# Risk Management – Introduction and Overview

Thomas Bronack, CBCP

## Presentation Topics

- Today’s Troubled Environment.
- Secure by Design from DHS/CISA.
- Understanding your Organization.
- Defining Compliance Requirements.
- Vulnerability Management
- Defining Recovery Requirements.
- Business Continuity Management.
- Application Factory /  Quality Gates.
- Continuous Monitoring.

## Tom Specializes in:

- Enterprise Resilience,
- Corporate Certification,
- Vulnerability Management,
- Strategic and Tactical Planning,
- Project and Team Management
- Awareness and Training

# Safeguarding your Environment

## Contact Information:

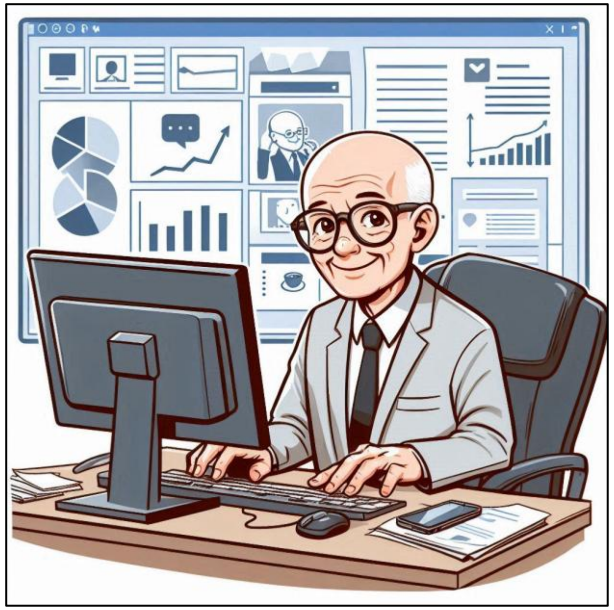
- bronackt@gmail.com
- bronackt@dcag.com
- http://www.dcag.com
- (917) 673-6992

# A word from Thomas Bronack

I am a senior level manager with in-depth experience in **Enterprise Resilience, Vulnerability Management, Risk Management, and Corporate Certification** for large enterprises in disciplines like: Banking, Brokerage, Finance, Insurance, Pharmaceuticals, and Manufacturing which provided me with a solid understanding of the risks faced by companies and how best to safeguard a firm through workflow, compliance, and recovery.

I have provided enterprise analysis, evaluation, recommendations, identification of Key Performance Indicators (KPIs), Enterprise Risk Management, and planning  materials to eliminate weaknesses and optimize operations. I have optimized the Planning, development, recovery, testing, and  production process to provide vulnerability-free and recoverable products / services, while training teams to achieve a safeguarded,  efficient, compliant, and vulnerability-free environment.

I follow the "**Whole of Nation**" and "**Secure by Design**" guidelines developed by DHS/CISA to integrate an Application Factory with Quality Control Gates to produce applications with all components at current release level and free of known vulnerabilities. Usa a Software Bill of Materials (SBOM) to identify  vulnerabilities for mitigation by the patch and release management team prior to production and (Continuous Threat Exposure Management) error identification while in production to identify new vulnerabilities for quick mitigation before hackers can exploit them. This supports the software supply chain and production environment.



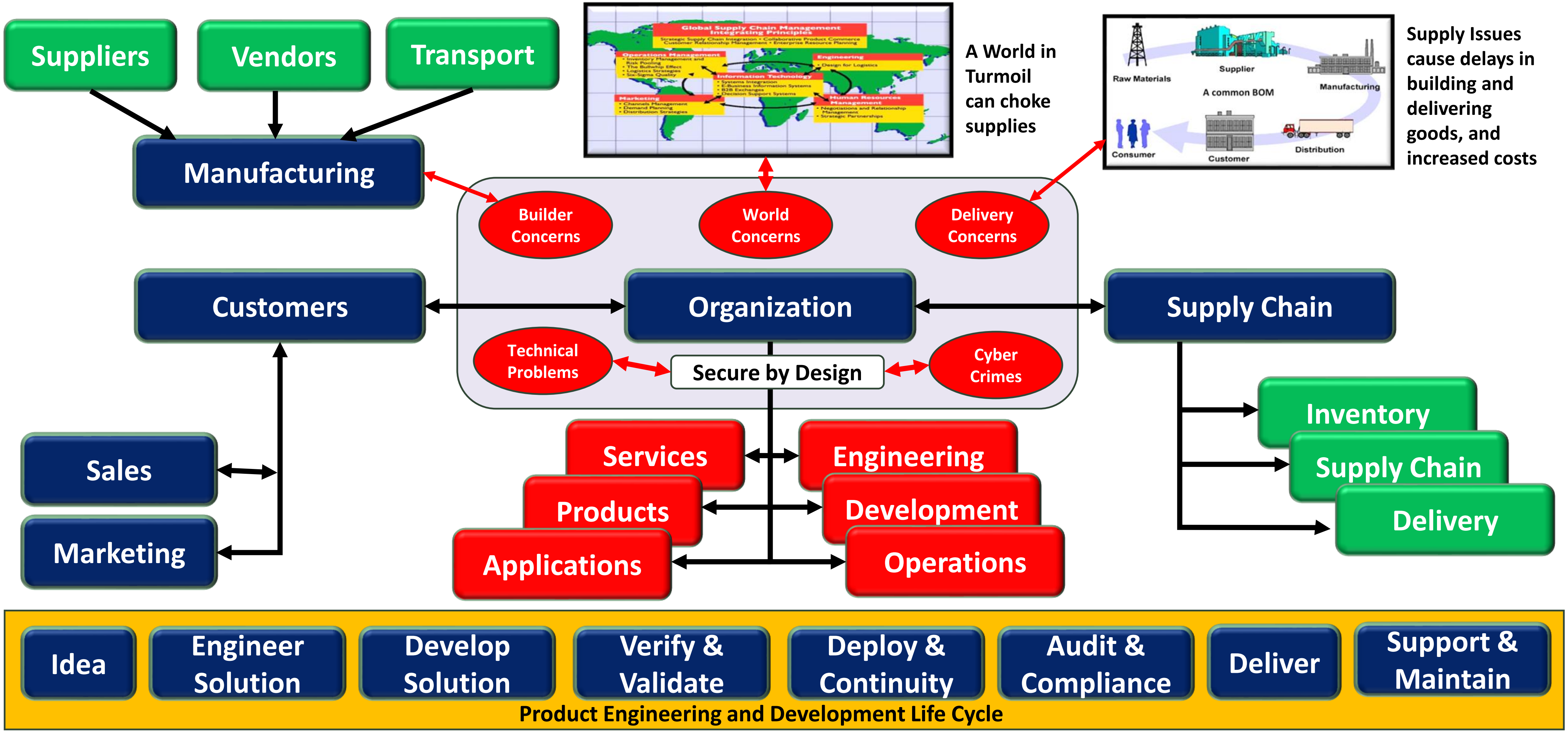
A strong generalist with extensive IT industry experience, ready to help you.

Thomas Bronack, CBCP
bronackt@gmail.com
(917) 673-6992

# Agenda

- Today's Troubled Environment.
- Secure by Design from DHS/CISA.
- Vulnerability Management.
- Understanding your Organization.
- Data Sensitivity and Controls.
- Business Continuity Management.
- Migrating Application to the Cloud.
- Types of Application Recoveries.
- Building Applications from idea to final delivery.
- Defining and Fulfilling Compliance Requirements.
- Application Factory / Quality Gates.
- Vulnerability Management.
- Optimizing Operations.
- Continuous Monitoring.
- Defining Recovery Requirements.
- Global Guidelines and Procedures.
- Emergency Operations Center.

# Protecting Organization is more difficult than ever


Global Supply Chain Management
Integrating Principles
Strategic Supply Chain Integration • Collaborative Product Commerce
Customer Relationship Management • Enterprise Resource Planning
Operations Management
• Inventory Management and Risk Pooling
• The Bullwhip Effect
• Logistics Strategies
• Six-Sigma Quality
Engineering
• Design for Logistics
Information Technology
• Systems Integration
• E-Business Information Systems
• B2B Exchanges
• Decision Support Systems
Marketing
• Channels Management
• Demand Planning
• Distribution Strategies
Human Resources Management
• Negotiations and Relationship Management
• Strategic Partnerships
Raw Materials
Supplier
Manufacturing
A common BOM
Consumer
Customer
Distribution

Suppliers

Vendors

Transport

Manufacturing

A World in Turmoil can choke supplies

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

Builder Concerns

World Concerns

Delivery Concerns

Customers

Organization

Supply Chain

Technical Problems

Secure by Design

Cyber Crimes

Sales

Marketing

Services

Engineering

Products

Development

Applications

Operations

Inventory

Supply Chain

Delivery

Idea

Engineer Solution

Develop Solution

Verify & Validate

Deploy & Continuity

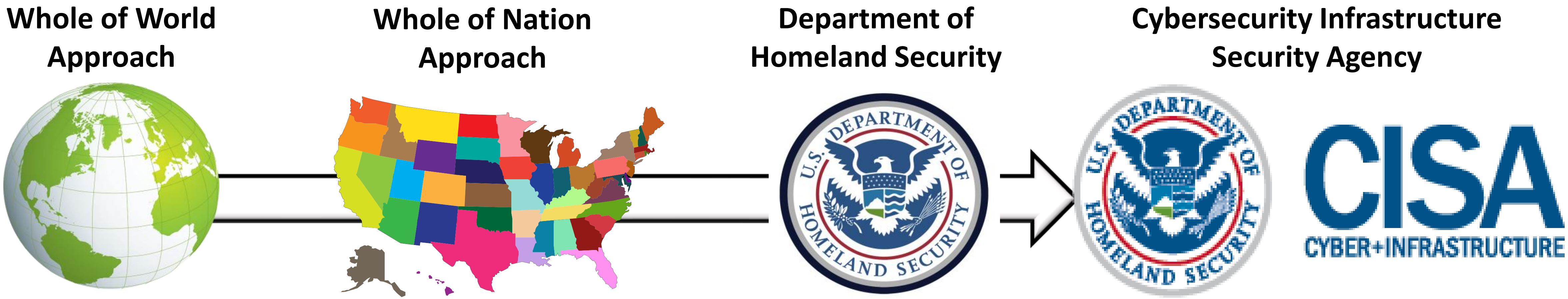
Audit & Compliance

Deliver

Support & Maintain

Product Engineering and Development Life Cycle

# A Whole of World approach to Cybersecurity


Whole of World Approach
Whole of Nation Approach
Department of Homeland Security
Cybersecurity Infrastructure Security Agency
CISA
CYBER+INFRASTRUCTURE

**2030 Most Significant Cyber Concerns:**

1. Supply Chain Compromises
2. Advanced disinformation campaigns
3. Rise of Digital Surveillance
4. Human error and legacy systems
5. Targeted Attacks
6. Lack of analysis and controls
7. Rise of advanced hybrid attacks
8. Skill shortage
9. Cross-border ICT suppliers as a single-point-of-failure
10. Artificial Intelligence abuse

**Vulnerability Management Process:**

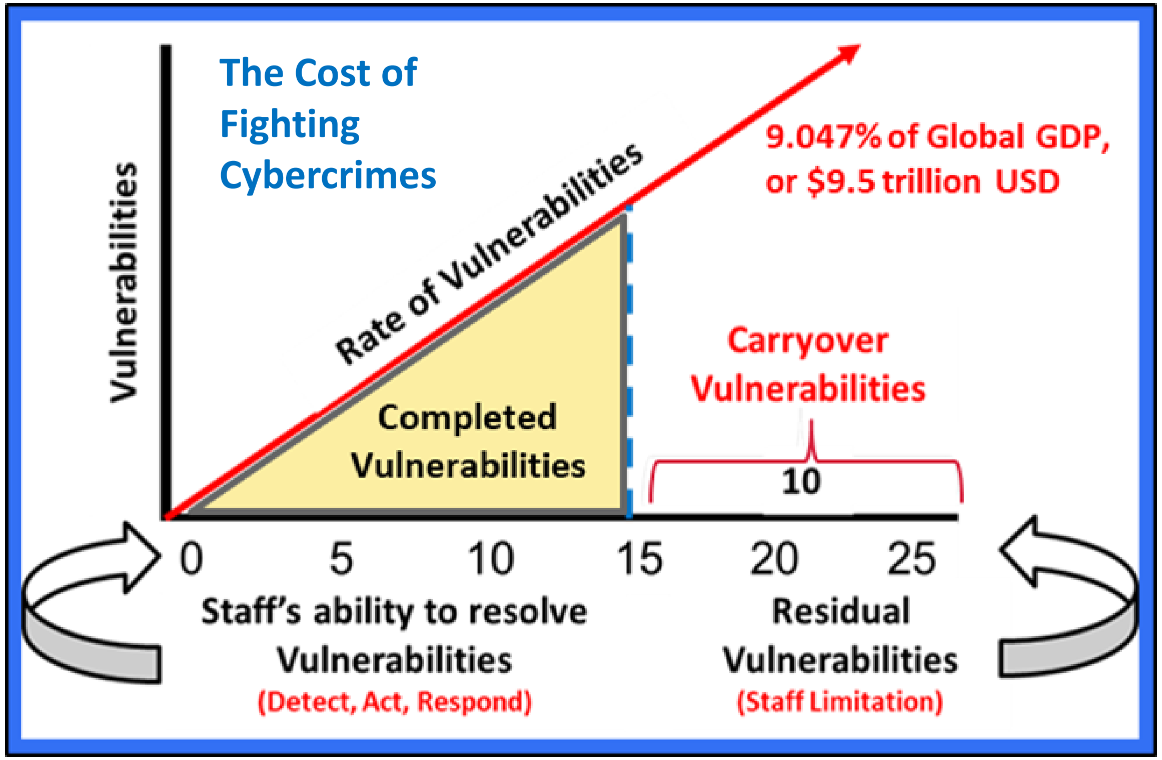
1. Detect Vulnerability (SBOM)
2. Assess the Risk (CVE)
3. Prioritize Remediation (CVSS, KVE, EPSS)
4. Confirm Remediation
5. Optimize through automation
6. Advance the use of BOMs for Software, Release Control, and Artificial Intelligence

**DHS/CISA - Secure by Design principles:**

1. Build security considerations into the software requirements specification
2. Address possible abuse cases (e.g., how users may misuse the software).
3. Create and enforce secure code guidelines.
4. Use appropriate security tools.
5. Conduct security audits at multiple stages of the SDLC.
6. Conduct vulnerability testing that includes negative testing and penetration testing.
7. Incorporate security within deployment and maintenance processes.
8. Ensure reused software is from trusted sources and properly evaluated.
9. Provide feedback throughout the process on security effectiveness.
10. Educate developers and QA teams on secure coding techniques.

# Fighting Cybercrime Costs with Secure by Design

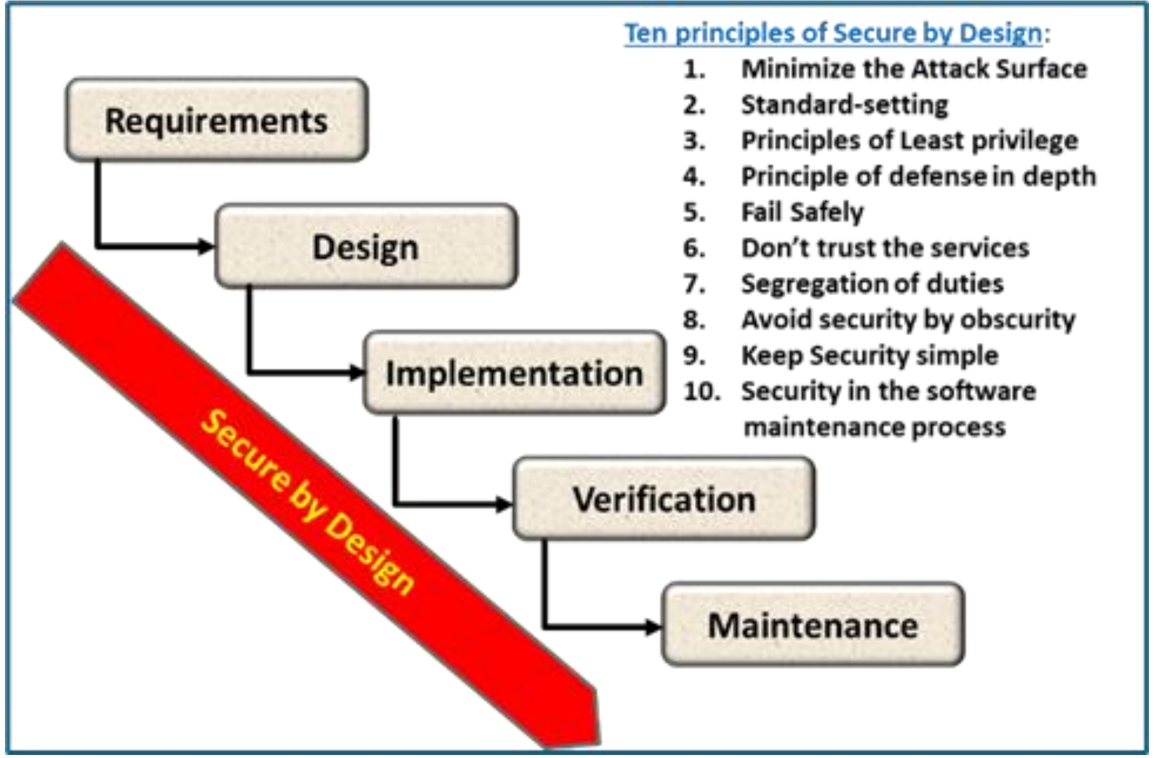
## Vulnerabilities



The Cost of Fighting Cybercrimes
Vulnerabilities
Rate of Vulnerabilities
9.047% of Global GDP, or $9.5 trillion USD
Completed Vulnerabilities
Carryover Vulnerabilities
10
0
5
10
15
20
25
Staff's ability to resolve Vulnerabilities
(Detect, Act, Respond)
Residual Vulnerabilities
(Staff Limitation)

The **cost of fighting cybercrimes** and technology threats is estimated at $9.5 Trillion and 9.04 % of Global GDP. Improving the vulnerability fix rate will greatly reduce costs and improve business service continuity and resilience.

## Secure by Design

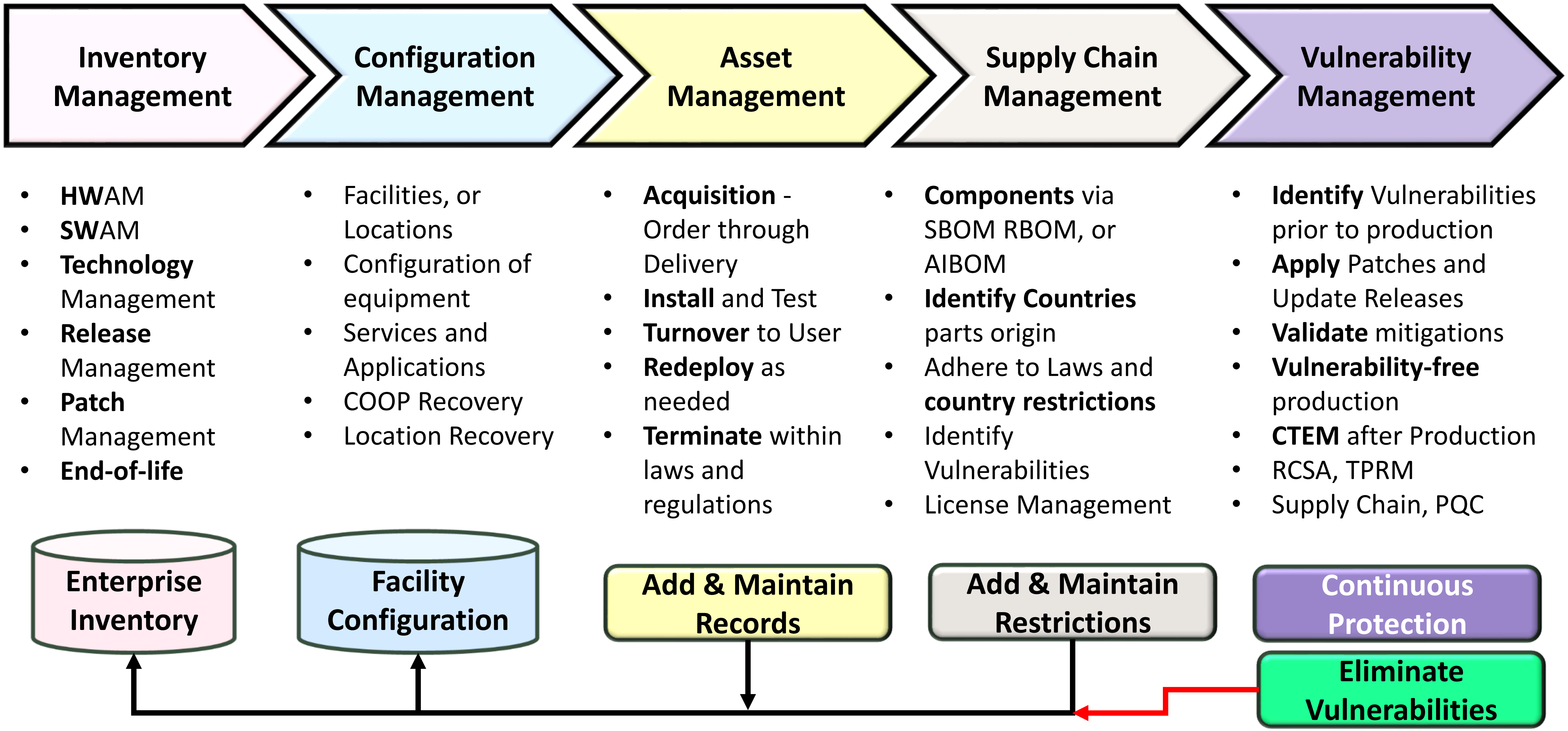


Ten principles of Secure by Design:

1. Minimize the Attack Surface
2. Standard-setting
3. Principles of Least privilege
4. Principle of defense in depth
5. Fail Safely
6. Don't trust the services
7. Segregation of duties
8. Avoid security by obscurity
9. Keep Security simple
10. Security in the software maintenance process

The government has developed a "**Whole of Nation**" approach to combat these costs through the "**Secure by Design**" methodology developed by DHS/CISA to safeguard Government, Business, Infrastructure, and Utilities from cybercrimes and technology threats.

# Know and Control your Environment



**Inventory Management**

- **HWAM**
- **SWAM**
- **Technology** Management
- **Release** Management
- **Patch** Management
- **End-of-life**

**Configuration Management**

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

**Asset Management**

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

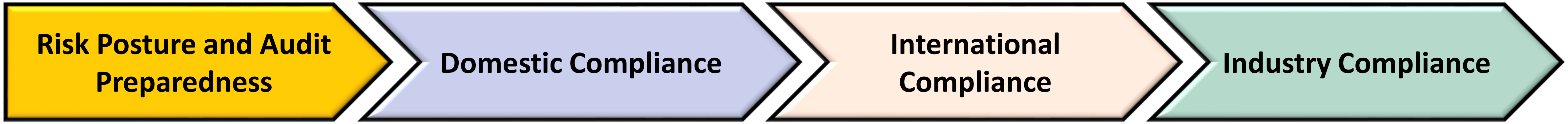
**Supply Chain Management**

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

**Vulnerability Management**

- **Identify** Vulnerabilities prior to production
- **Apply** Patches and Update Releases
- **Validate** mitigations
- **Vulnerability-free** production
- **CTEM** after Production
- RCSA, TPRM
- Supply Chain, PQC

# 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
- **TPRM**, Supply Chain
- **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
- **PQC** – Post-Quantum Cryptography

## 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
- Vulnerability Management

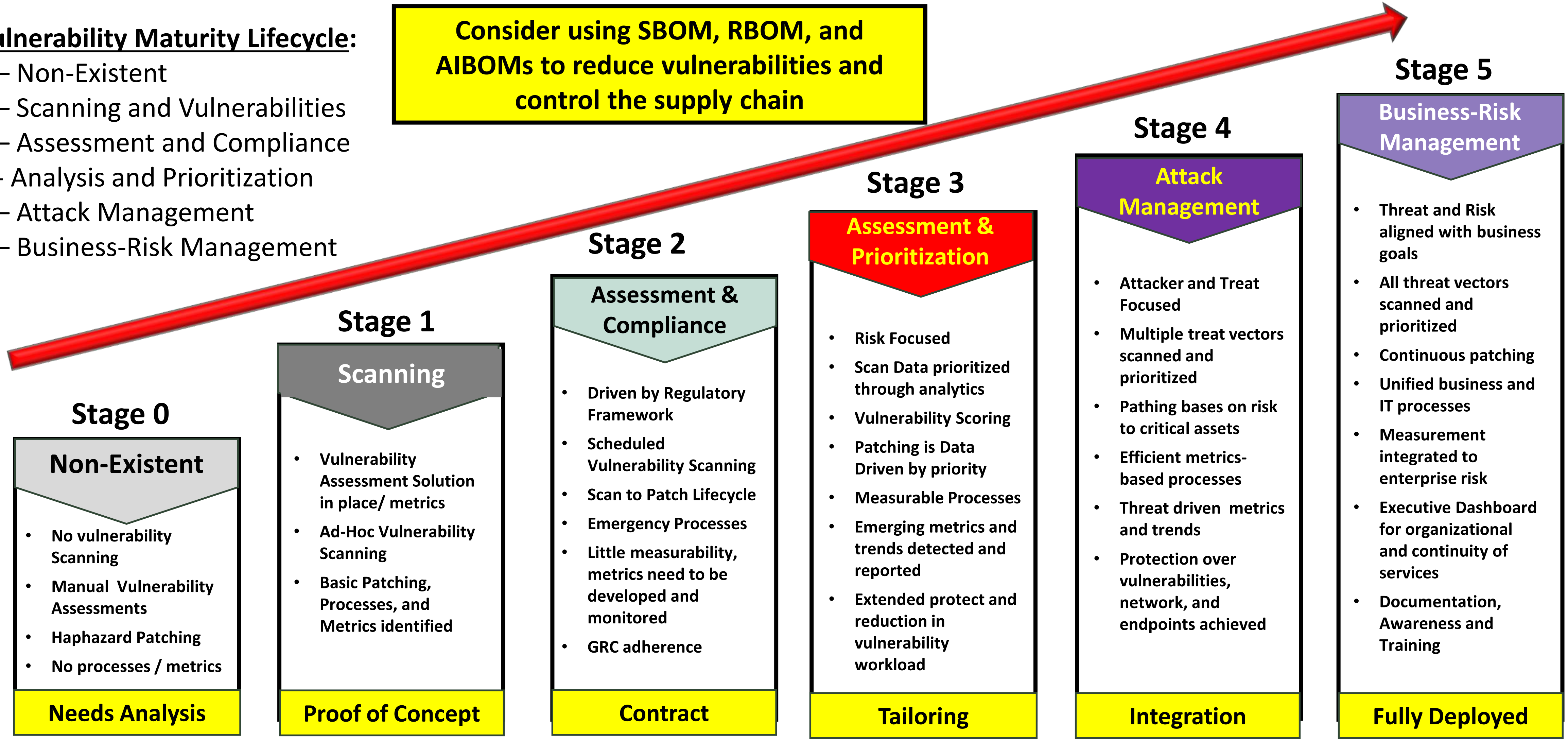
## Industry Compliance

- **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**”

# Vulnerability Management Maturity Lifecycle

**Vulnerability Maturity Lifecycle:**
0 – Non-Existent
1 – Scanning and Vulnerabilities
2 – Assessment and Compliance
3 - Analysis and Prioritization
4 – Attack Management
5 – Business-Risk Management

**Consider using SBOM, RBOM, and AIBOMs to reduce vulnerabilities and control the supply chain**



**Stage 0**

**Non-Existent**

- No vulnerability Scanning
- Manual Vulnerability Assessments
- Haphazard Patching
- No processes / metrics

**Needs Analysis**

**Stage 1**

**Scanning**

- Vulnerability Assessment Solution in place/ metrics
- Ad-Hoc Vulnerability Scanning
- Basic Patching, Processes, and Metrics identified

**Proof of Concept**

**Stage 2**

**Assessment & Compliance**

- Driven by Regulatory Framework
- Scheduled Vulnerability Scanning
- Scan to Patch Lifecycle
- Emergency Processes
- Little measurability, metrics need to be developed and monitored
- GRC adherence

**Contract**

**Stage 3**

**Assessment & Prioritization**

- Risk Focused
- Scan Data prioritized through analytics
- Vulnerability Scoring
- Patching is Data Driven by priority
- Measurable Processes
- Emerging metrics and trends detected and reported
- Extended protect and reduction in vulnerability workload

**Tailoring**

**Stage 4**

**Attack Management**

- Attacker and Treat Focused
- Multiple treat vectors scanned and prioritized
- Pathing bases on risk to critical assets
- Efficient metrics-based processes
- Threat driven metrics and trends
- Protection over vulnerabilities, network, and endpoints achieved

**Integration**

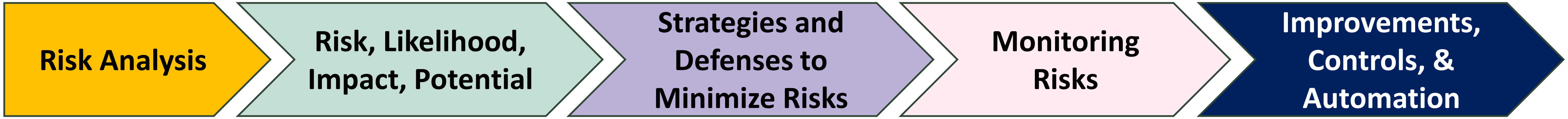
**Stage 5**

**Business-Risk Management**

- Threat and Risk aligned with business goals
- All threat vectors scanned and prioritized
- Continuous patching
- Unified business and IT processes
- Measurement integrated to enterprise risk
- Executive Dashboard for organizational and continuity of services
- Documentation, Awareness and Training

**Fully Deployed**

# Performing and Optimizing Risk Management



### Risk Analysis

- Conduct a Risk Assessment to locate gaps, exceptions, and weaknesses,
- Identify Assets and their importance,
- Ensure adherence to laws and regulations and provide business service continuity.

### Risk, Likelihood, Impact, Potential

- Identify Gaps, Exceptions, and Weaknesses.
- Rate the Impact and Likelihood.
- Develop Controls and other resolutions.
- Enter into Risk Register.
- Create POA&M to mitigate / mediate risk.
- Validate correction.

### Strategies and Defenses to Minimize Risks

- Define Requirements and effort associated with Risk Assessments to ensure compliance to laws and regulations, both domestically and internationally.
- Determine Costs and Efforts.
- Perform an Analysis of Alternatives.
- Select & Implement strategies best suited to enterprise.

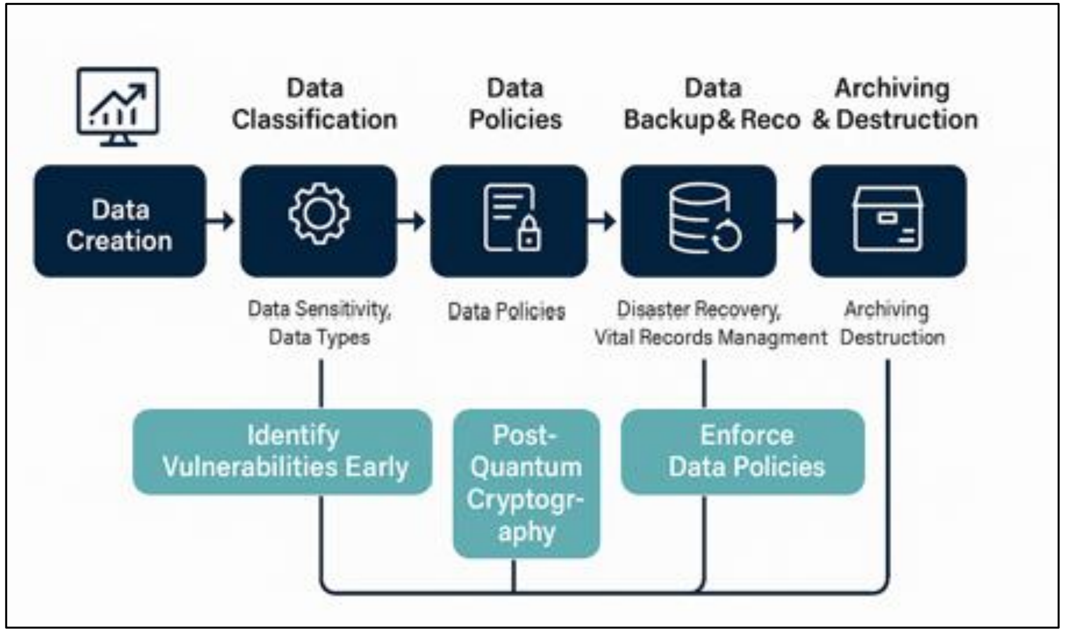
### Monitoring Risks

- Develop Risk Monitoring Dashboard system.
- Ensure integration with,
- Crosswalks,
- Risk Assessment Audit Guidelines,
- Worksheets,
- Questionnaires,
- Risk Reports,
- Risk Controls Self-Assessments (RCSA)
- Supply Chain
- Third-Party Risk Management

### Improvements, Controls, & Automation

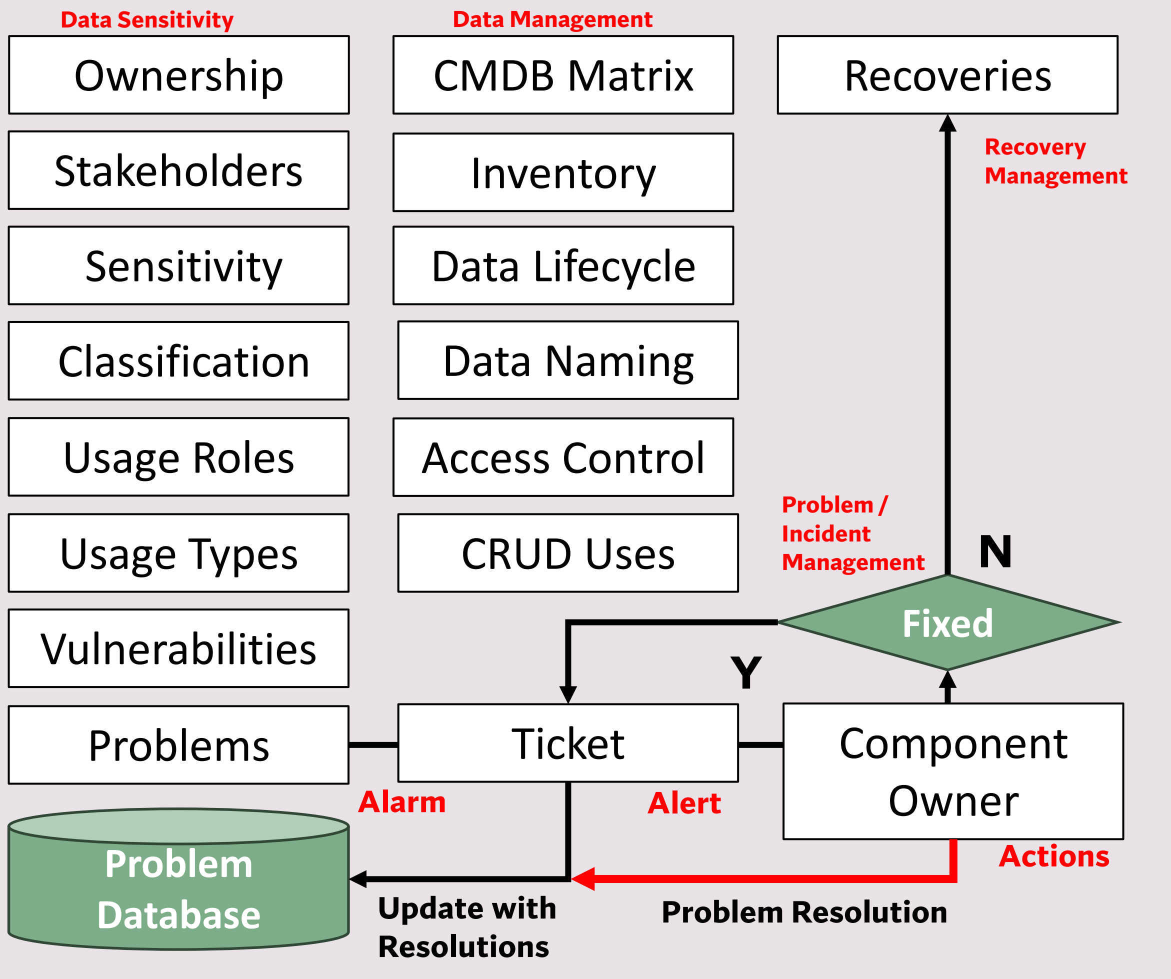
- Reviews to identify improvements,
- Improve and repeat until optimized.
- Automate process if desired,
- Conduct Cost vs Benefit Analysis to determine best direction.
- Develop POA&M
- Assign Teams and Management

# Data Sensitivity, Security, and Problems Resolution



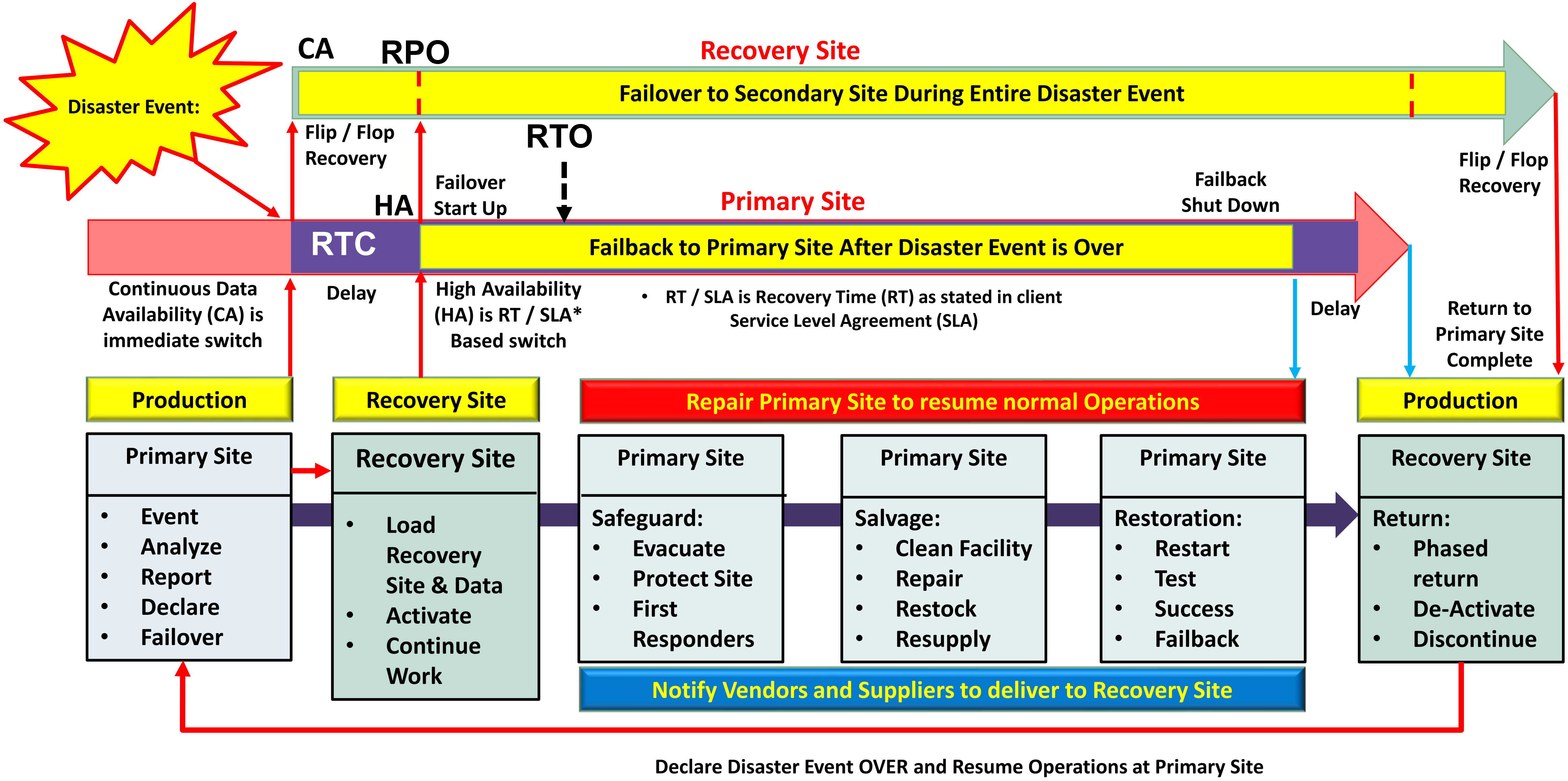
- Identify Data and its owner, then
- Define Sensitivity and Protection Requirements,
- Data Lifecycle and Naming conditions,
- Employ Data Security & Encryption, and
- Allow access based on Location, Group and Usage Type (RBAC).
- Include in Problem and Vulnerability Management system, by tying component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

## Data Sensitivity and Lifecycle Management



# 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



Disaster Event:

CA

RPO

Recovery Site

Failover to Secondary Site During Entire Disaster Event

Flip / Flop Recovery

RTO

Failover Start Up

HA

Primary Site

Failback Shut Down

Flip / Flop Recovery

RTC

Failback to Primary Site After Disaster Event is Over

Continuous Data Availability (CA) is immediate switch

Delay

High Availability (HA) is RT / SLA* Based switch

- RT / SLA is Recovery Time (RT) as stated in client Service Level Agreement (SLA)

Delay

Return to Primary Site Complete

Production

Recovery Site

Repair Primary Site to resume normal Operations

Production

**Primary Site**

- Event
- Analyze
- Report
- Declare
- Failover

**Recovery Site**

- Load Recovery Site & Data
- Activate
- Continue Work

**Primary Site**

Safeguard:
- Evacuate
- Protect Site
- First Responders

**Primary Site**

Salvage:
- Clean Facility
- Repair
- Restock
- Resupply

**Primary Site**

Restoration:
- Restart
- Test
- Success
- Failback

**Recovery Site**

Return:
- Phased return
- De-Activate
- Discontinue

Notify Vendors and Suppliers to deliver to Recovery Site

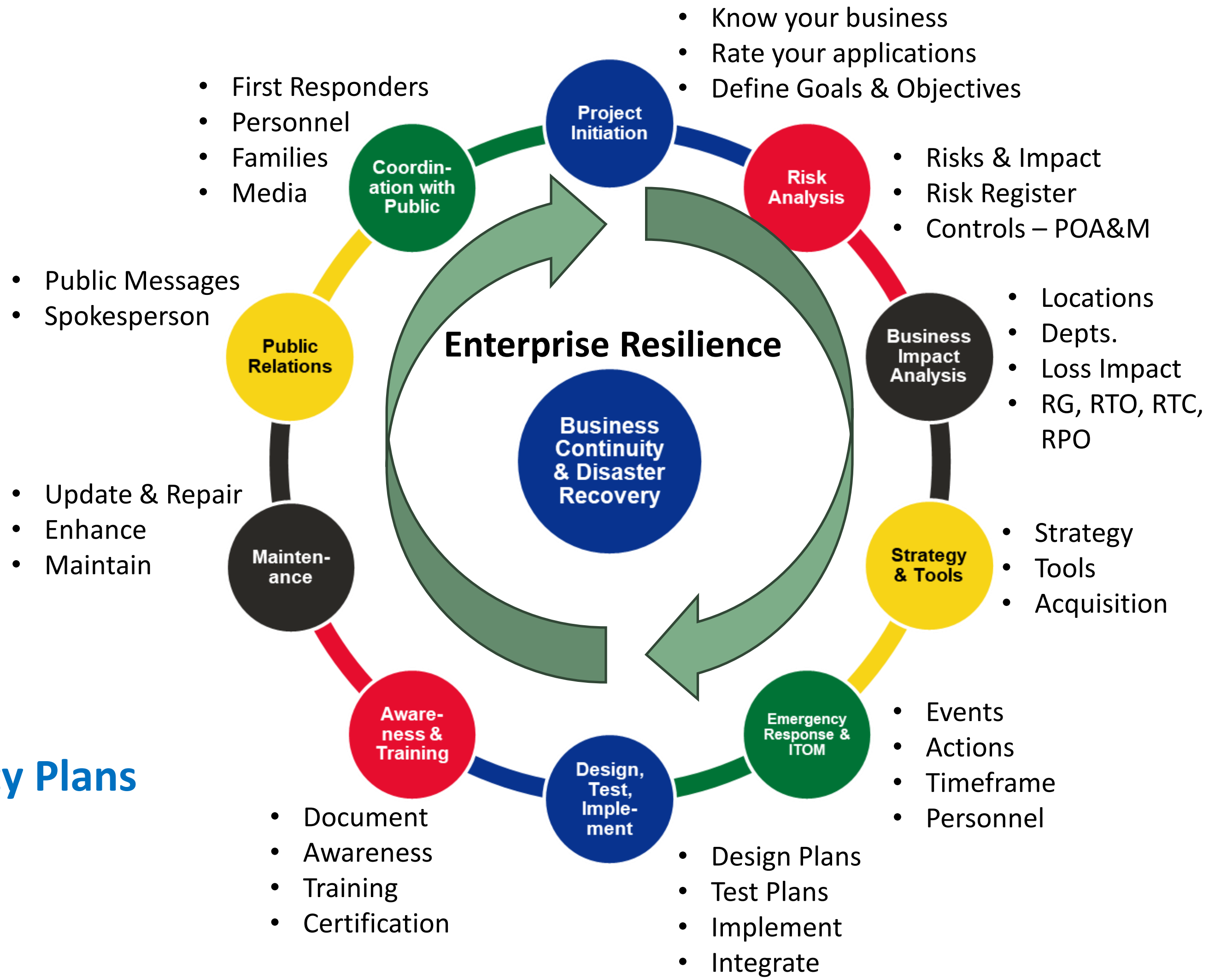
Declare Disaster Event OVER and Resume Operations at Primary Site

# Ten Step Process to establish BCM/DR Practice

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



- Know your business
- Rate your applications
- Define Goals & Objectives

- Risks & Impact
- Risk Register
- Controls – POA&M

- Locations
- Depts.
- Loss Impact
- RG, RTO, RTC, RPO

- Strategy
- Tools
- Acquisition

- Events
- Actions
- Timeframe
- Personnel

- Design Plans
- Test Plans
- Implement
- Integrate

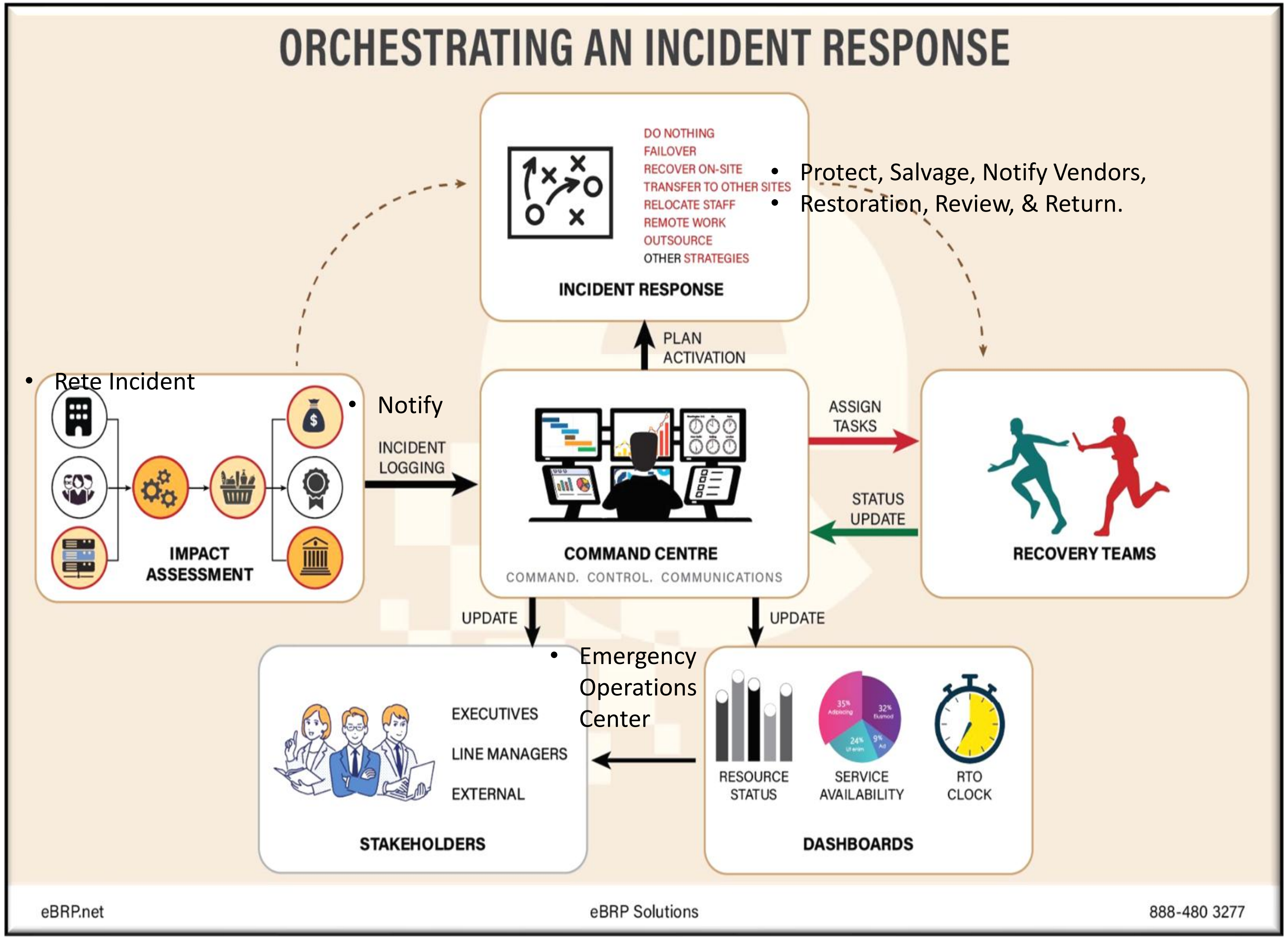
- Document
- Awareness
- Training
- Certification

- Update & Repair
- Enhance
- Maintain

- Public Messages
- Spokesperson

- First Responders
- Personnel
- Families
- Media

# Business Continuity Center



- Rete Incident

- Notify

- Protect, Salvage, Notify Vendors,
- Restoration, Review, & Return.

- Emergency Operations Center

## 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
7. Incident Tracked until Completed
8. Post Incident Review
9. Improvements
10. Update & Maintain Recovery Plans

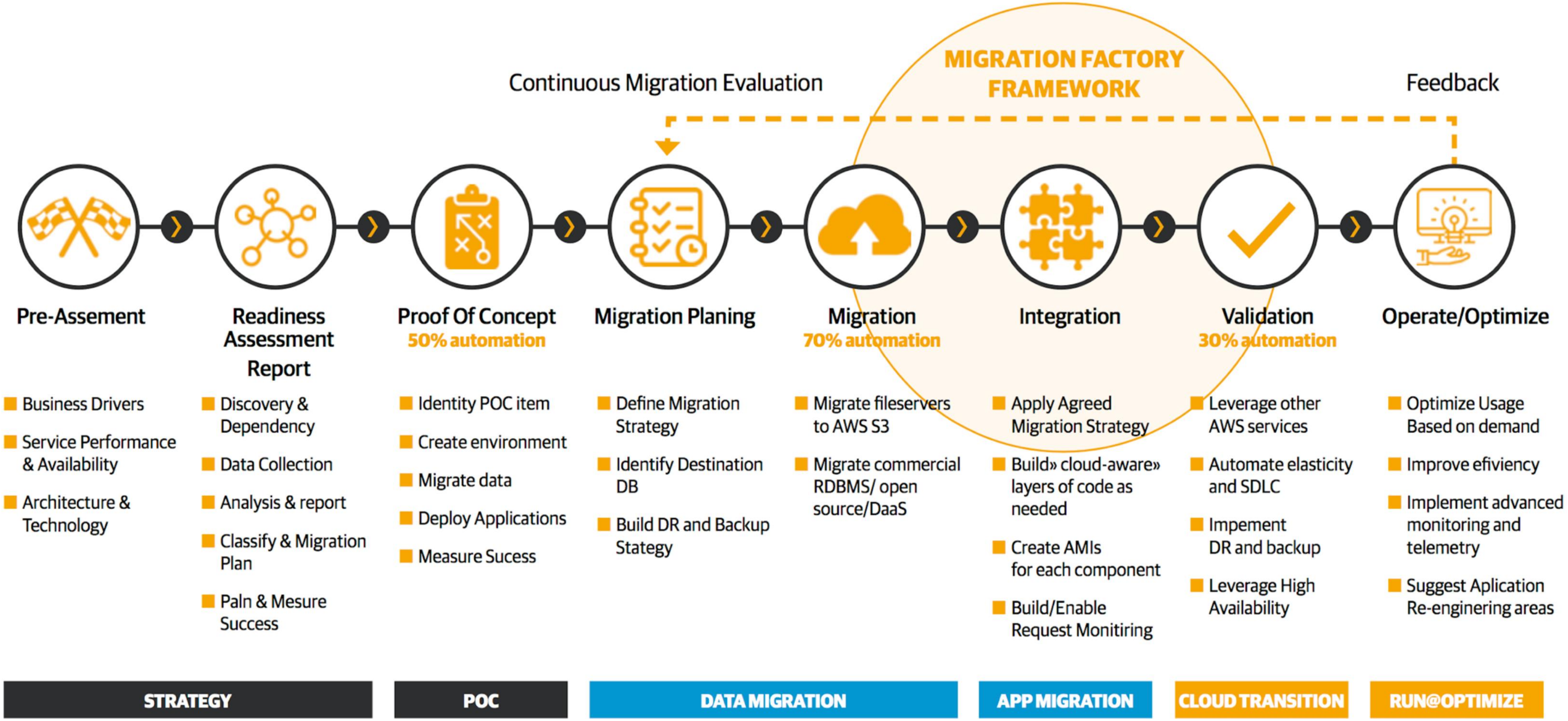
**Overall Benefits**

**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.

# Planning for Migrating Applications to the Cloud



Continuous Migration Evaluation

MIGRATION FACTORY FRAMEWORK

Feedback

**Pre-Assement**

- Business Drivers
- Service Performance & Availability
- Architecture & Technology

**Readiness Assessment Report**

- Discovery & Dependency
- Data Collection
- Analysis & report
- Classify & Migration Plan
- Paln & Mesure Success

**Proof Of Concept**
50% automation

- Identity POC item
- Create environment
- Migrate data
- Deploy Applications
- Measure Sucess

**Migration Planing**

- Define Migration Strategy
- Identify Destination DB
- Build DR and Backup Stategy

**Migration**
70% automation

- Migrate fileservers to AWS S3
- Migrate commercial RDBMS/ open source/DaaS

**Integration**

- Apply Agreed Migration Strategy
- Build» cloud-aware» layers of code as needed
- Create AMIs for each component
- Build/Enable Request Monitiring

**Validation**
30% automation

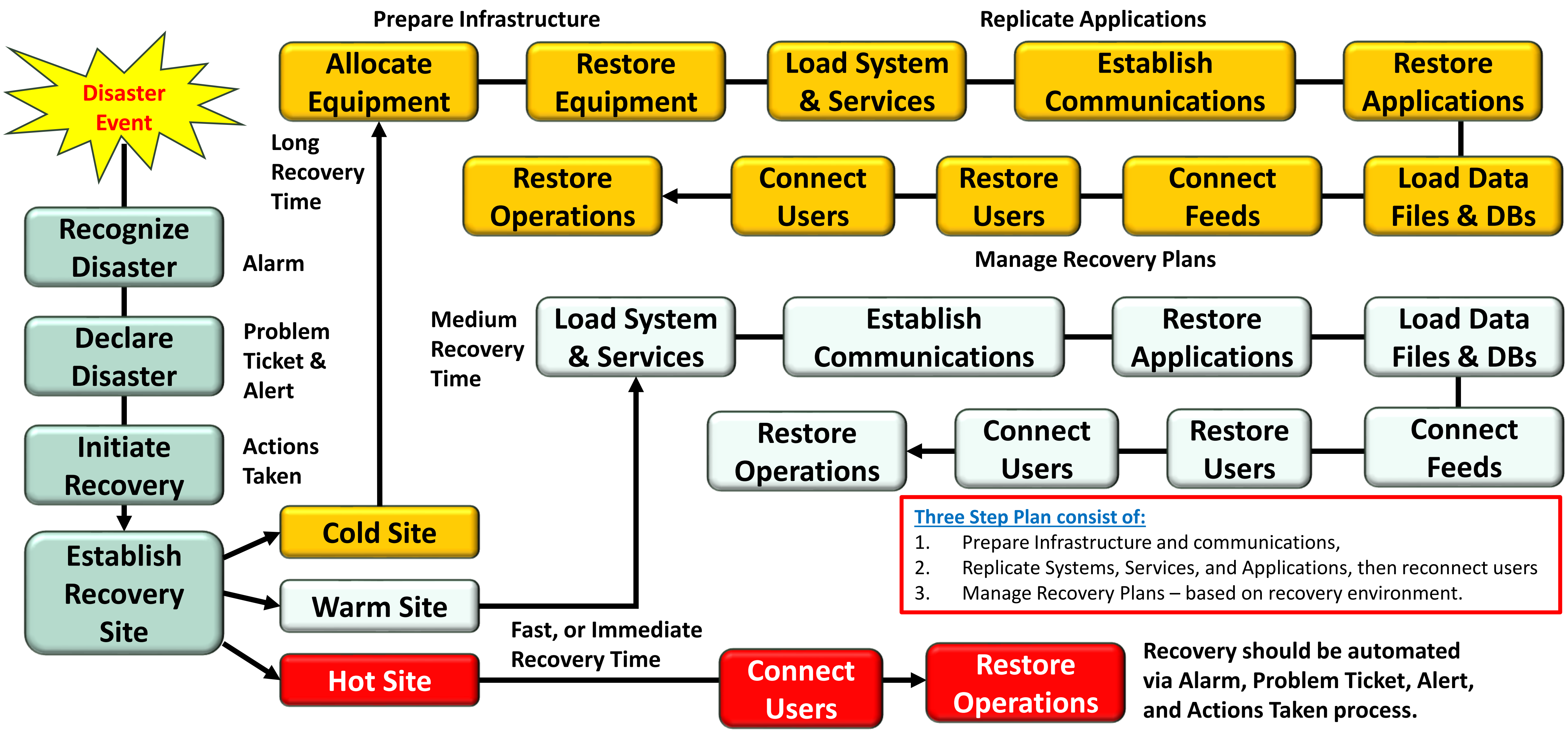
- Leverage other AWS services
- Automate elasticity and SDLC
- Impement DR and backup
- Leverage High Availability

**Operate/Optimize**

- Optimize Usage Based on demand
- Improve efiviency
- Implement advanced monitoring and telemetry
- Suggest Aplication Re-enginering areas

STRATEGY | POC | DATA MIGRATION | APP MIGRATION | CLOUD TRANSITION | RUN@OPTIMIZE

# Sequence of Events to enact a Recovery Operation



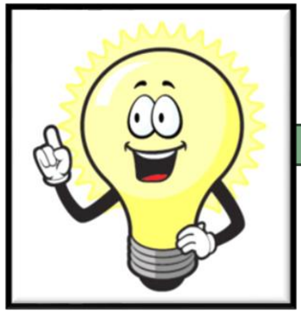
**Three Step Plan consist of:**

1. Prepare Infrastructure and communications,
2. Replicate Systems, Services, and Applications, then reconnect users
3. Manage Recovery Plans – based on recovery environment.

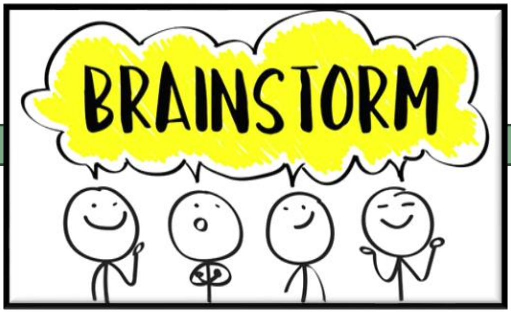
**Recovery should be automated via Alarm, Problem Ticket, Alert, and Actions Taken process.**

# Designing and Building Systems from idea to production

Idea

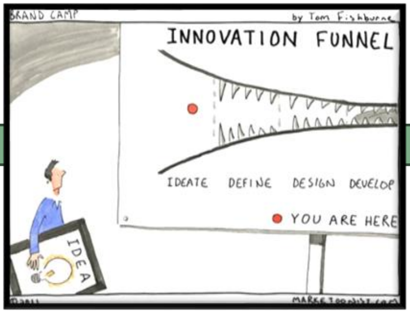


Brainstorm



Collaborate

Innovate



RTM

Requirements Transparency Matrix (RTM)

- Project Management
- Agile Epic
- Features
- Functions
- Programs
- Stories
- Sprints
- Confluence
- SharePoint
- Awareness
- Training

Architect & Solutions

Systems Engineering Life Cycle (SELC)

Post-Quantum Cryptography (PQC)

Cloud & Programming

Systems Development Life Cycle (SDLC)

Supply Chain

Third-Party Risk Management

Testing Criteria & Compliance

Testing

IV&V, Regression

IA, Chaos Testing

Continuity

Compliance

Vulnerability Management

Risk Assessment

Risk Controls Self-Assessment

Production

Quality Assurance

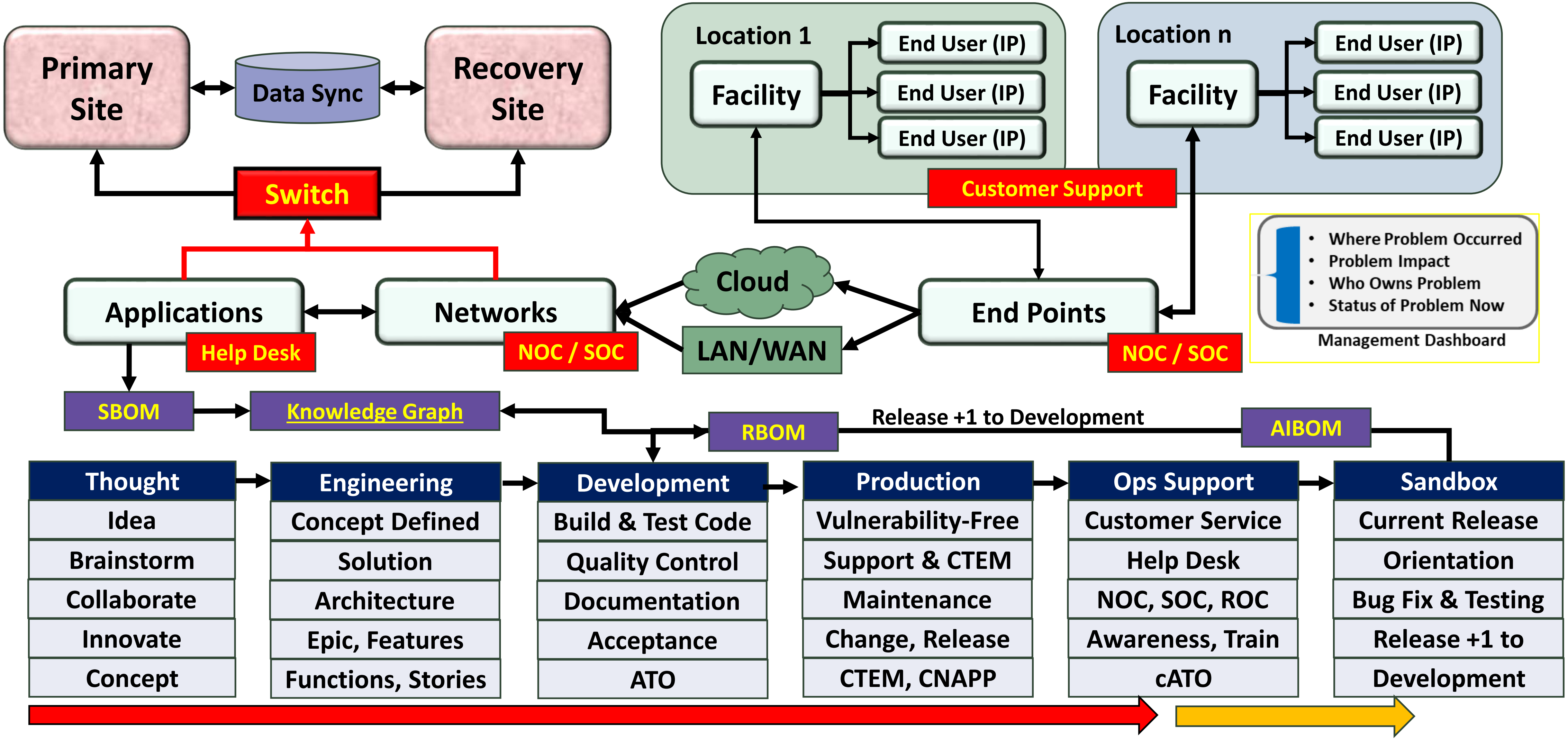
Acceptance

Production

Support

Maintenance

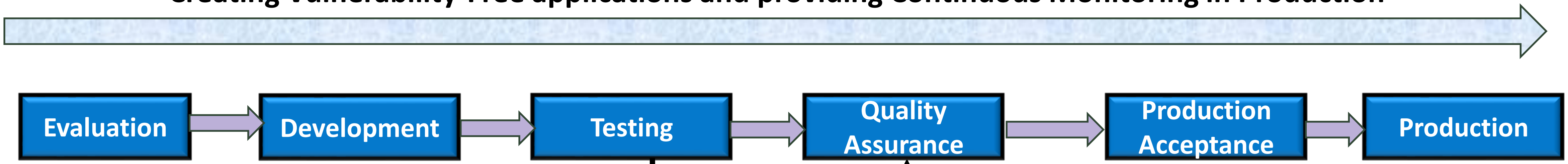
# From Idea to Product, with Support and Recovery



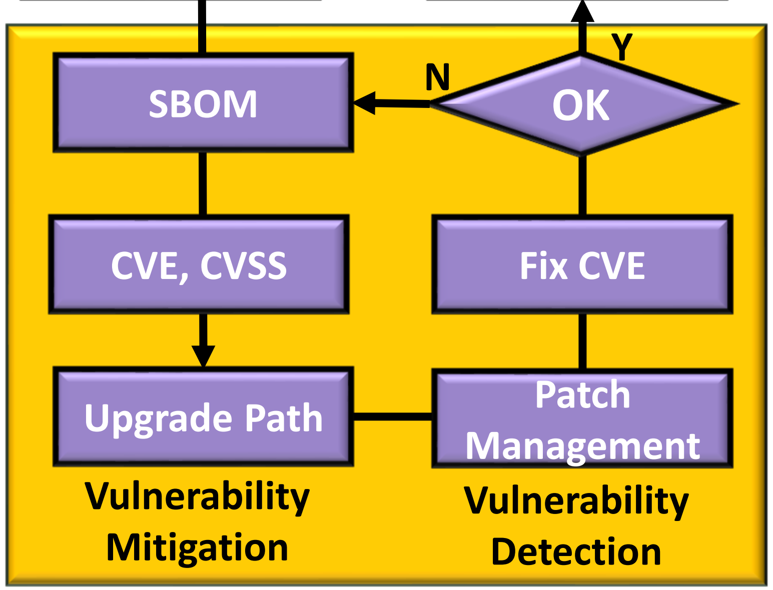
| Thought | Engineering | Development | Production | Ops Support | Sandbox |
|---|---|---|---|---|---|
| Idea | Concept Defined | Build & Test Code | Vulnerability-Free | Customer Service | Current Release |
| Brainstorm | Solution | Quality Control | Support & CTEM | Help Desk | Orientation |
| Collaborate | Architecture | Documentation | Maintenance | NOC, SOC, ROC | Bug Fix & Testing |
| Innovate | Epic, Features | Acceptance | Change, Release | Awareness, Train | Release +1 to |
| Concept | Functions, Stories | ATO | CTEM, CNAPP | cATO | Development |

# Application Factory with Quality Control Gates

**Creating Vulnerability-Free applications and providing Continuous Monitoring in Production**



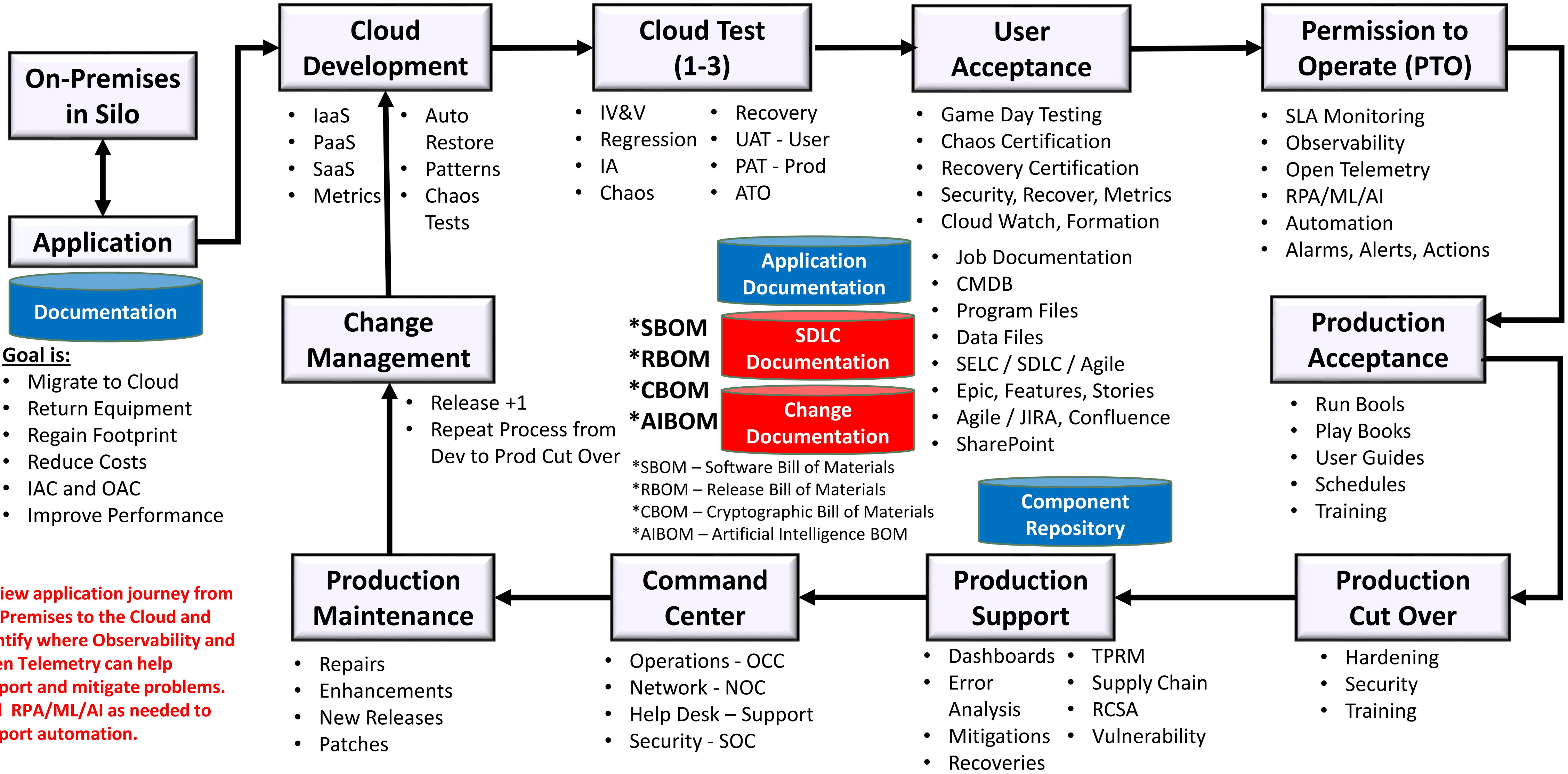
1. ProCap 360 detects vulnerabilities via SBOMs, provides Security Scores and Upgrade Path to Mitigate Vulnerability
2. Patch Management mitigates vulnerabilities by applying Upgrade Path, via  patches or upgrading program release level.
3. Automating Patch Management can reduce time and costs.
4. Error Loop process in repeated via Quality Gates for every stage of product/service production.



**Vulnerability Management Detection and Mitigation**

5. All Application Components are at current release levels and Vulnerability-Free when they are delivered to the production environment, after production acceptance, so Assurance to Operate (ATO) is achieved.
6. Continuous Monitoring detects new vulnerabilities in production to achieve (cATO)
7. Manpower savings through automation ensures a safe application & service environment
8. Cost Savings and quick ROI

# Migrating Applications to the Cloud



On-Premises in Silo

Application

Documentation

Goal is:
- Migrate to Cloud
- Return Equipment
- Regain Footprint
- Reduce Costs
- IAC and OAC
- Improve Performance

Cloud Development
- IaaS
- PaaS
- SaaS
- Metrics
- Auto Restore
- Patterns
- Chaos Tests

Cloud Test (1-3)
- IV&V
- Regression
- IA
- Chaos
- Recovery
- UAT - User
- PAT - Prod
- ATO

User Acceptance
- Game Day Testing
- Chaos Certification
- Recovery Certification
- Security, Recover, Metrics
- Cloud Watch, Formation

Permission to Operate (PTO)
- SLA Monitoring
- Observability
- Open Telemetry
- RPA/ML/AI
- Automation
- Alarms, Alerts, Actions

Change Management
- Release +1
- Repeat Process from Dev to Prod Cut Over

Application Documentation

*SBOM
*RBOM
*CBOM
*AIBOM

SDLC Documentation

Change Documentation

- Job Documentation
- CMDB
- Program Files
- Data Files
- SELC / SDLC / Agile
- Epic, Features, Stories
- Agile / JIRA, Confluence
- SharePoint

*SBOM – Software Bill of Materials
*RBOM – Release Bill of Materials
*CBOM – Cryptographic Bill of Materials
*AIBOM – Artificial Intelligence BOM

Component Repository

Production Acceptance
- Run Bools
- Play Books
- User Guides
- Schedules
- Training

Production Cut Over
- Hardening
- Security
- Training

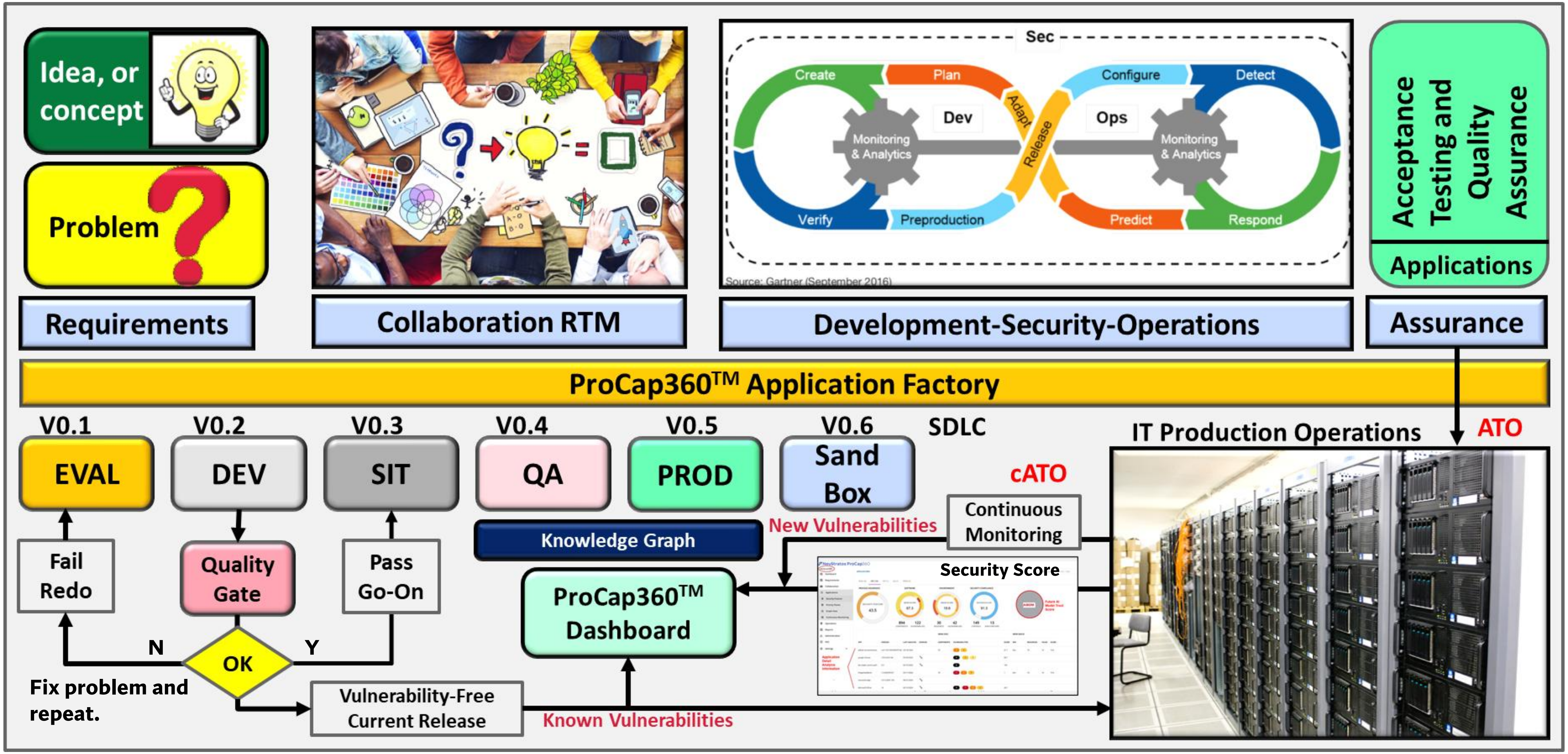
Production Support
- Dashboards
- Error Analysis
- Mitigations
- Recoveries
- TPRM
- Supply Chain
- RCSA
- Vulnerability

Command Center
- Operations - OCC
- Network - NOC
- Help Desk – Support
- Security - SOC

Production Maintenance
- Repairs
- Enhancements
- New Releases
- Patches

**Review application journey from On-Premises to the Cloud and identify where Observability and Open Telemetry can help support and mitigate problems. Add RPA/ML/AI as needed to support automation.**

# From Concept to Applications via DevSecOps



Idea, or concept

Problem

Requirements

Collaboration RTM

Source: Gartner (September 2016)

Development-Security-Operations

Acceptance Testing and Quality Assurance

Applications

Assurance

ProCap360TM Application Factory

V0.1 EVAL

V0.2 DEV

V0.3 SIT

V0.4 QA

V0.5 PROD

V0.6 Sand Box

SDLC

IT Production Operations

ATO

cATO

Fail Redo

Quality Gate

Pass Go-On

OK

N

Y

Fix problem and repeat.

Vulnerability-Free Current Release

Knowledge Graph

New Vulnerabilities

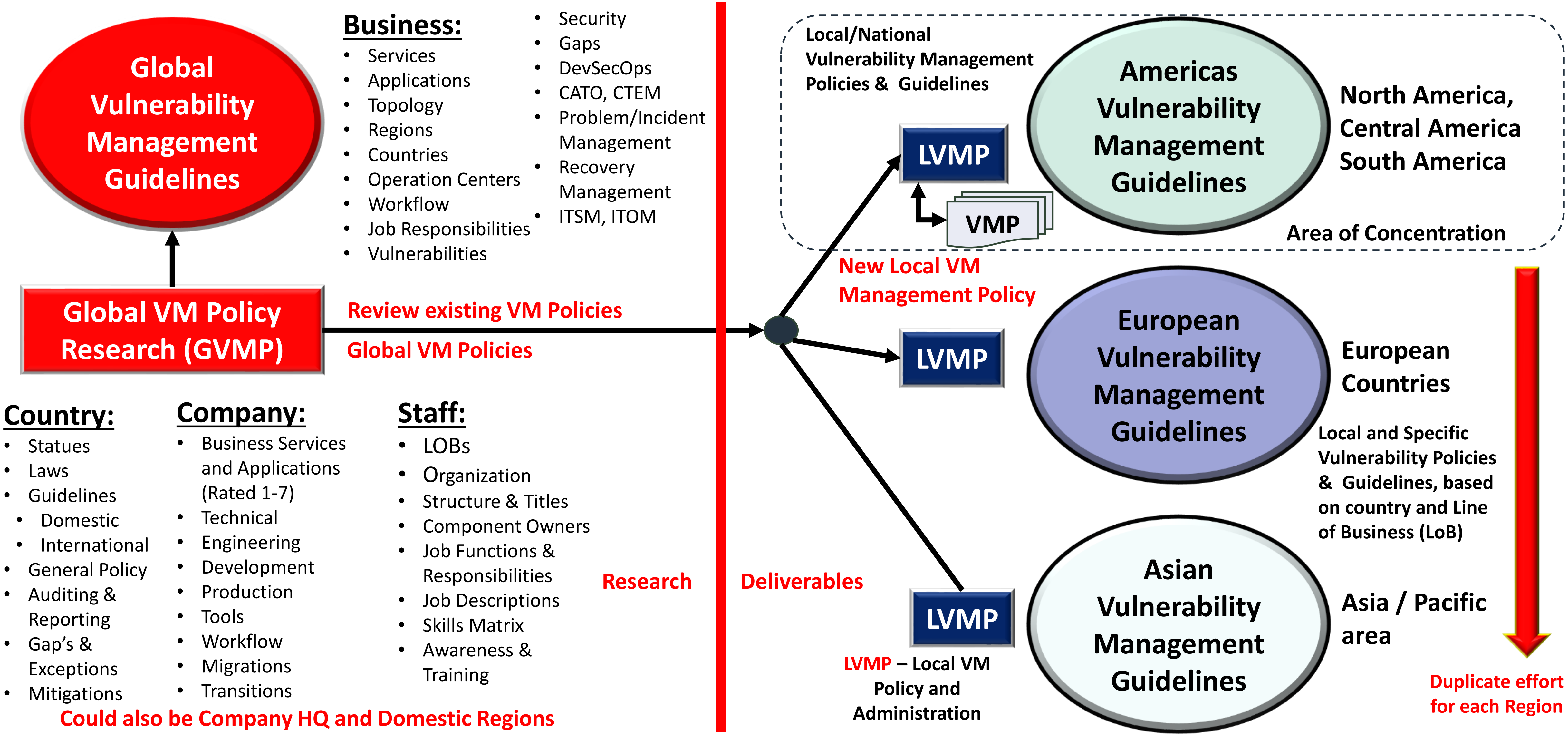
Continuous Monitoring

Security Score

ProCap360TM Dashboard

Known Vulnerabilities

# Global Vulnerability Management Policy generation



Global Vulnerability Management Guidelines

Global VM Policy Research (GVMP)

Review existing VM Policies

Global VM Policies

**Business:**

- Services
- Applications
- Topology
- Regions
- Countries
- Operation Centers
- Workflow
- Job Responsibilities
- Vulnerabilities
- Security
- Gaps
- DevSecOps
- CATO, CTEM
- Problem/Incident Management
- Recovery Management
- ITSM, ITOM

**Country:**

- Statues
- Laws
- Guidelines
  - Domestic
  - International
- General Policy
- Auditing & Reporting
- Gap's & Exceptions
- Mitigations

**Company:**

- Business Services and Applications (Rated 1-7)
- Technical
- Engineering
- Development
- Production
- Tools
- Workflow
- Migrations
- Transitions

**Staff:**

- LOBs
- Organization
- Structure & Titles
- Component Owners
- Job Functions & Responsibilities
- Job Descriptions
- Skills Matrix
- Awareness & Training

Could also be Company HQ and Domestic Regions

Research

Deliverables

Local/National Vulnerability Management Policies & Guidelines

LVMP

VMP

Americas Vulnerability Management Guidelines

North America, Central America South America

Area of Concentration

New Local VM Management Policy

LVMP

European Vulnerability Management Guidelines

European Countries

Local and Specific Vulnerability Policies & Guidelines, based on country and Line of Business (LoB)

LVMP

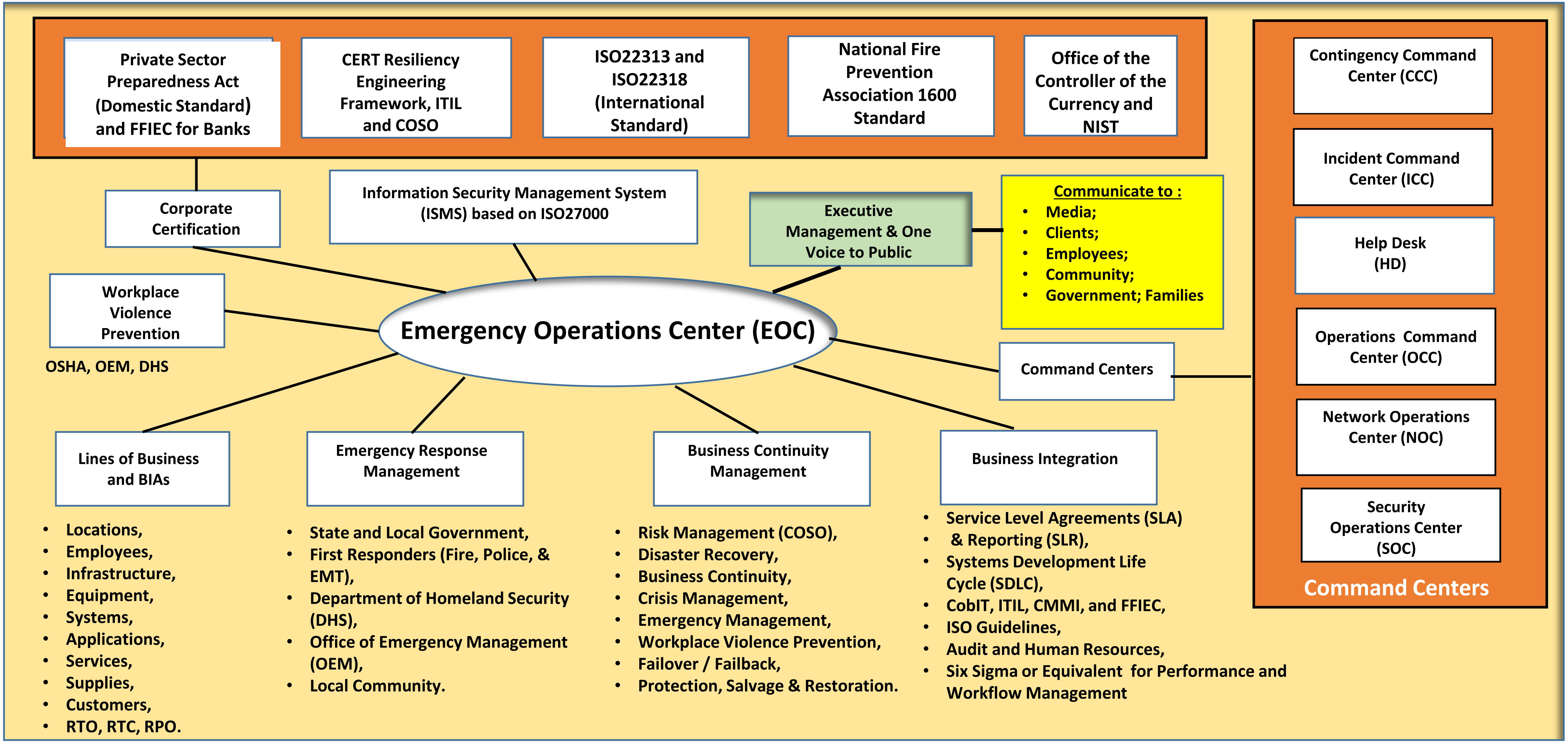
Asian Vulnerability Management Guidelines

Asia / Pacific area

LVMP – Local VM Policy and Administration

Duplicate effort for each Region

# Emergency Operations Center (EOC)



Private Sector Preparedness Act (Domestic Standard) and FFIEC for Banks

CERT Resiliency Engineering Framework, ITIL and COSO

ISO22313 and ISO22318 (International Standard)

National Fire Prevention Association 1600 Standard

Office of the Controller of the Currency and NIST

Corporate Certification

Information Security Management System (ISMS) based on ISO27000

Executive Management & One Voice to Public

**Communicate to :**

- Media;
- Clients;
- Employees;
- Community;
- Government; Families

Workplace Violence Prevention

OSHA, OEM, DHS

Emergency Operations Center (EOC)

Command Centers

Lines of Business and BIAs

- Locations,
- Employees,
- Infrastructure,
- Equipment,
- Systems,
- Applications,
- Services,
- Supplies,
- Customers,
- RTO, RTC, RPO.

Emergency Response Management

- State and Local Government,
- First Responders (Fire, Police, & EMT),
- Department of Homeland Security (DHS),
- Office of Emergency Management (OEM),
- Local Community.

Business Continuity Management

- Risk Management (COSO),
- Disaster Recovery,
- Business Continuity,
- Crisis Management,
- Emergency Management,
- Workplace Violence Prevention,
- Failover / Failback,
- Protection, Salvage & Restoration.

Business Integration

- Service Level Agreements (SLA)
- & Reporting (SLR),
- Systems Development Life Cycle (SDLC),
- CobIT, ITIL, CMMI, and FFIEC,
- ISO Guidelines,
- Audit and Human Resources,
- Six Sigma or Equivalent for Performance and Workflow Management

Contingency Command Center (CCC)

Incident Command Center (ICC)

Help Desk (HD)

Operations Command Center (OCC)

Network Operations Center (NOC)

Security Operations Center (SOC)

Command Centers