GRC - Governance, Risk Management, and Compliance

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:

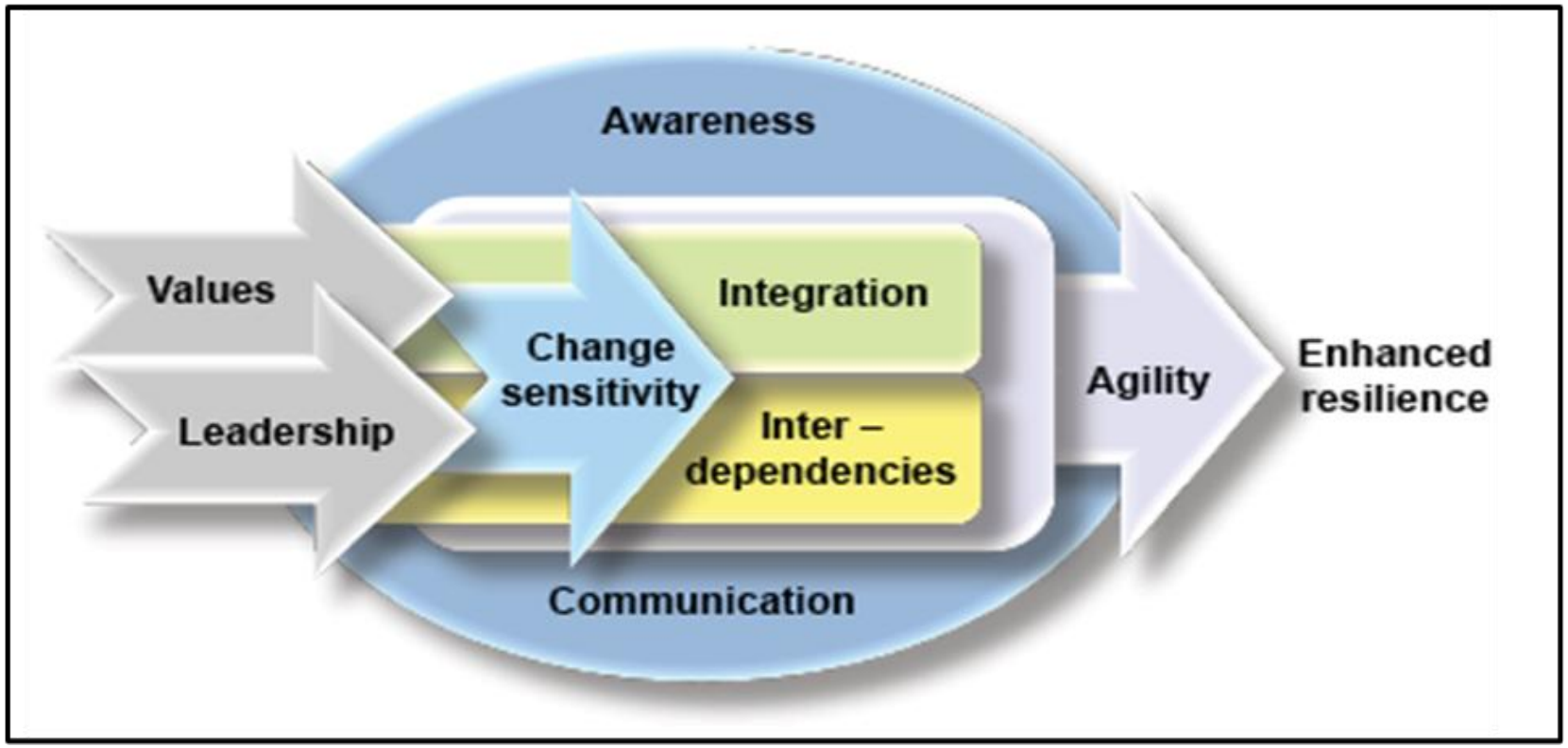
- Enterprise Resilience,
- Corporate Certification,
- Vulnerability Management,
- Risk and Cyber Security Management,
- Post Quantum Cryptography (PQC),
- Inventory, Configuration & Asset Management,
- Strategic and Tactical Planning,
- Project and Team Management
- Awareness and Training

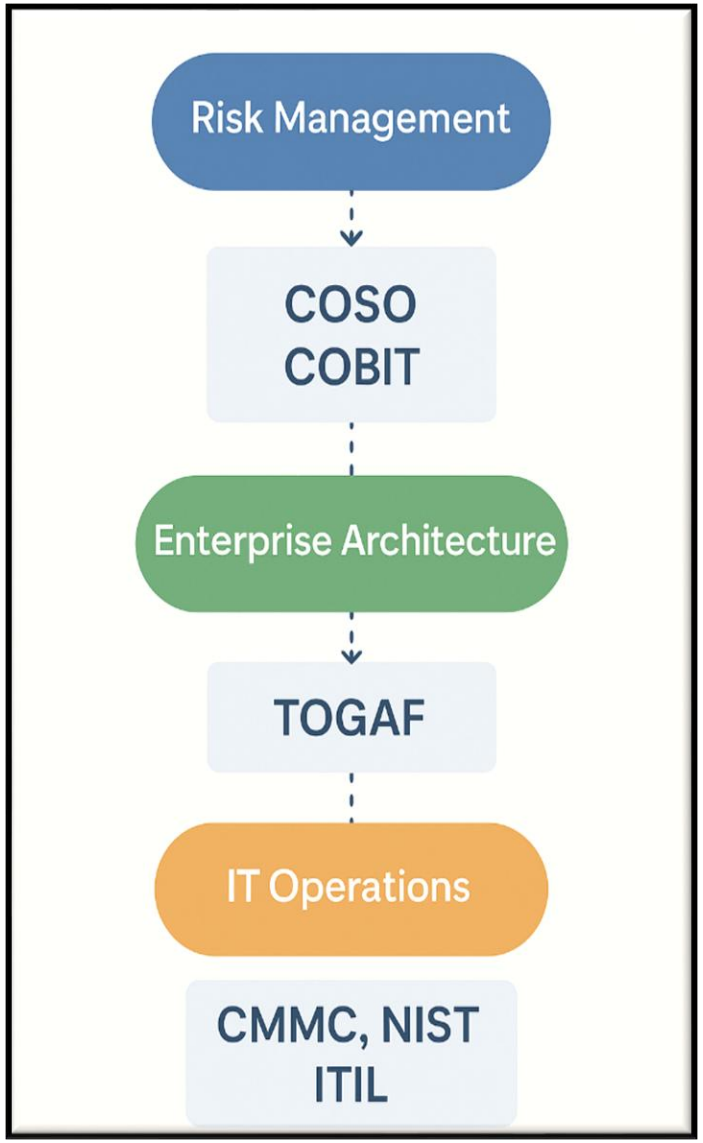
Enterprise Resilience and Corporate Certification based on GRC and Application Factory with Control Gates

Contact Information:

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

The Pathway to a Resilient Business





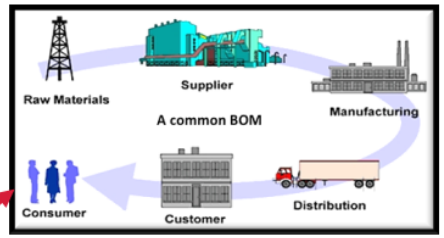
- Know your Business (i.e., Products, Services, Clients, GRC, Problem Mgmt.
- Relate your business goals to IT Services (i.e., Develop & Deploy).
- Analyze Risks and Define Controls(Support & Maintain).
- Build your Service Environment and ensure quality (Vulnerabilities).
- Provide Service Continuity and Recovery Management
- Ongoing Monitoring and improvement (CTEM, CNAPP)

Agenda - Enterprise Resilience and Corporate Certification

- **Know your company** and its business (Products, Services, Client Relations).
- **Understand the problems** faced by your organization and how to provide continuing business services during times of peril.
- **Define your company organization**, executives, managers, stakeholders, and component owners.
- **Know your environment**:
  - Architecture, Engineering Solutions, and Systems Development.
  - Inventory, Asset, and Configuration Management,
  - Third Party Risk Management and Supply Chain Management,
  - Data Sensitivity, Naming and Lifecycle, and Data Management, and
  - Post Quantum Cryptography.
- **Employ automation whenever possible** (ML, AI, RPA, BOTs. AI Agentic, Robots, etc.).
  - Application Factory with Quality Control Gates,
  - Risk Management, Assessments, Audits and Risk Controls Self-Assessment (RCSA),
  - Site Reliability Engineering, and
  - Business Continuity Management with Personal Safety and Violence Prevention.
- **Provide Corporate Compliance** adherence.
- **Provide Awareness**, Training, Certifications, and Career Pathing for personnel.

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)

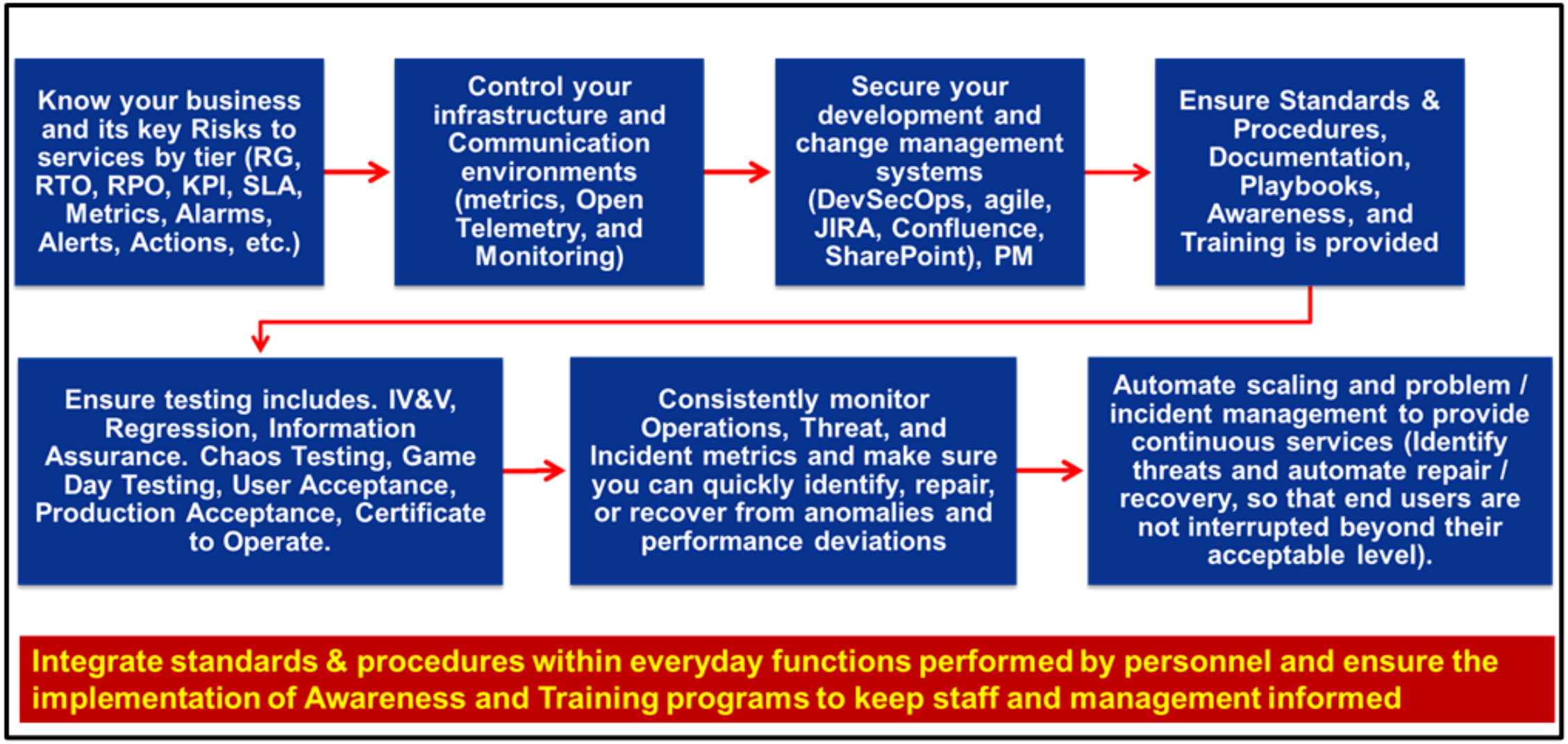
Know your Environment:

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.

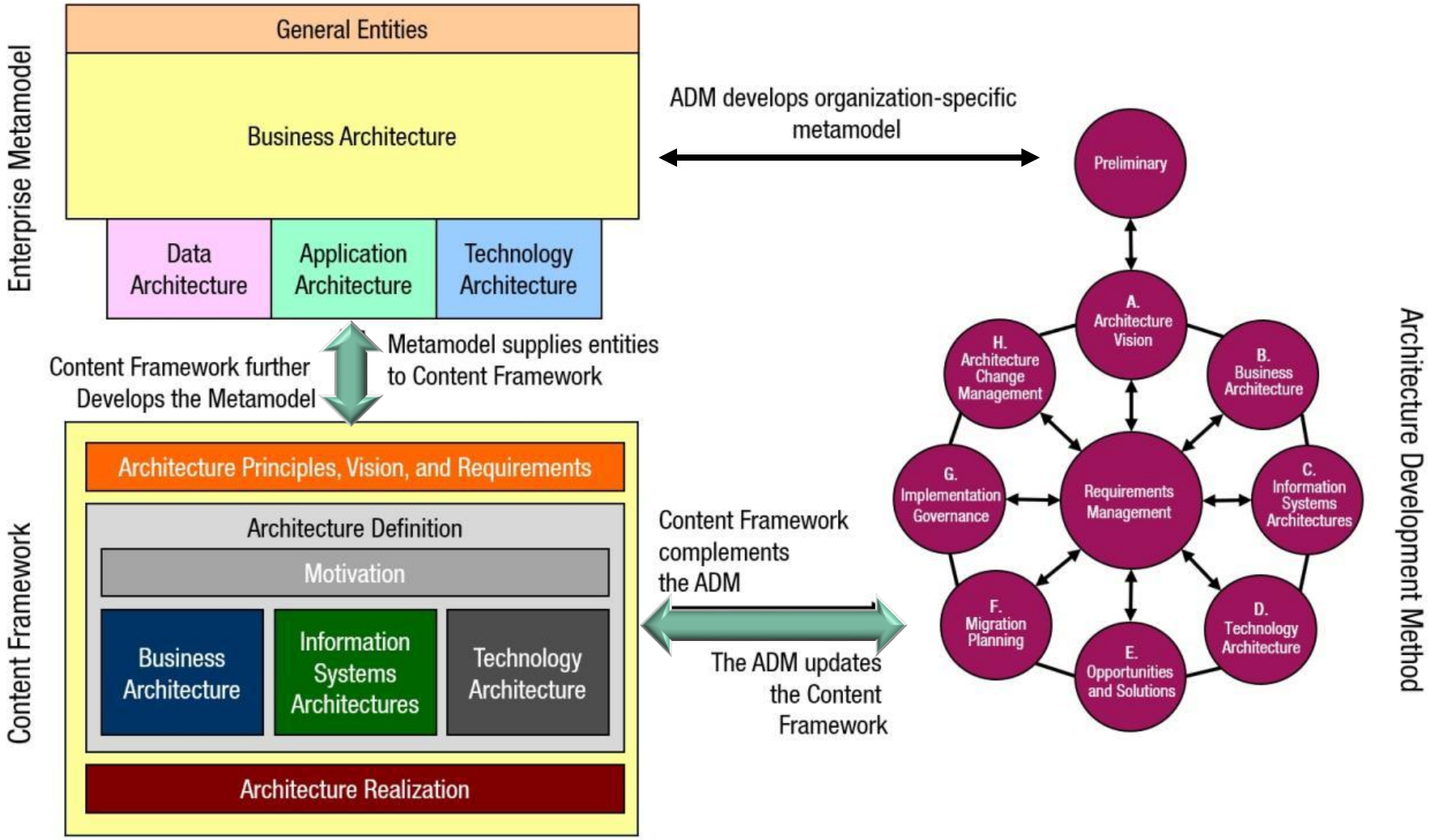
Set you direction:

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



Company Architecture - TOGAF & Archimate Language



A. What hardware Environment do you envision.
B. How do you want to support your business by IT Operations.
C. Define Systems Architecture.
D. Select Technology Architecture.
E. Solutions Planning for Development, Engineering, Testing, and Deployment.
F. Migration.
G. Deployment.
H. Support and Change Management.

Know and Control your Environment

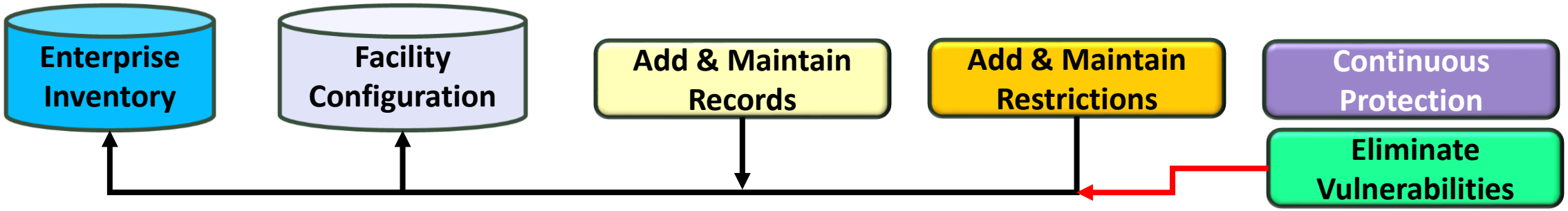
- **HW**AM
- **SW**AM
- **Technology** Management
- **Release** Management
- **Patch** Management
- **End-of-life**

- Facilities, or Locations
- Configuration of equipment
- Services and Applications
- COOP Recovery
- Location Recovery

- **Acquisition** - Order through Delivery
- **Install** and Test
- **Turnover** to User
- **Redeploy** as needed
- **Terminate** within laws and regulations

- **Components** via SBOM RBOM, or AIBOM
- **Identify Countries** parts origin
- Adhere to Laws and **country restrictions**
- Identify Vulnerabilities
- License Management

- **Identify** Vulnerabilities prior to production
- **Apply** Patches and Update Releases
- **Validate** mitigations
- **Vulnerability-free** production
- **CTEM** after Production



Laws and Regulations, by groups

Risk Posture and Audit Preparedness

- Risk Analysis
- Define Domestic and International needs
- Likelihood
- Impact
- Defense Strategies
- Controls
- Insurance
- Audit Universe
- Crosswalks
- Audit Questionnaire and Artefacts
- Audit Schedule
- Reporting & Monitoring
- Improvement & Automation

Domestic Compliance

- **COSO** – Risk Appetite
- **COBIT** – IT Governance Framework
- **RMF** – Risk Management Framework
- **CSF 2.0** – Cybersecurity Framework
- **CIA** – Confidentiality, Integrity, and Availability
- **GRC** – Governance, Risk, and Compliance
- **NIST** – National Institute of Standards and Technology
- **EO** – Executive Orders

International Compliance

- ISO - International Organization for Standardization:
- **ISO 3001 –** Risk Management
- **ISO 9000** – Quality Management
- **ISO 22301** – Business Continuity Management
- **ISO 14000** – IT Environment
- **ISO 20000** – IT Services
- **ISO 27000** – Information Security
- DORA, GDPR. NIS 2,

Industry Compliance

- **PCI DSS** – Payment Card Industry Data Security Standards
- **FDA** – Food & Drug Agency
- **OMB** – Office of Management and Budget
- **SEC** – Securities Exchange Commission
- **FFIEC** – Federal Financial Institutions Examination Council
- "**Whole of World**"
- "**Whole of Nation**"
- "**Secure by Design**"

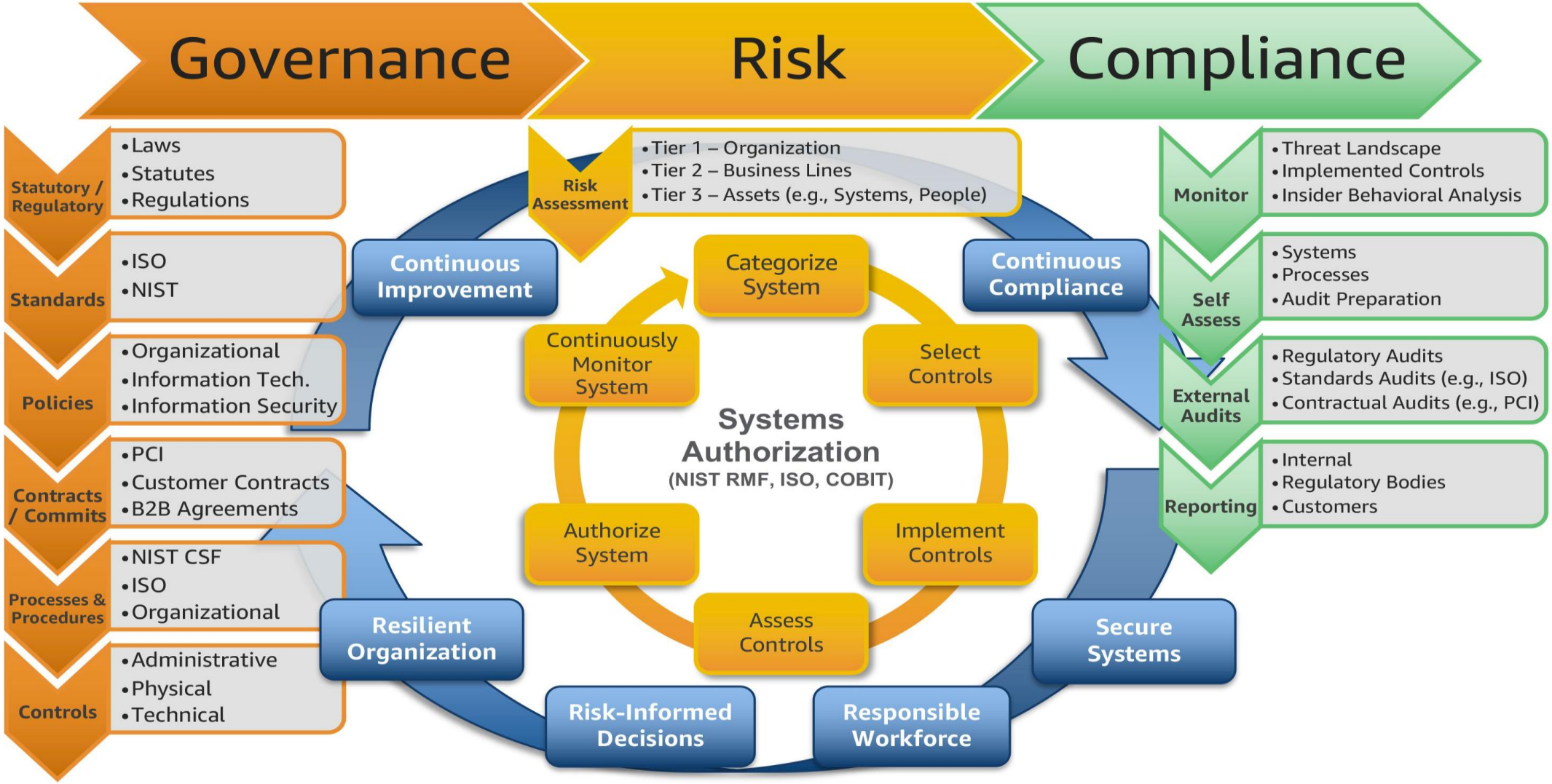
Existing laws and regulations

- **Gramm Leach Bliley** – Safeguard Act (was Bank Holding Act);
- **HIPAA** – Healthcare regulations (including ePHI, HITECH, and Final Ombudsman Rule);
- **Sarbanes – Oxley Act** (sections 302, 404, and 409) on financial assessment and reporting by authorized "Signing Officer";
- **EPA and Superfund** (how it applies to Dumping and Asset Management Disposal);
- **Supply Chain Management "**Laws and Guidelines" included in ***ISO 24762*** (SSAE 16 for Domestic compliance and SSAE 3402 for International Compliance, and NIST 800-34);
- **Supply Chain Management "**Technical Guidelines" described in ***ISO 27031***;
- **Patriots Act** (Know Your Customer, Money Laundering, etc.);
- **Workplace Safety and Violence Prevention** via OSHA, OEM, DHS, and governmental regulations (State Workplace Guidelines and Building Requirements);
- **Income Tax and Financial Information protection** via ***Office of the Comptroller of the Currency*** (OCC) regulations (***Foreign Corrupt Practices Act***, **OCC-177** Contingency Recovery Plan, **OCC-187** Identifying Financial Records, **OCC-229** Access Controls, and **OCC-226** End User Computing).

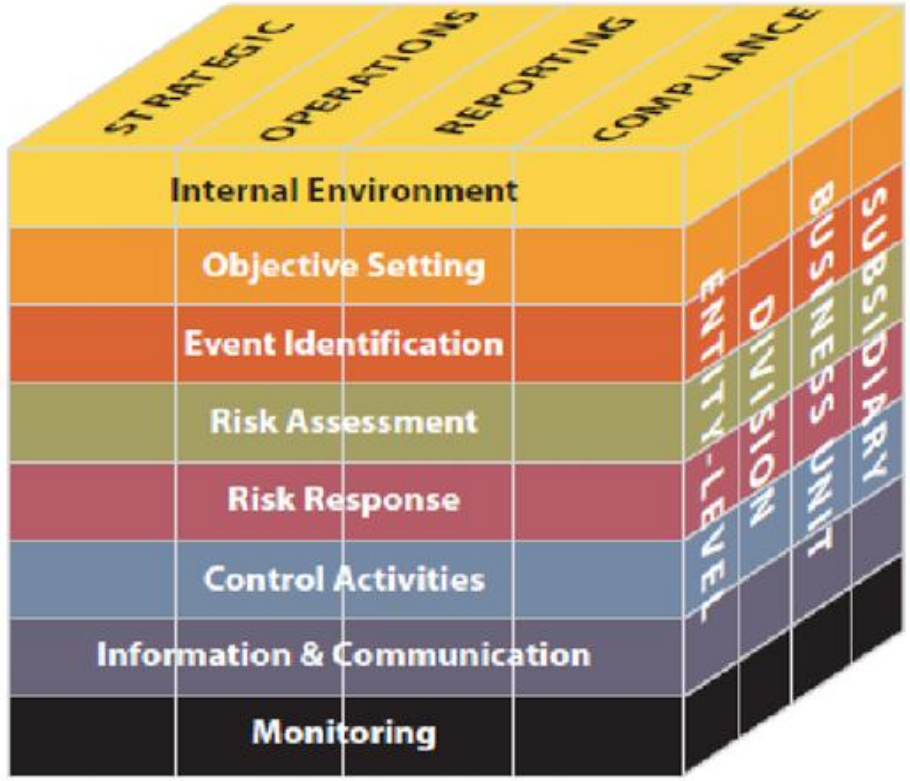
These laws and regulations have been around for many years (Starting with OCC regulations and growing from there) and have served as the basis for Governance Regulations and Compliance (GRC). Additional industry compliance requirements like SEC, FFIEC and HITECH must be adhered to as well.

The CIA (Confidentiality, Integrity, Availability) deals with security and should be adhered to with the same aggressiveness as GRC.

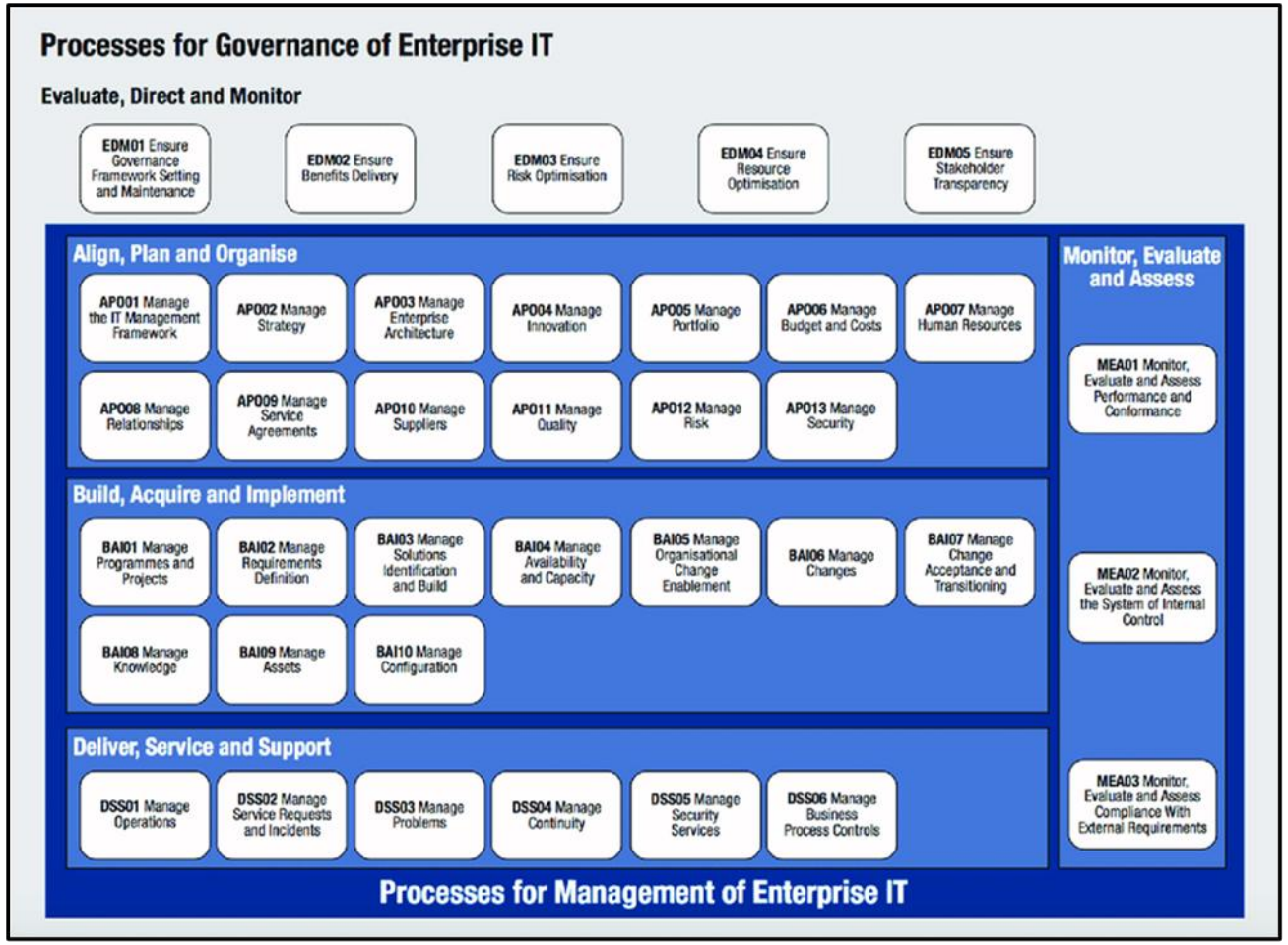
The three pillars of GRC – Governance, Risk, and Compliance



COSO and COBIT Analysis Frameworks

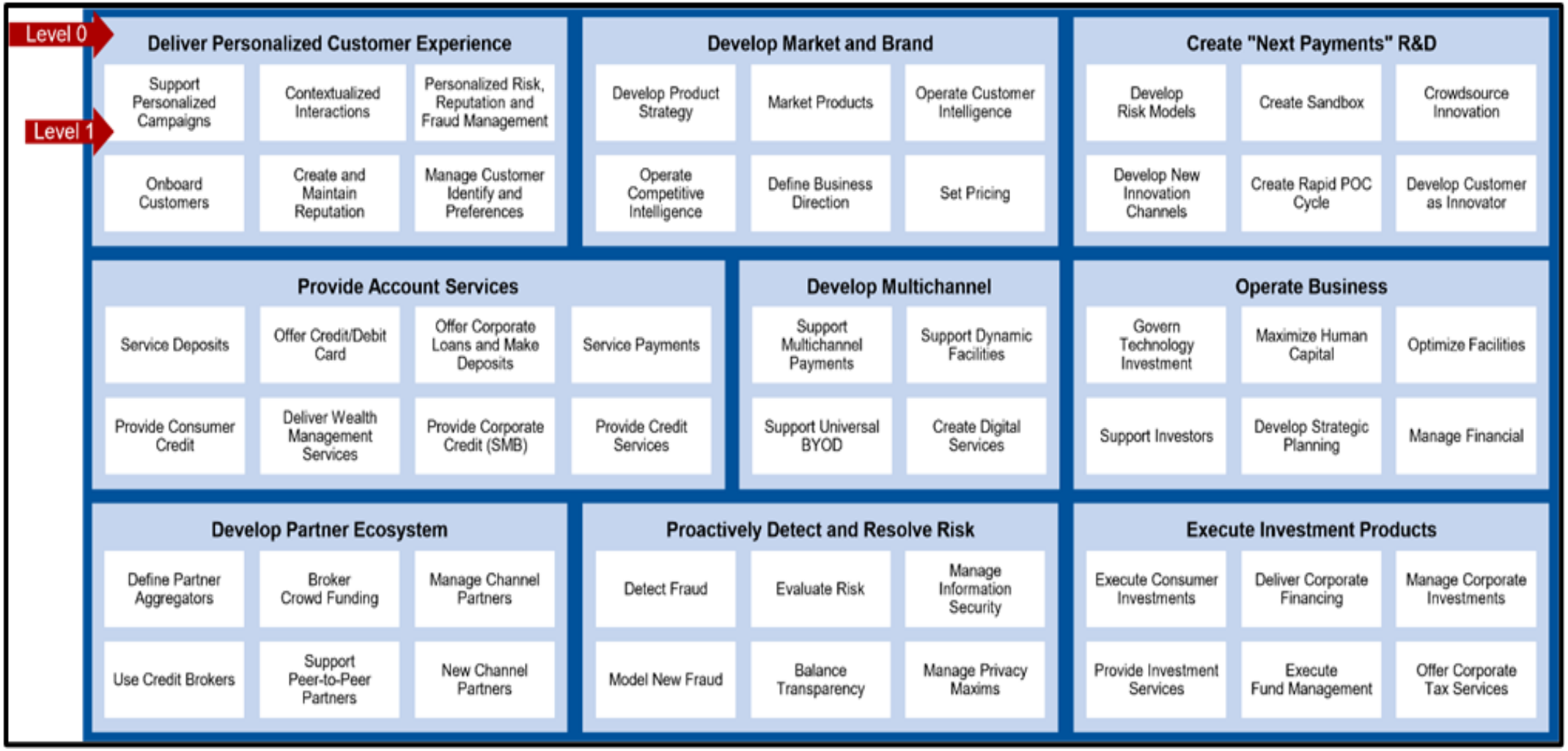


COSO – Committee of Sponsoring Organizations for Risk Management

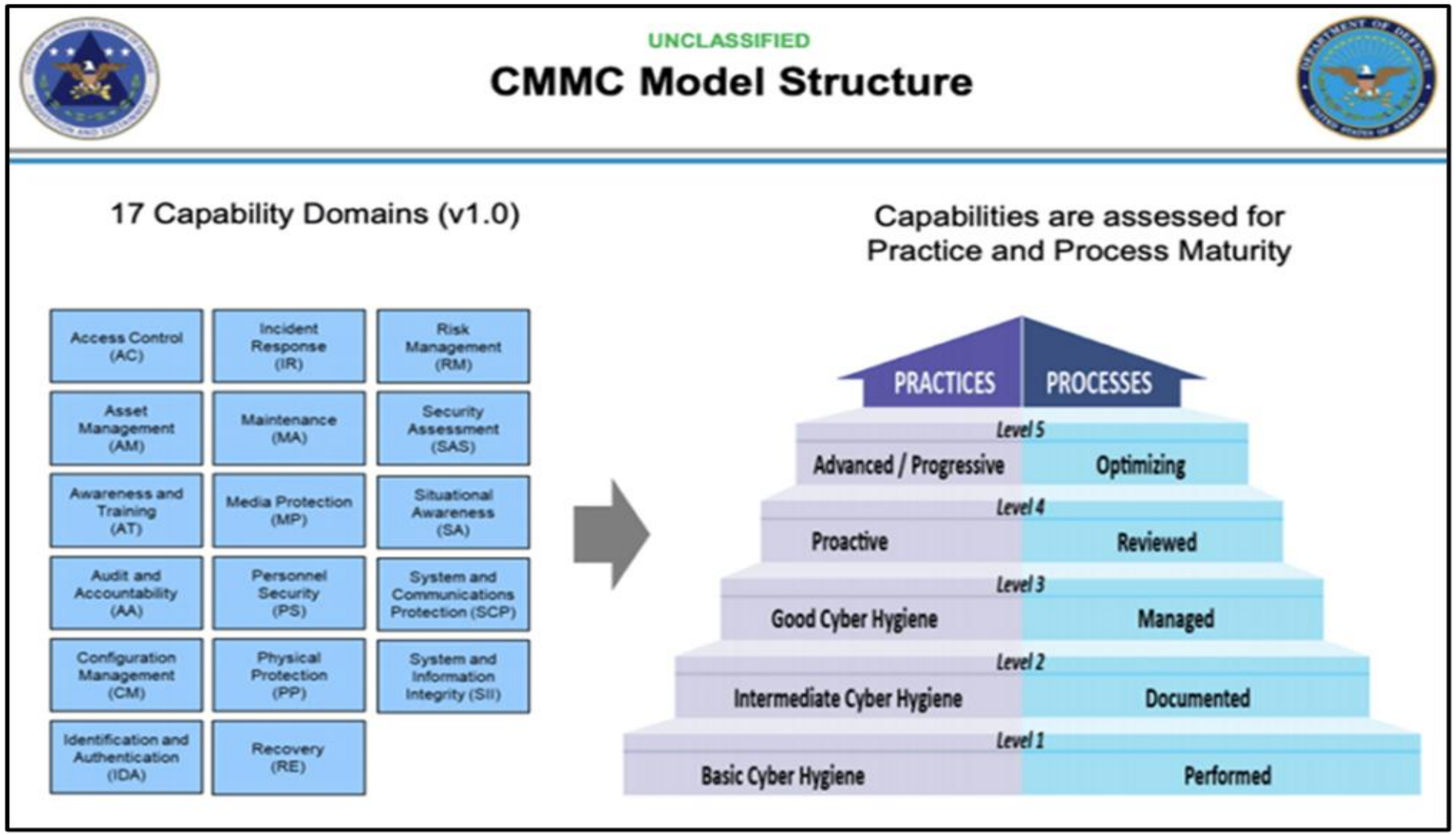


COBIT - Control Objectives for Information and Related Technology to convert Products to IT Operations

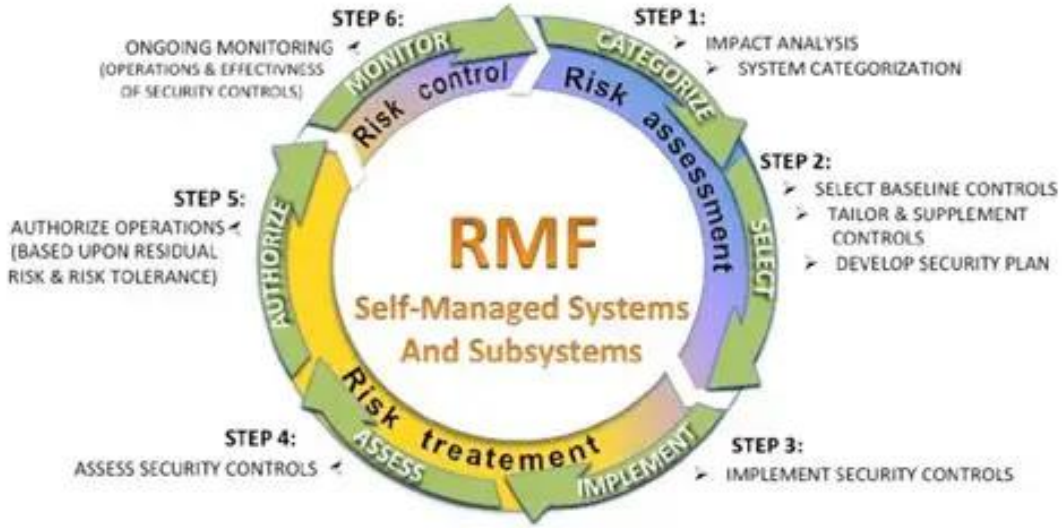
CMMI - Cybersecurity Maturity Model Integration



CMMC - Cybersecurity Maturity Model Certification



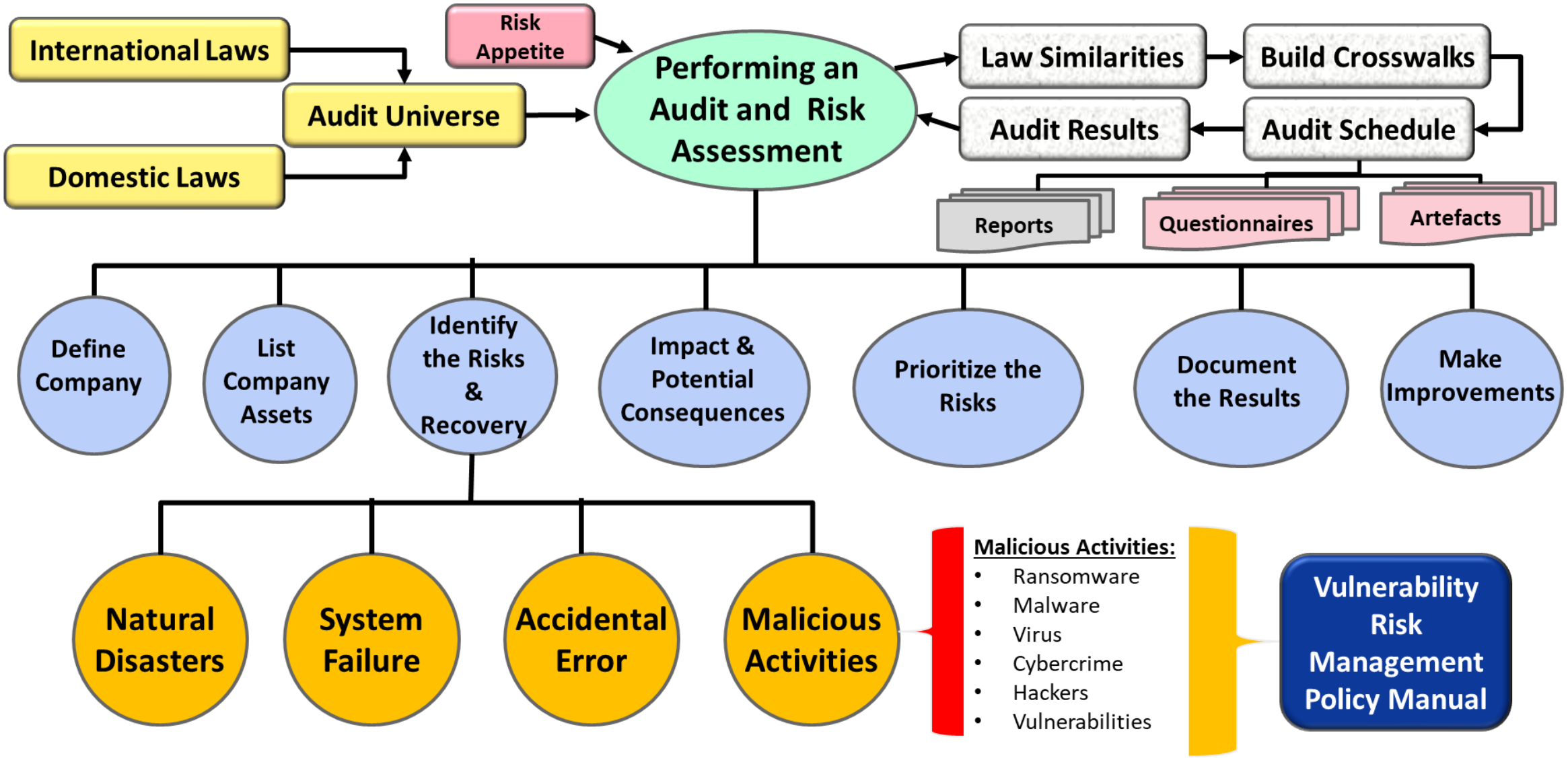
Risk Management Framework (RMF) NIST SP 800-37



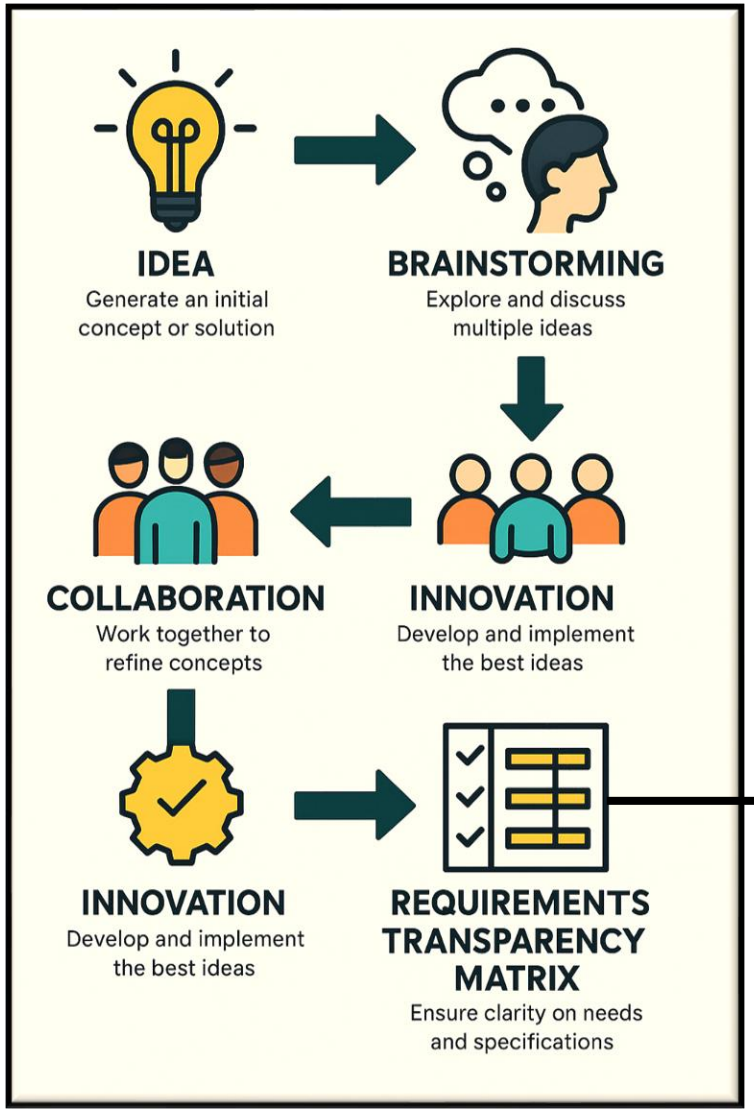
RMF Stages:

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

Performing an Audit and Risk Assessment



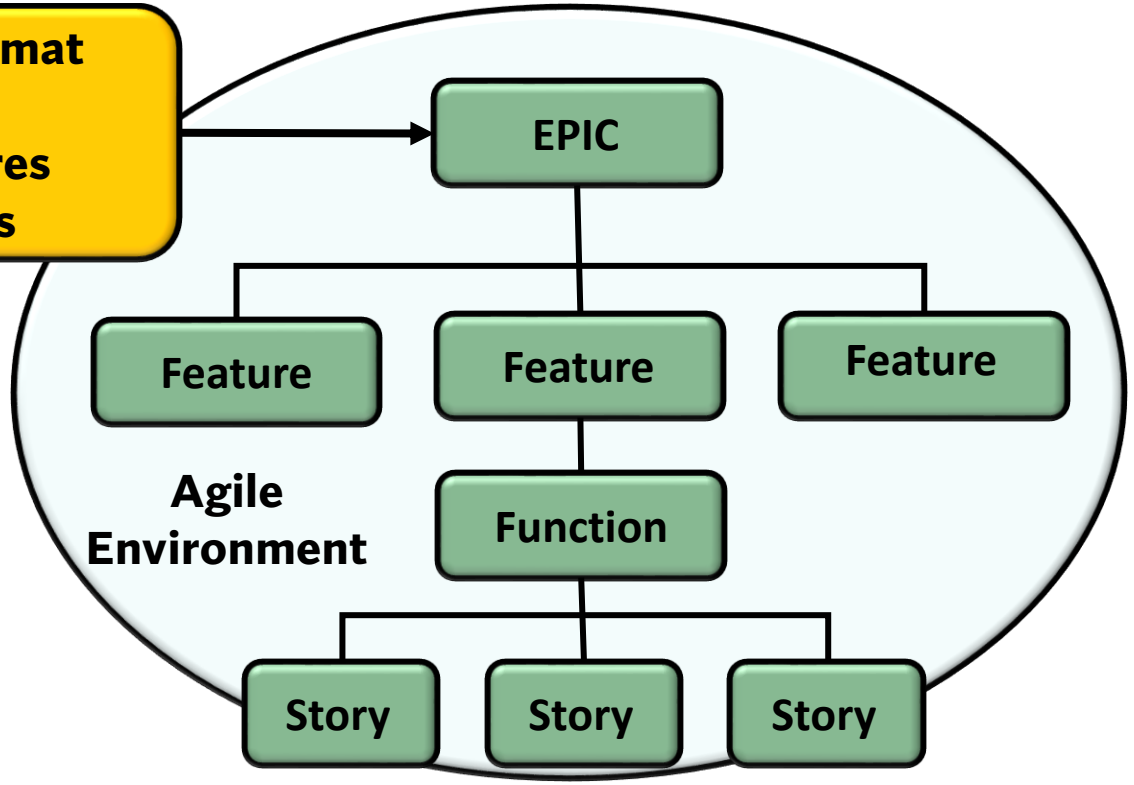
Concept to Requirements Transparency Matrix (RTM)



Requirements Transparency Matrix (RTM)

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

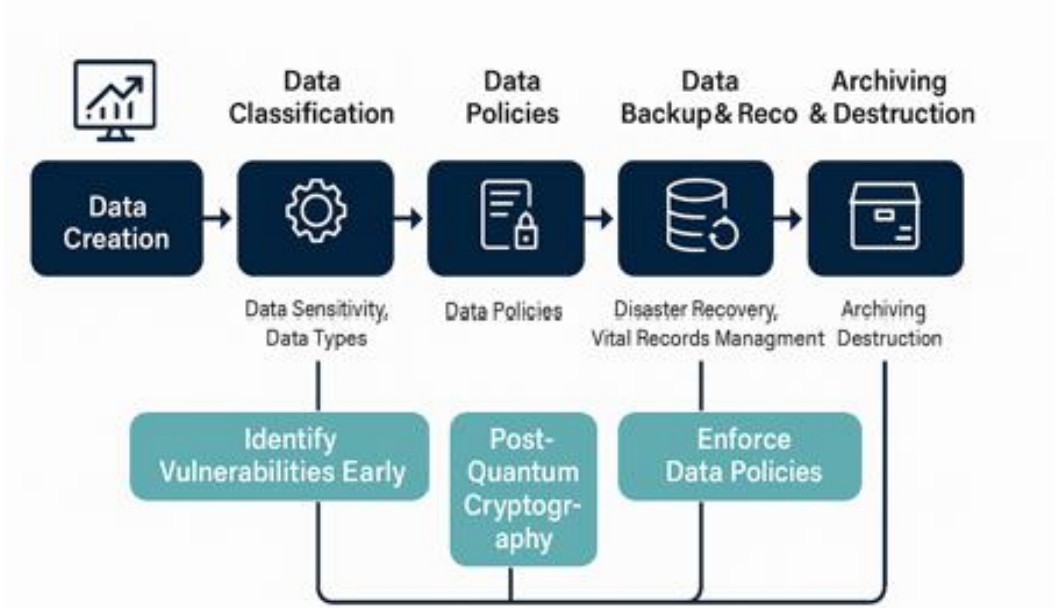
Agile Format
- Epic
- Features
- Stories



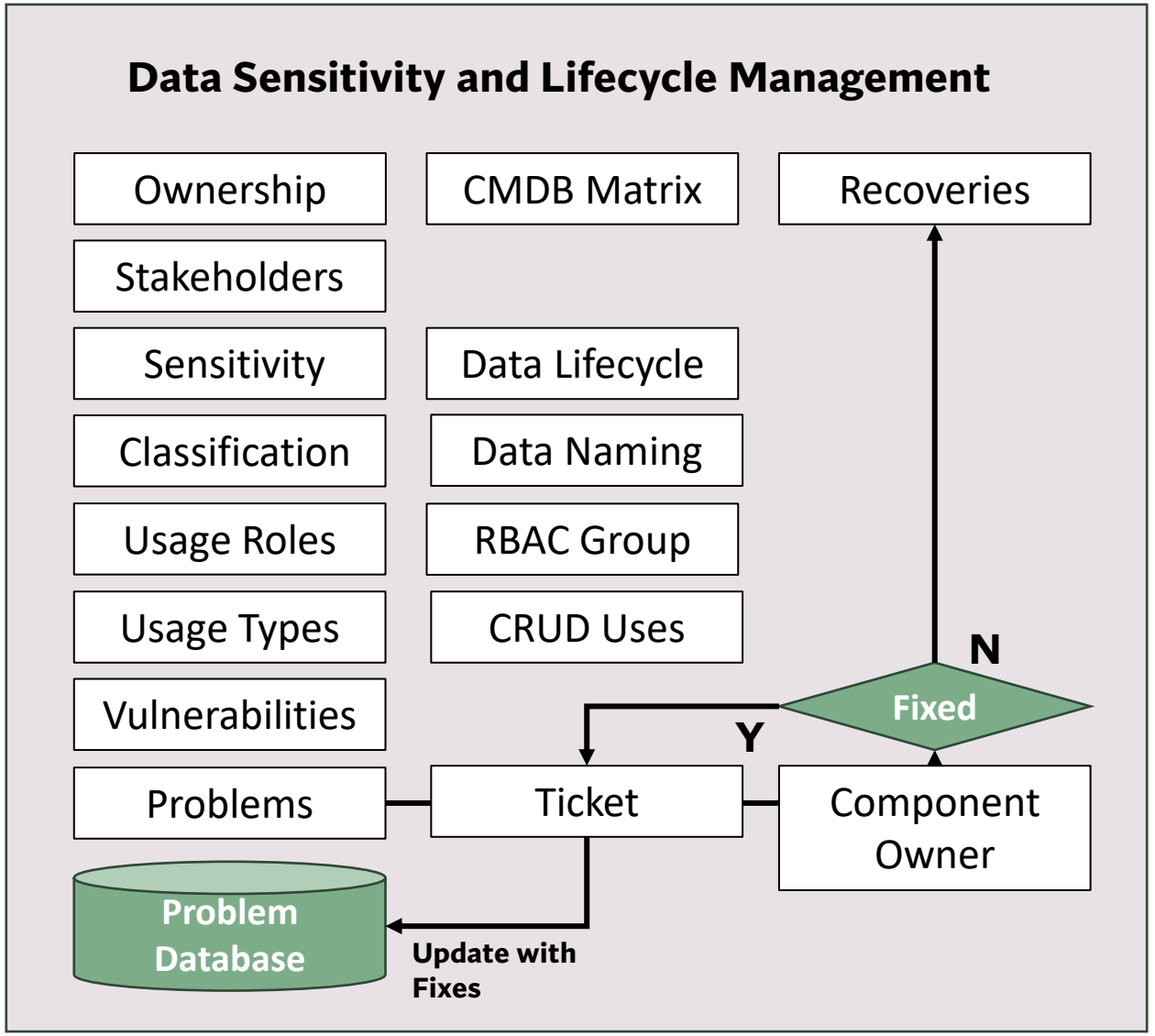
Requirements Transparency Matrix (RTM)

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 for quick repair and update.



Identity and Access Management technologies

Personal Records

Permission Based Access Control (PBAC) – (Read, Edit, Delete)

Identity Management

Identity Access Management

Role Based Access Control (RBAC)

Multi-Factor Authentication (MFA)

Attribute Based Access Control (ABAC)

Zero-Trust Authentication (ZTA)

User Identification Path

Application

Authentication

Pass

Control

Data Elements

Session Manager

Certificate

Session

Zero Trust Authentication (ZTA)

ABAC / RBAC

Userid/Pswd

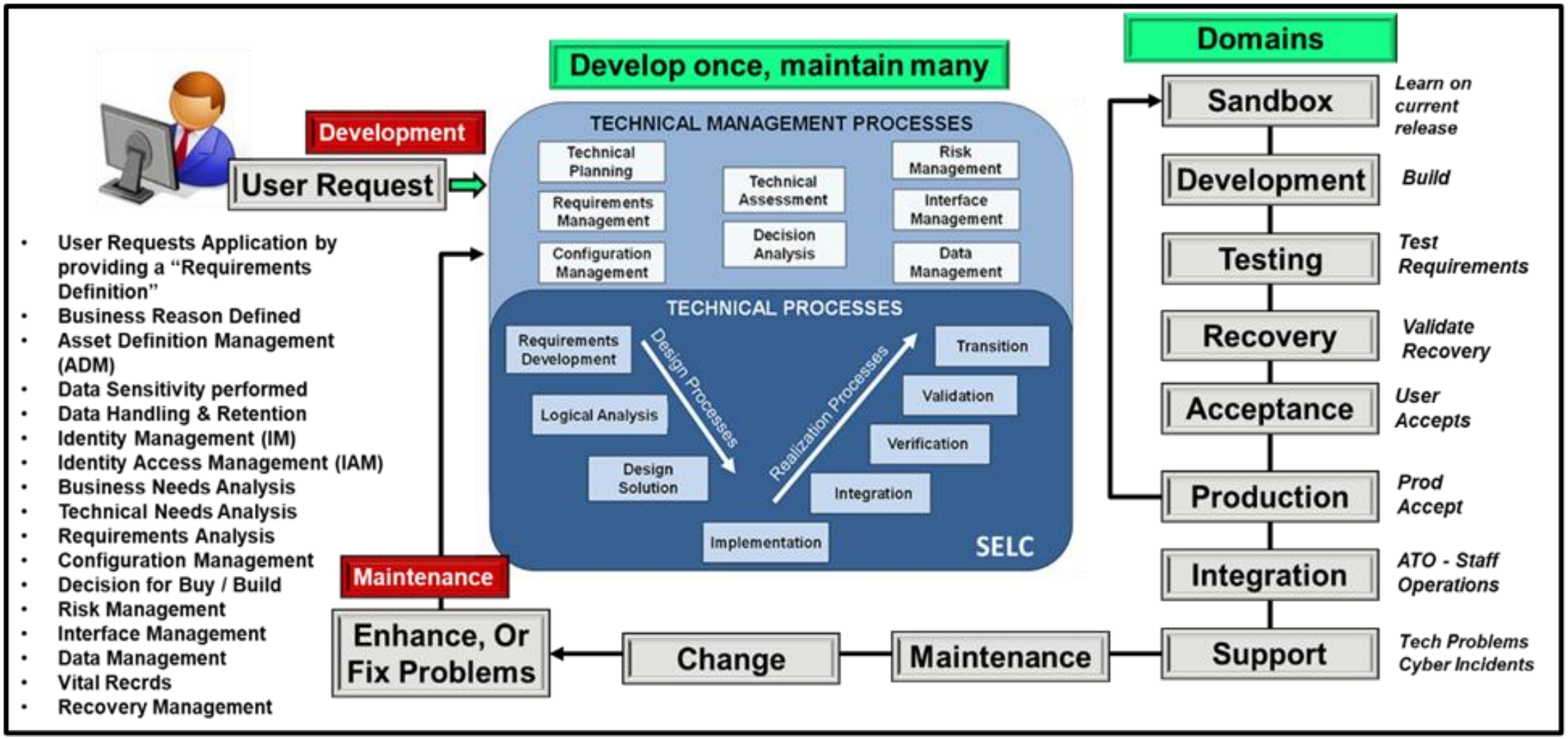
MFA

Biometrics

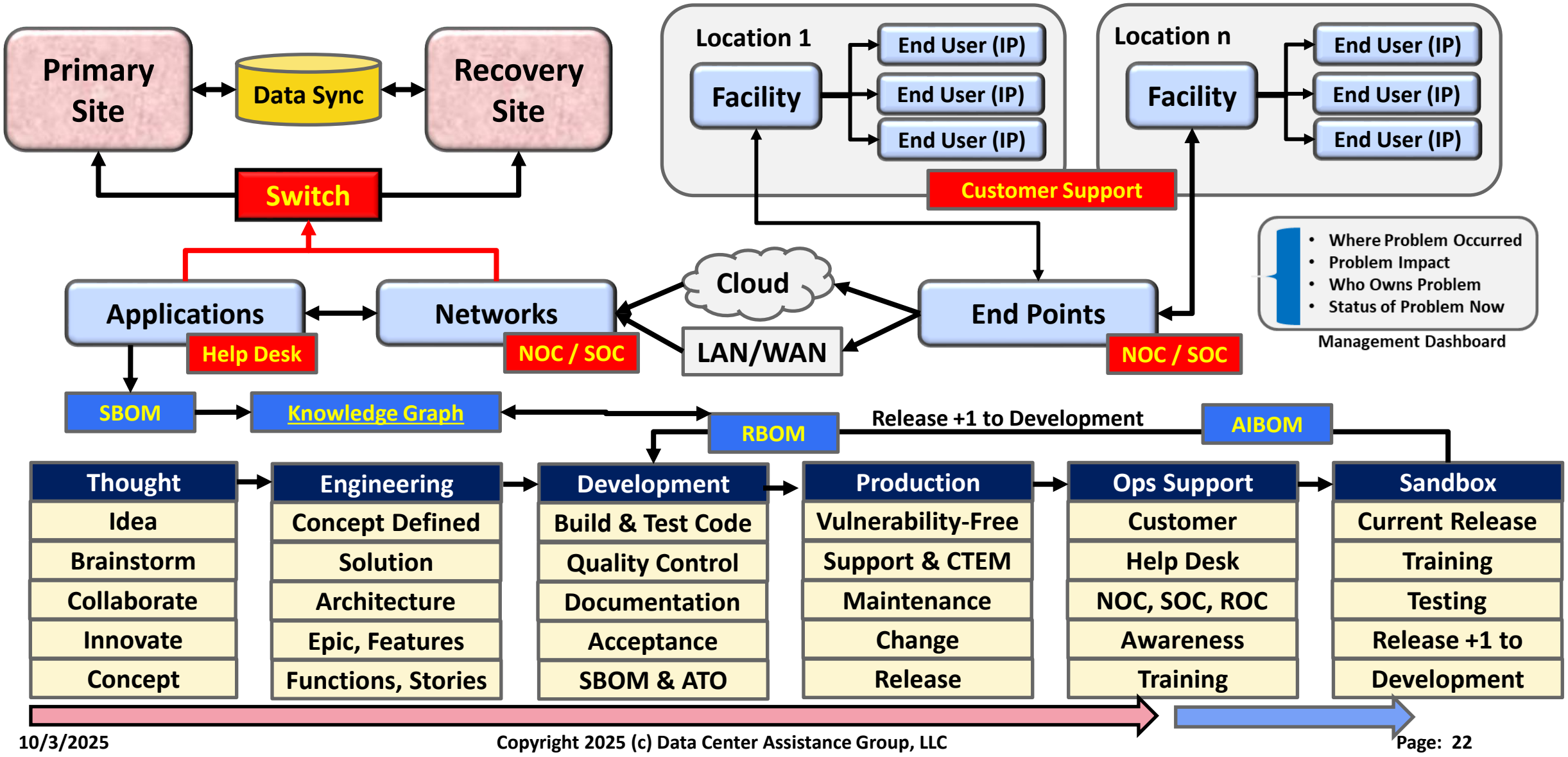
IM / IAM

Authorization path with Zero Trust Authentication (ZTA)

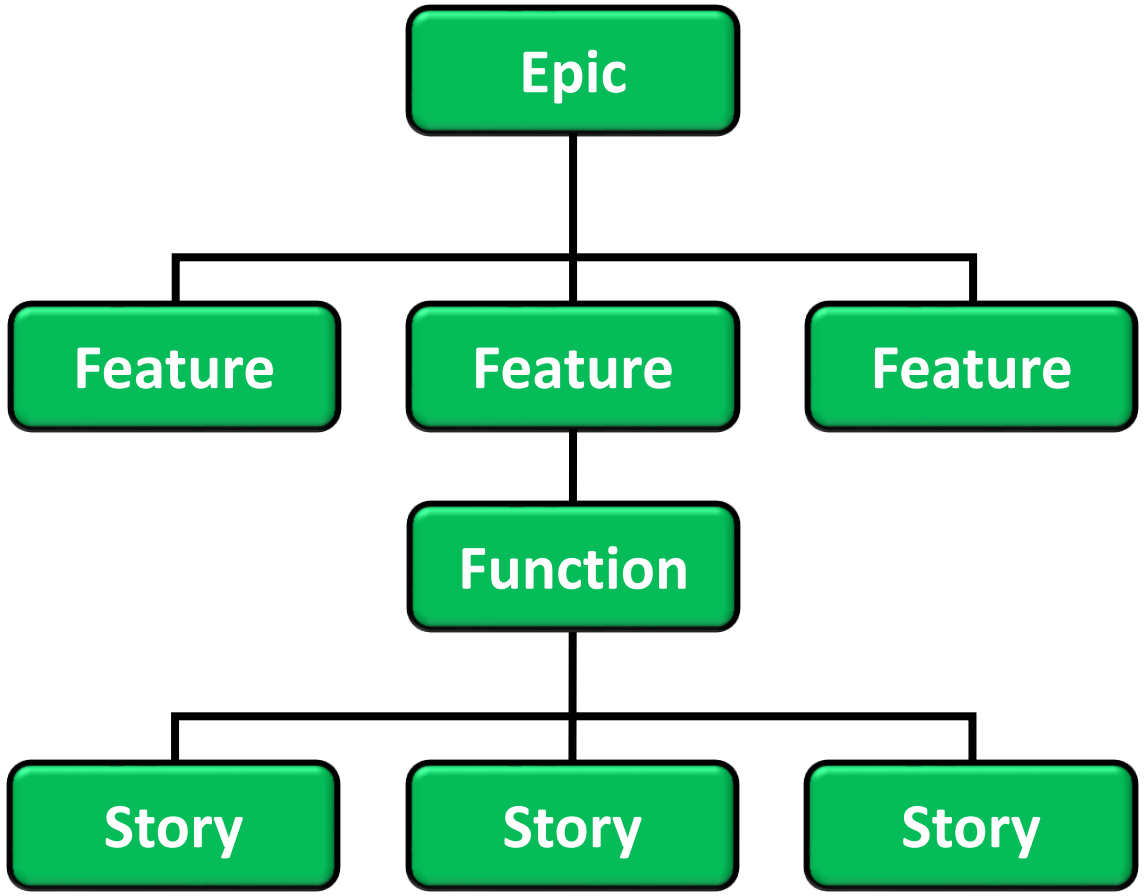
Applications Development Stages



From Idea to Product, with Support and Recovery



Epics, Features, and Stories



Epics describe the end goal of the project (i.e., product or service develop and deploy to Clients

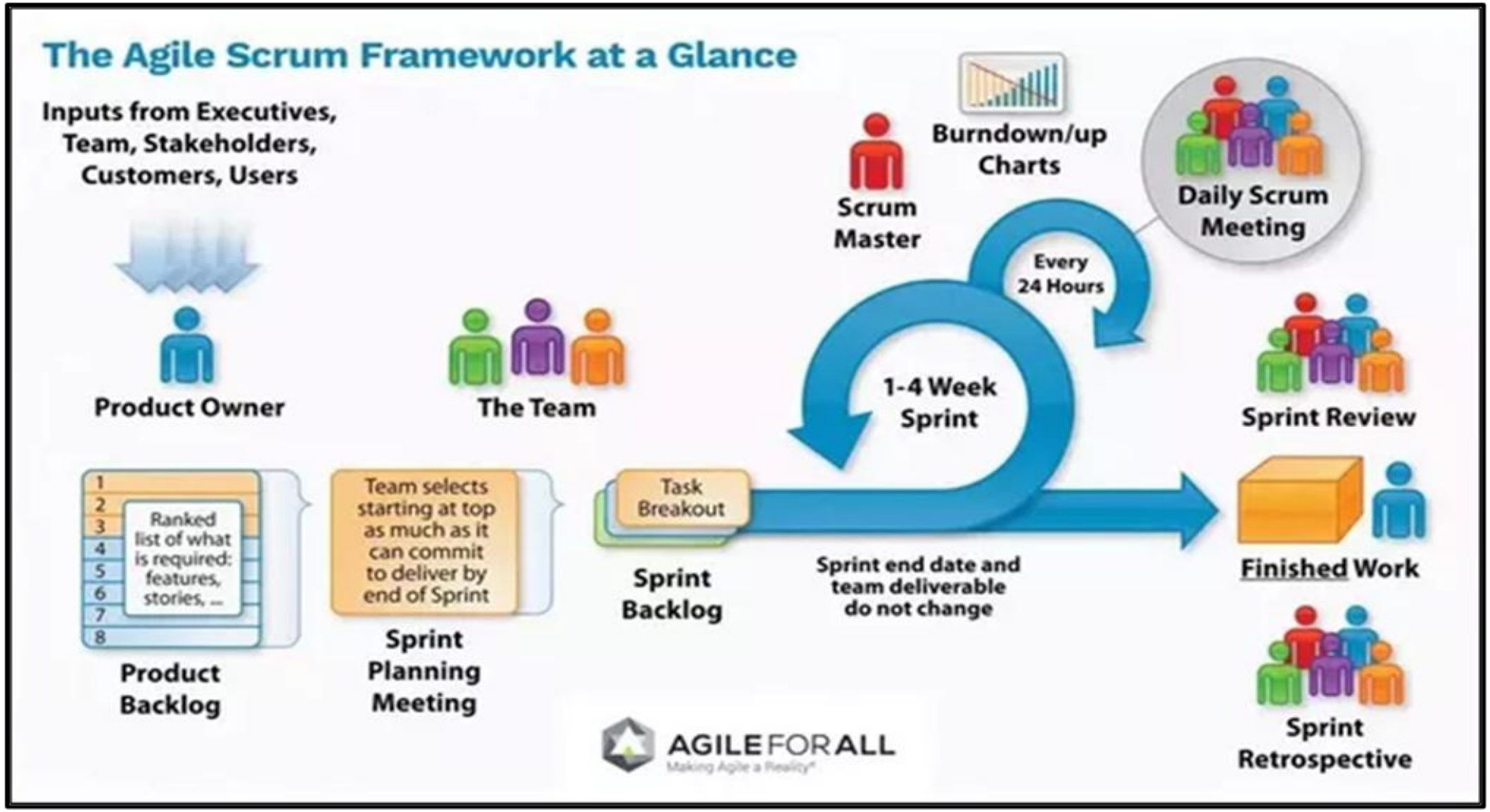
Features depict phases of development like Marketing Program, Sales, Closes, Deployment, Support, Maintain, Awareness, Training.

Functions are sub-features or specific purposes used to support a feature and developed via specific paths or groups (i.e., SaaS product or Mobile product).

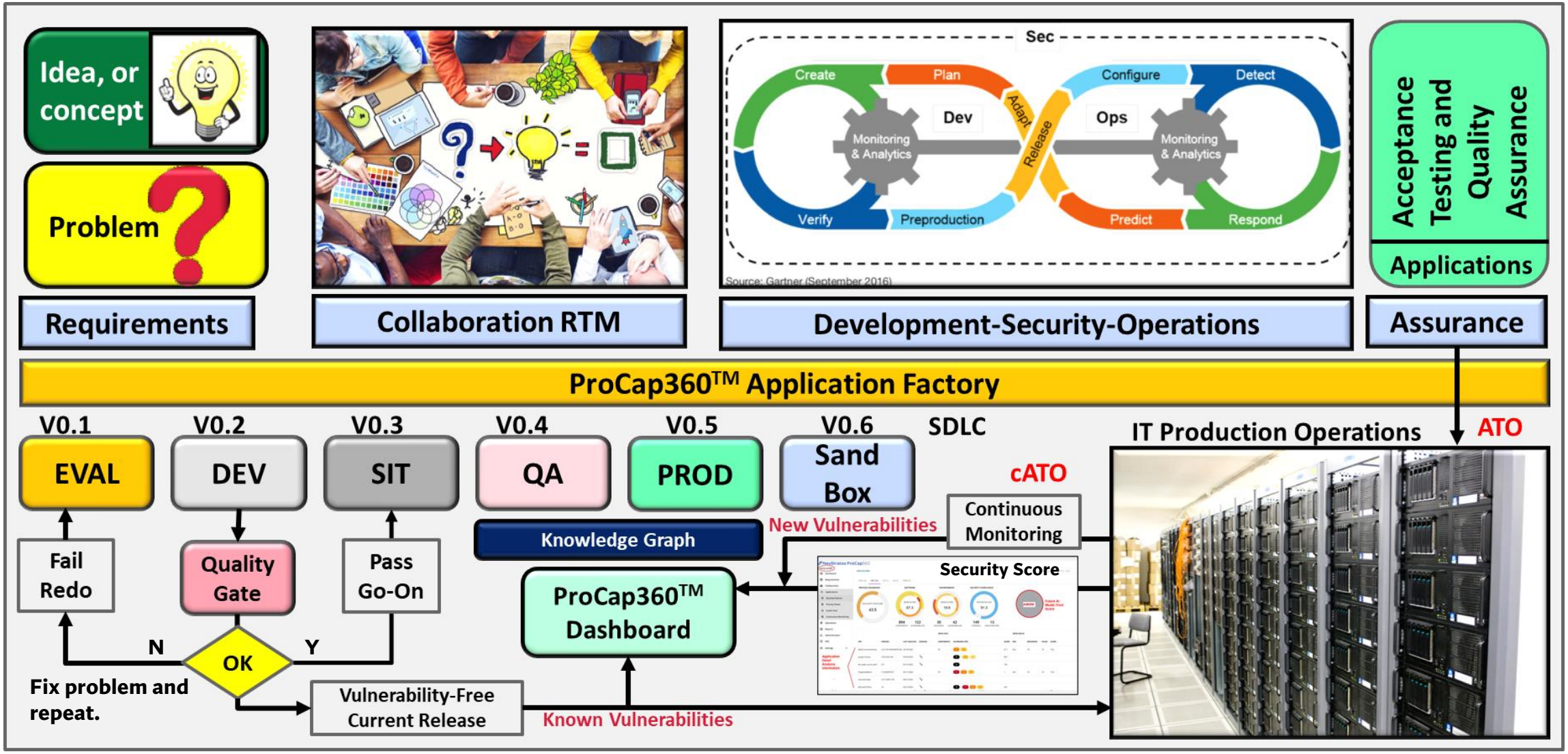
Stories provide specific tasks that must be performed for every feature)i.e., Marketing Materials, Marketing Program, Advertising Program, Sales Follow-up on Prospects, Closing Clients, Deploying Produce or Services, Awareness and Training Sessions, Supporting Customers, Maintaining and Enhancing Products and Services, etc.)

Project Management provides schedules, status, costs analysis, action items, and reporting.

Agile, JIRA, Confluence, and SharePoint



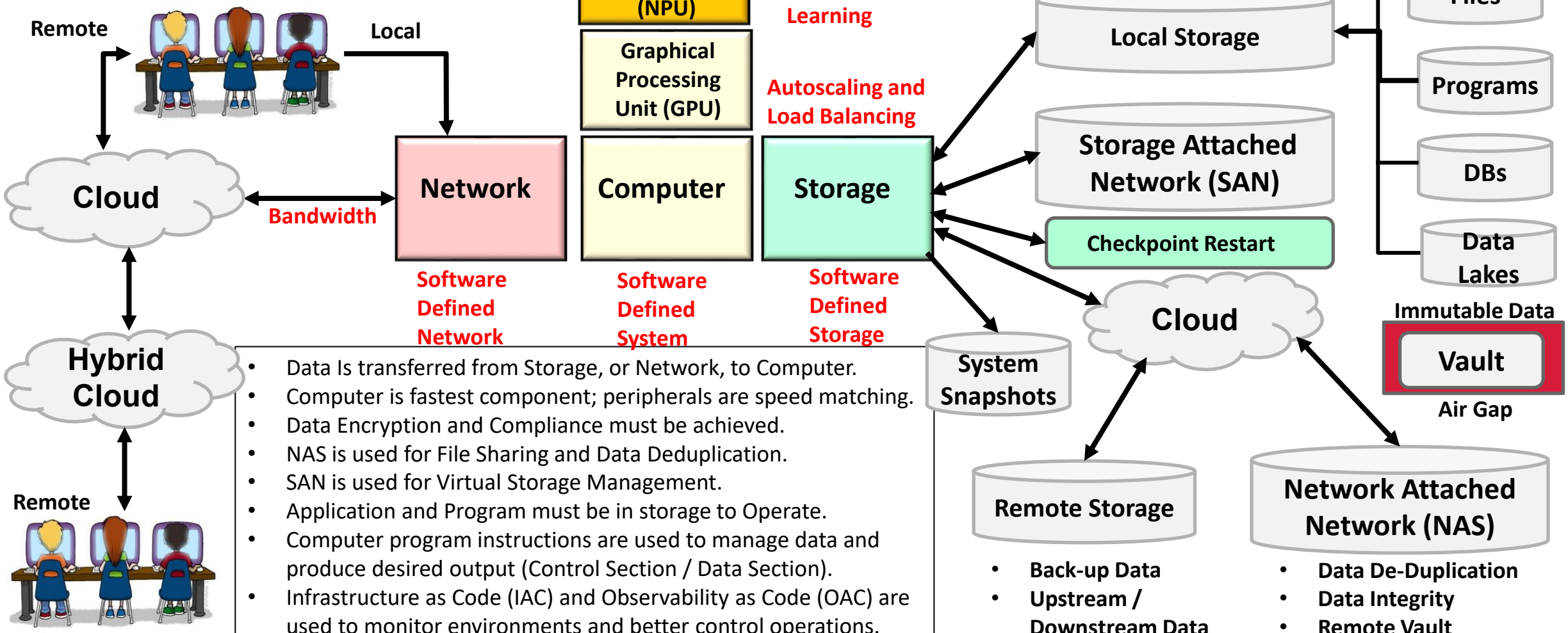
From Concept to Applications via DevSecOps



Monitoring Operations and Controlling Resources

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

Know your company's infrastructure

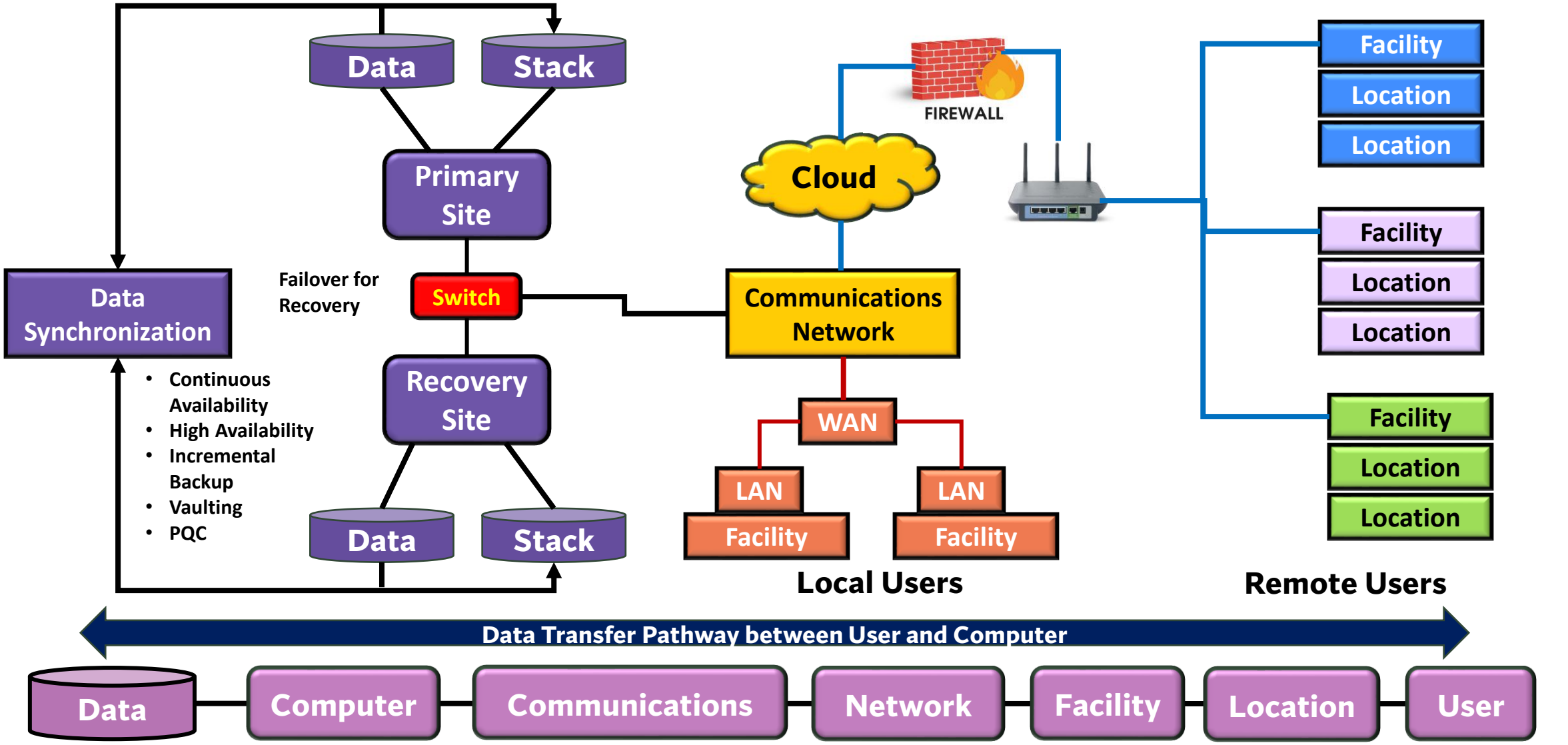


- Data Is transferred from Storage, or Network, to Computer.
- Computer is fastest component; peripherals are speed matching.
- Data Encryption and Compliance must be achieved.
- NAS is used for File Sharing and Data Deduplication.
- SAN is used for Virtual Storage Management.
- Application and Program must be in storage to Operate.
- Computer program instructions are used to manage data and produce desired output (Control Section / Data Section).
- Infrastructure as Code (IAC) and Observability as Code (OAC) are used to monitor environments and better control operations.

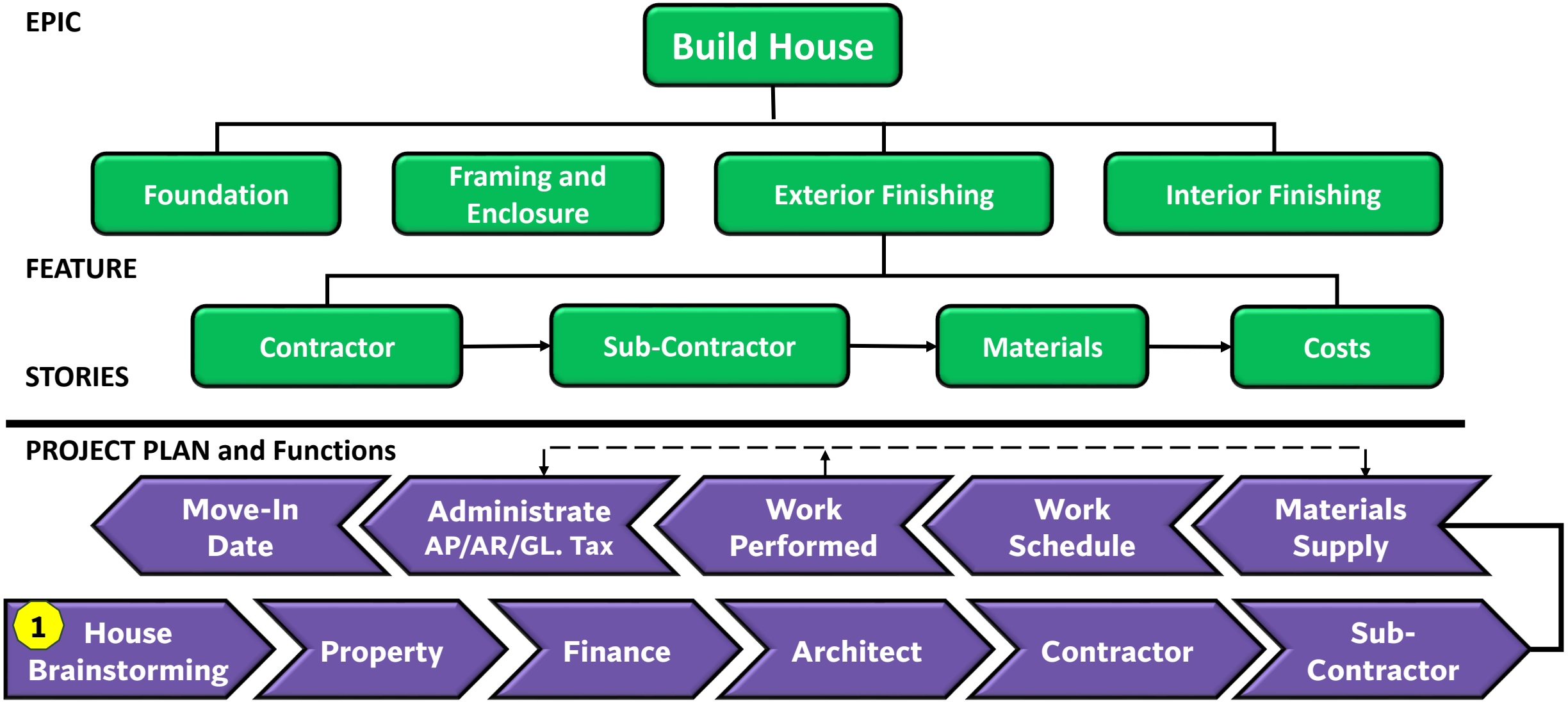
- Back-up Data
- Upstream / Downstream Data
- Secure Vaulting

- Data De-Duplication
- Data Integrity
- Remote Vault
- Immutable Data

IT Environment Overview and Recovery



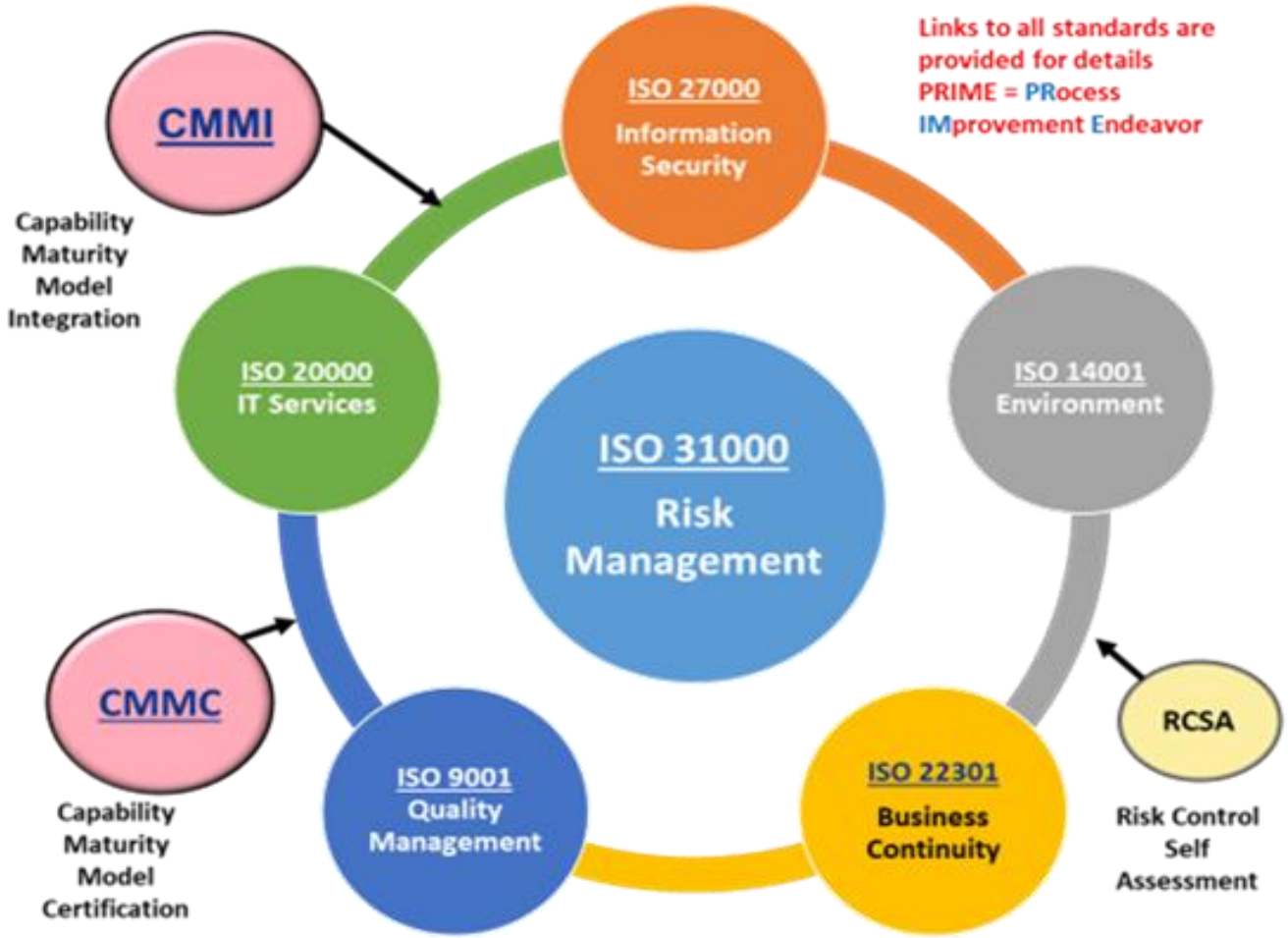
Example of Applying Agile to building a house - Anology



Integrating Protection Frameworks

The newest Integration Model – PRIME Approach

ISO – Internation Standards
NIST – Domestic Standards



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).

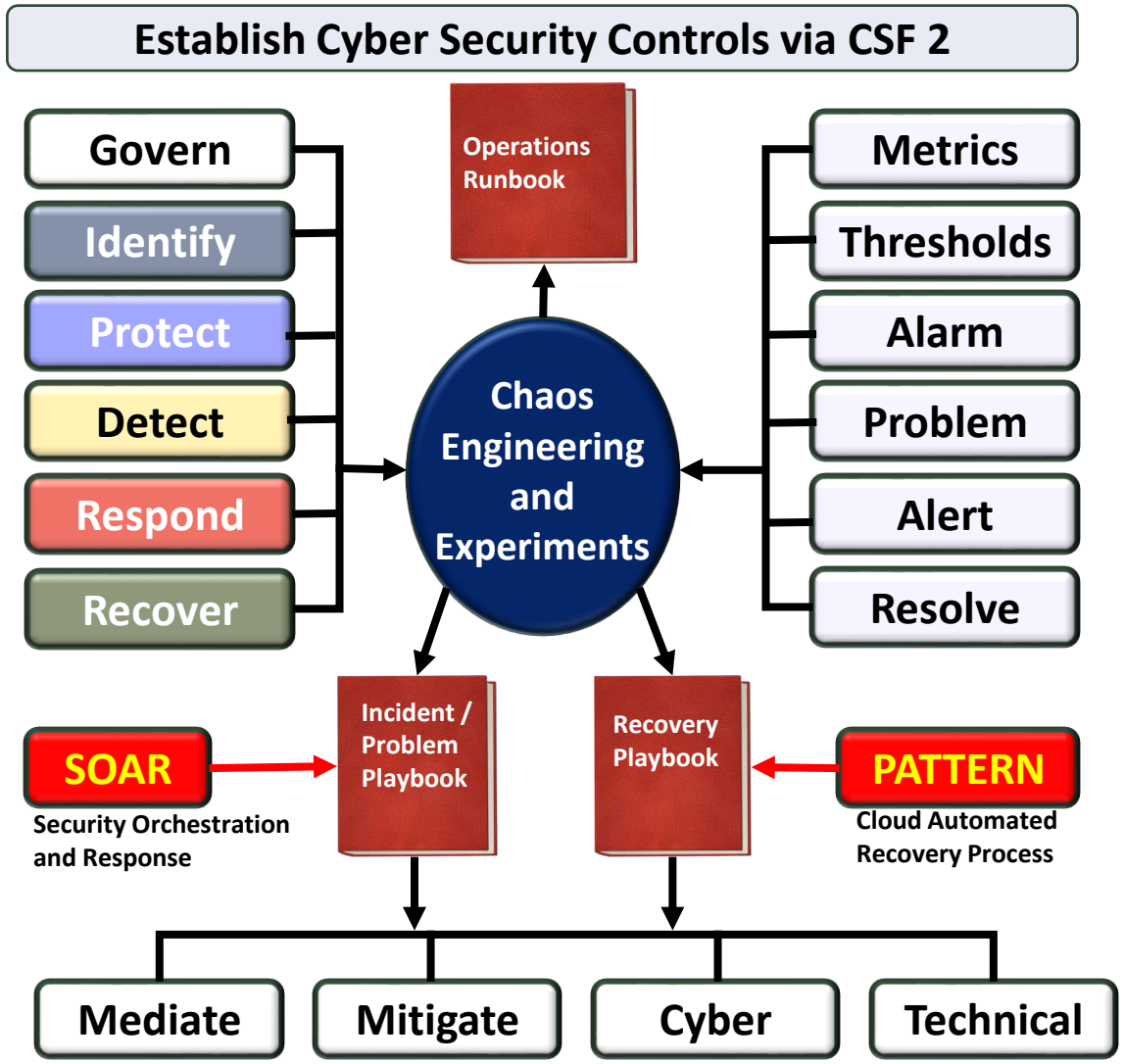
Then implement your **Business Continuity** (ISO 22301) Recovery Certification Process for Emergency, Crisis, Business, and IT Disaster Recovery Management.

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.

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



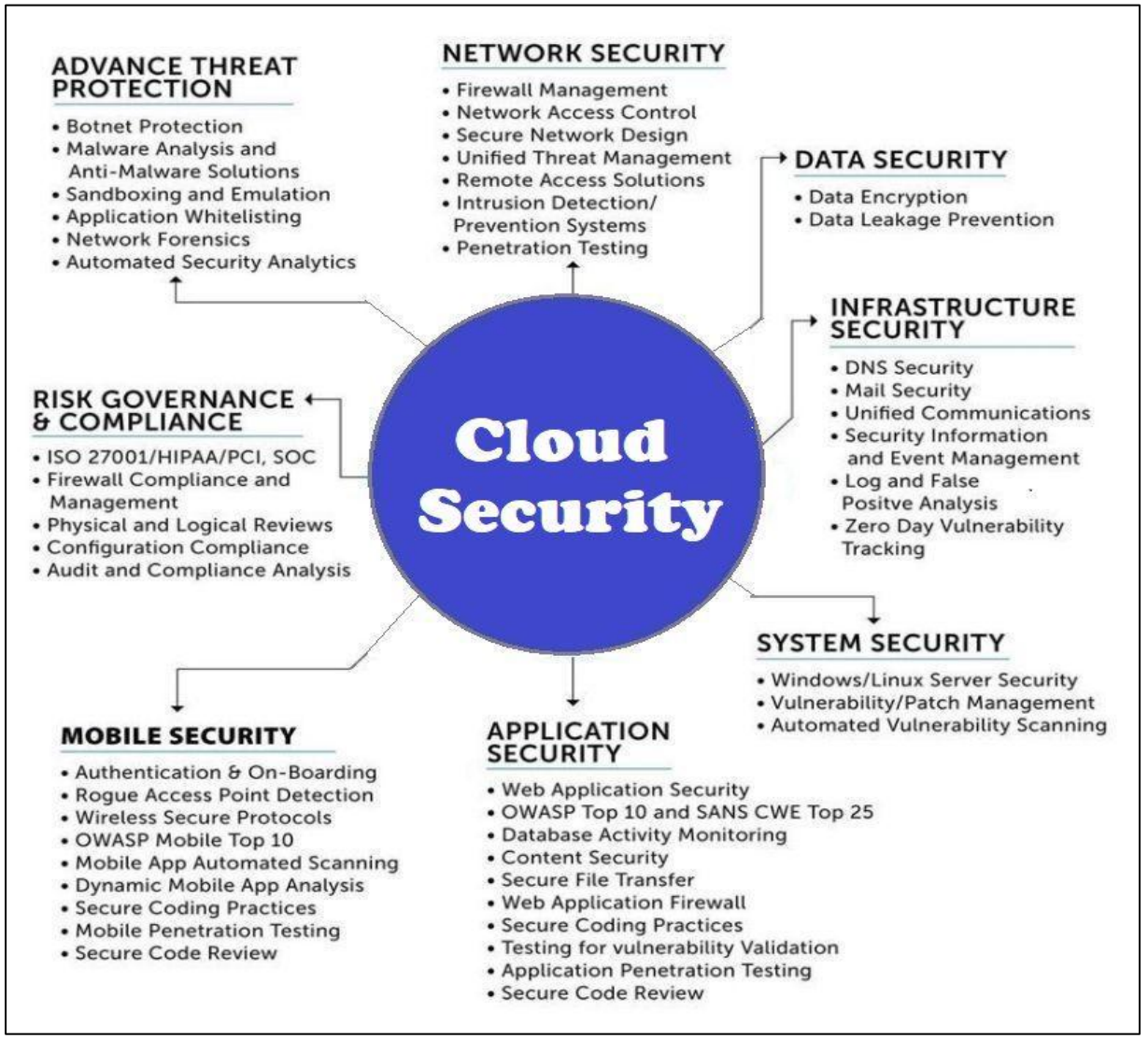
Cloud Security Disciplines

Advanced Threat Protection:
- Botnet Protection
- Malware Analysis and Anti-Malware Solutions
- Sandboxing and Emulation
- Application Whitelisting
- Network Forensics
- Automated Security Analytics

Risk Governance & Compliance:
- ISO 27001/HIPAA/PCI. SOC
- Firewall Compliance & Management
- Physical & Logical Reviews
- Configuration Compliance
- Audit and Compliance Analysis

Mobile Security:
- Authenticating & On-Boarding
- Rogue Access Point Detection
- Wireless Security Protocols
- OWASP Mobile Top Ten
- Mobile App Automated Scanning
- Dynamic Mobile App Analysis
- Secure Coding Practices
- Mobile Penetration Testing
- Secure Code Review

Data Security:
- Data Encryption
- Data Leakage Prevention



Network Security:
- Firewall Management
- Network Access Control
- Secure Network Design
- Unified Threat Management
- Remote Access Solutions
- Intrusion Detection
- Prevention Systems
- Penetration Testing

Infrastructure Security:
- DNS Security
- Mail Security
- Unified Communications
- Security Information and Event Management
- Logs and False Positive Analysis
- Zero Day Vulnerability Management

System Security:
- Windows/Linux Server Security
- Vulnerability/Patch Management
- Automated Vulnerability Scanning

Application Security:
- WEB Application Security
- OWASP Top 10 and SANS CWE Top 25
- Database Activity Monitoring
- Content Security
- Secure File Transfer
- Secure SDLC practices
- DevSecOps implementation.

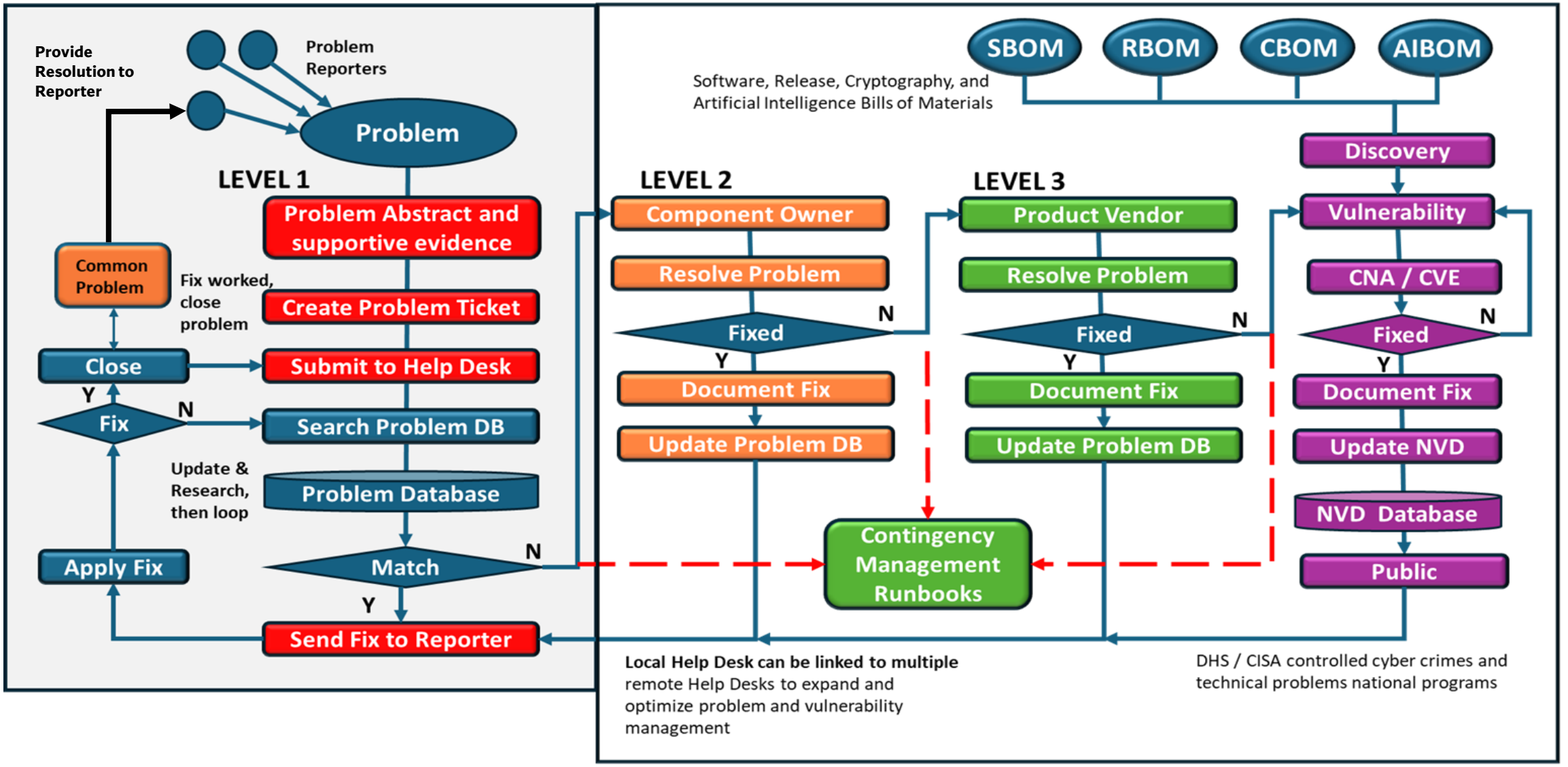
NIST – Secure Software Development Framework (SDDF)

NIST Guidelines for developing Secure Software as part of the "Secure by Design" directive from DHS/CISA.

- A NIST consortium including NCCoE computer security experts and 14 industry partners has drafted a high-level overview of guidelines it is developing to help organizations develop software in a secure, agile fashion and test for security vulnerabilities.
- NIST is soliciting comments from the public on the draft until Sept. 12, and the agency is planning a virtual event to showcase the project and gather feedback on Aug. 27.
- The consortium and draft guidelines respond to a June 2025 executive order to strengthen the nation's cybersecurity.

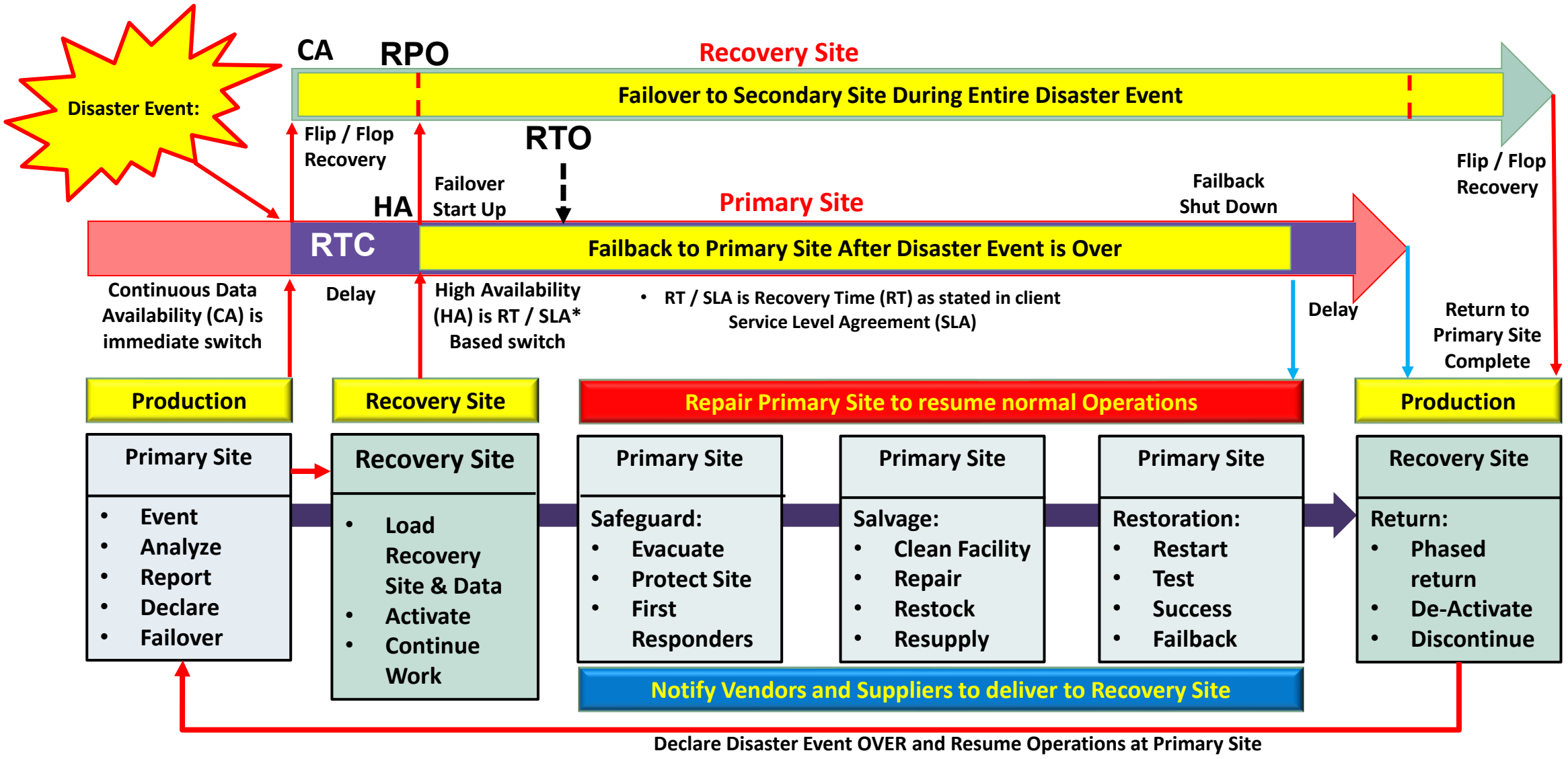
Link to detailed article on SDDF
Link to NIST article on DevSecOps
Link to NCCoE DevSecOps article

Problem Management and Control



The Disaster Event Life Cycle

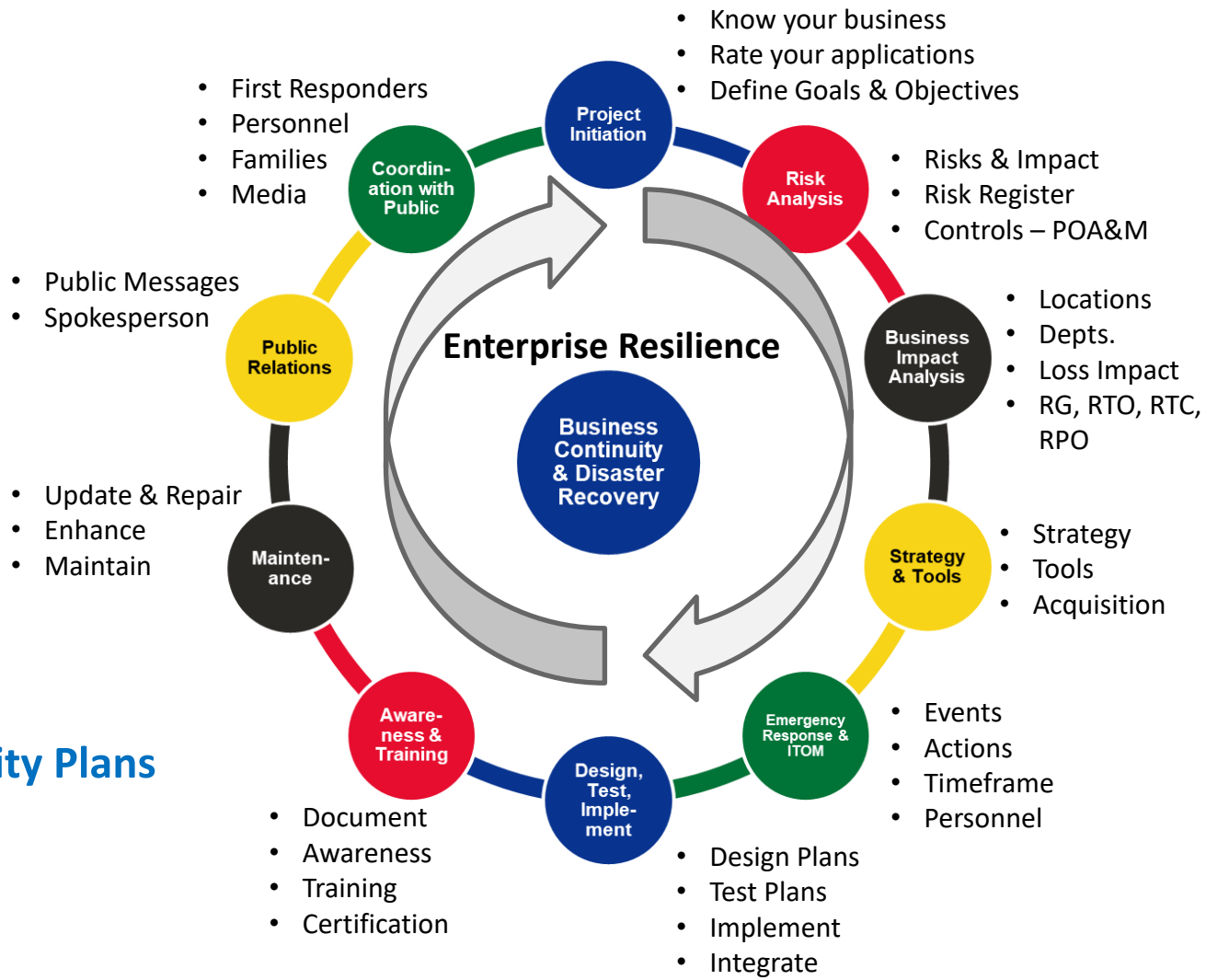
CA is Continuous Availability
HA is High Availability
RTO – Recovery Time Objective
RPO – Recovery Point Objective
RTC – Recovery Time Capability
MTO – Maximum Tolerable Outage



Ten Step Process to establish BCM/DR Practice

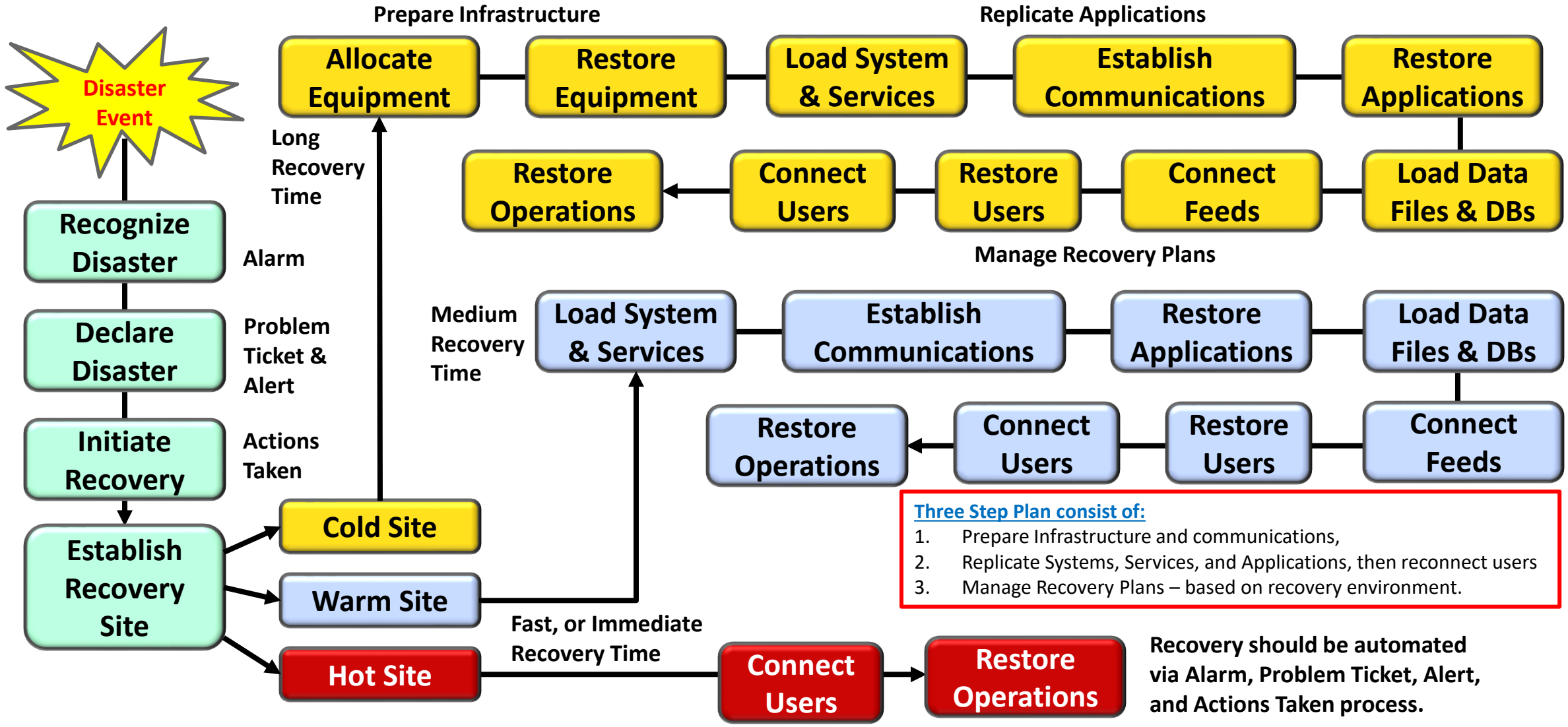
Thomas Bronack
Email: bronackt@dcag.com
Phone: (917) 673-6992

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

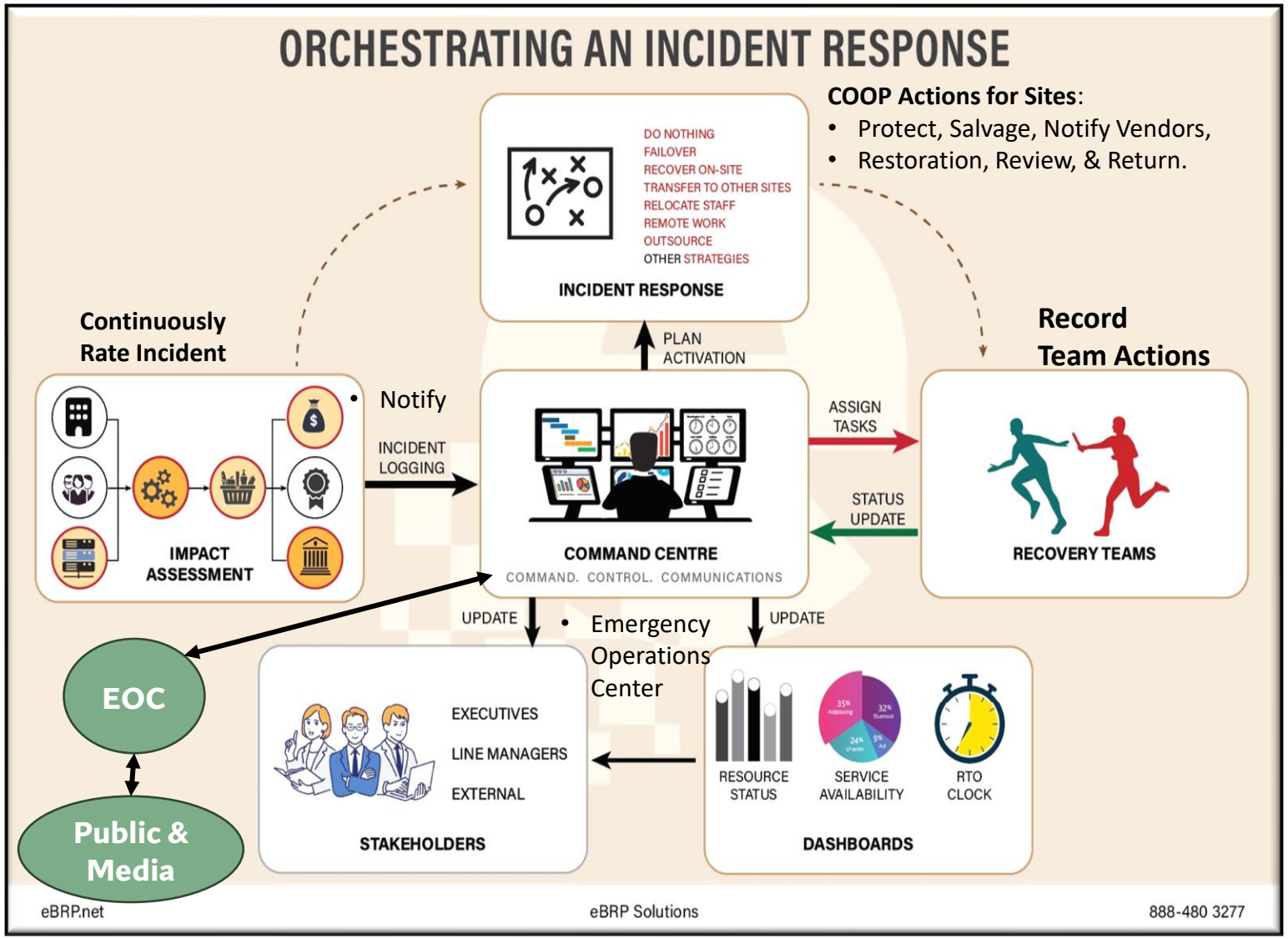


Sequence of Events to enact a Recovery Operation

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



Business Continuity Command Center → EOC



Incident and Recovery Management.

1. Incident Occurs – Problem Ticket, Alarm
2. Impact Assessment performed – Problem Ticket completed and failing component
3. Command Center notifies Recovery Teams
4. Stakeholders are informed
5. Dashboards Maintained
6. Status Reports provided to EOC
7. EOC only Talks to Public & Media (single voice)
8. Incident Tracked until Completed
9. Post Incident Review
10. Improvements
11. Update & Maintain Recovery Plans

Overall Benefits

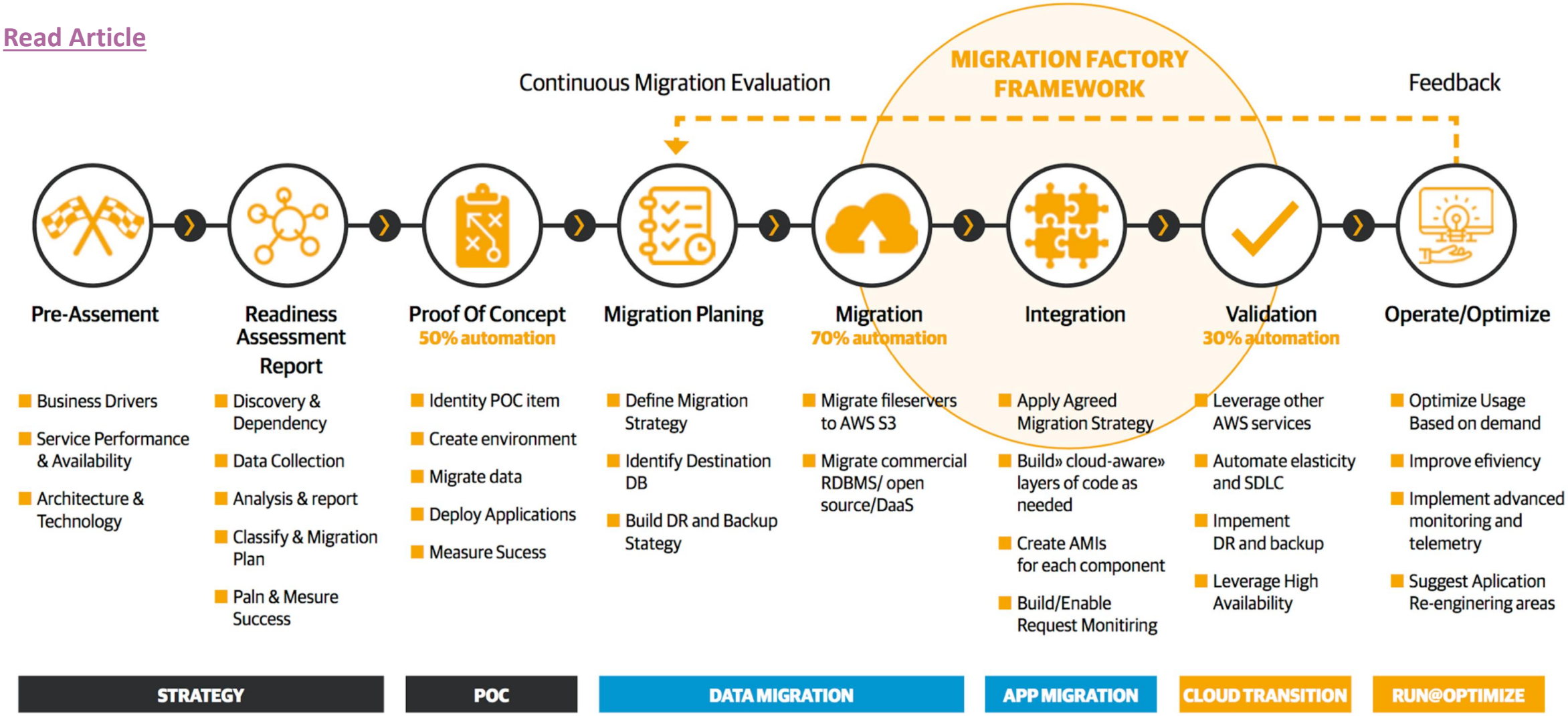
Efficiency: Centralized control improves response times and reduces the duplication of efforts.

Effectiveness: Enhanced coordination and resource allocation lead to more effective incident handling.

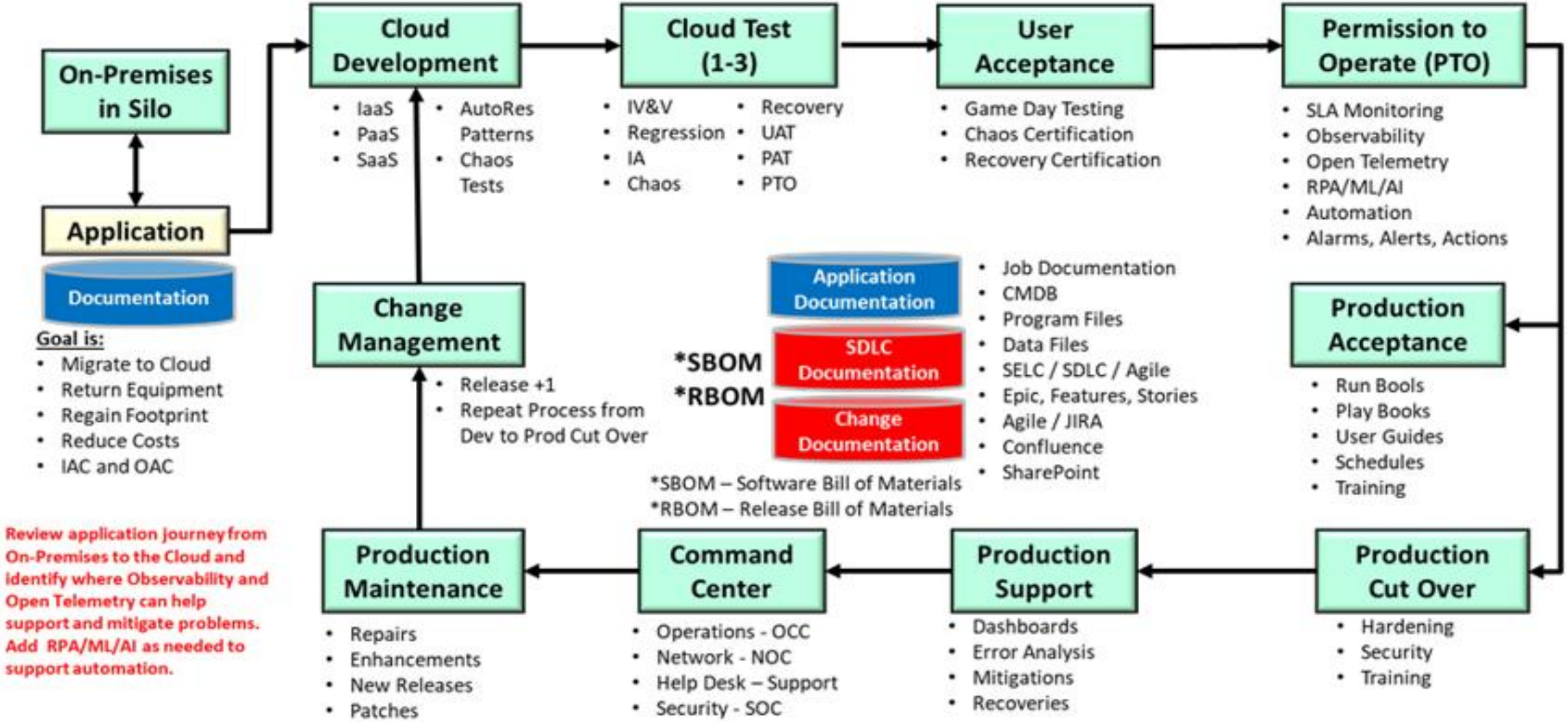
Compliance and Reporting: Ensures that response efforts are documented and reported, meeting regulatory and compliance requirements.

Using AI Planning for Migrating Applications to AWS Cloud

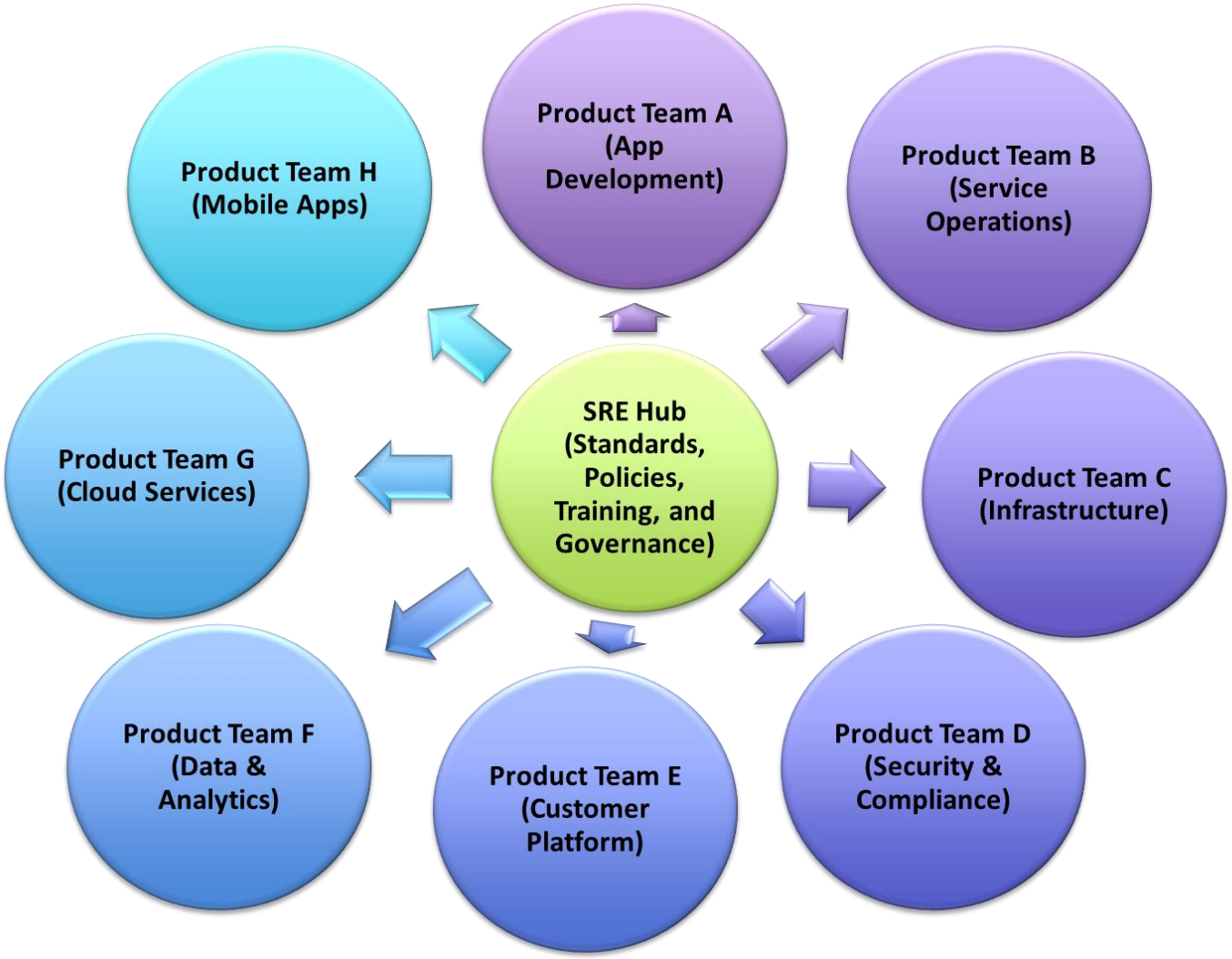
Read Article



Migrating Applications to the Cloud



Site Reliability Engineer (SRE) Hub Process Overview



Pillar	Description	Example Tools
Reliability	Ensuring systems meet SLOs & SLAs	SLO dashboards
Scalability	Systems grow without bottlenecks	Kubernetes, autoscaling
Observability	Metrics, logs, traces	Prometheus, Grafana, ELK
Automation	Replacing manual ops with code	Terraform, Ansible
Efficiency	Cost vs. performance balance	Cloud spend analysis
Incident Response	Detect/respond to outages quickly	PagerDuty, Opsgenie

SRE Pillars:

1. **Reliability (SLA, SLO, RTO, RPO, etc.)**
2. **Scalability (Kubernetes)**
3. **Observability (Monitoring and Reporting)**
4. **Automation (Replacing Manual Tasks)**
5. **Efficiency (Reducing Toil)**
6. **Problem and Incident Management (Reducing MTTR)**
7. **Awareness and Training**

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

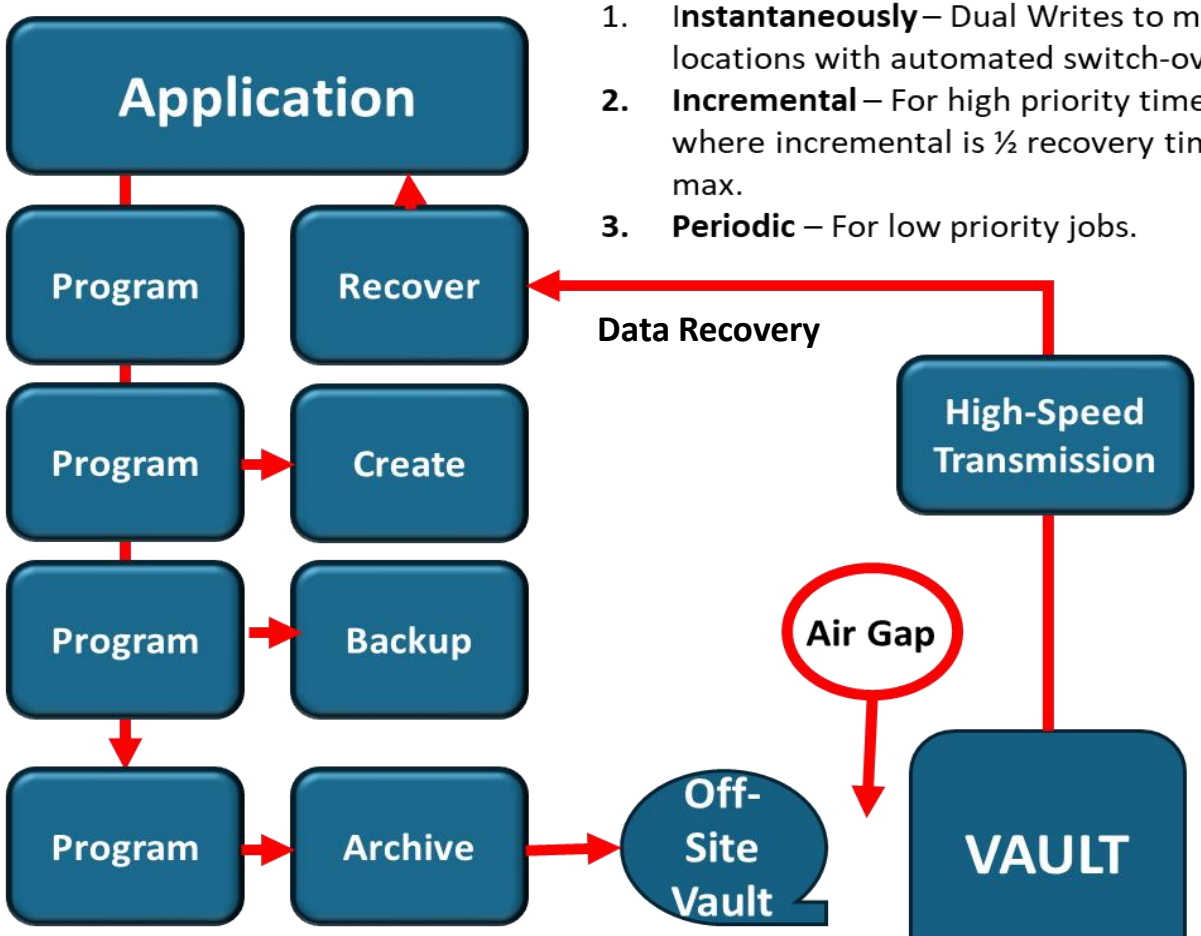
- Implement hybrid cloud solutions for scalability and flexibility
- Utilize cloud-based disaster recovery

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

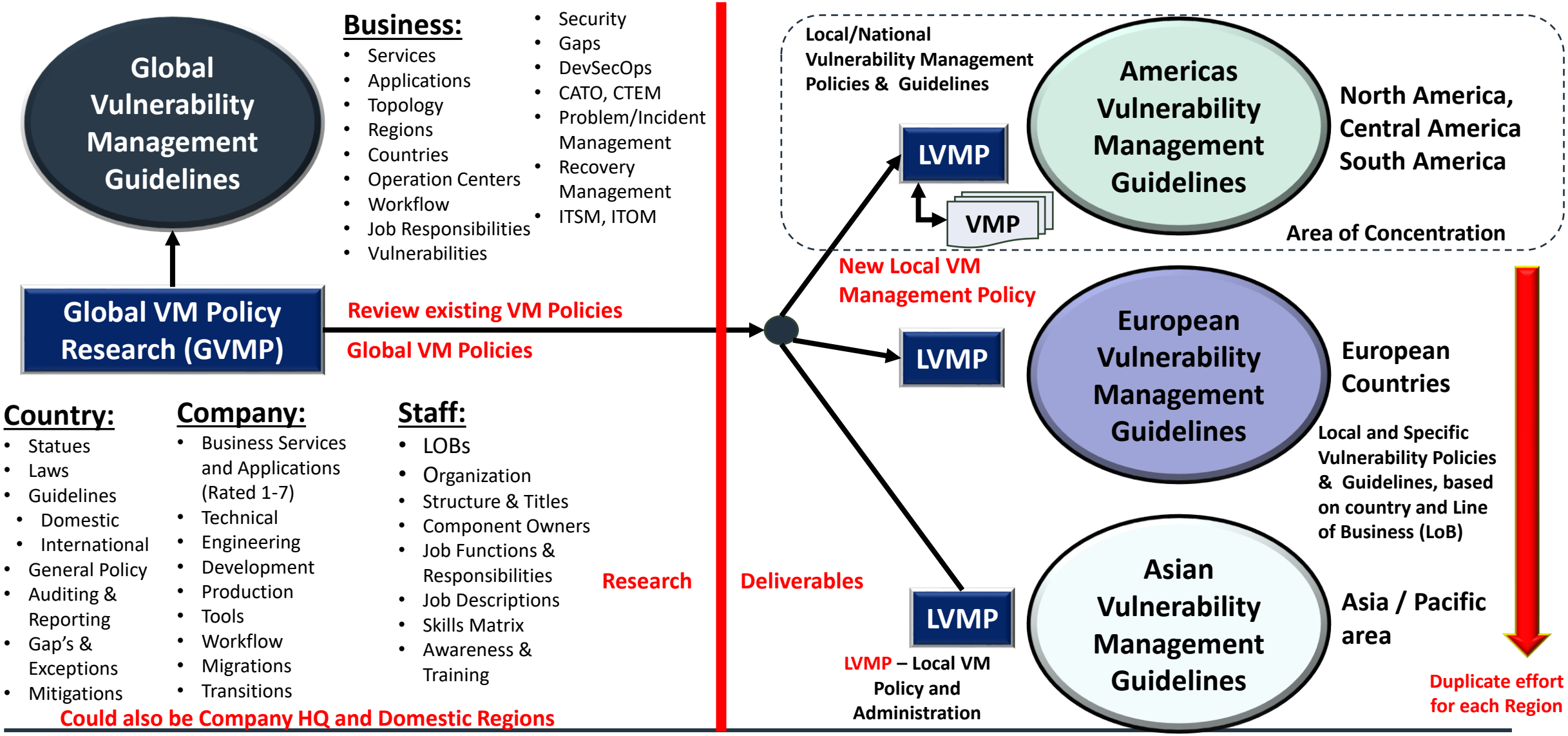
Downtime can cost up to $9,000 per minute



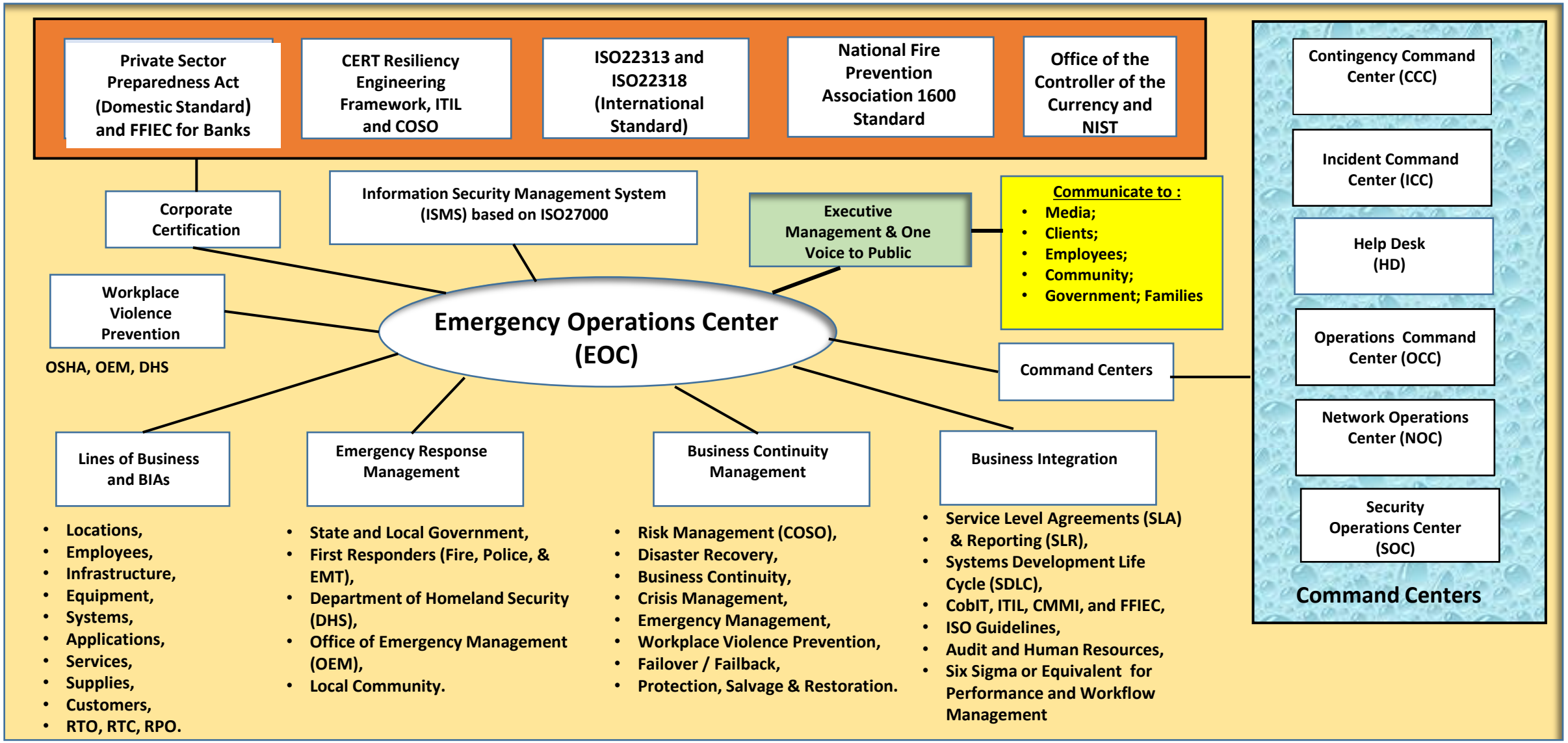
Backup / Recovery Times by RTO:

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.

Global Vulnerability Management Policy generation



Emergency Operations Center (EOC)

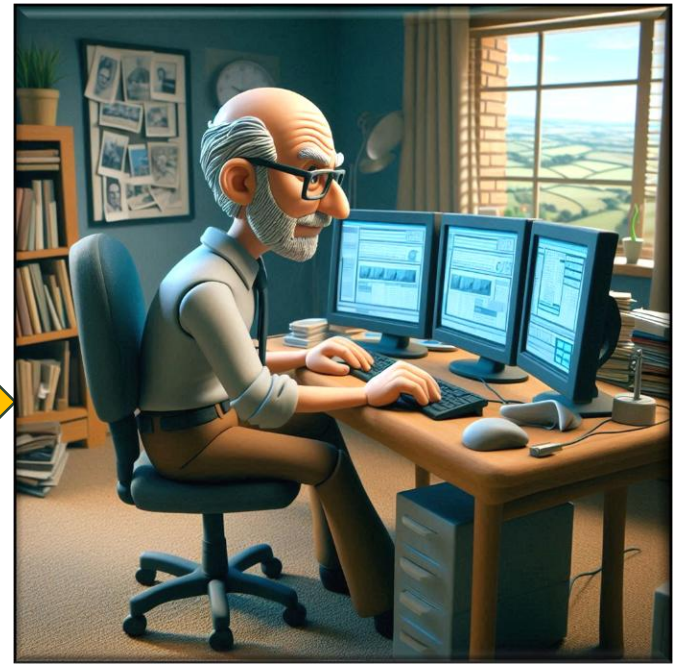


Reaching out to assist our clients

- 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
Website: http://www.dcag.com
bronackt@dcag.com
bronackt@gmail.com
917-673-6992