Achieving Enterprise Resiliency And Corporate Certification

By

Combining Recovery Operations through a

Common Recovery Language and Recovery Tools,

While adhering to

Domestic and International Compliance Standards

Created by:

Thomas Bronack, CBCP
Bronackt@dcag.com
Phone: (718) 591-5553
Cell: (917) 673-6992

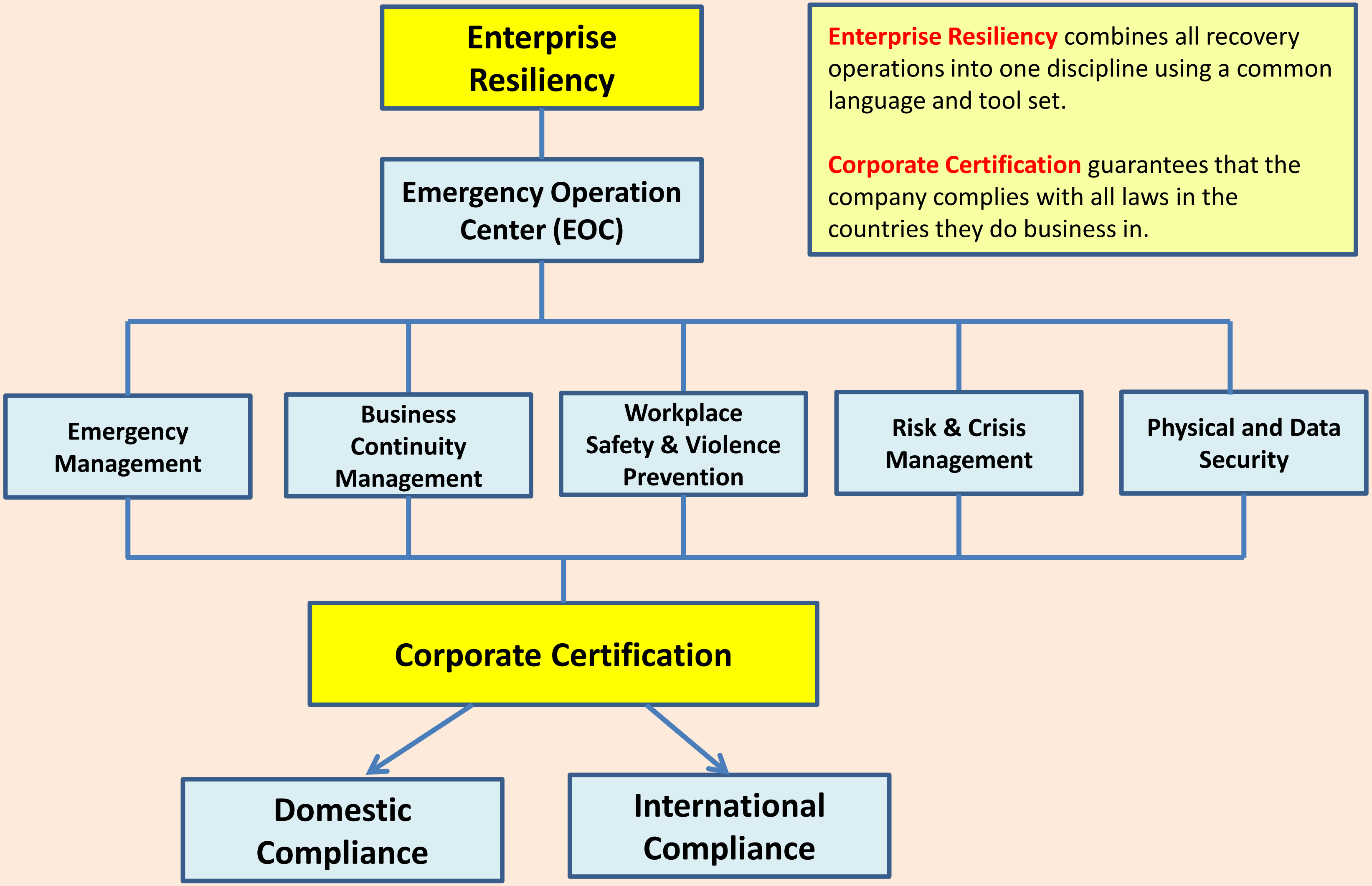
Enterprise Resiliency combines all recovery operations into one discipline using a common language and tool set.

Corporate Certification guarantees that the company complies with all laws in the countries they do business in.

Abstract

- Are you utilizing your recovery personnel to achieve **maximum protection**?
- Have you implemented a common recovery glossary of terms so that personnel speak the **same language** and can best communicate and respond to disaster events?
- Is your company utilizing a **common recovery management toolset**?
- Want to reduce disaster events, improve risk management, and insure fewer business interruptions through **automated tools and procedures**?
- Does your company **adhere to regulatory requirements** in the countries that you do business in?
- Can you monitor and report on **security violations**, both **physical and data**, to best protect personnel, control data access, eliminate data corruption, support failover /failback operations, and protect company locations against workplace violence?
- Are you **protecting data** by using backup, vaulting, and recovery procedures?
- Can you **recover operations** in accordance to SLA/SLR and RTO/RPO?
- Is your **supply chain** able to continue to provide services and products if a disaster event occurs through SSAE 16 (Domestic), SSAE 3402 (World)?
- Do you **coordinate recovery operations** with the community and government agencies like OSHA, OEM, FEMA, Homeland Security, local First Responders, etc.?
- Do you have appropriate **insurance** against disaster events?
- Can you **certify that applications** can recover within High Availability (2 hours – 72 hours) or Continuous Availability (immediate) guidelines?
- **If not**, this presentation will help you achieve the above goals.

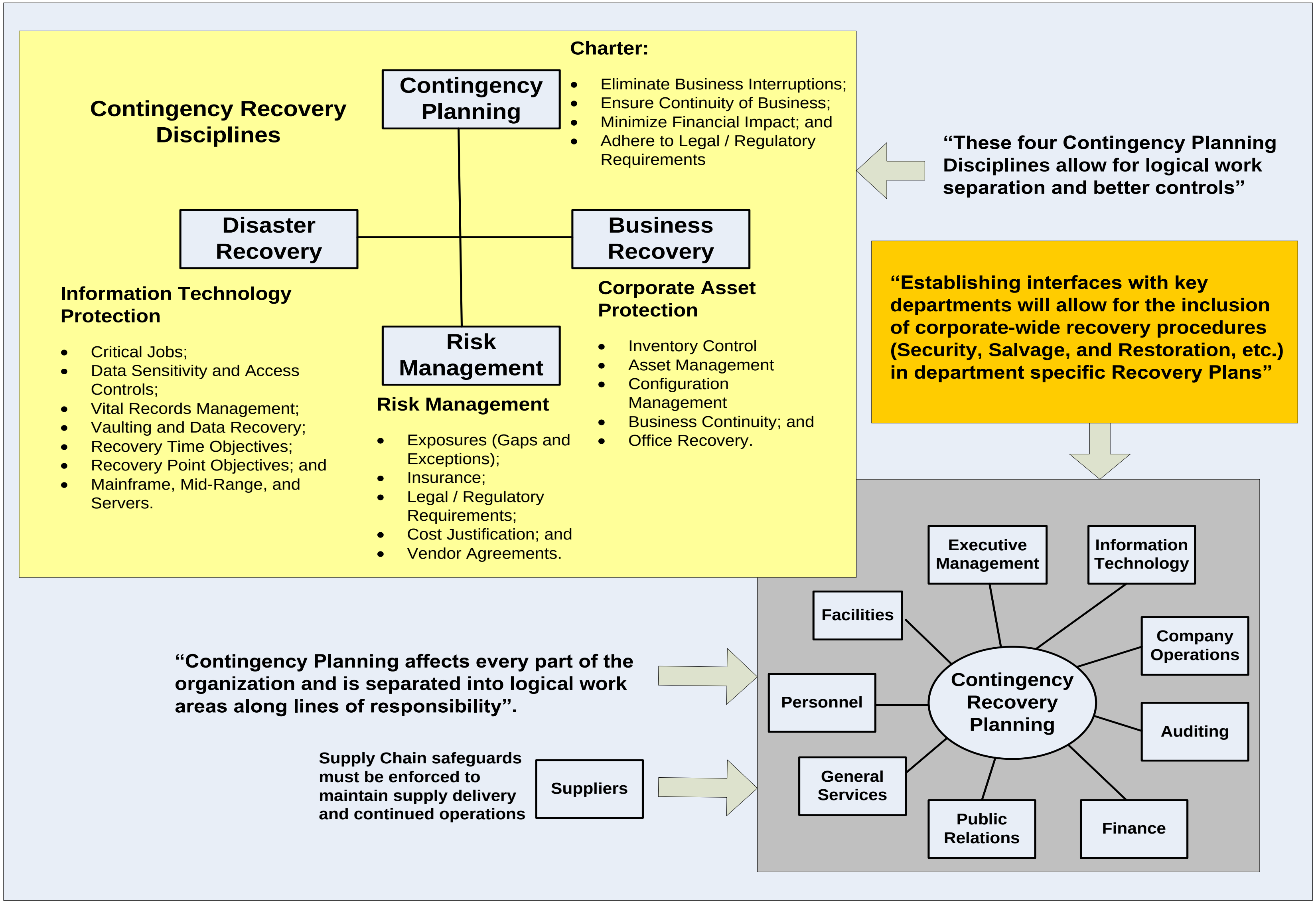
What is Enterprise Resiliency and Corporate Certification



Enterprise Resiliency combines all recovery operations into one discipline using a common language and tool set.

Corporate Certification guarantees that the company complies with all laws in the countries they do business in.

Business Continuity Management Disciplines and Integration



Contingency Recovery Disciplines

Contingency Planning

Charter:

- Eliminate Business Interruptions;
- Ensure Continuity of Business;
- Minimize Financial Impact; and
- Adhere to Legal / Regulatory Requirements

Disaster Recovery

Business Recovery

Risk Management

Information Technology Protection

- Critical Jobs;
- Data Sensitivity and Access Controls;
- Vital Records Management;
- Vaulting and Data Recovery;
- Recovery Time Objectives;
- Recovery Point Objectives; and
- Mainframe, Mid-Range, and Servers.

Risk Management

- Exposures (Gaps and Exceptions);
- Insurance;
- Legal / Regulatory Requirements;
- Cost Justification; and
- Vendor Agreements.

Corporate Asset Protection

- Inventory Control
- Asset Management
- Configuration Management
- Business Continuity; and
- Office Recovery.

"These four Contingency Planning Disciplines allow for logical work separation and better controls"

"Establishing interfaces with key departments will allow for the inclusion of corporate-wide recovery procedures (Security, Salvage, and Restoration, etc.) in department specific Recovery Plans"

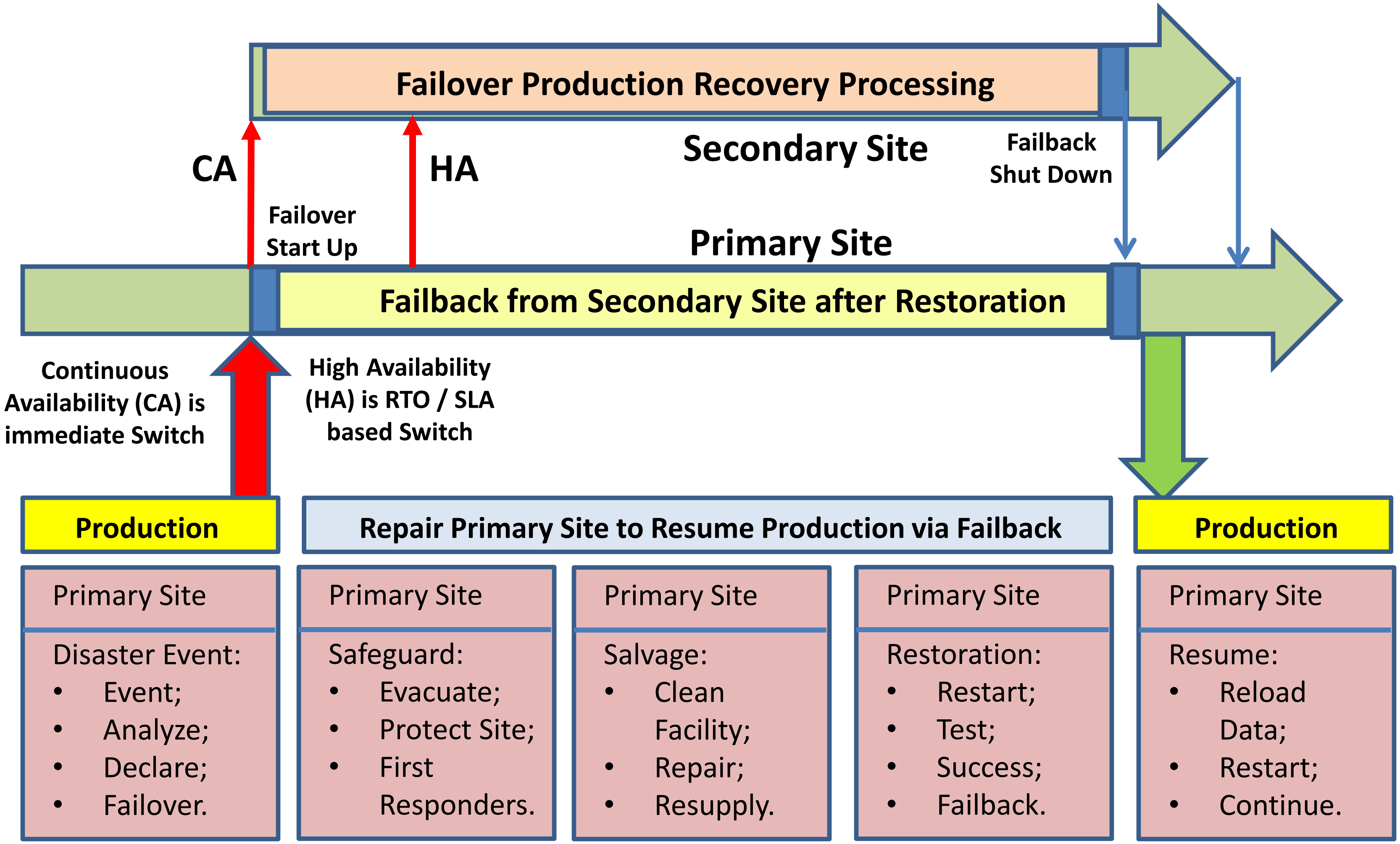
"Contingency Planning affects every part of the organization and is separated into logical work areas along lines of responsibility".

Supply Chain safeguards must be enforced to maintain supply delivery and continued operations

Suppliers

Lifecycle of a Disaster Event (Why we create Recovery Plans)

"The goal of Enterprise Resiliency is to achieve ZERO DOWNTIME by implementing Application Recovery Certification for HA and Gold Standard Recovery Certification for CA Applications"

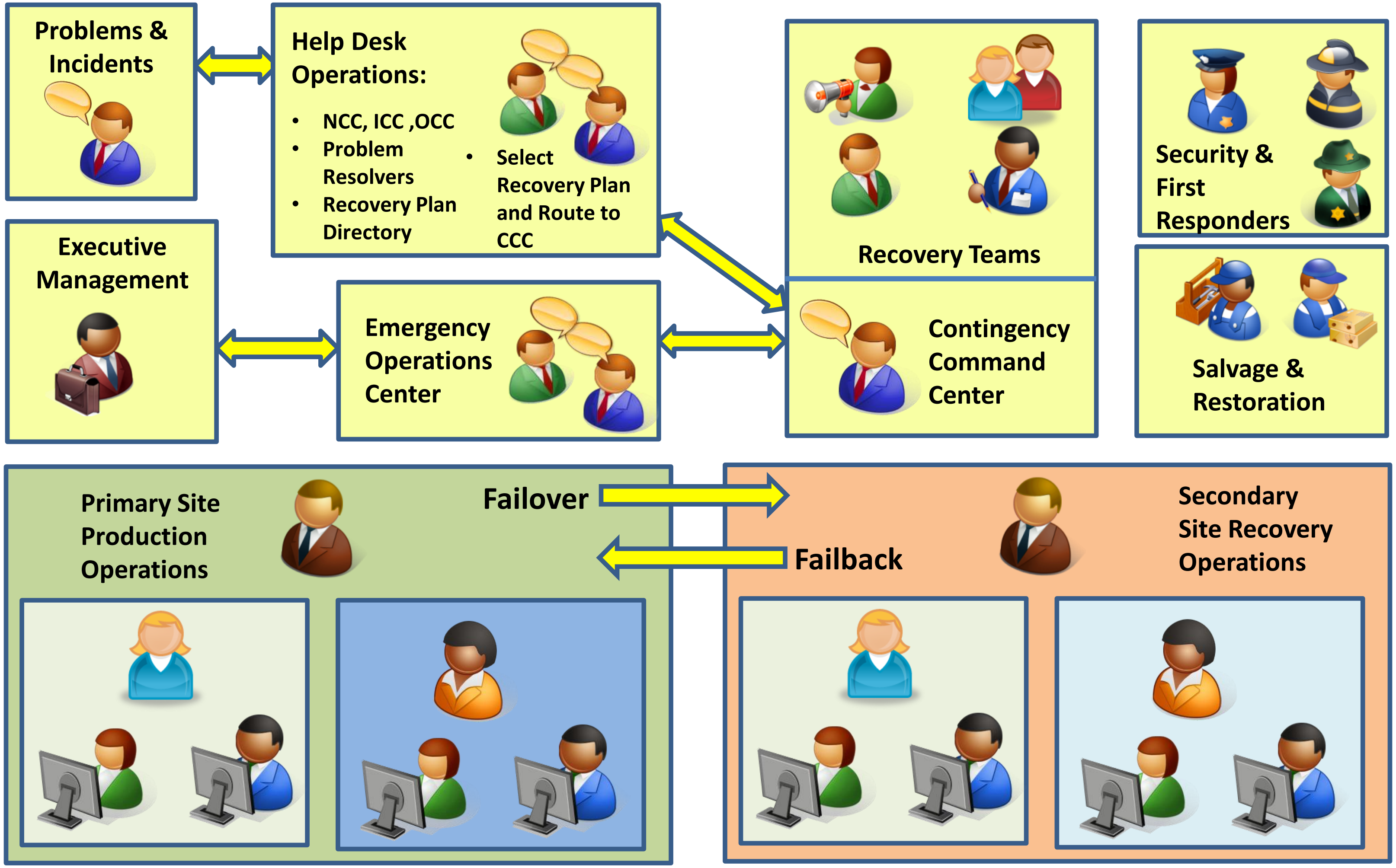


Failover Production Recovery Processing
Secondary Site
Failback
Shut Down
CA
HA
Failover
Start Up
Primary Site
Failback from Secondary Site after Restoration
Continuous Availability (CA) is immediate Switch
High Availability (HA) is RTO / SLA based Switch
Production
Repair Primary Site to Resume Production via Failback
Production

Primary Site	Primary Site	Primary Site	Primary Site	Primary Site
Disaster Event: • Event; • Analyze; • Declare; • Failover.	Safeguard: • Evacuate; • Protect Site; • First Responders.	Salvage: • Clean Facility; • Repair; • Resupply.	Restoration: • Restart; • Test; • Success; • Failback.	Resume: • Reload Data; • Restart; • Continue.

People Involved with Recovery Planning and Operations

"Many people from various departments contribute to the Problem / Incident Response Planning process; from initial compliance and recovery identification through recovery planning, and Recovery Plan enactment."



Problems & Incidents

Help Desk Operations:

- NCC, ICC ,OCC
- Problem Resolvers
- Recovery Plan Directory
- Select Recovery Plan and Route to CCC

Recovery Teams

Security & First Responders

Executive Management

Emergency Operations Center

Contingency Command Center

Salvage & Restoration

Primary Site Production Operations

Failover

Failback

Secondary Site Recovery Operations

Charter and Mission Statement

1. Achieve “**Enterprise Resilience”** to optimize recovery operations;
2. Insure **“Corporate Certification”** in countries where you do business***;***
3. Adhere to Service Level Agreements (**SLA / SLR**);
4. Guaranty **Data Security and Recovery (RTO** / **RPO)**;
5. **Protect Personnel** through Physical Security and a Safe Workplace;
6. Utilize **“Best Practices”** to achieve goals;
7. Achieve “**Zero Downtime**” through “**Certified Recovery”** via Failover / Failback for HA applications and Flip / Flop for “**Gold Standard Certification”** of CA applications
8. **Integrate Enterprise Resiliency and Corporate Certification World-Wide;**
9. **Update Documentation;**
10. Provide **educational awareness and training** programs; and,
11. Provide ongoing **Support and Maintenance** going forward.

Goals and Objectives:

Protecting the Business

• Eliminate / Reduce Business Interruption	• Insure Continuity of Business by certifying application recovery	• Conduct Risk Management and Insurance Protection reviews
• Provide Personnel Protections (HRM, Safe Workplace, and Employee Assistance Programs)	• Vendors - Supply Chain Management & Control • (ISO 24672 / ISO 27031)	• Protect Clients (Products / Services) via adherence to SLA / SLR guidelines
• Locations / Infrastructure	• Community / Business / Personnel	• Lines of Business
• Physical / Data Security	• Compliance	• Recovery Management
• Optimized Operations	• Insurance	• Reputation

Protecting Information Technology

• Build IT Location (Safe Site, HVAC, Water, Electrical, Raised Floor, etc.)	• Asset Management (Asset Acquisition, Redeployment, and Termination)	• Configuration Management / Version and Release Management
• Use Best Practices like CERT / COSO, CobIT, ITIL.v3	• Mainframe, Mid-Range, Client / Server, and PC safeguards	• Communications (Local, LAN, WAN, Internet, cloud)
• System Development Life Cycle (SDLC) optimization	• Products and Service Support Development, Enhancement	• Support and Maintenance for problems and enhancements
• Data Management (Dedupe/ VTL / Snapshots / CDP)	• Information Security Management System via ISO27000	• Data Sensitivity and Access Controls (Applid / Userid / Pswd)
• Vaulting, Backup, and Recovery	• Disk / File copy retrieve utilities	• RTO, RPO, RTC

Risk Management, Objectives and Process

- Define **Risk Management Process**;
- Define **Legal and Regulatory Requirements**;
- Determine **Compliance Requirements**;
- Perform a **Risk Assessment** to uncover Obstacles, Gaps, and Exceptions;
- Define **Mitigations / Mediations;**
- Calculate **cost to Mitigate / Mediate** and prioritize responses;
- Review **Vendor Agreements** and possible **Supply Chain** interruptions;
- Obtain **Insurance** Quotes and select appropriate insurance protection;
- **Integrate** within the everyday functions performed by personnel;
- Create “**Crisis Response Plans**” to respond to Risks;
- Develop documentation, **awareness, and training** materials; and
- Provide ongoing **Support and Maintenance** going forward.

Establishing the Recovery Management process

- Formulate Recovery Management Business Plan;
- Develop a Project Plan;
- Define Organization Structure and Job Functions;
- Implement Recovery Document Library Management;
- Identify and Train Recovery Management Coordinators from Business Units;
- Develop a Common Recovery Management Language;
- Select automated Recovery Management Tools;
- Create, Test, Certify, and Implement Recovery Plans;
- Integrate Recovery Management and Train Staff; and,
- Support and Maintain Recovery Management going forward.

Achieving Enterprise Resiliency and Corporate Certification

1. **Review existing Security and Recovery Management Operations.**

2. **Define Domestic and International Compliance Requirements;**

3. **Evaluate Command Centers and their Recovery Operations;**

4. **Define Company Lines of Business (LOB's);**

5. **Determine Integration Requirements;**

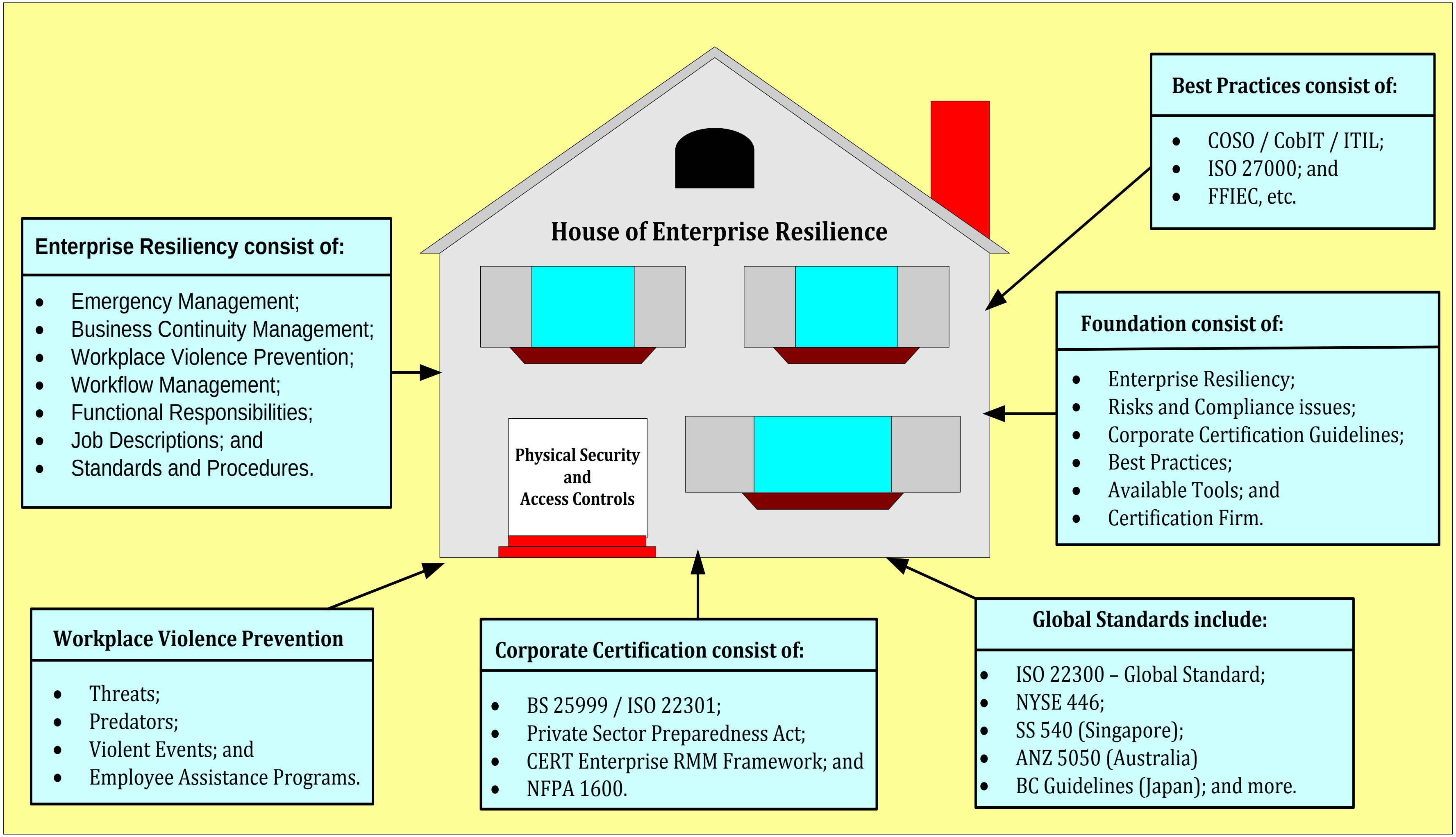
6. **Create Business and Implementation Plan;**

7. **Document Process and provide Training;**

8. **Integrate through Job Descriptions and Workflow Procedures;**

9. **Provide ongoing Support and Maintenance.**

Enterprise Resiliency must be built upon a Solid Foundation



House of Enterprise Resilience

Physical Security and Access Controls

Enterprise Resiliency consist of:

- Emergency Management;
- Business Continuity Management;
- Workplace Violence Prevention;
- Workflow Management;
- Functional Responsibilities;
- Job Descriptions; and
- Standards and Procedures.

Best Practices consist of:

- COSO / CobIT / ITIL;
- ISO 27000; and
- FFIEC, etc.

Foundation consist of:

- Enterprise Resiliency;
- Risks and Compliance issues;
- Corporate Certification Guidelines;
- Best Practices;
- Available Tools; and
- Certification Firm.

Workplace Violence Prevention

- Threats;
- Predators;
- Violent Events; and
- Employee Assistance Programs.

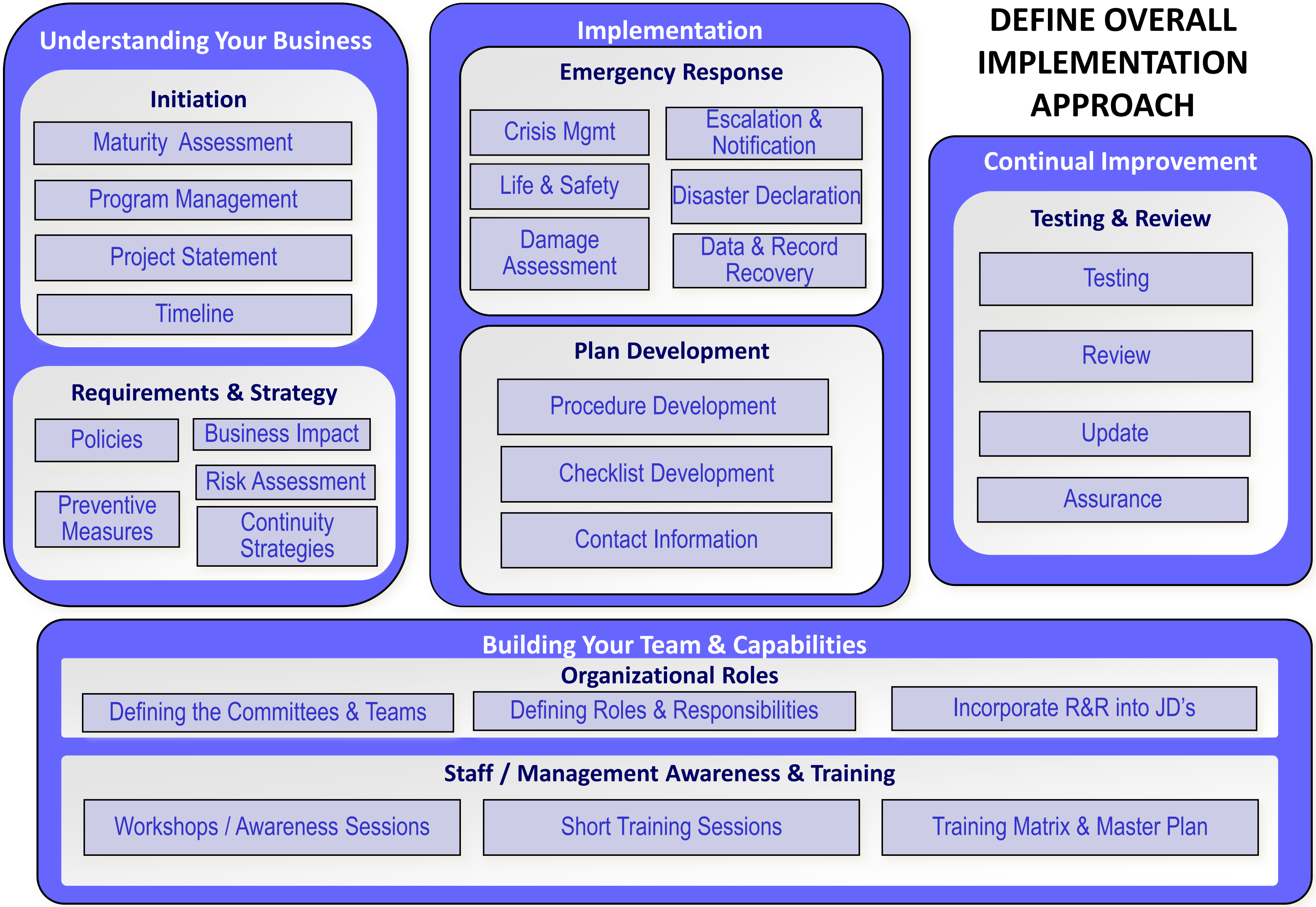
Corporate Certification consist of:

- BS 25999 / ISO 22301;
- Private Sector Preparedness Act;
- CERT Enterprise RMM Framework; and
- NFPA 1600.

Global Standards include:

- ISO 22300 – Global Standard;
- NYSE 446;
- SS 540 (Singapore);
- ANZ 5050 (Australia)
- BC Guidelines (Japan); and more.

DEFINE OVERALL IMPLEMENTATION APPROACH



Understanding Your Business

Initiation
- Maturity Assessment
- Program Management
- Project Statement
- Timeline

Requirements & Strategy
- Policies
- Business Impact
- Risk Assessment
- Preventive Measures
- Continuity Strategies

Implementation

Emergency Response
- Crisis Mgmt
- Escalation & Notification
- Life & Safety
- Disaster Declaration
- Damage Assessment
- Data & Record Recovery

Plan Development
- Procedure Development
- Checklist Development
- Contact Information

Continual Improvement

Testing & Review
- Testing
- Review
- Update
- Assurance

Building Your Team & Capabilities

Organizational Roles
- Defining the Committees & Teams
- Defining Roles & Responsibilities
- Incorporate R&R into JD's

Staff / Management Awareness & Training
- Workshops / Awareness Sessions
- Short Training Sessions
- Training Matrix & Master Plan

COSO Risk Assessment

Committee Of Sponsoring Organizations (COSO) was formed to develop Risk Management and Mitigation Guidelines throughout the industry.

Designed to protect Stakeholders from uncertainty and associated risk that could erode value.

A Risk Assessment in accordance with the COSO Enterprise Risk Management Framework, consists of (see www.erm.coso.org for details):

- Internal Environment Review,
- Objective Setting,
- Event Identification,
- Risk Assessment,
- Risk Response,
- Control Activities,
- Information and Communication,
- Monitoring and Reporting.

Creation of Organizational Structure, Personnel Job Descriptions and Functional Responsibilities, Workflows, Personnel Evaluation and Career Path Definition, Human Resource Management.

Implementation of Standards and Procedures guidelines associated with Risk Assessment to guaranty compliance to laws and regulations.

Employee awareness training, support, and maintenance going forward.

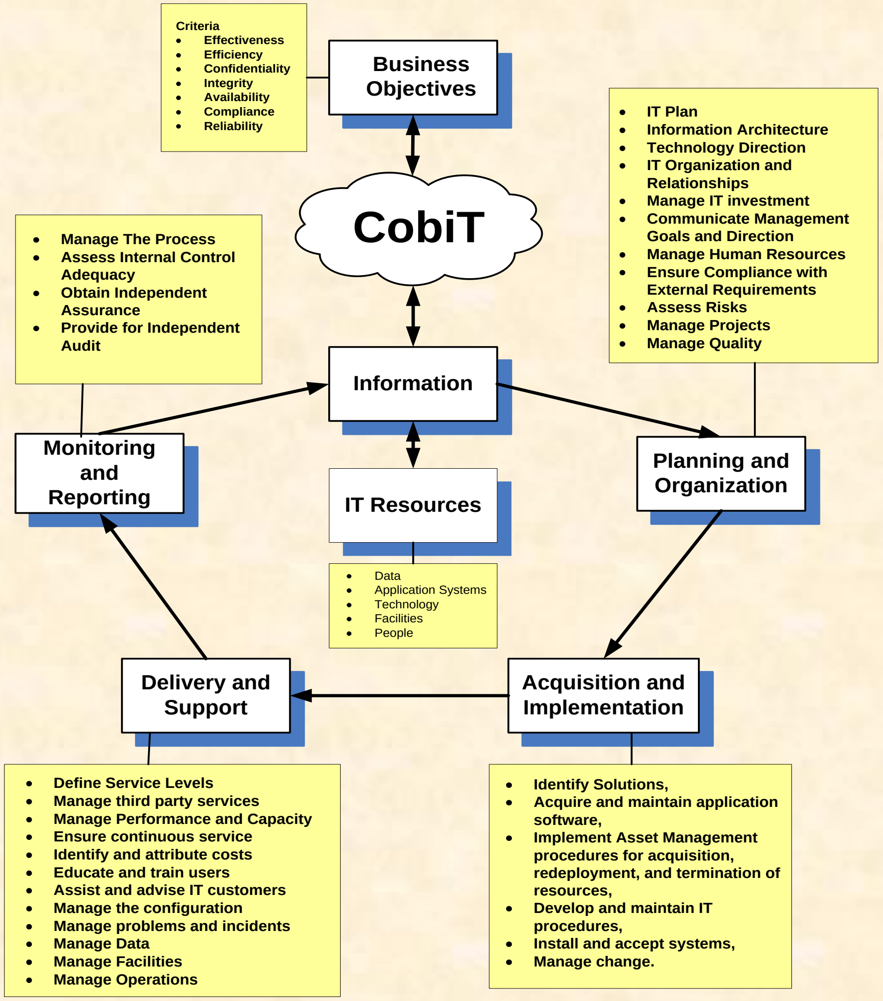
CobiT Framework

Control Objectives for Information Technology (CobiT)

Is designed to extend COSO controls over the IT environment by:

- Providing guidelines for Planning and integrating new products and services into the IT Organization
- Integrating new acquisitions;
- Delivering new Acquisitions / Mergers and supporting them going forward;
- Monitoring IT activity, capacity, and performance; so that
- Management can meet Business Objectives, while protecting Information and IT Resources.

CobiT Framework and Functionality



Criteria
- Effectiveness
- Efficiency
- Confidentiality
- Integrity
- Availability
- Compliance
- Reliability

Business Objectives

CobiT

Information

IT Resources

- Data
- Application Systems
- Technology
- Facilities
- People

Monitoring and Reporting

- Manage The Process
- Assess Internal Control Adequacy
- Obtain Independent Assurance
- Provide for Independent Audit

Planning and Organization

- IT Plan
- Information Architecture
- Technology Direction
- IT Organization and Relationships
- Manage IT investment
- Communicate Management Goals and Direction
- Manage Human Resources
- Ensure Compliance with External Requirements
- Assess Risks
- Manage Projects
- Manage Quality

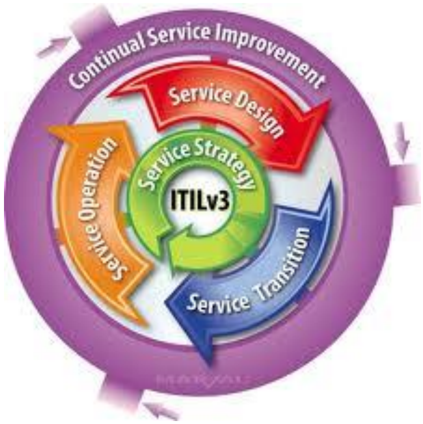
Delivery and Support

- Define Service Levels
- Manage third party services
- Manage Performance and Capacity
- Ensure continuous service
- Identify and attribute costs
- Educate and train users
- Assist and advise IT customers
- Manage the configuration
- Manage problems and incidents
- Manage Data
- Manage Facilities
- Manage Operations

Acquisition and Implementation

- Identify Solutions,
- Acquire and maintain application software,
- Implement Asset Management procedures for acquisition, redeployment, and termination of resources,
- Develop and maintain IT procedures,
- Install and accept systems,
- Manage change.

ITIL V3 Overview



ITIL Five Phase approach to IT Service Support

1. Service Strategy,
2. Service Design,
3. Service Transition,
4. Service Operation, and
5. Continual Service Improvement.

ITIL Available Modules

1. **Service Strategy**
   - Service Portfolio Management (available Services and Products)
   - Financial Management (PO, WO, A/R, A/P, G/L, Taxes and Treasury)

2. **Service Design**
   - Service Catalogue Management
   - Service Level Management (**SLA / SLR**)
   - Risk Management (**CERT / COSO**)
   - Capacity and Performance Management
   - Availability Management (**SLA / SLR**)
   - IT Service Continuity Management **(BCM)**
   - Information Security Management **(ISMS)**
   - Compliance Management **(Regulatory**)
   - Architecture Management **(AMS, CFM)**
   - Supplier Management **(Supply Chain)**

3. **Service Transition**
   - Change Management
   - Project Management **(Transition Planning and Support)**
   - Release and Deployment Management (**V & R Mgmnt**)
   - Service Validation and Testing
   - Application Development and Customization
   - Service Asset and Configuration Management
   - Knowledge Management

4. **Service Operation**
   - Event Management
   - Incident Management
   - Request Fulfillment
   - Access Management
   - Problem Management
   - IT Operations Management
   - Facilities Management

Adhering to Compliance Laws

- **Gramm Leach Bliley** – Safeguard Act (was Bank Holding Act);
- **Dodd – Frank** – Wall Street Reform and Consumer Protection 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).

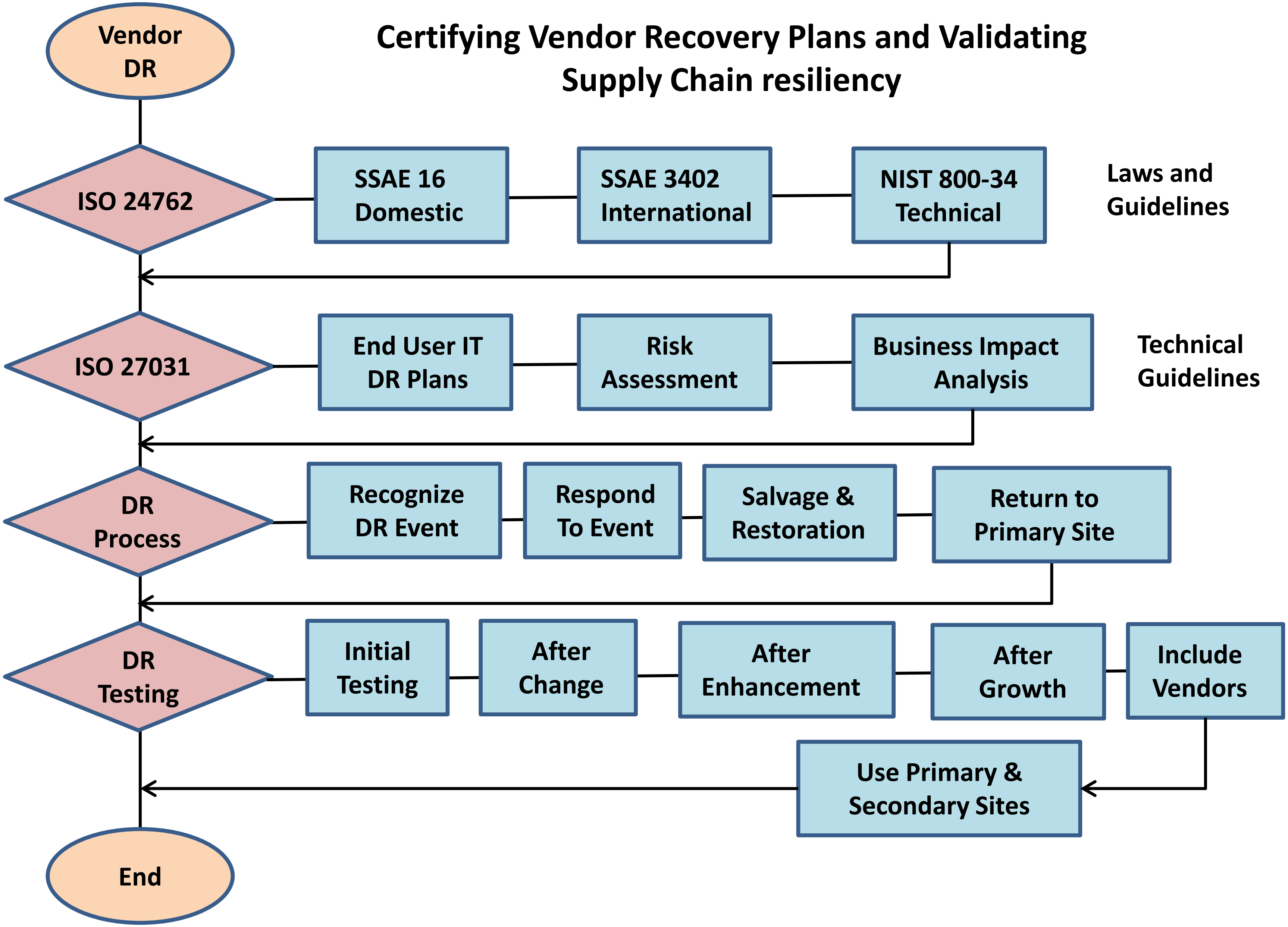
How do we comply?

Laws and Regulations concentrate on the VALIDITY of PROVIDED DATA, so we start with a review of how sensitive data is described, created, protected, and used, including:

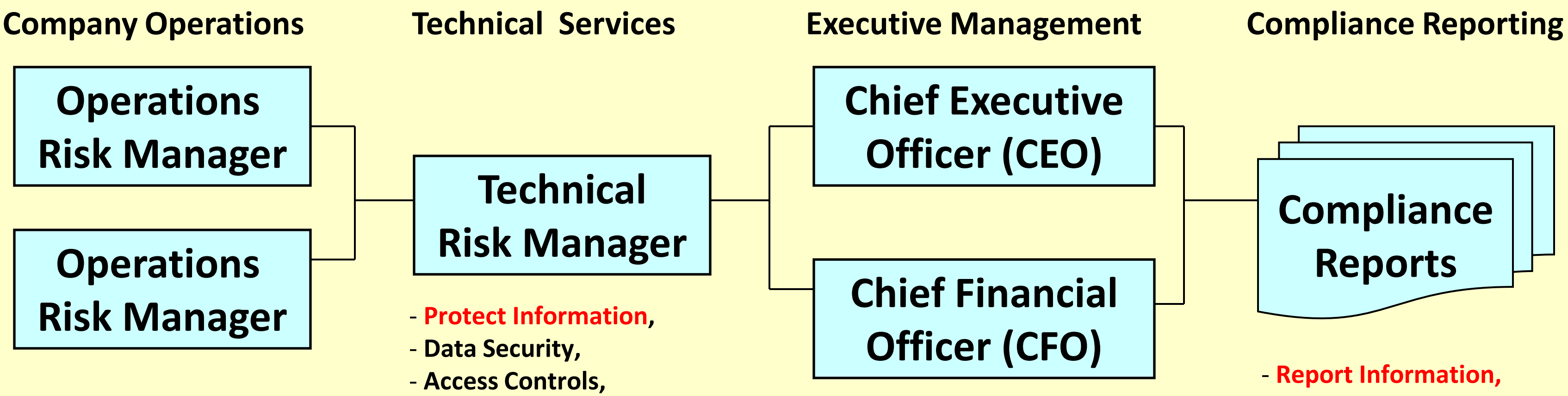
- **Identify the lifecycle of data used in financial reporting and compliance;**
  - **Where does it come from and who owns it?**
  - **What form is it in (Excel, Database, manual, fax, email, etc.),**
  - **Who has access to the data and how can they impact data (*CRUD* - create, read, update, and delete).**
- **Review current Data Sensitivity and IT Security procedures;**
- **Examine Library Management, Backup, Recovery, and Vaulting procedures associated with sensitive data;**
- **Review Business Continuity Planning and Disaster Recovery procedures used to protect and safeguard critical Information Technology and Business facilities;**
- **Utilize existing Standards and Procedures to duplicate process and identify errors; and,**
- **Examine the available Employee Awareness and Education programs.**

As a result of this study, it will be possible to identify weaknesses and develop procedures to overcome weaknesses and improve data efficiency and productivity.

Certifying Vendor Recovery Plans and Validating Supply Chain resiliency



How reporting is accomplished



Company Operations

Operations Risk Manager

Operations Risk Manager

Technical Services

Technical Risk Manager

Executive Management

Chief Executive Officer (CEO)

Chief Financial Officer (CFO)

Compliance Reporting

Compliance Reports

- Extract Information,
- Generate Financial Reports,
- Ensure Record Safeguards,
- Ensure Record Formats,
- Generate Compliance Reports,
- Validate Information,
- Submit Reports.

- Protect Information,
- Data Security,
- Access Controls,
- Library Management,
- Production Acceptance,
- Version and Release Mgmt.,
- Business Continuity,
- Disaster Recovery,
- Emergency Management,
- Standards and Procedures.

- Validate Information,
- Establish Reporting Criteria,
- Gather data and report,
- Review Reports,
- Attest to their accuracy,
- Submit Reports.

- Report Information,
- Submitted Quarterly,
- Attested to Annually,
- Reviewed by SEC and other agencies to insure compliance.

Section 404 of the Sarbanes-Oxley Act (SOX) says that publicly traded companies must establish, document, and maintain internal controls and procedures for Financial and Compliance reporting. It also requires companies to check the effectiveness of internal controls and procedures for Financial and Compliance reporting.

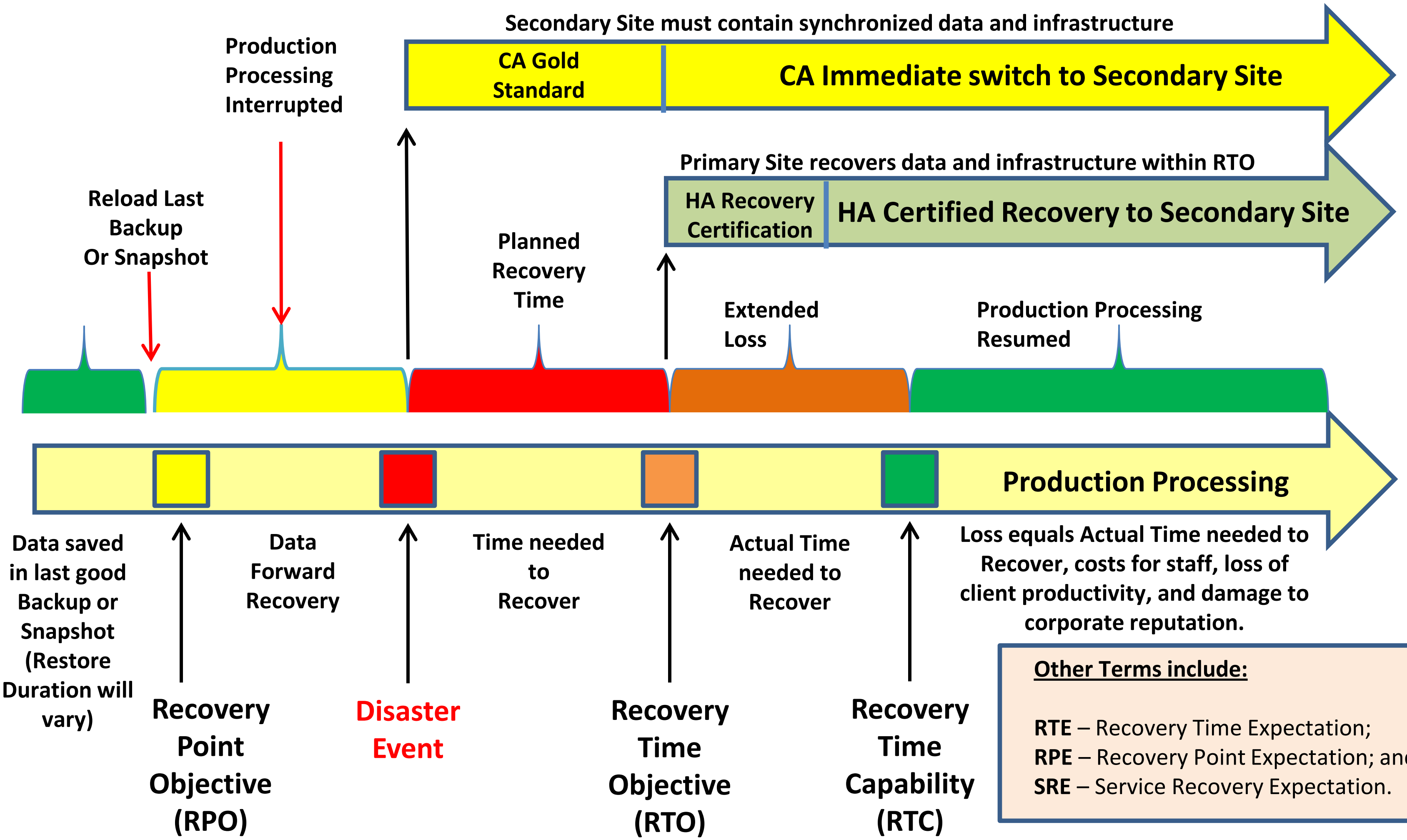
In order to do this, companies must:

- Document existing controls and procedures that relate to financial reporting.
- Test their effectiveness.
- Report on any gaps or poorly documented areas, then determine if mitigation should be performed.
- Repair deficiencies and update any Standards and Procedures associated with the defects.

Strategies for Eliminating Audit Exceptions

- Review of Compliance Requirements (Business and Industry)
- Ensure Data Sensitivity, IT Security and Vital Records Management,
- Eliminate Data Corruption and Certify HA / CA Application recovery,
- Adhere to Systems Development Life Cycle (SDLC),
- Utilize Automated Tools whenever practical,
- Elimination of Single-Point-Of-Failure concerns,
- Create Inventory / Configuration / Asset Management guidelines,
- Develop Incident / Problem and Crisis Management procedures,
- Integrate Work-Flow automation through Re-Engineering processes,
- Implement and conduct Training and Awareness programs.

Achieving Recovery Time Objective (RTO) / Recovery Point Objective (RPO) and Recovery Time Capability (RTC)

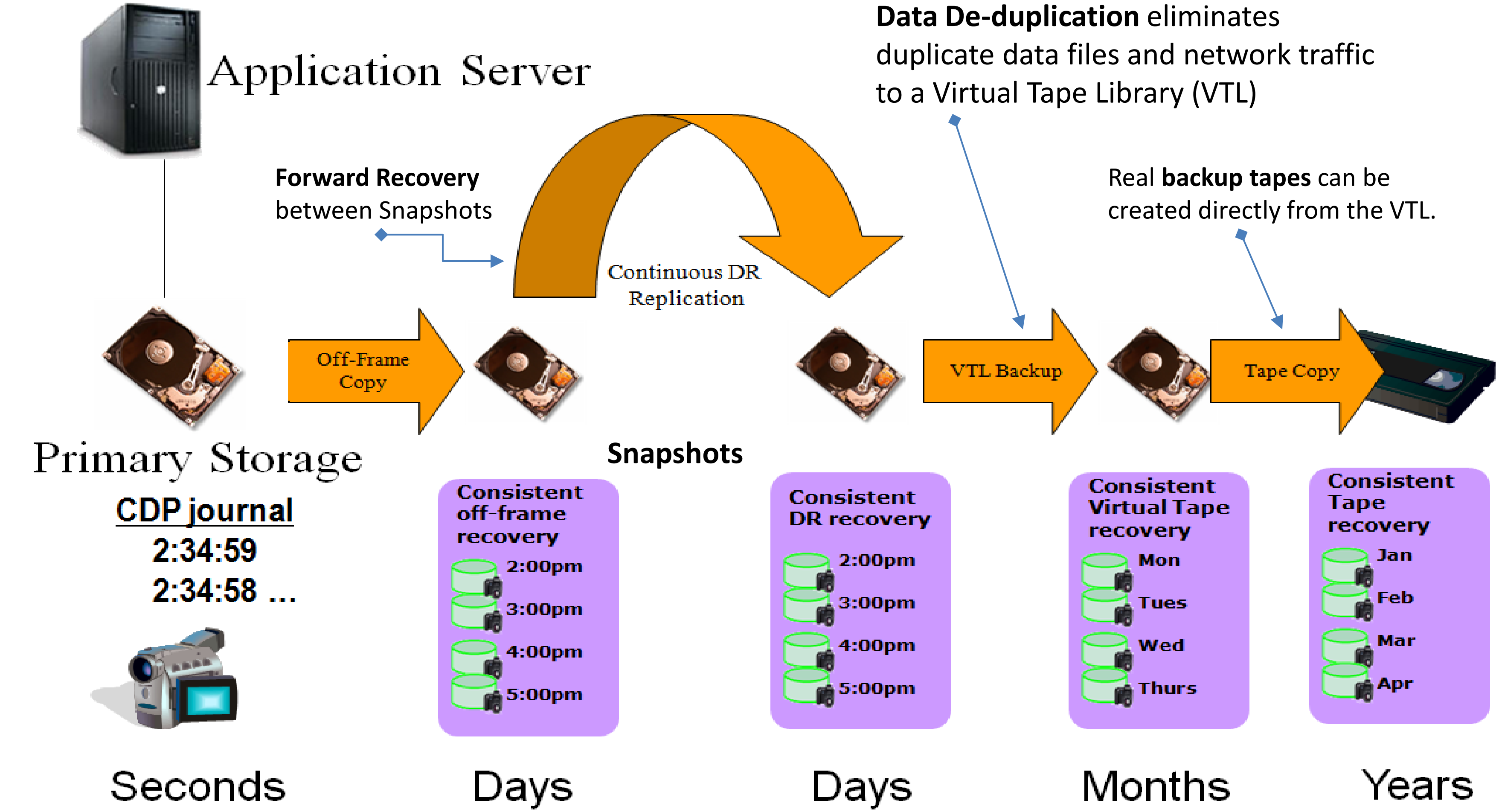

Secondary Site must contain synchronized data and infrastructure
CA Gold Standard
CA Immediate switch to Secondary Site
Primary Site recovers data and infrastructure within RTO
HA Recovery Certification
HA Certified Recovery to Secondary Site
Production Processing Interrupted
Reload Last Backup Or Snapshot
Planned Recovery Time
Extended Loss
Production Processing Resumed
Production Processing
Data saved in last good Backup or Snapshot (Restore Duration will vary)
Data Forward Recovery
Time needed to Recover
Actual Time needed to Recover
Loss equals Actual Time needed to Recover, costs for staff, loss of client productivity, and damage to corporate reputation.
Recovery Point Objective (RPO)
Disaster Event
Recovery Time Objective (RTO)
Recovery Time Capability (RTC)

Other Terms include:

RTE – Recovery Time Expectation;
RPE – Recovery Point Expectation; and
SRE – Service Recovery Expectation.

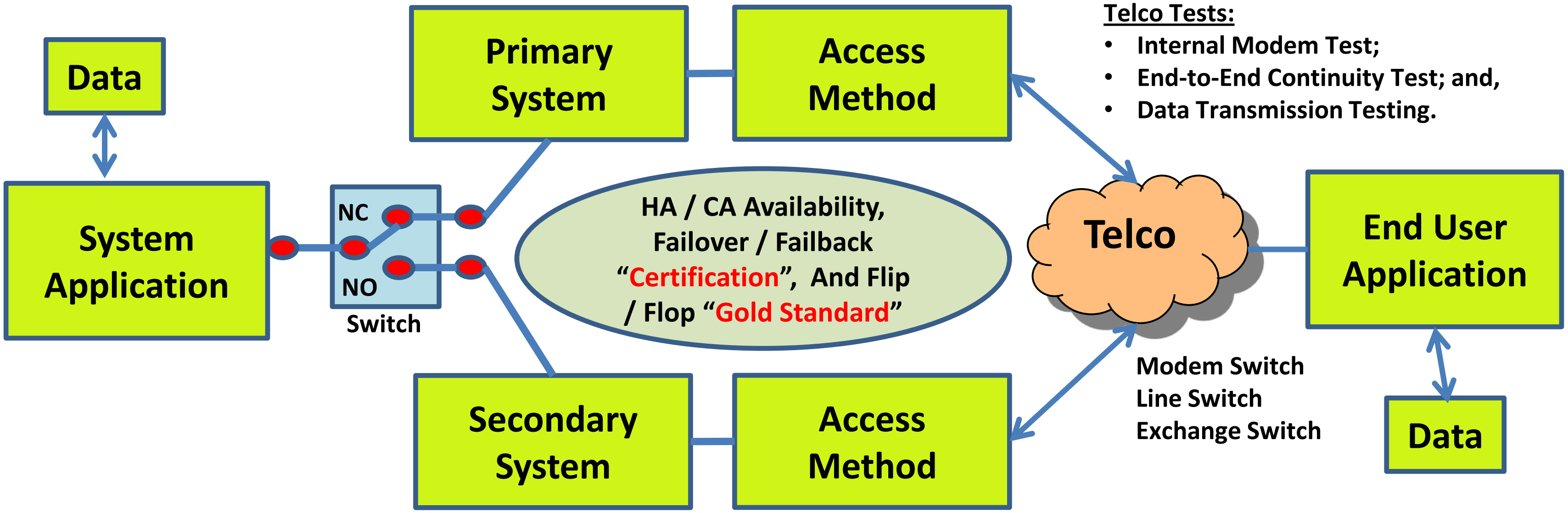
Optimized Protection / Recovery Data Services

Data Recovery Timeline: Automated Life Cycle Management


Application Server
Data De-duplication eliminates duplicate data files and network traffic to a Virtual Tape Library (VTL)
Forward Recovery between Snapshots
Real **backup tapes** can be created directly from the VTL.
Continuous DR Replication
Off-Frame Copy
VTL Backup
Tape Copy
Primary Storage
Snapshots
CDP journal
2:34:59
2:34:58 ...
Consistent off-frame recovery
2:00pm
3:00pm
4:00pm
5:00pm
Consistent DR recovery
2:00pm
3:00pm
4:00pm
5:00pm
Consistent Virtual Tape recovery
Mon
Tues
Wed
Thurs
Consistent Tape recovery
Jan
Feb
Mar
Apr
Seconds
Days
Days
Months
Years

Store and Forward concept for safe data transmission / reception and achieving "Zero Downtime"

Because Data stays in "Originating" buffer until a "Positive Acknowledgement" is received, it is protected from loss. If failure occurs, data is not transmitted and error message generated so that recovery and corrective actions can be performed. You should eliminate any "Single Points of Failure" to achieve an alternate path should the primary path fail.

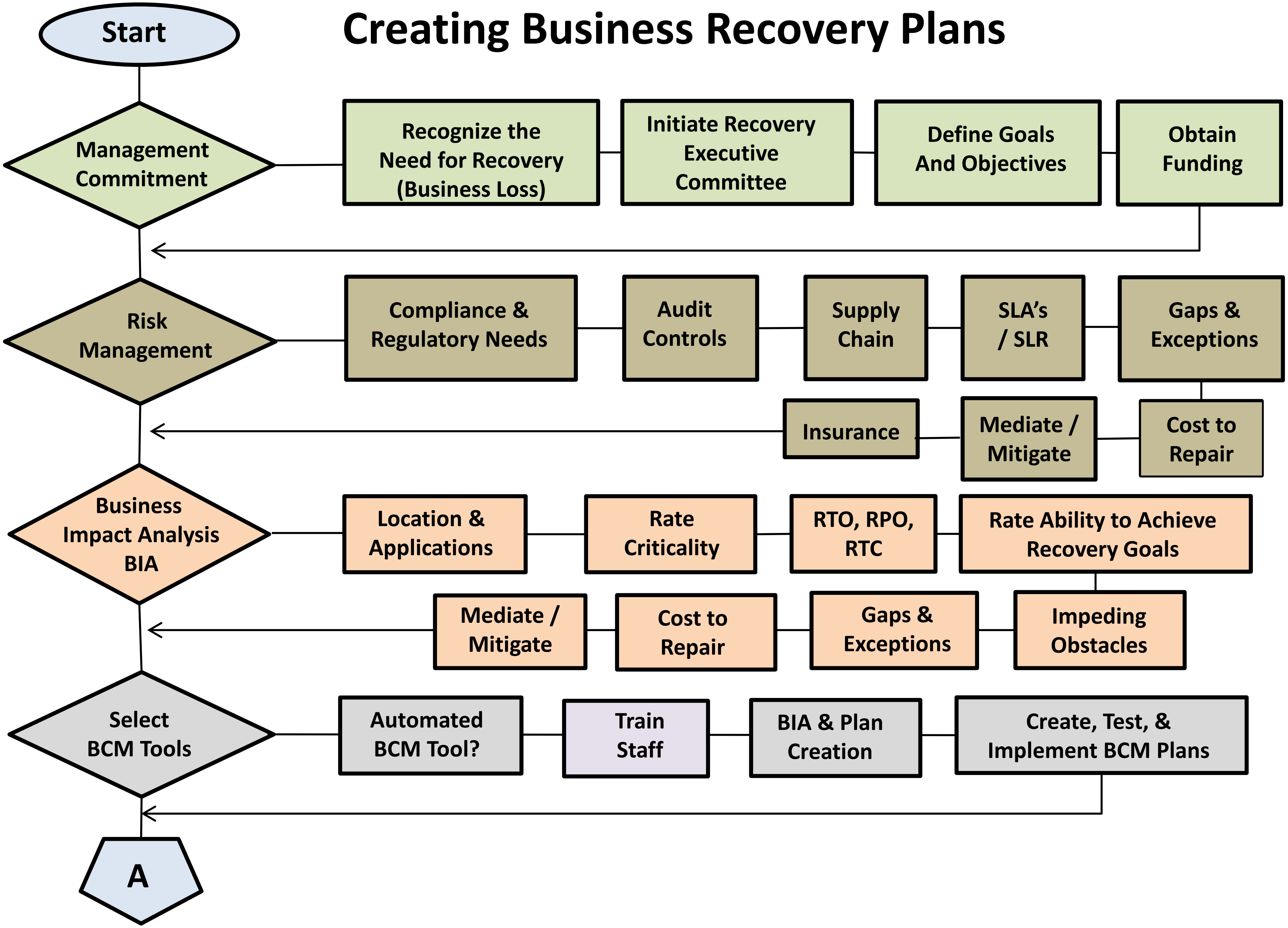


Telco Tests:

- Internal Modem Test;
- End-to-End Continuity Test; and,
- Data Transmission Testing.

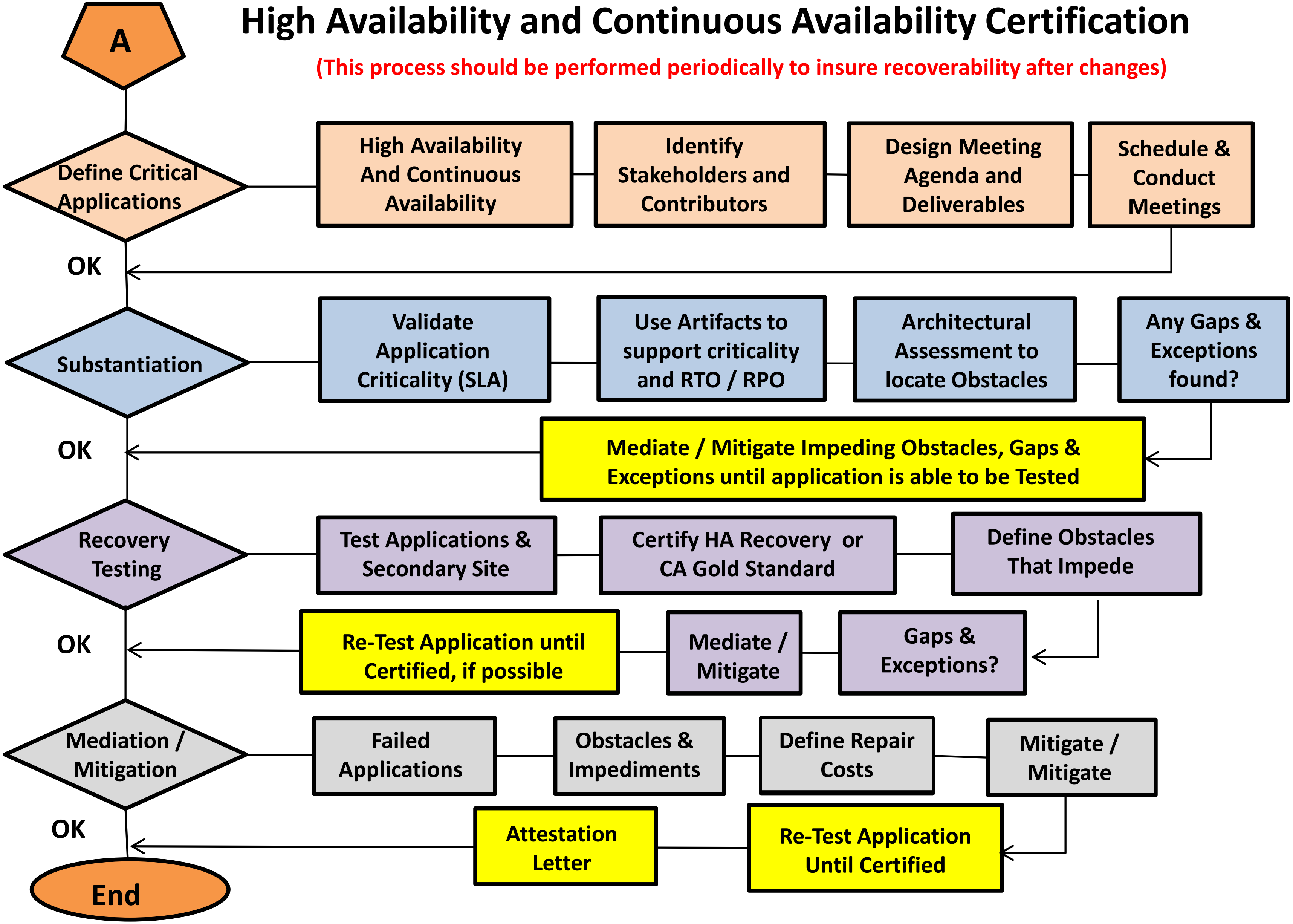
"**Zero Downtime**" can be achieved through "**Recovery Certification**" for HA Applications and "**Gold Standard Recovery Certification**" for CA Applications. Using the "**Store and Forward**" concepts shown here and eliminating any "**Single Points of Failure**" will help you achieve the goals.

Creating Business Recovery Plans

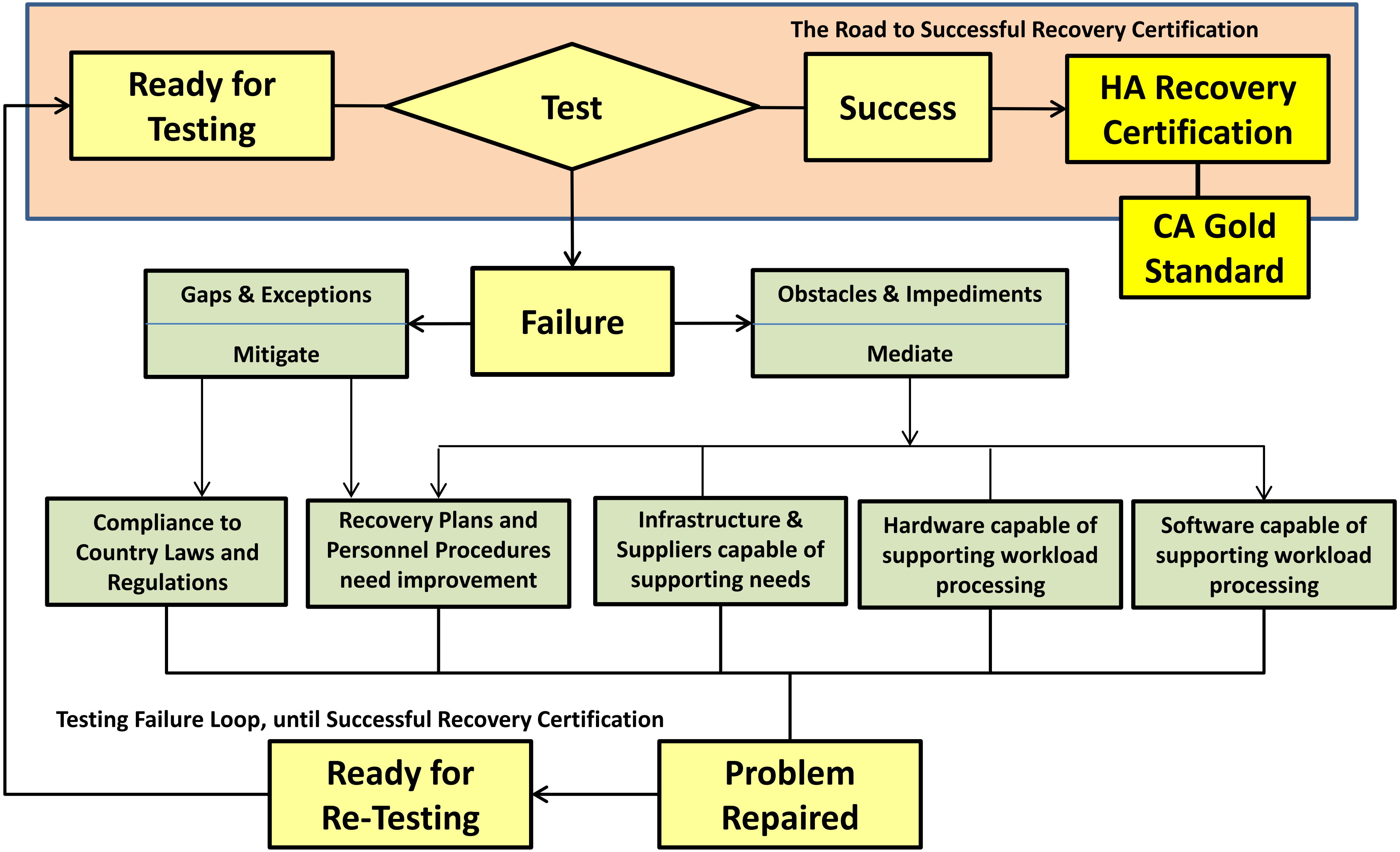


High Availability and Continuous Availability Certification

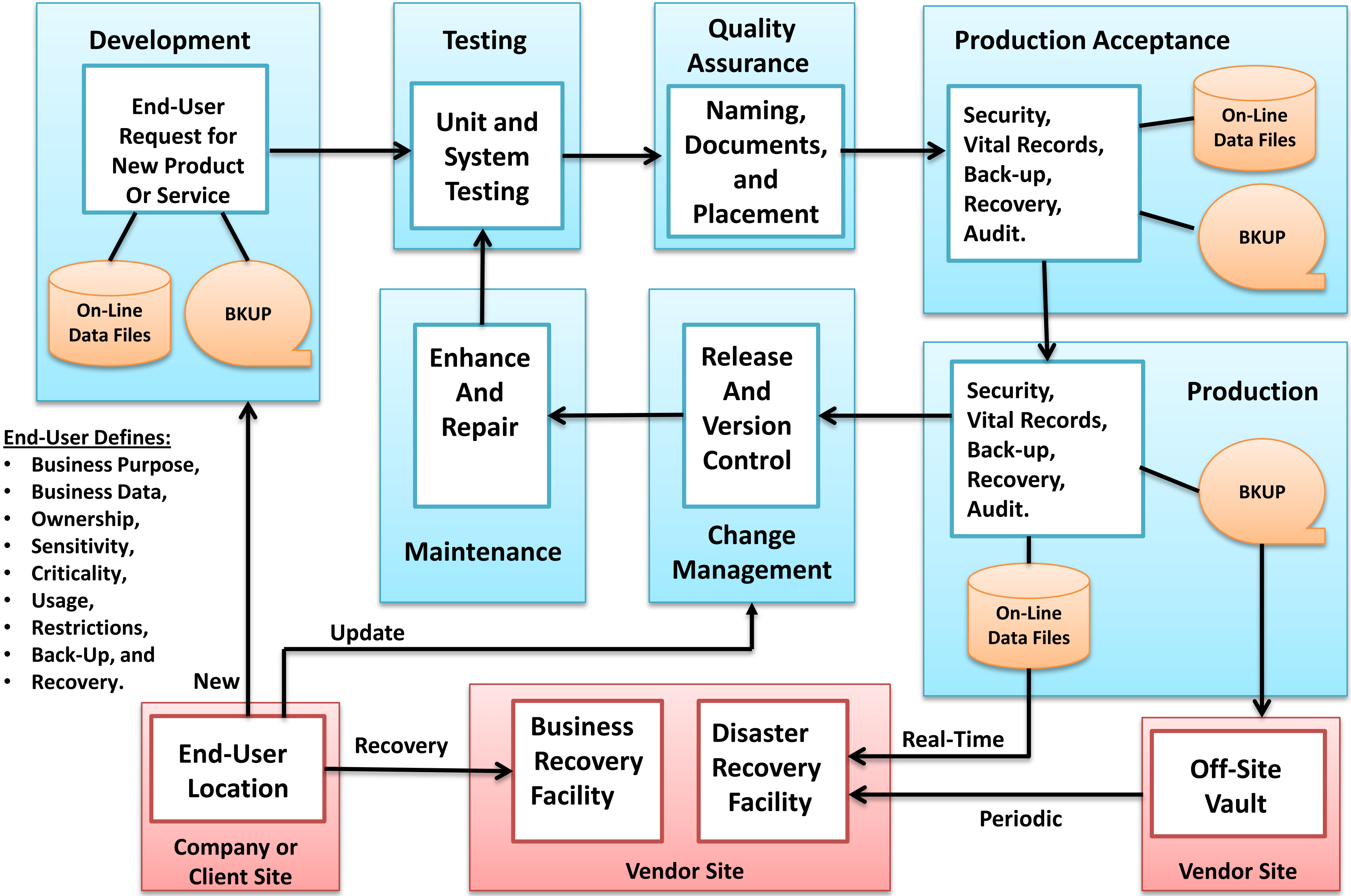
(This process should be performed periodically to insure recoverability after changes)


A
Define Critical Applications
High Availability And Continuous Availability
Identify Stakeholders and Contributors
Design Meeting Agenda and Deliverables
Schedule & Conduct Meetings
OK
Substantiation
Validate Application Criticality (SLA)
Use Artifacts to support criticality and RTO / RPO
Architectural Assessment to locate Obstacles
Any Gaps & Exceptions found?
Mediate / Mitigate Impeding Obstacles, Gaps & Exceptions until application is able to be Tested
OK
Recovery Testing
Test Applications & Secondary Site
Certify HA Recovery or CA Gold Standard
Define Obstacles That Impede
Gaps & Exceptions?
Mediate / Mitigate
Re-Test Application until Certified, if possible
OK
Mediation / Mitigation
Failed Applications
Obstacles & Impediments
Define Repair Costs
Mitigate / Mitigate
Re-Test Application Until Certified
Attestation Letter
OK
End

Testing High Availability (HA) and Continuous Availability (CA) for Recovery Certification and ability to Flip / Flop between Primary and Secondary Sites


The Road to Successful Recovery Certification
Ready for Testing
Test
Success
HA Recovery Certification
CA Gold Standard
Failure
Gaps & Exceptions
Mitigate
Obstacles & Impediments
Mediate
Compliance to Country Laws and Regulations
Recovery Plans and Personnel Procedures need improvement
Infrastructure & Suppliers capable of supporting needs
Hardware capable of supporting workload processing
Software capable of supporting workload processing
Testing Failure Loop, until Successful Recovery Certification
Ready for Re-Testing
Problem Repaired

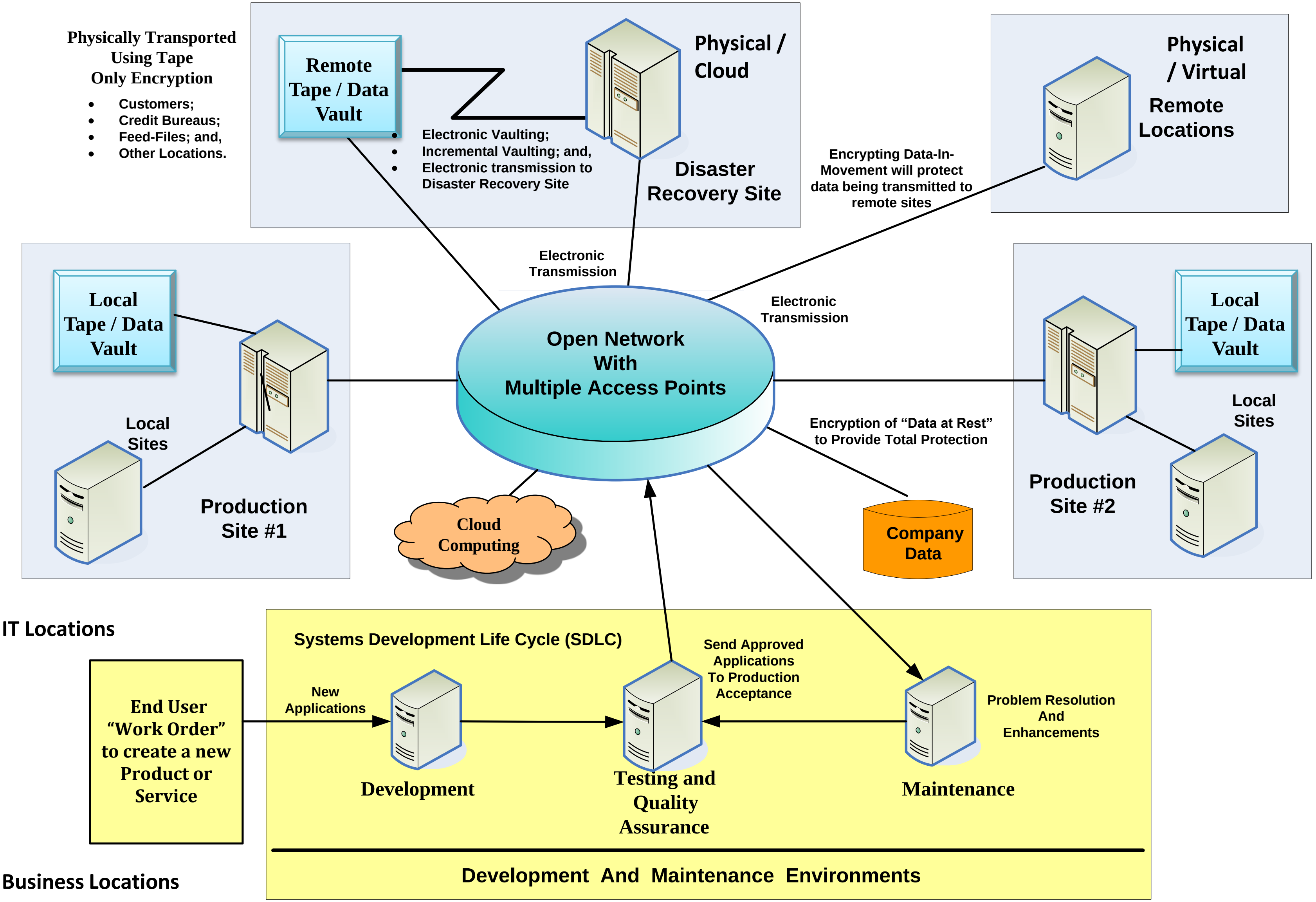
Systems Development Life Cycle (SDLC), Components and flow



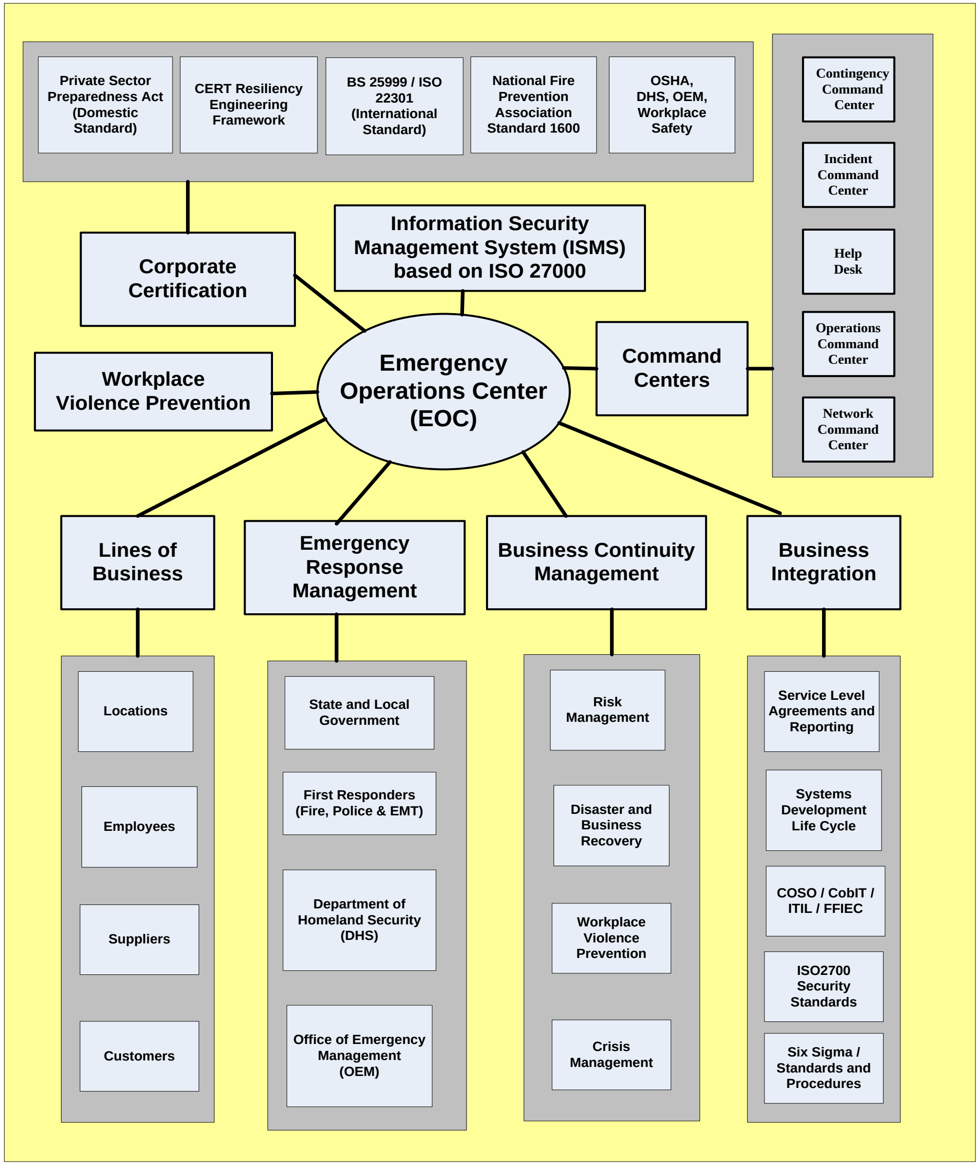
<u>End-User Defines:</u>

- Business Purpose,
- Business Data,
- Ownership,
- Sensitivity,
- Criticality,
- Usage,
- Restrictions,
- Back-Up, and
- Recovery.

Overview of the Enterprise Information Technology Environment


Physically Transported Using Tape Only Encryption
- Customers;
- Credit Bureaus;
- Feed-Files; and,
- Other Locations.
Remote Tape / Data Vault
Physical / Cloud
Disaster Recovery Site
- Electronic Vaulting;
- Incremental Vaulting; and,
- Electronic transmission to Disaster Recovery Site
Encrypting Data-In-Movement will protect data being transmitted to remote sites
Physical / Virtual
Remote Locations
Electronic Transmission
Electronic Transmission
Local Tape / Data Vault
Local Sites
Production Site #1
Open Network With Multiple Access Points
Cloud Computing
Encryption of "Data at Rest" to Provide Total Protection
Company Data
Local Tape / Data Vault
Local Sites
Production Site #2
IT Locations
Systems Development Life Cycle (SDLC)
End User "Work Order" to create a new Product or Service
New Applications
Development
Send Approved Applications To Production Acceptance
Testing and Quality Assurance
Problem Resolution And Enhancements
Maintenance
Development And Maintenance Environments
Business Locations

Fully Integrated Recovery Operations and Disciplines (Physical End Goal)



Private Sector Preparedness Act (Domestic Standard)

CERT Resiliency Engineering Framework

BS 25999 / ISO 22301 (International Standard)

National Fire Prevention Association Standard 1600

OSHA, DHS, OEM, Workplace Safety

Corporate Certification

Information Security Management System (ISMS) based on ISO 27000

Workplace Violence Prevention

Emergency Operations Center (EOC)

Command Centers

Contingency Command Center

Incident Command Center

Help Desk

Operations Command Center

Network Command Center

Lines of Business

- Locations
- Employees
- Suppliers
- Customers

Emergency Response Management

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

Business Continuity Management

- Risk Management
- Disaster and Business Recovery
- Workplace Violence Prevention
- Crisis Management

Business Integration

- Service Level Agreements and Reporting
- Systems Development Life Cycle
- COSO / CobIT / ITIL / FFIEC
- ISO2700 Security Standards
- Six Sigma / Standards and Procedures

A fully integrated recovery organization will include the components shown in this picture.

Corporate Certification is achieved through the compliance laws and regulations used to provide domestic and international guidelines that enterprises must adhere to before they can do business in a country.

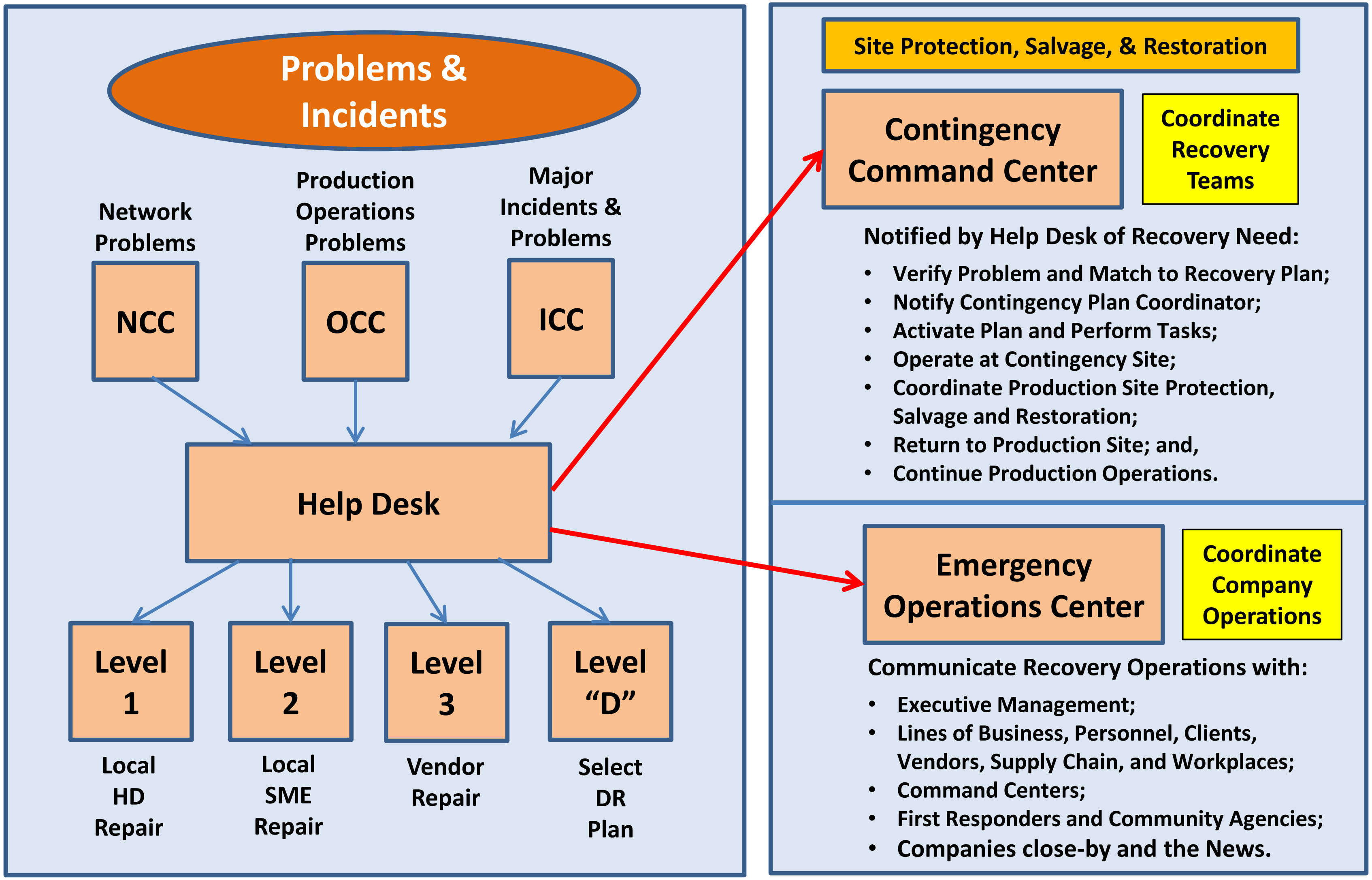
Workplace Violence Prevention and **Information Security** is adhered to by implementing guidelines to protect personnel and data by following the latest guidelines related to these topics.

Internal **command centers** responsible for monitoring operations, network, help desk, and the contingency command center will provide vital information to the **Emergency Operations Center** staff.

Organizational departments, locations, and functions should be identified and connections provided to the EOC so that communications and coordination can be achieved in a more accurate and speedy manner.

Using this structure will help organizations better collect recovery information and develop recovery operations to lessen business interruptions and protect the company's reputation.

Activating and Coordinating Disaster Recovery Plans



Problems & Incidents
Network Problems
NCC
Production Operations Problems
OCC
Major Incidents & Problems
ICC
Help Desk
Level 1
Local HD Repair
Level 2
Local SME Repair
Level 3
Vendor Repair
Level "D"
Select DR Plan
Site Protection, Salvage, & Restoration
Contingency Command Center
Coordinate Recovery Teams
Emergency Operations Center
Coordinate Company Operations

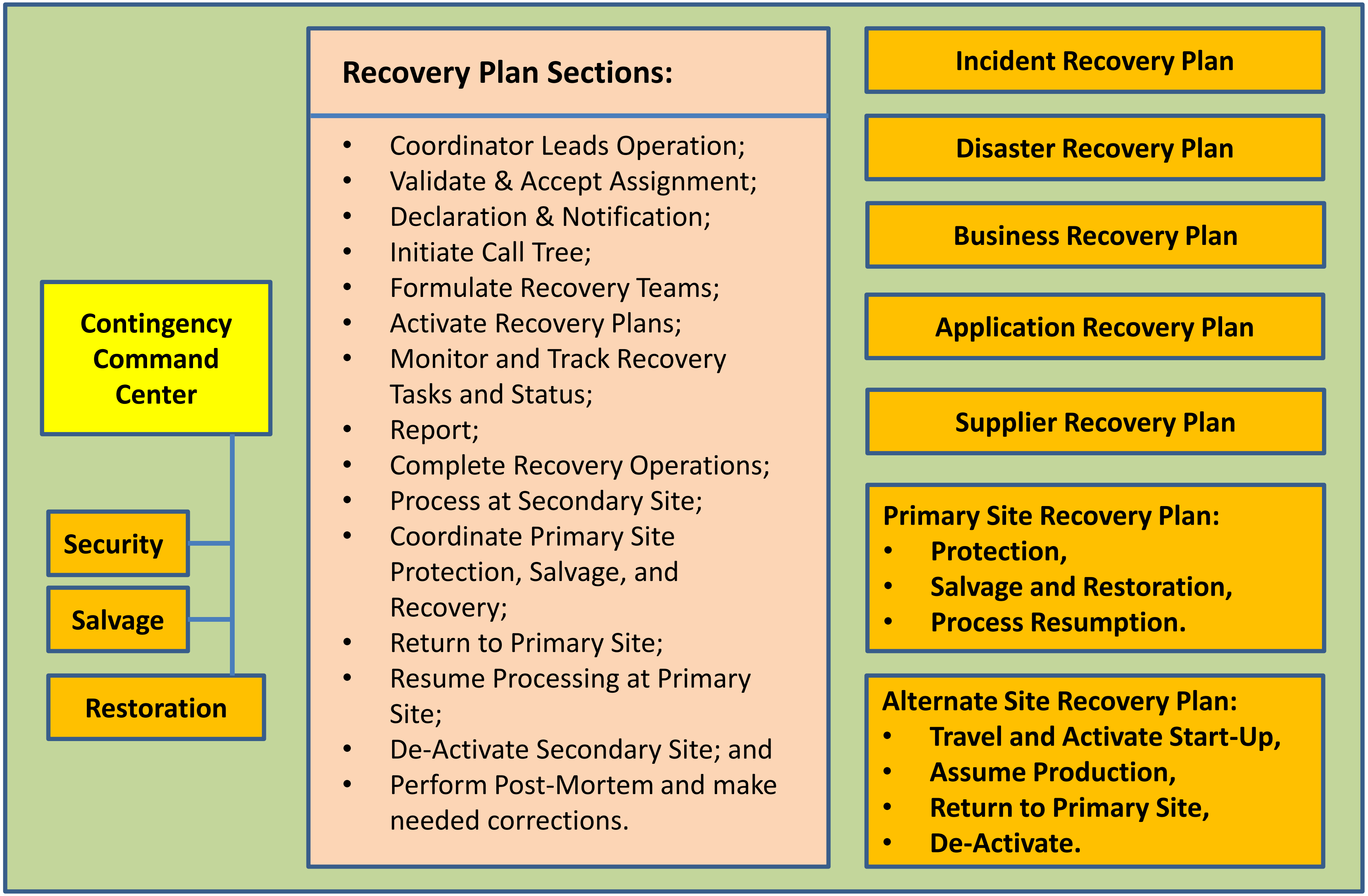
Notified by Help Desk of Recovery Need:

- Verify Problem and Match to Recovery Plan;
- Notify Contingency Plan Coordinator;
- Activate Plan and Perform Tasks;
- Operate at Contingency Site;
- Coordinate Production Site Protection, Salvage and Restoration;
- Return to Production Site; and,
- Continue Production Operations.

Communicate Recovery Operations with:

- Executive Management;
- Lines of Business, Personnel, Clients, Vendors, Supply Chain, and Workplaces;
- Command Centers;
- First Responders and Community Agencies;
- Companies close-by and the News.

Types of Recovery Plans and their Sections



Contingency Command Center

Security

Salvage

Restoration

Recovery Plan Sections:

- Coordinator Leads Operation;
- Validate & Accept Assignment;
- Declaration & Notification;
- Initiate Call Tree;
- Formulate Recovery Teams;
- Activate Recovery Plans;
- Monitor and Track Recovery Tasks and Status;
- Report;
- Complete Recovery Operations;
- Process at Secondary Site;
- Coordinate Primary Site Protection, Salvage, and Recovery;
- Return to Primary Site;
- Resume Processing at Primary Site;
- De-Activate Secondary Site; and
- Perform Post-Mortem and make needed corrections.

Incident Recovery Plan

Disaster Recovery Plan

Business Recovery Plan

Application Recovery Plan

Supplier Recovery Plan

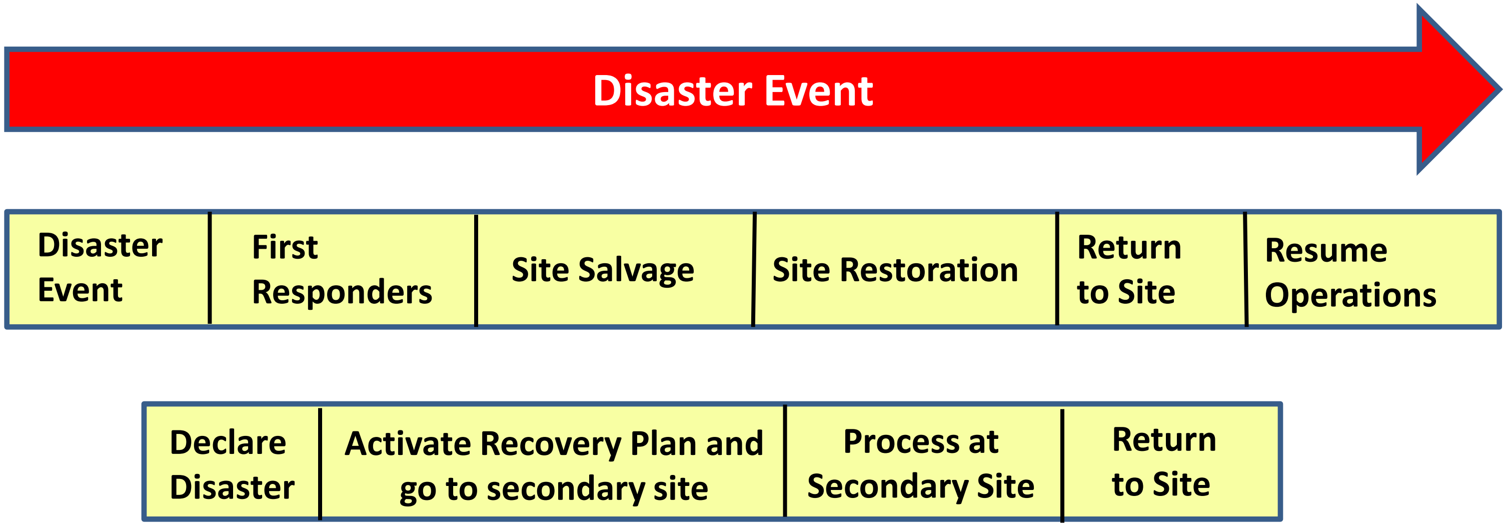
Primary Site Recovery Plan:

- **Protection,**
- **Salvage and Restoration,**
- **Process Resumption.**

Alternate Site Recovery Plan:

- **Travel and Activate Start-Up,**
- **Assume Production,**
- **Return to Primary Site,**
- **De-Activate.**

Responding to Disaster Events



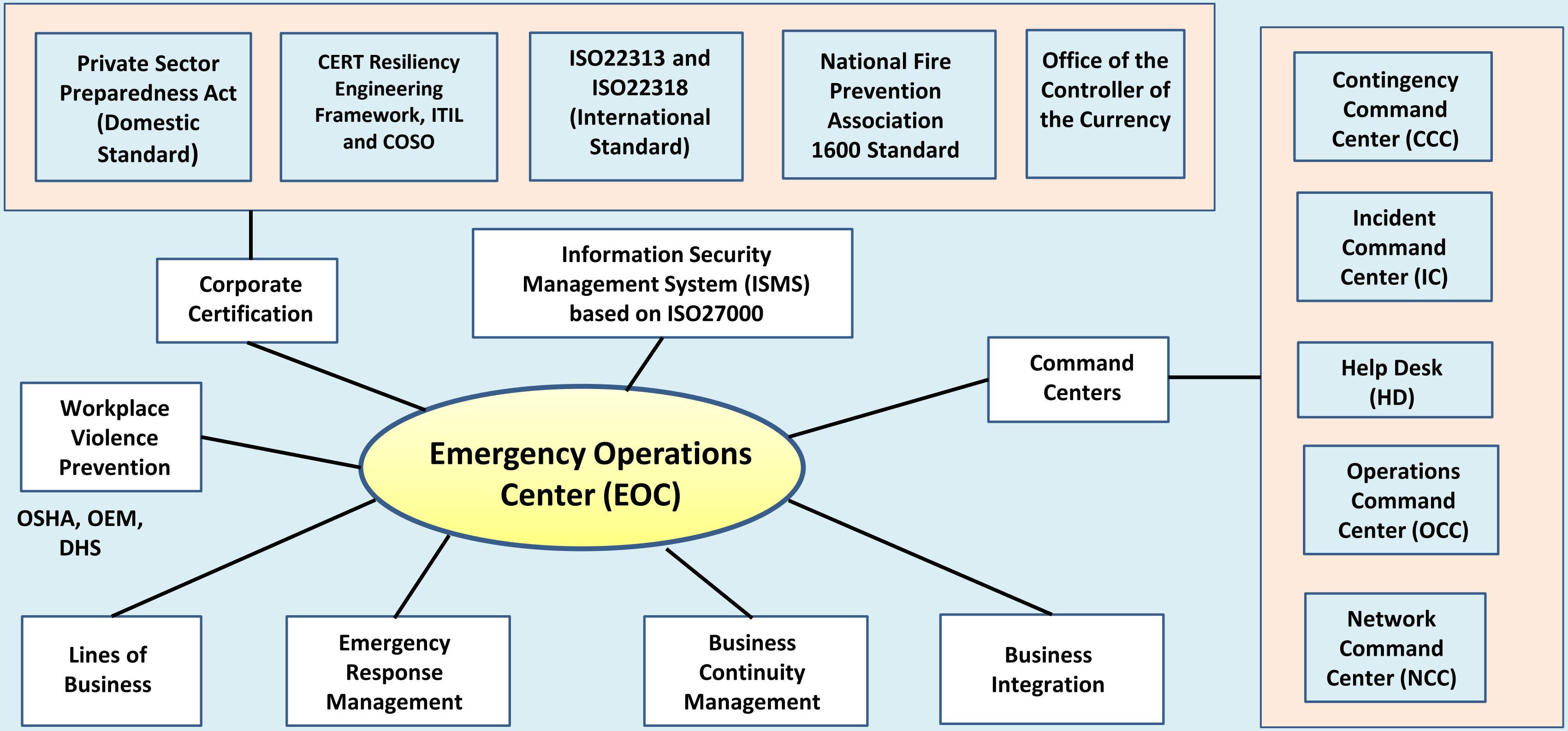
Disaster Event

Disaster Event	First Responders	Site Salvage	Site Restoration	Return to Site	Resume Operations

Declare Disaster	Activate Recovery Plan and go to secondary site	Process at Secondary Site	Return to Site

Coordinating recovery operations with the First Responders, Security, Salvage, and Restoration is a critical factor in recovery planning and should be included in all recovery planning procedures.

Fully Integrated Resiliency Operations and Disciplines (Logical End Goal)



Private Sector Preparedness Act (Domestic Standard)

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

Corporate Certification

Information Security Management System (ISMS) based on ISO27000

Emergency Operations Center (EOC)

Workplace Violence Prevention

OSHA, OEM, DHS

Command Centers

Contingency Command Center (CCC)

Incident Command Center (IC)

Help Desk (HD)

Operations Command Center (OCC)

Network Command Center (NCC)

Lines of Business

Emergency Response Management

Business Continuity Management

Business Integration

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

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

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

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

Where do we go from here

- **Presentation** to your management and technical staffs.
- **Agree** that you want to achieve Enterprise Resiliency and Corporate Certification.
- Perform a **Risk Assessment** that will define your needs.
- Obtain management approval to **initiate the project** with their strong support.
- Identify **Stakeholders** and Participants.
- Formulate **teams** and train them on the goals and objectives of this project.
- Create a detailed **Project Plan** and start teams working.
- Develop, Test, Implement "**Proof of Concept**", and gain approval to go forward.
- "**Rollout**" Enterprise Resiliency and Corporate Certification to all locations.
- Fully **document and Integrate** within the everyday staff functions performed.
- Deliver Awareness and **Training** services.
- Provide **Support and Maintenance** services going forward.