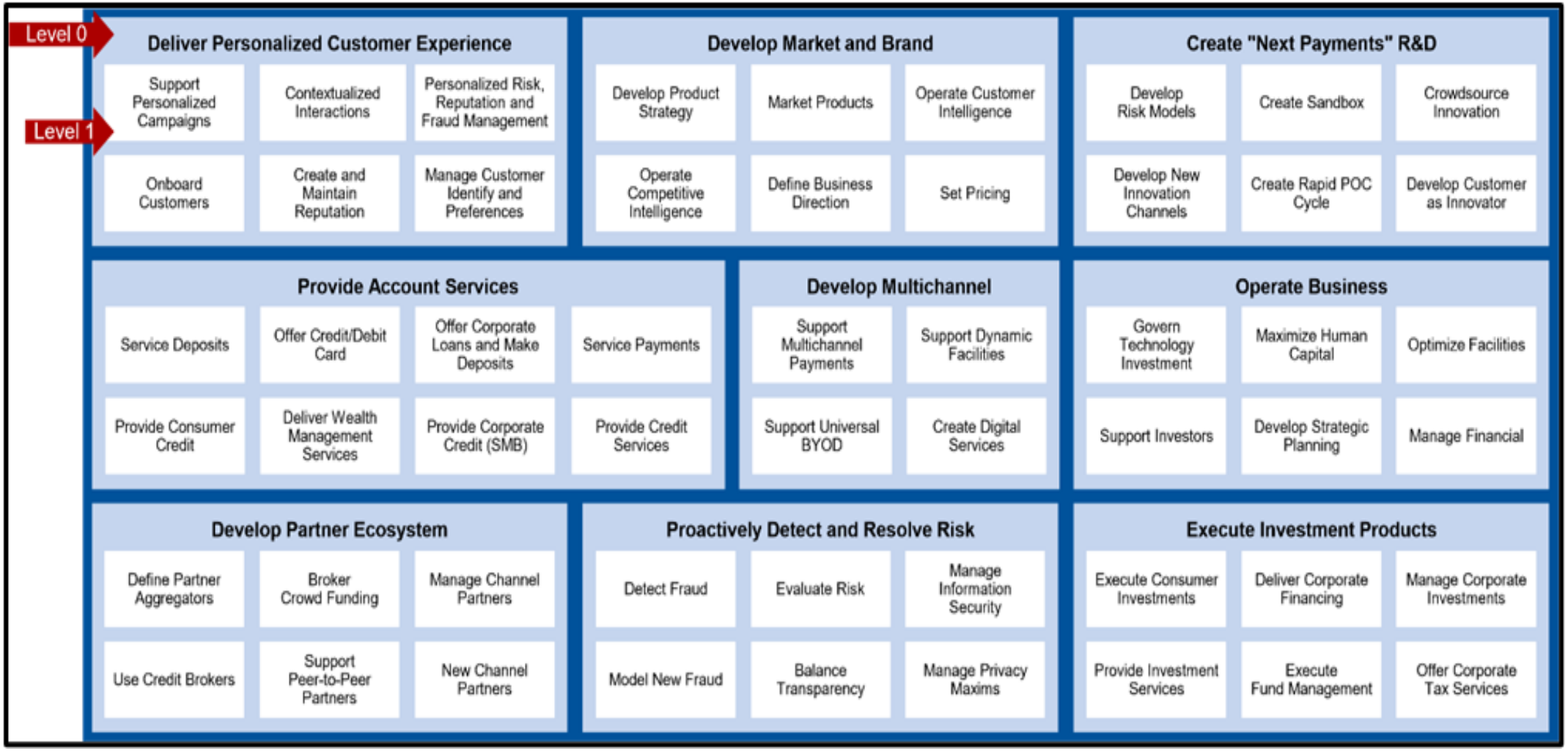


COSO – Committee of Sponsoring Organizations

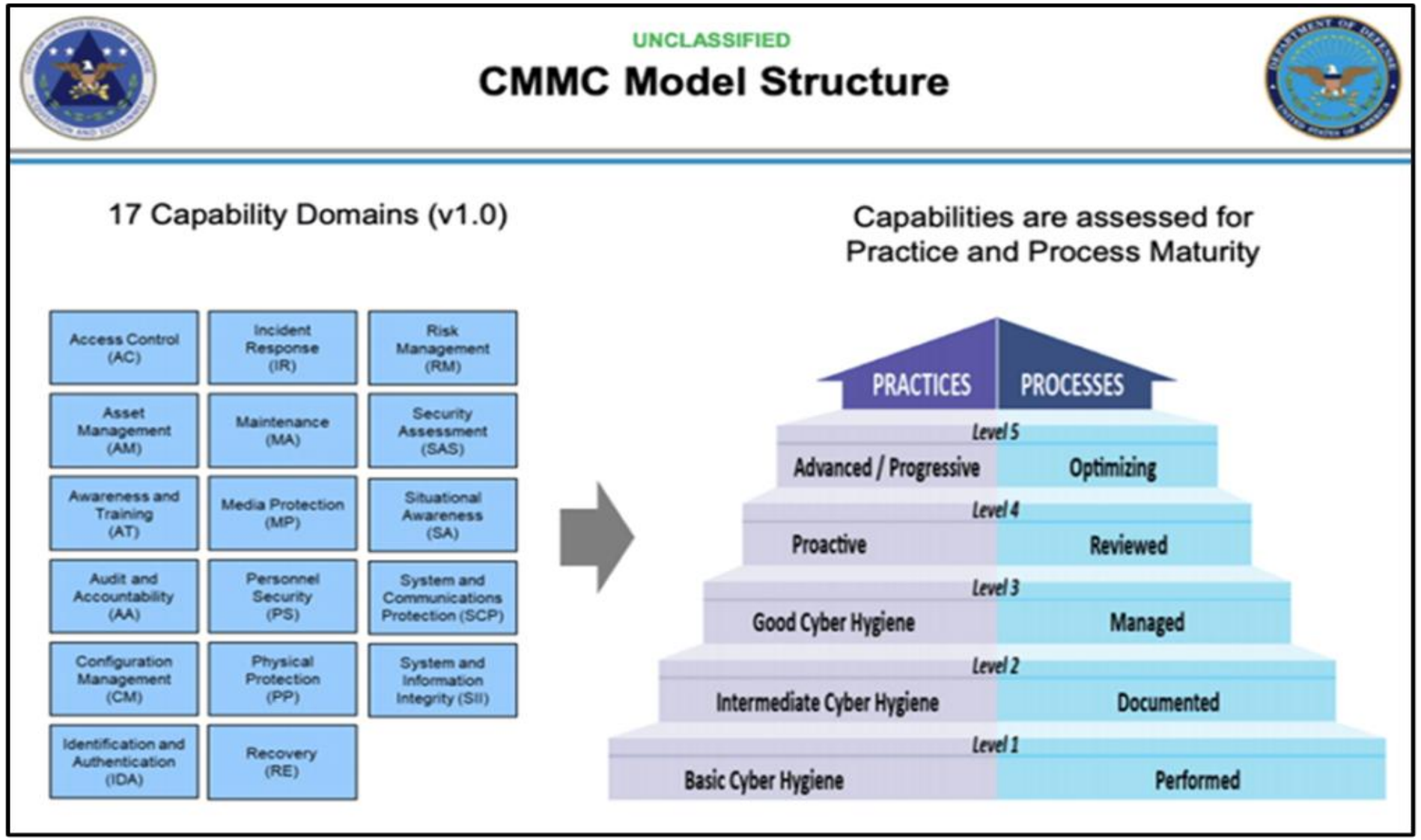


COBIT - Control Objectives for Information and Related Technology

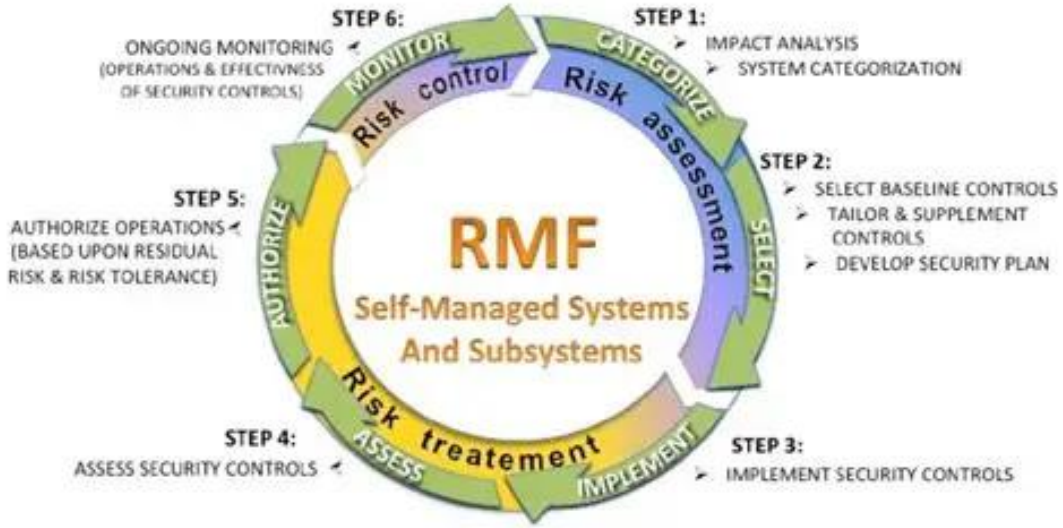
CMMI - Cybersecurity Maturity Model Integration



CMMC - Cybersecurity Maturity Model Certification



Risk Management Framework (RMF) NIST SP 800-37

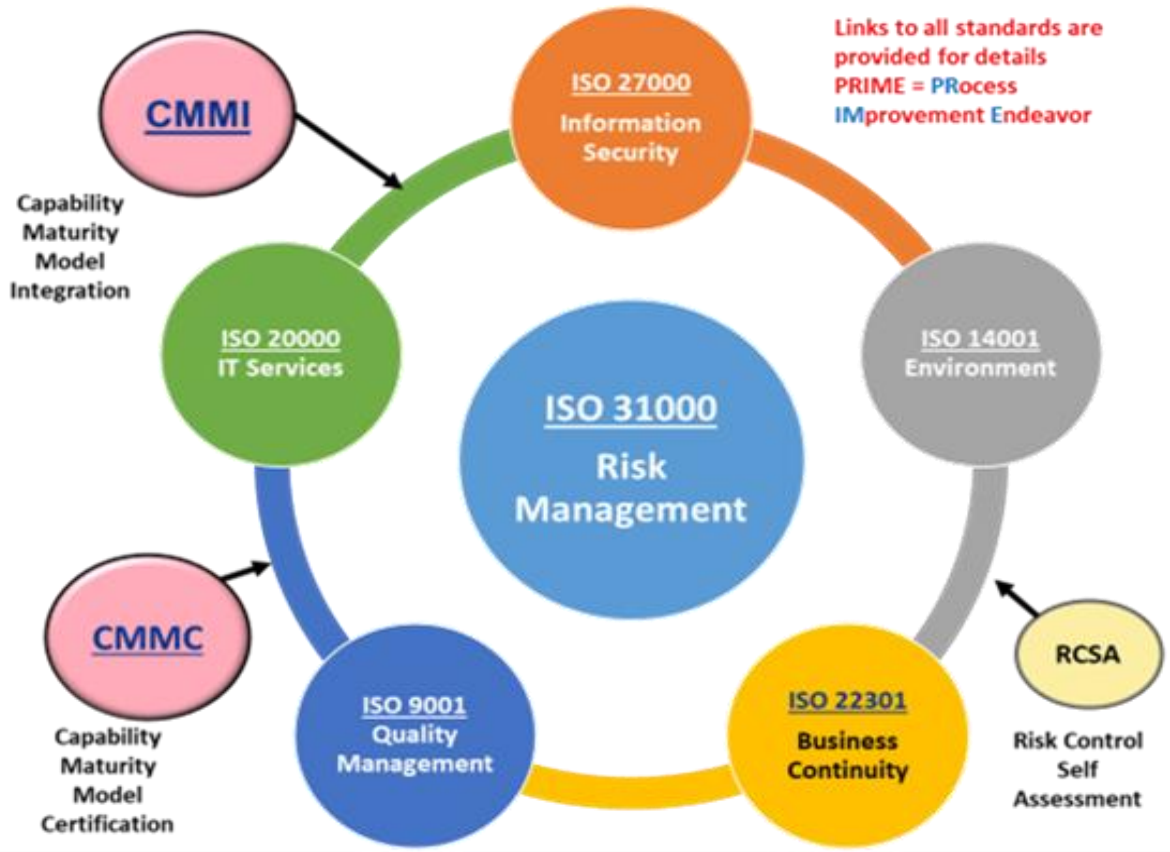


RMF Stages:

1. **Impact Analysis**
2. **Baseline Controls**
3. **Security Controls**
4. **Assess Security Controls**
5. **Authorize Operations (ATO & cATO)**
6. **Monitoring and Repair**

Integrating Protection Frameworks

The newest Integration Model – PRIME Approach



Developing a business optimization approach that combines these ISO Standards will help your company achieve certification more quickly.

Implementing the standards separately will result in overlaps and inefficiencies.

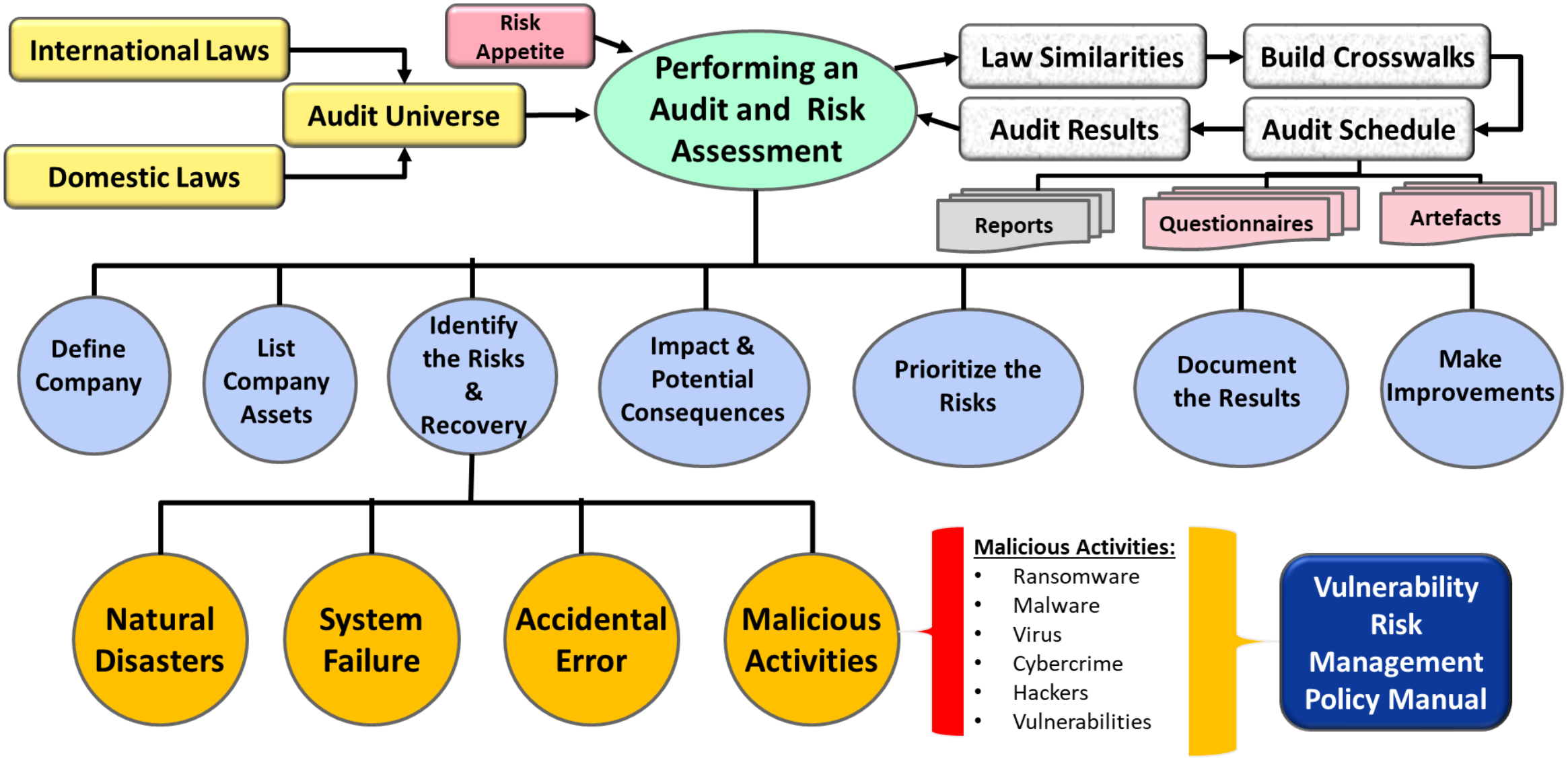
Start with **Risk Management** (31000) and ensure that **Information Security** (ISO 27000) is current and best suited to protect your **Data** and **Environmental facilities** (ISO 14001).

Then implement your **Business Continuity** (ISO 22301) Recovery Certification Process for Emergency, Crisis, Business, and IT Disaster Recovery Management.

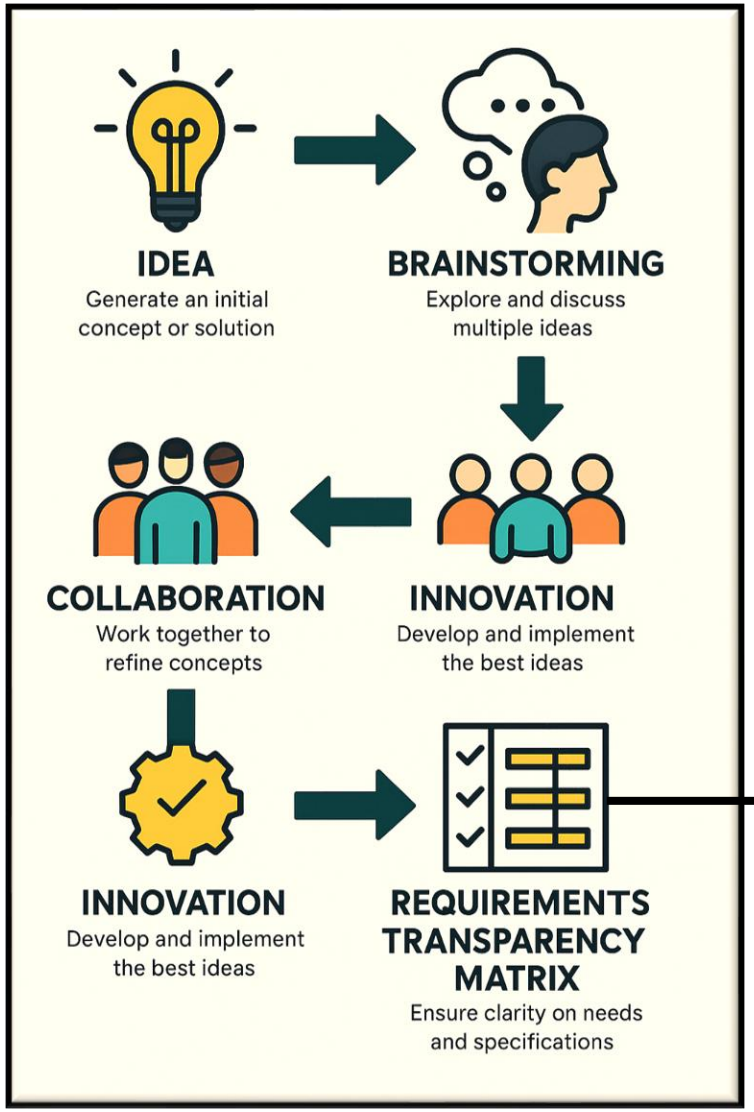
Integrate Quality Management (ISO 9001) within all of your processes to ensure the products and services your company delivers will be of the highest quality and capable of protecting your brand and reputation.

Finally ensure your **IT Services** (ISO 20000) are of the highest quality possible and that all ISO standards are adhered to in compliance with existing laws and regulations, so that you never have to fear failing an audited.

Performing an Audit and Risk Assessment



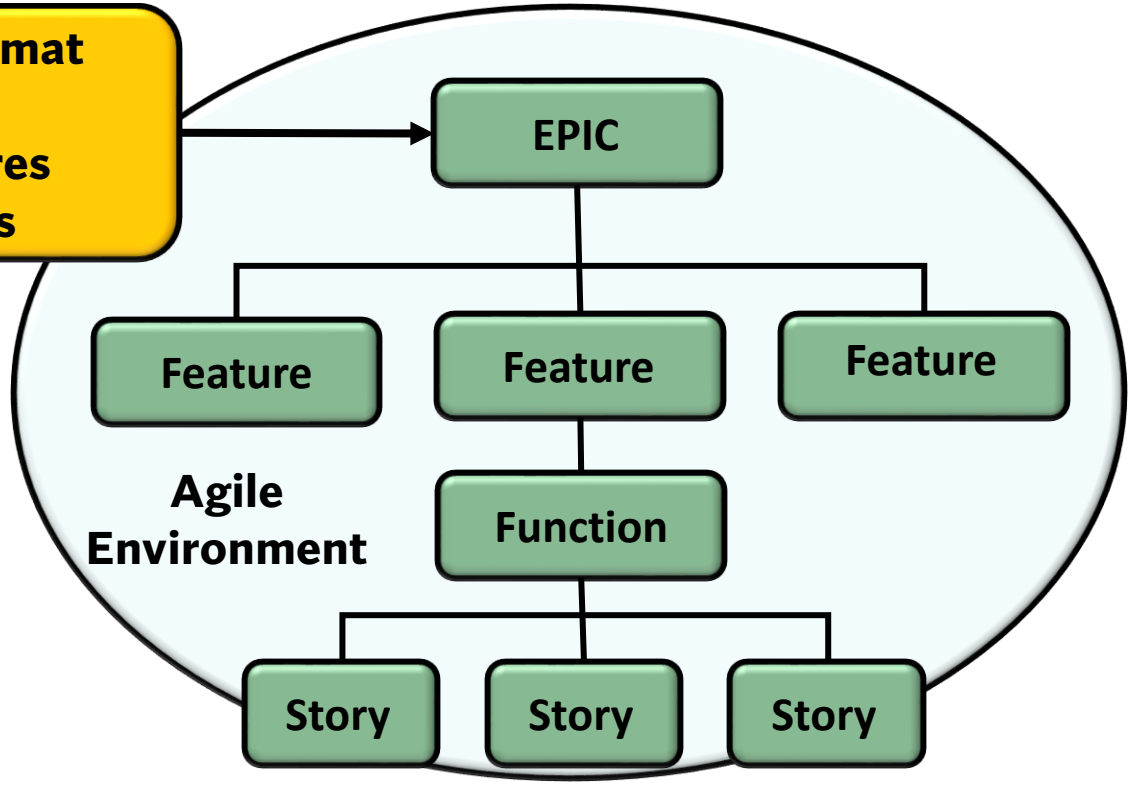
Concept to Requirements Transparency Matrix (RTM)



Requirements Transparency Matrix (RTM)

RTM Review
- Acceptance Review
- Features & Functions
- Specific Operations

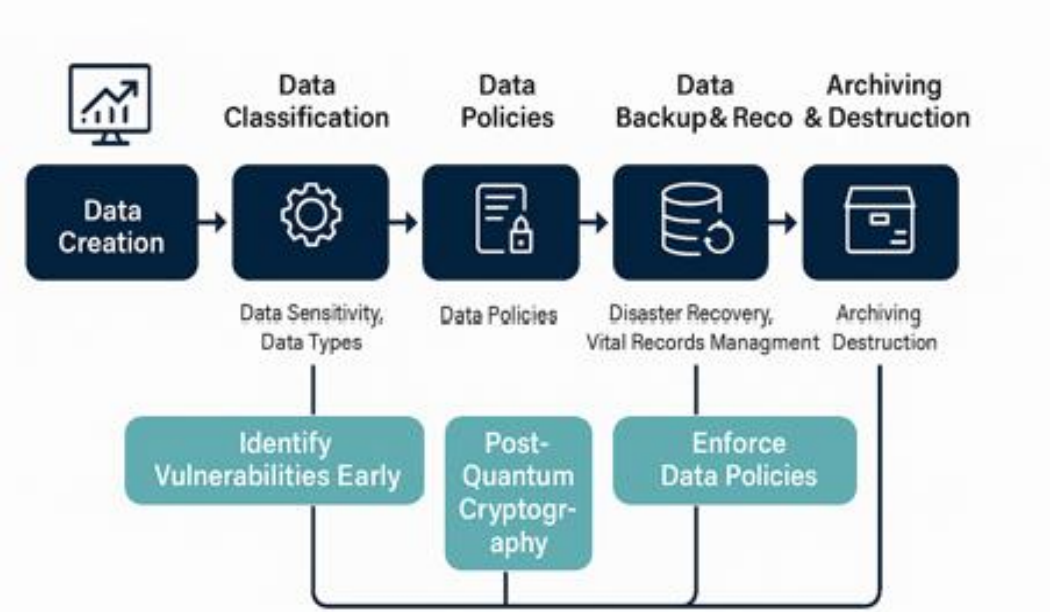
Agile Format
- **Epic**
- **Features**
- **Stories**



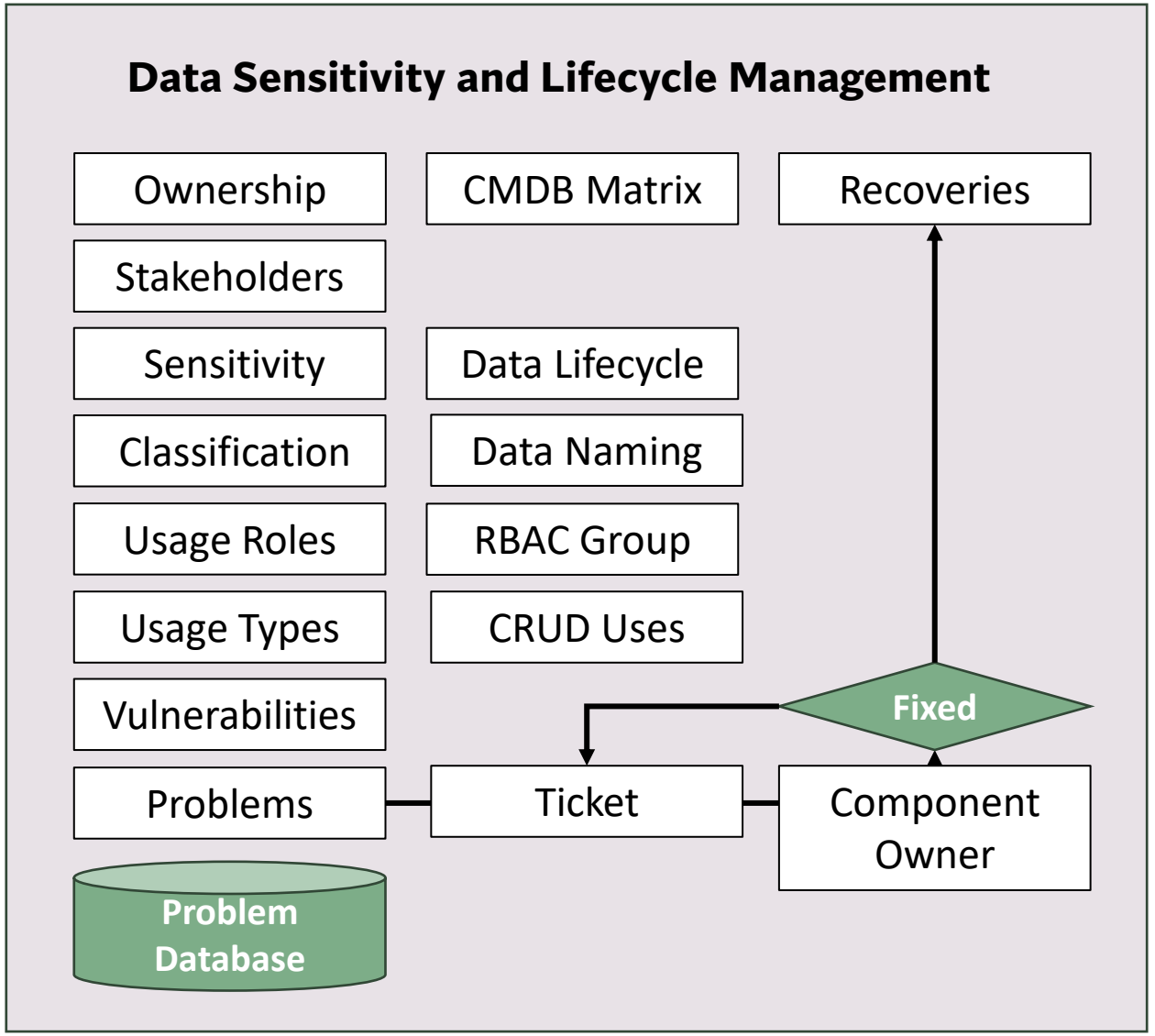
Requirements Transparency Matrix (RTM)

Requirements Transparency Matrix (RTM)	
Column Title	**Description**
Requirement ID	Unique identifier for traceability (e.g., REQ-001)
Requirement Name	Short title or label for the requirement
Description	Clear and detailed explanation of the requirement
Source / Stakeholder	Origin of the requirement (department, person, or document)
Business Objective	Related strategic goal or business driver
Priority (High/Med/Low)	Relative importance or urgency of the requirement
Type (Functional/Non-Functional)	Categorization of requirement type
Status (Proposed/In Progress/Met)	Current state of the requirement
Owner / Responsible Party	Individual or team accountable for delivery
Dependencies	Other requirements or systems that this one depends on
Acceptance Criteria	Conditions or tests for requirement to be considered fulfilled
Verification Method	How the requirement will be tested or validated
Traceability to Use Case / Feature	Related use case, user story, or system feature
Change History	Notes or logs of revisions to the requirement
Comments / Notes	Additional context or communication between stakeholders

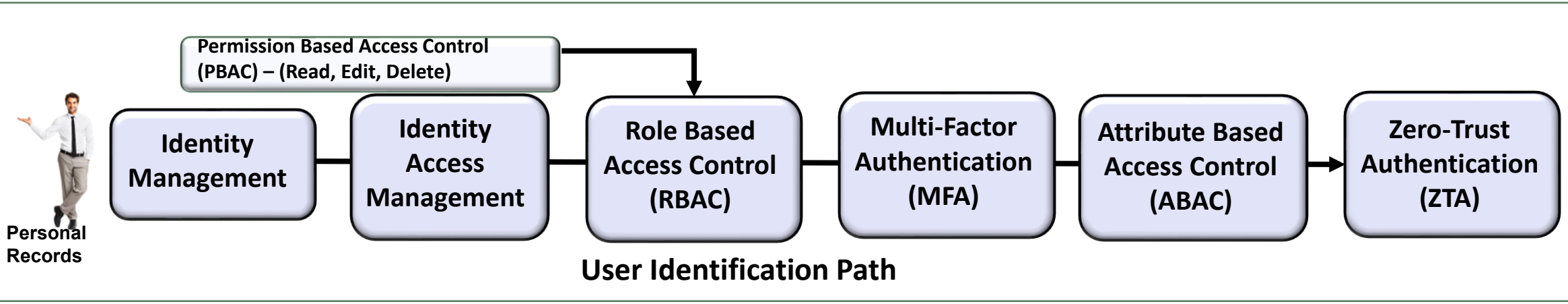
Data Sensitivity, Security, and Problems Resolution

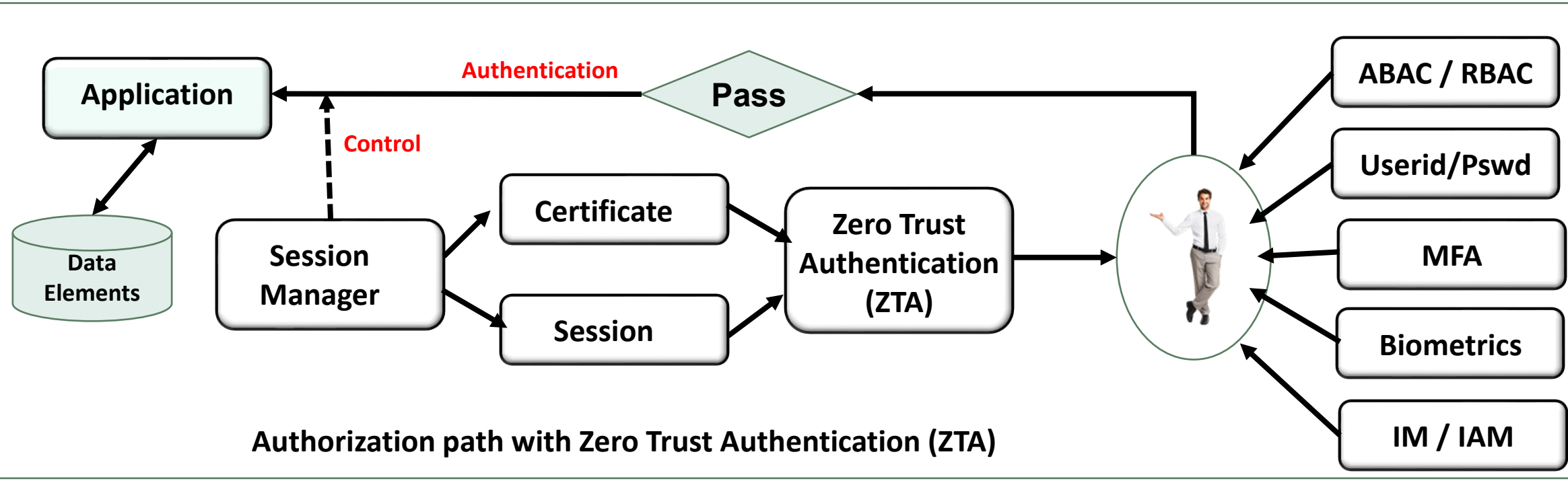


- Identify Data and its owner, then
- define Sensitivity and Protection Requirements,
- Data Lifecycle and Naming conditions,
- Employ Data Security & Encryption, and
- Allow access based on Location, Group and Usage Type (RBAC).
- Include in Problem and Vulnerability Management system, by tying component to owner.



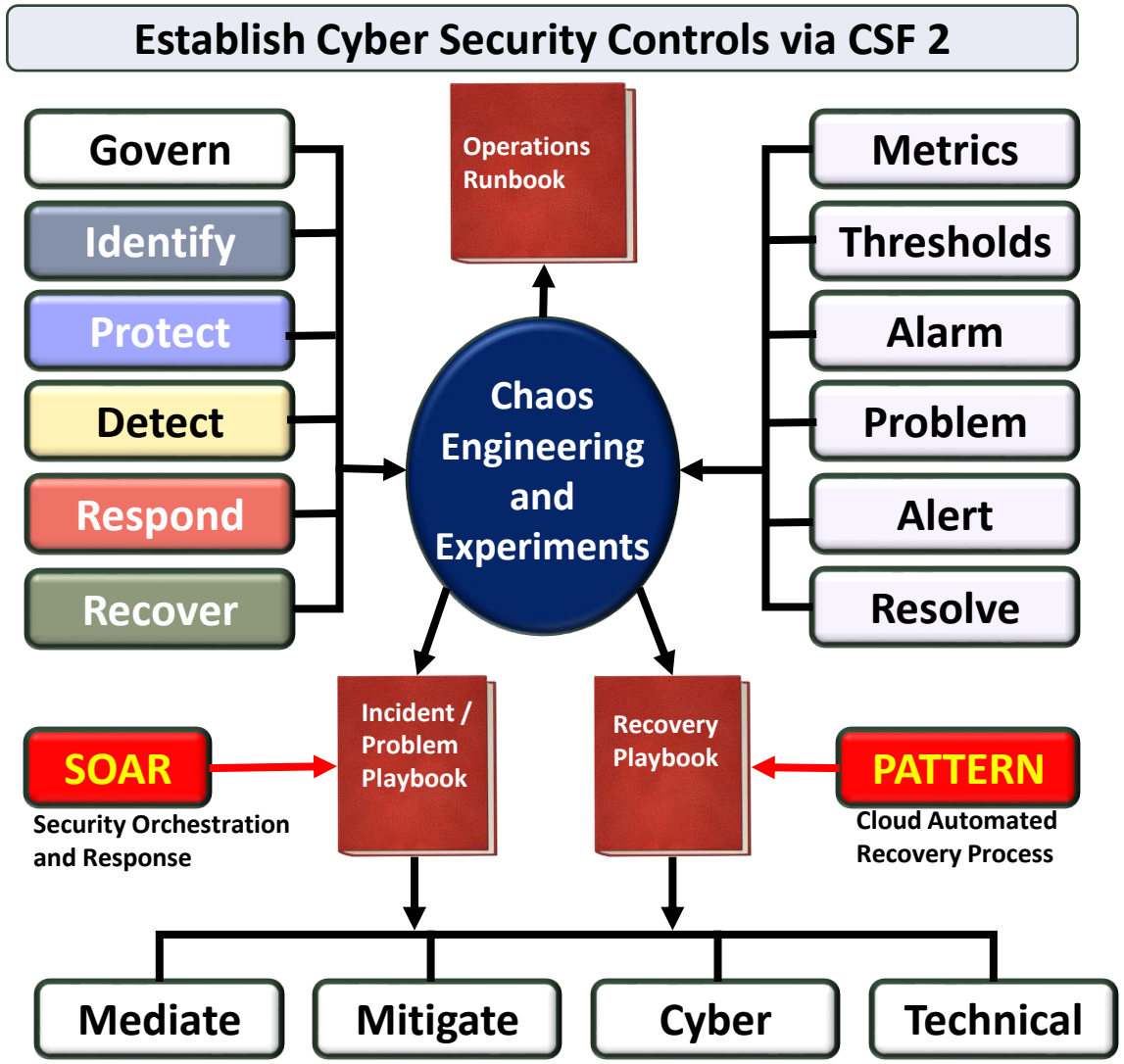
Identity and Access Management technologies



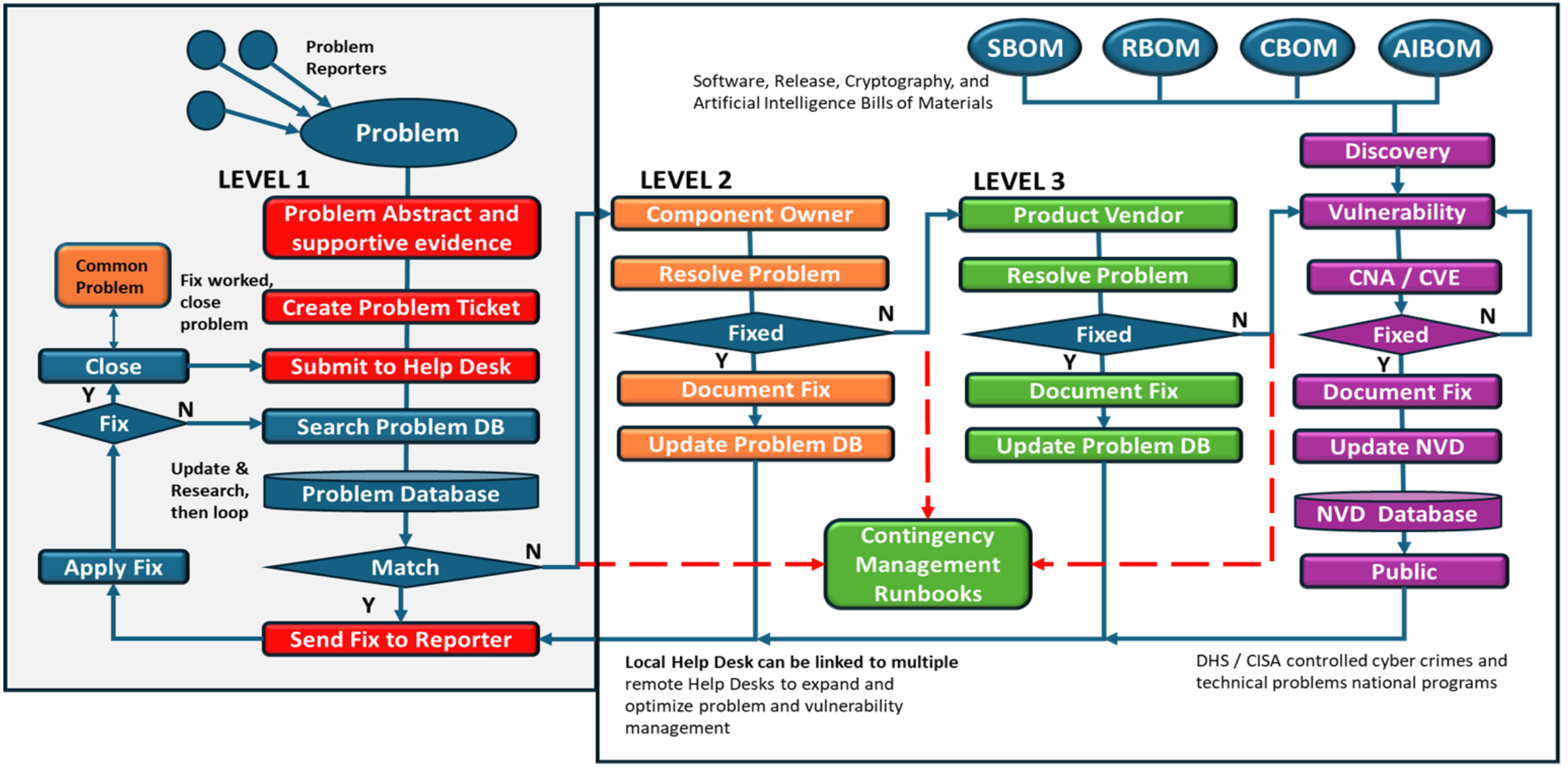


NIST CSF 2.0 Categories and Application

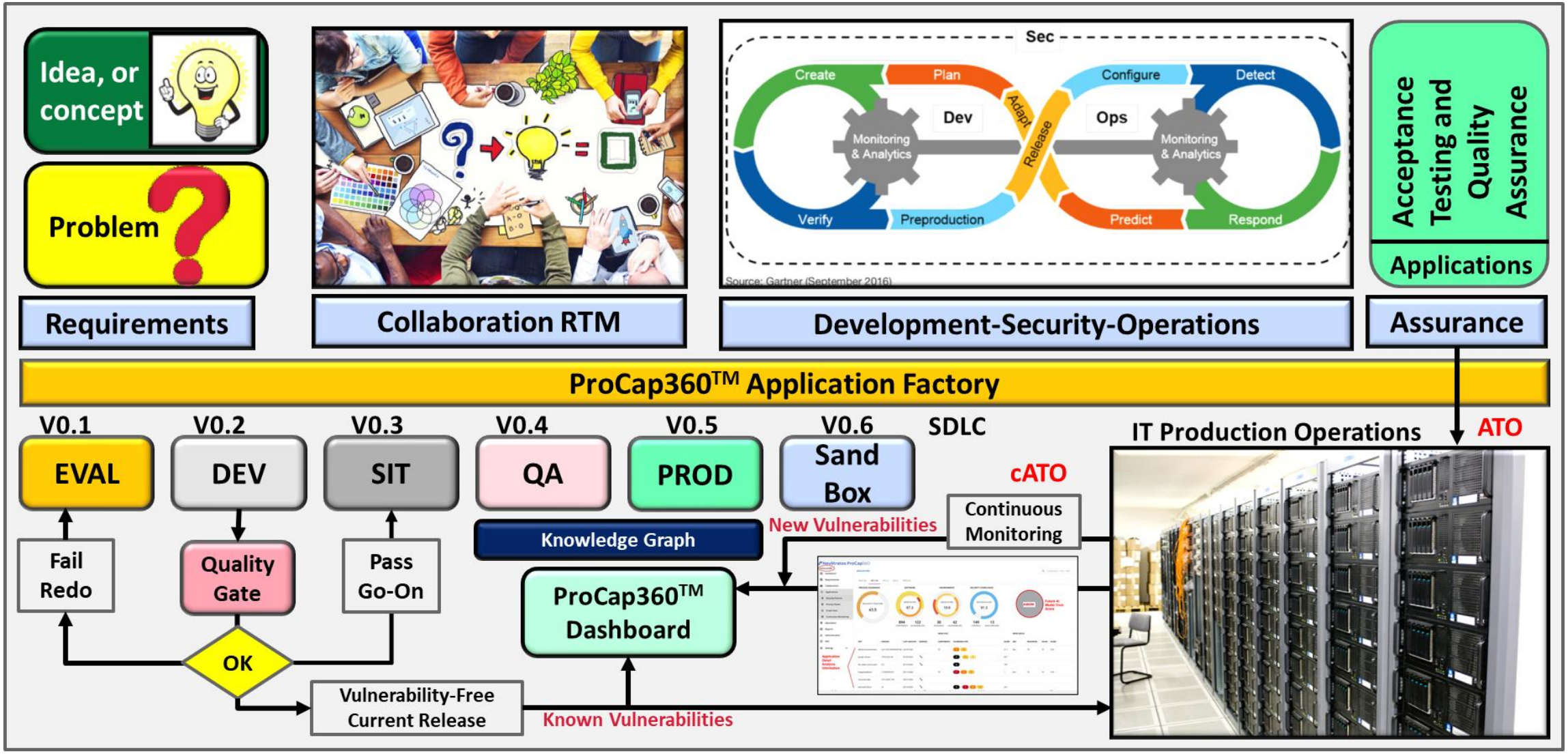
NIST Cybersecurity Framework 2.0		
CSF 2.0 Function	**CSF 2.0 Category**	**CSF 2.0 Category Identifier**
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles and Responsibilities	GV.RR
	Policies and Procedures	GV.PO
Identity (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	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



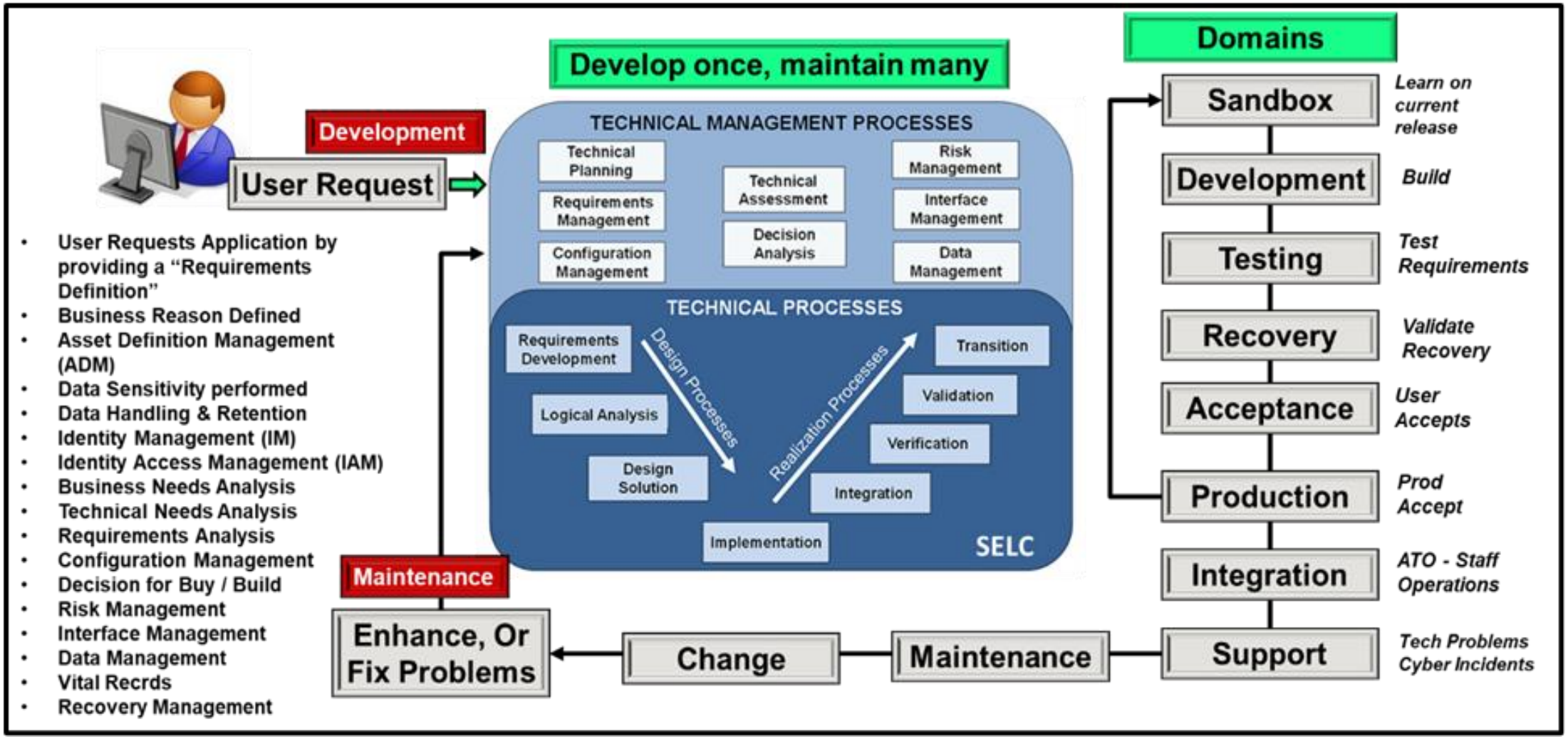
Problem Management and Control



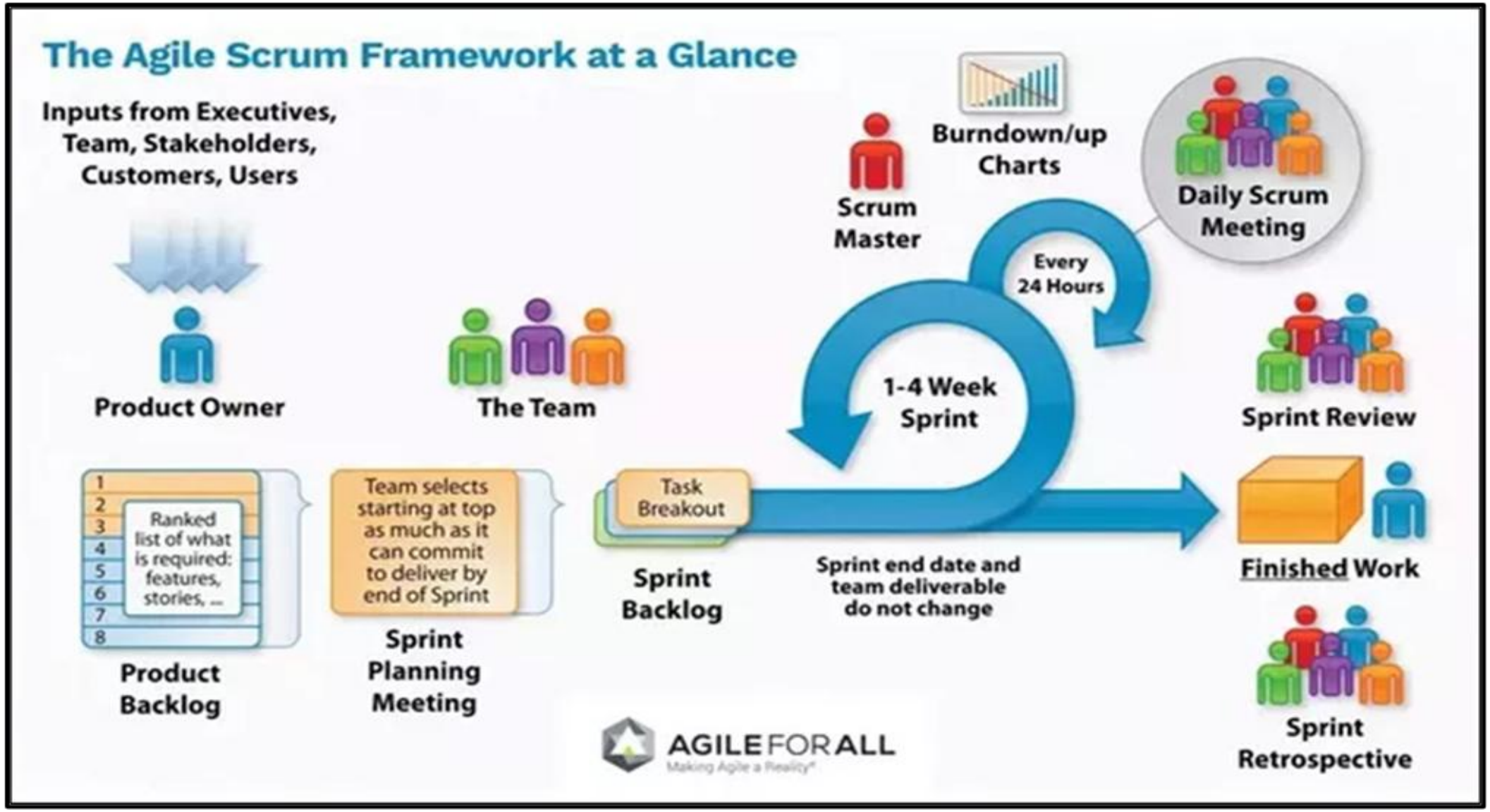
From Concept to Applications via DevSecOps



Applications Development Stages



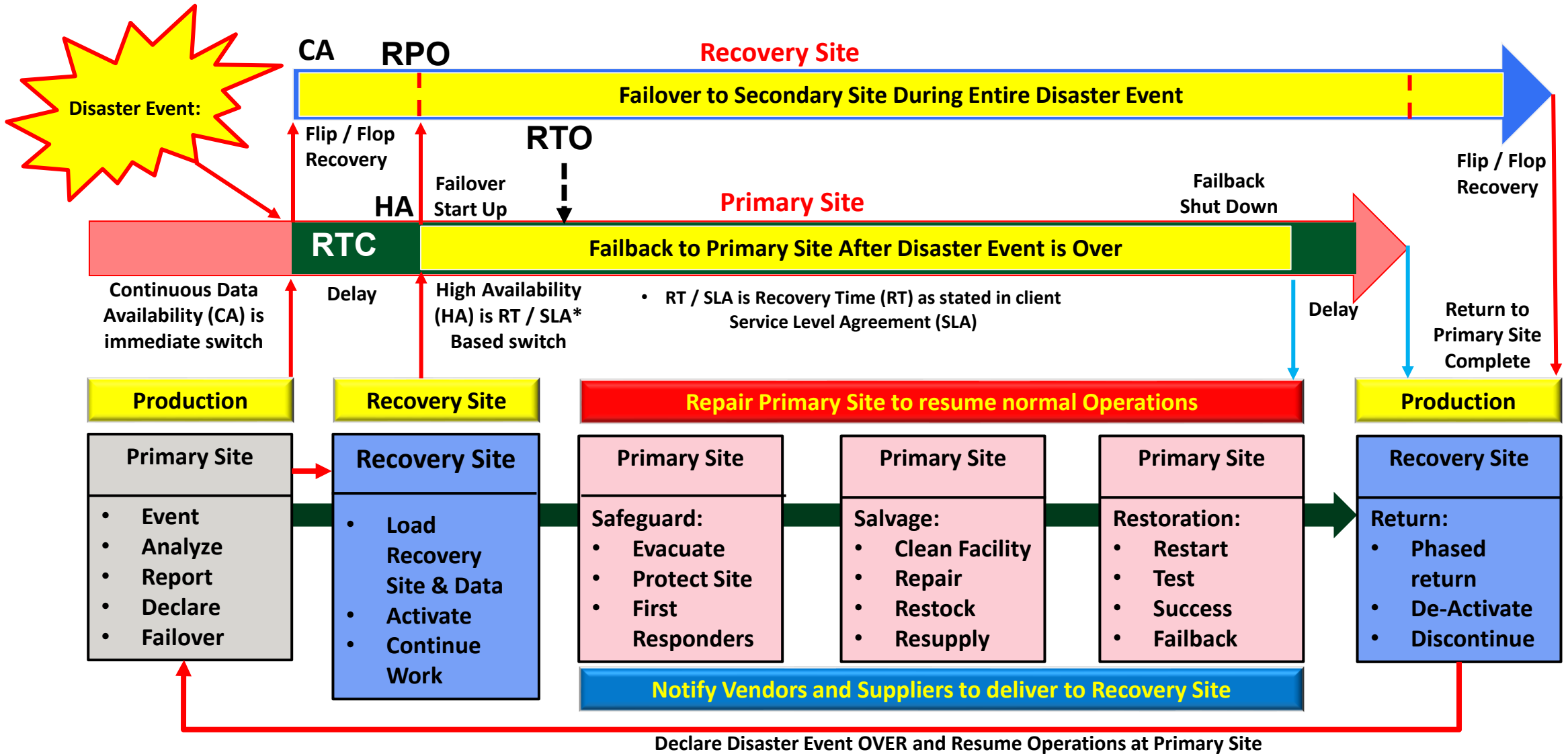
Agile, JIRA, Confluence, and SharePoint



The Disaster Event Life Cycle

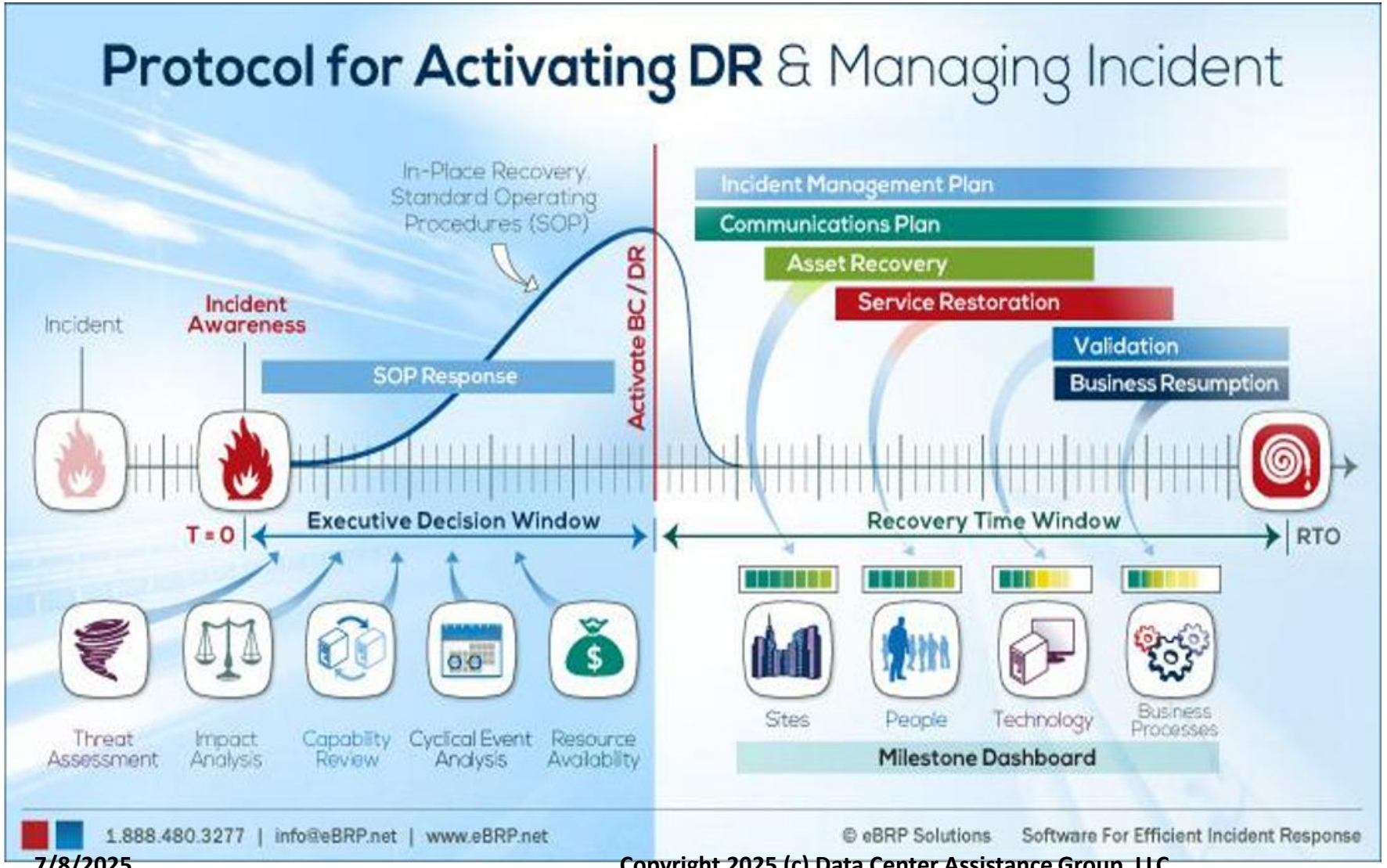
CA is Continuous Availability
HA is High Availability
RTO – Recovery Time Objective
RPO – Recovery Point Objective
RTC – Recovery Time Capability
MTO – Maximum Tolerable Outage

Thomas Bronack
Email: bronackt@dcag.com
Phone: (917) 673-6992



The Business Recovery Life Cycle

Thomas Bronack
Email: bronackt@dcag.com
Phone: (917) 673-6992



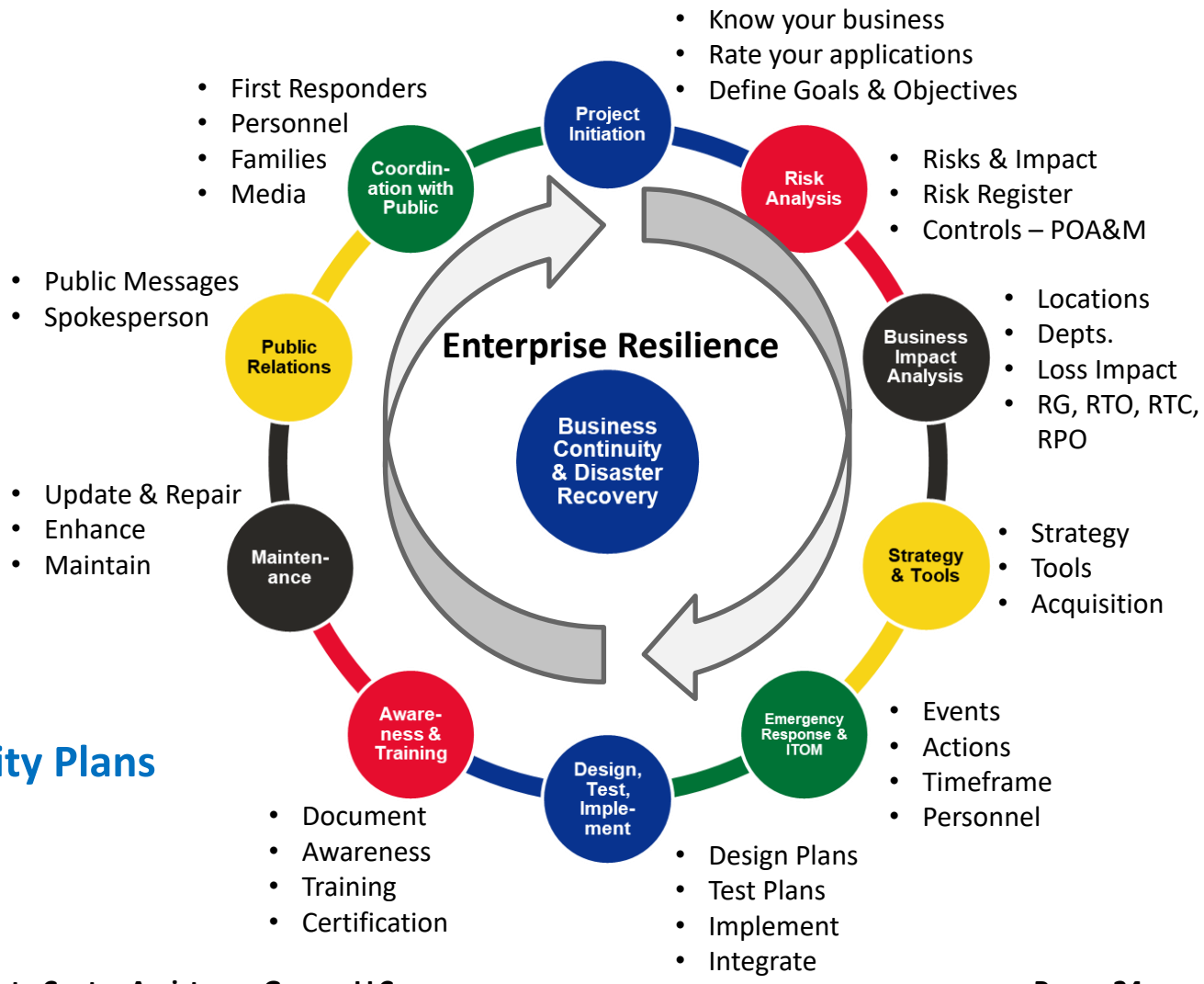
DR Life Cycle:

1. **Executive Decision Window**
   a. Incident occurs
   b. Incident awareness (RPO)
   c. Threat Assessment
   d. Impact Analysis
   e. Capability Review
   f. Cyclical Event Analysis
   g. Resource Availability
   h. SOP Response
   i. Activate BC/DR Plan
2. **Recovery Time Window**
   a. Incident Management
   b. Communications
   c. Asset Recovery
   d. Service Restoration
   e. Validation
   f. Business Resumption (RTO)
3. **Milestones Dashboard**
   a. Sites (Primary / Recovery)
   b. People
   c. Technology
   d. Business Processes

Ten Step Process to establish BCM/DR Practice

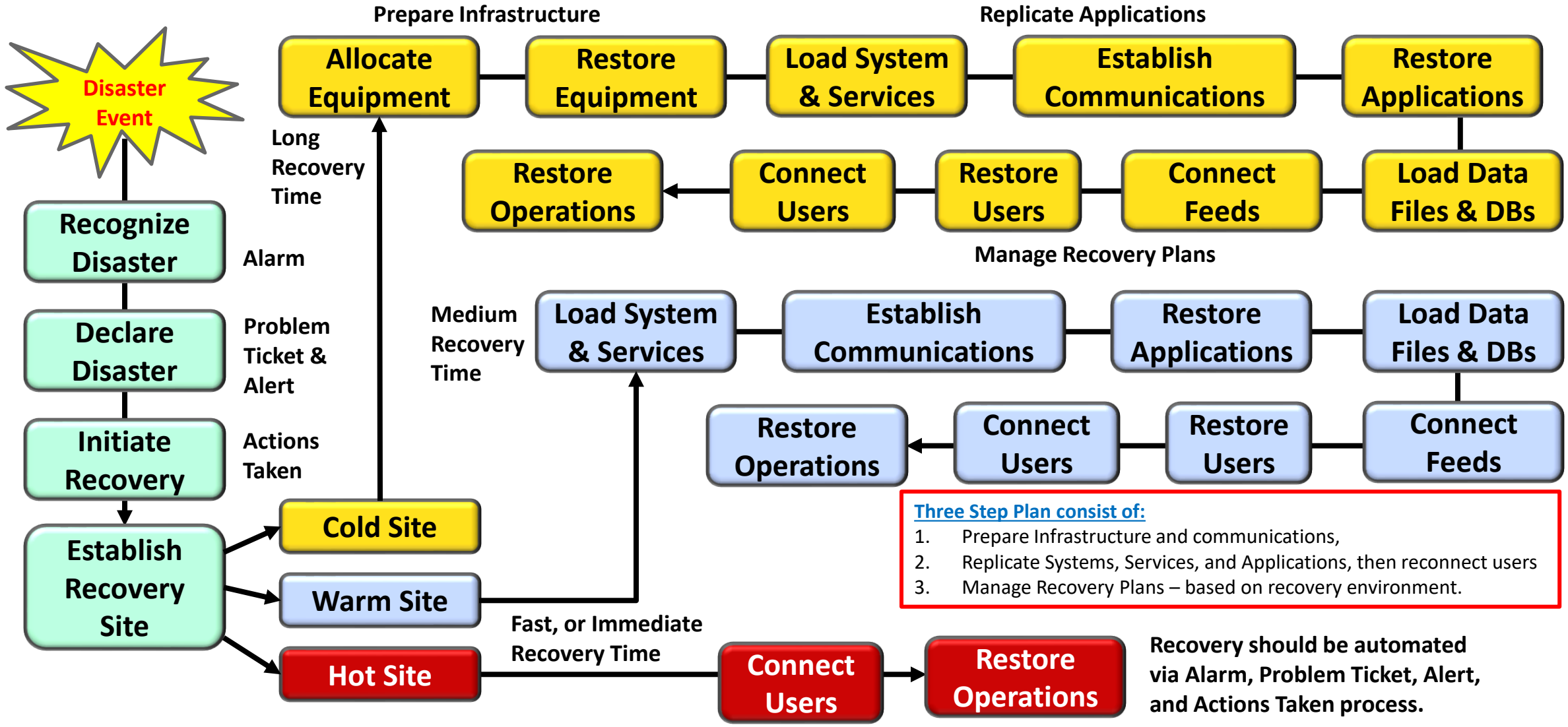
Thomas Bronack
Email: bronackt@dcag.com
Phone: (917) 673-6992

1. Project Initiation and Management
2. Risk Evaluation and Controls Improvement
3. Business Impact Analysis
4. Developing Business Continuity Strategies
5. Emergency Response and Operations Restoration (Backup, Vaulting, Restoration)
6. Designing and Implementing Business Continuity Plans
7. Awareness and Training
8. Maintaining and Exercising Business Continuity Plans
9. Public Relations and Crisis Communications
10. Coordinating with Public Authorities



Sequence of Events to enact a Recovery Operation

Thomas Bronack
Email: bronackt@dcag.com
Phone: (917) 673-6992



Backup, Archive, and Recover Data Files

BEYOND BACKUPS: TRUE DIGITAL RESILIENCE

Incident Response

- Develop and maintain a comprehensive incident response plan
- Conduct regular simulations to ensure readiness

Cloud Solutions

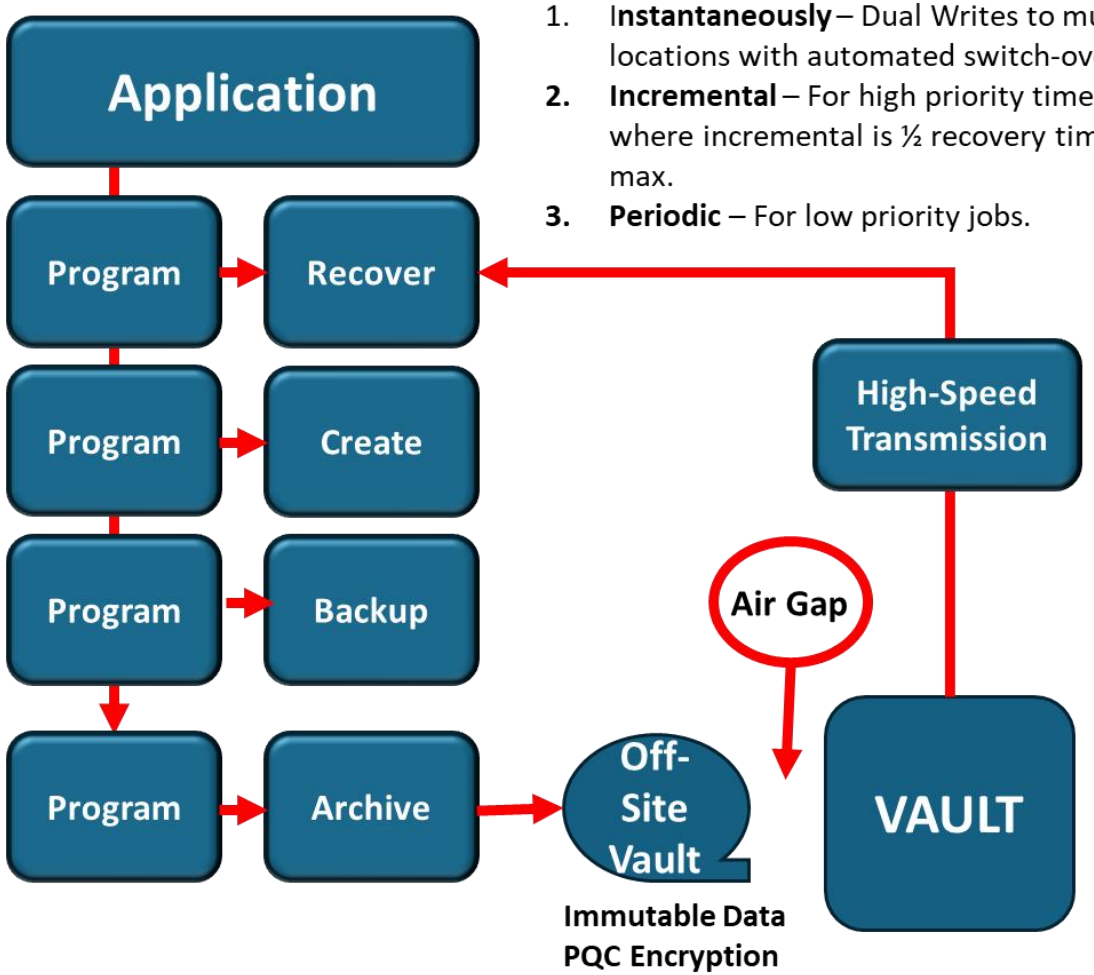
- Implement hybrid cloud solutions for scalability and flexibility
- Utilize cloud-based disaster recovery

RTO/RPO Metrics

- Recovery Time Objective (RTO): maximum acceptable time to restore functions
- Recovery Point Objective (RPO): maximum acceptable data loss measured in time
- Define RTO and RPO to establish clear recovery goals

Case Studies

Downtime can cost up to $9,000 per minute



Backup / Recovery Times by RTO:

1. **Instantaneously** – Dual Writes to multiple locations with automated switch-over.
2. **Incremental** – For high priority times where incremental is ½ recovery time at max.
3. **Periodic** – For low priority jobs.