Achieving Enterprise Resiliency And Corporate Certification

DCAG
Service Offering

By

Combining Recovery Operations through a Common Recovery Language and Recovery Tools, while adhering to Domestic and International Compliance Standards

Helping Management eliminate business interruptions, achieve service and recovery objectives, and protect the company reputation.

Combining disciplines will insure operations, improve efficiency, and reduce recovery times.

Public Advocate will provide insurance review, recovery coordination, and claims processing.

Enterprise Resiliency combines all recovery operations into one discipline using a common language and tool set that is constructed via ***best practices*** guidelines.

Site Infrastructure Management for primary and secondary locations to ensure infrastructure, sizing, and successful recovery (includes Asset, Inventory & Configuration Management).

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

Security, Salvage and Recovery protects your assets and repairs your damaged site in preparation for returning to normal production operations.

Supply Chain Management to guaranty delivery of supplies and materials to the appropriate location.

Created by:

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

Overview of our Services

(Part 1 of 2 - Consulting)

We provide Consulting, Compliance, and Personnel Placement Services to assist clients achieve a safeguarded and efficient Business environment that adheres to domestic and international laws and regulations and able to recover business operations within time frame obligations.

Services

Consulting

Project Management

- Project Definition & Scope,
- Goals and Objectives,
- Team identification,
- Team Assignment,
- Team Training,
- Project Plan Creation,
- Project Management & Status Reporting,
- Analysis of Results,
- Improvements and Problem Management formulation,
- Conclusions,
- Recommendations,
- Management Report,
- Management Presentation,
- Lessons Learned,
- Improvements going forward.

Risk Assessments

- COSO Format, including:
  - Internal Environment,
  - Objective Setting,
  - Event Identification,
  - Risk Assessment,
  - Risk Responses,
  - Control Activities,
  - Information and Communications,
  - Monitoring and Reporting,
  - Cost Benefit Analysis.
- Management Report.
- Management Presentation.
- Implementing Management Recommendations and Direction.

Security (Physical / IT)

- Physical Security, including:
  - Workplace Safety & Violence Prevention,
  - Perimeter and Guards,
  - Access Controls,
  - Surveillance & Reporting,
  - Fire Safety Protection,
  - OSHA, OEM, NFPA 1600.
- IT Security, including:
  - Data Sensitivity,
  - Encryption,
  - Access Controls,
  - Vital Records,
  - Backup & Restoration.
  - Data Management Tools,
  - Mirror and Incremental Data Backup / Recovery,
  - ISO 27000 ISMS.

Compliance

Enterprise Resiliency

- Disaster Recovery,
- Business Continuity,
- Emergency Management,
- Enterprise Resiliency & Corporate Certification,
- Business Impact Analysis,
- Contingency & Emergency Command Center,
- Team Selection,
- Team Training,
- Plan Building & Testing,
- Documentation,
- Training and Awareness,
- Support and Maintenance,
- Version & Release Management,
- Security, Salvage, and Restoration,
- Insurance and Claims Processing.

Placement

Productivity Optimization

- Organizational Structure,
- Systems & Workflow Management,
- Forms Management,
- Functional Responsibilities,
- Job Descriptions,
- Employee Assistance Programs (EAP),
- SLA / SLR / Contracts,
- Standards & Procedures,
- Personnel Training,
- Problem / Incident Management,
- Change / Enhance Management,
- Version and Release Management,
- Supply Chain Management,
- Protection / Salvage / Restoration of failing site after disaster.

Overview of our Compliance Services

(Part 2 of 2)

We provide compliance services for all domestic and international laws and regulations in order to support Corporate Certification for all countries that the firm does business in. Compliance also includes: Dodd-Frank, Basel II / III, and all OCC regulations and other new laws and regulations as enacted.

Services

Consulting

Compliance

Placement

Sarbanes Oxley

All Public Companies over $75 Million in Revenue:

- Sections 302, 404, and 409
- Risk Assessment
- Checks & Balances
- IT Security
- Systems Development Life Cycle
- Systems Management
- Recovery
- Standards & Procedures
- Documentation & Training
- Support
- Maintenance

Gramm Leach Bliley

All Financial Organizations That possess, process, or Transmit private customer data:

- Risk Assessment
- Responsible Employee Selection
- IT Security
- Oversight of "Service Providers"
- Testing and Monitoring
- Evaluation & Reporting to management
- Standards & Procedures

HIPAA

All Companies that possess, Process, or transmit Electronic Protected Health Information:

- Risk Assessment
- Standards & Procedures
- IT Security
- BCP and DR Planning
- Security Officer & BCP Officer
- Documentation & Training
- Periodic Audits
- Agreement with Business associates to adhere to policies
- Ongoing Testing & Maintenance

The Patriot Act

Terrorism Act to protect Americans from attack:

- Risk Assessment
- Customer Screening Procedures
- Customer Information Program (CIP)
- Protecting Confidentiality, while aiding investigations
- Foreign Intelligence Investigations
- Money Laundering
- Standards & Procedures
- Documentation & Training

EPA / Superfund

Protecting the environment And cleaning up land fills:

- Risk Assessment
- Toxic Materials
- Protect Employees
- Protect people in area
- Waste Removal Procedures
- Standards & Procedures
- Documentation & Training
- Support & Maintenance

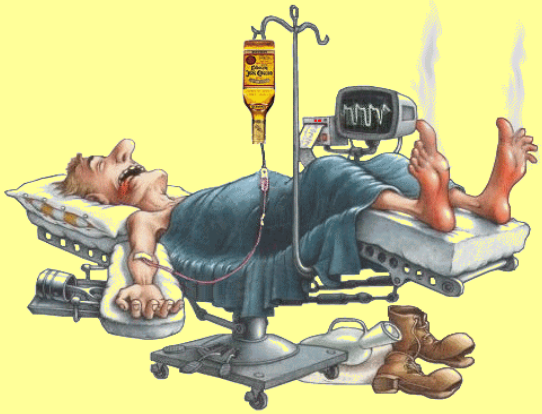
Objectives to be achieved, include:

- **Safeguarded and Optimized Information Technology Environment that complies with all national and international laws and regulations, as required;**
- **Built upon "Best Practices" to insure best of breed standards;**
- **Integrated Systems Development Life Cycle (SDLC), Support and Maintenance procedures that reduce business outages and protect the company reputation;**
- **Systems Management and Controls integration to optimize performance;**
- **Fully Documented environment;**
- **Fully integrated environment, where the everyday functions performed by the staff maintains all documentation in adherence to standards and procedures;**
- **Fully trained staff with career path assistance to ensure loyalty and retention;**
- **Inclusion of clients via Service Level Agreements (SLA), Performance Key Indicators (PKI), or Service Contracts; and,**
- **Ability to respond to disaster situations within the client contracted recovery time objective (RTO).**

Table of Contents:

Abstract – Recovery Management is hard and demanding on management

- 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**?
- Do you 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 access, backup, vaulting, and recovery procedures?
- Can you **recover operations** in accordance to contracted 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 and reduce your pain.

Protecting your Environment

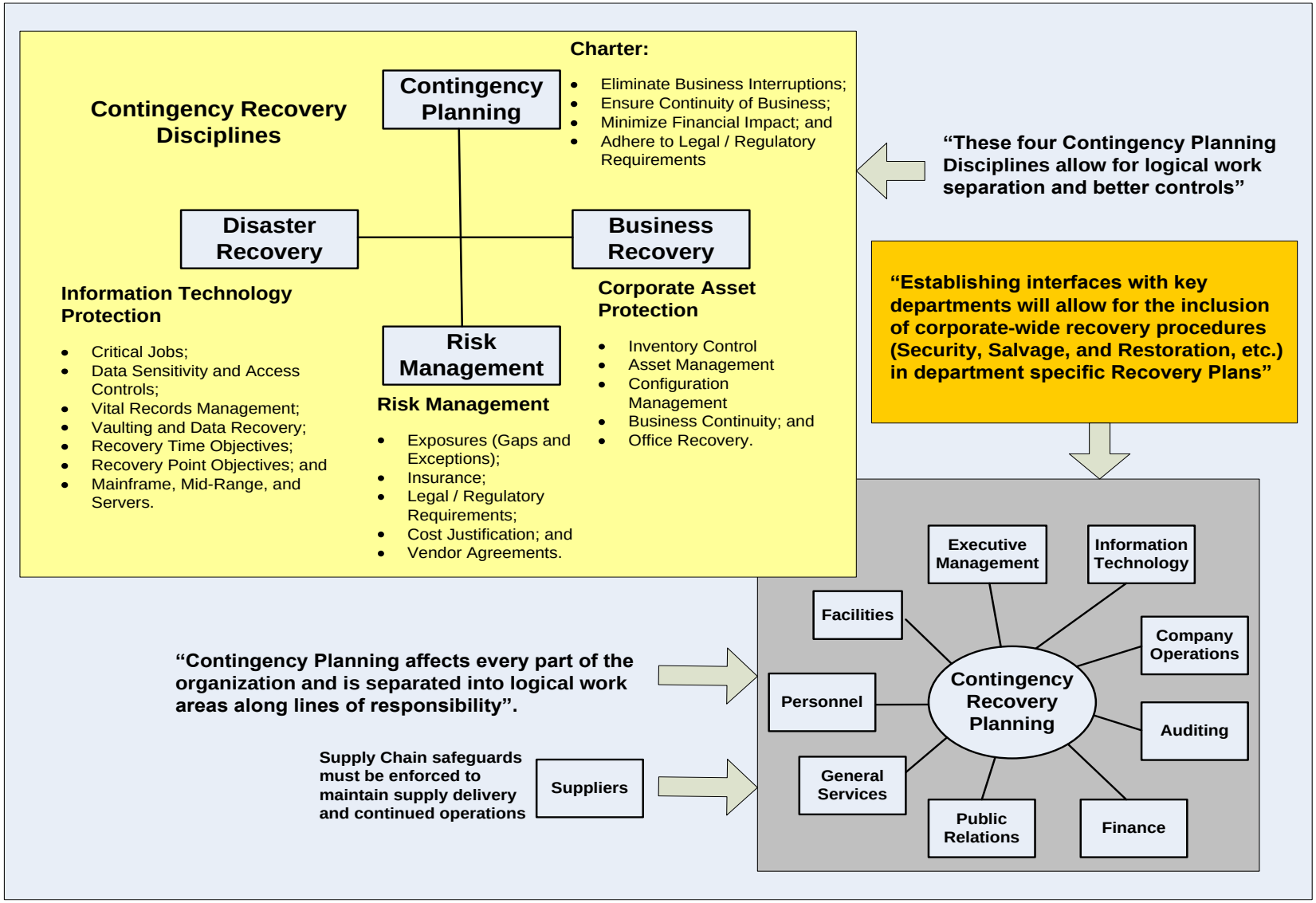
- **Define** your Business Goals and Procedures, including Information Technology;
- **Formulate** Organizational Structure and personnel Functional Responsibilities;
- **Create** Functional Responsibilities, Job Descriptions, and Career Path directions;
- **Develop** Standards and Procedures and other required documentation;
- **Provide** personnel Training and Awareness;
- **Implement** a Systems Development Life Cycle (SDLC);
- **Define** Support, Maintenance, and Recovery requirements and procedures;
- **Implement** methods for adhering to required Laws and Regulations, world-wide as needed;
- **Define** and support SLA / SLR and Client Contract requirements;
- **Conduct** periodic Risk Management and Audit Reviews;
- **Respond** to Gaps, Exceptions, and Obstacles impeding production / recovery objectives;
- **Implement** an Emergency Operations Center (EOC) organizational structure ("War Room");
- **Achieve** Enterprise Resiliency and Corporate Certification to optimize recover and compliance requirements, both domestically and internationally;
- **Utilize** industry "**Best Practices**" to achieve goals and objectives and guaranty results;
- **Utilize Automated Tools** and the latest technologies to support goals and objectives;
- **Create** Recovery Plans and procedures, while periodically testing and improving plans;
- **Integrate** Recovery Operations within the everyday functions performed by personnel so that recovery operations is synchronized with Version and Release Management;
- **Communicate** with government, local business community, and media when disasters occur;
- **Achieve** an efficient and compliant environment that best supports business objectives and protects / enhances the company reputation.

Objective of our Offering

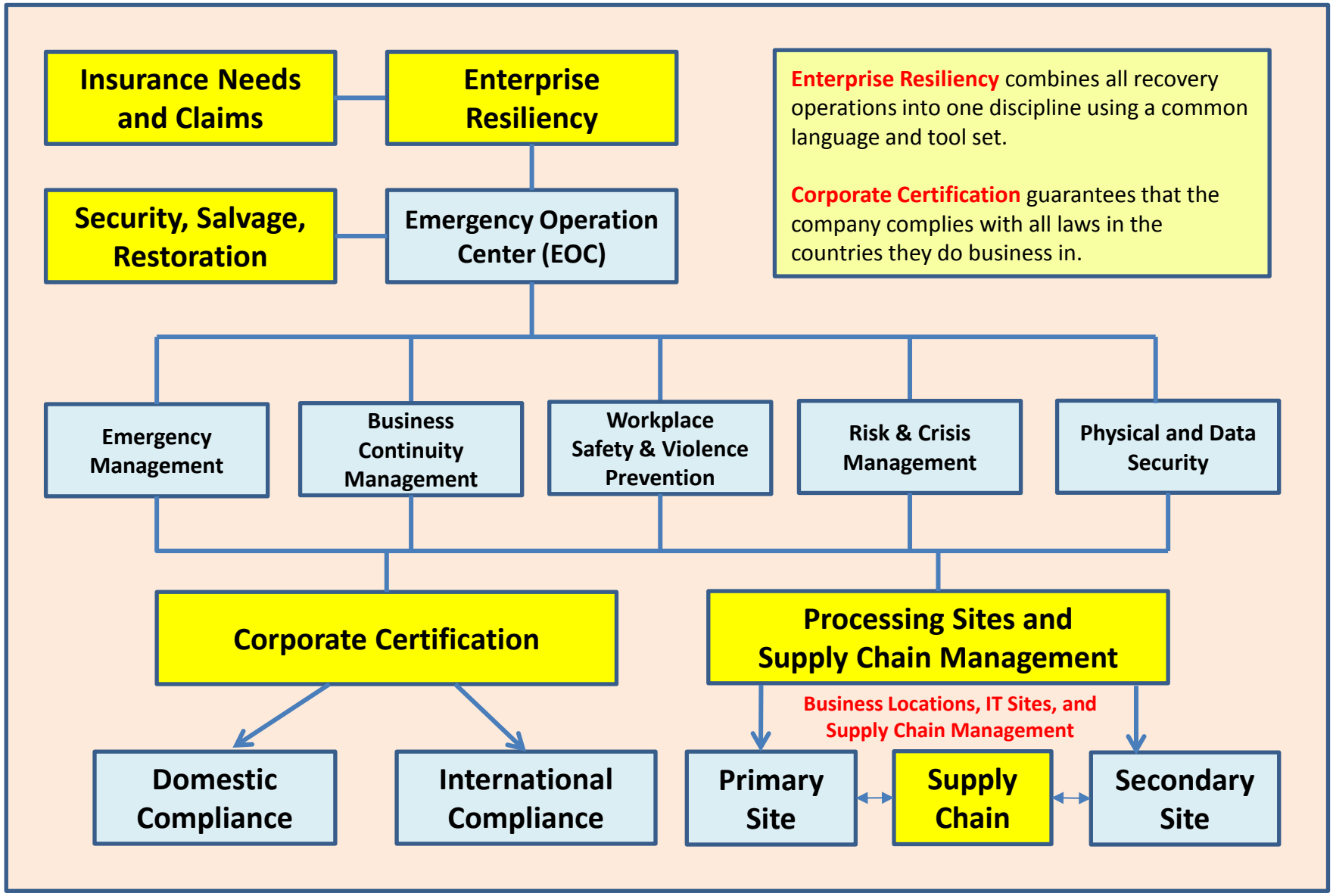
("protecting a Chick in an Alligator Nest")

- Help management protect their business and reputation;
- Provide a single source to help fulfill / manage recovery and insurance needs;
- Review existing recovery and insurance profile;
- Review existing Workplace Safety and Violence Prevention procedures;
- Achieve corporate support for service delivery and recovery time objectives;
- Use "Best Practices" to achieve compliance and recovery operations;
- Help develop and implement recovery operations (all disciplines into one);
- Assist management achieve a safeguarded and compliant environment;
- Improve insurance profile to gain better financial protection;
- Integrate recovery operations within everyday functions performed by staff; and,
- Provide ongoing support and maintenance of recovery and insurance safeguards.

Business Continuity Management Disciplines and Integration

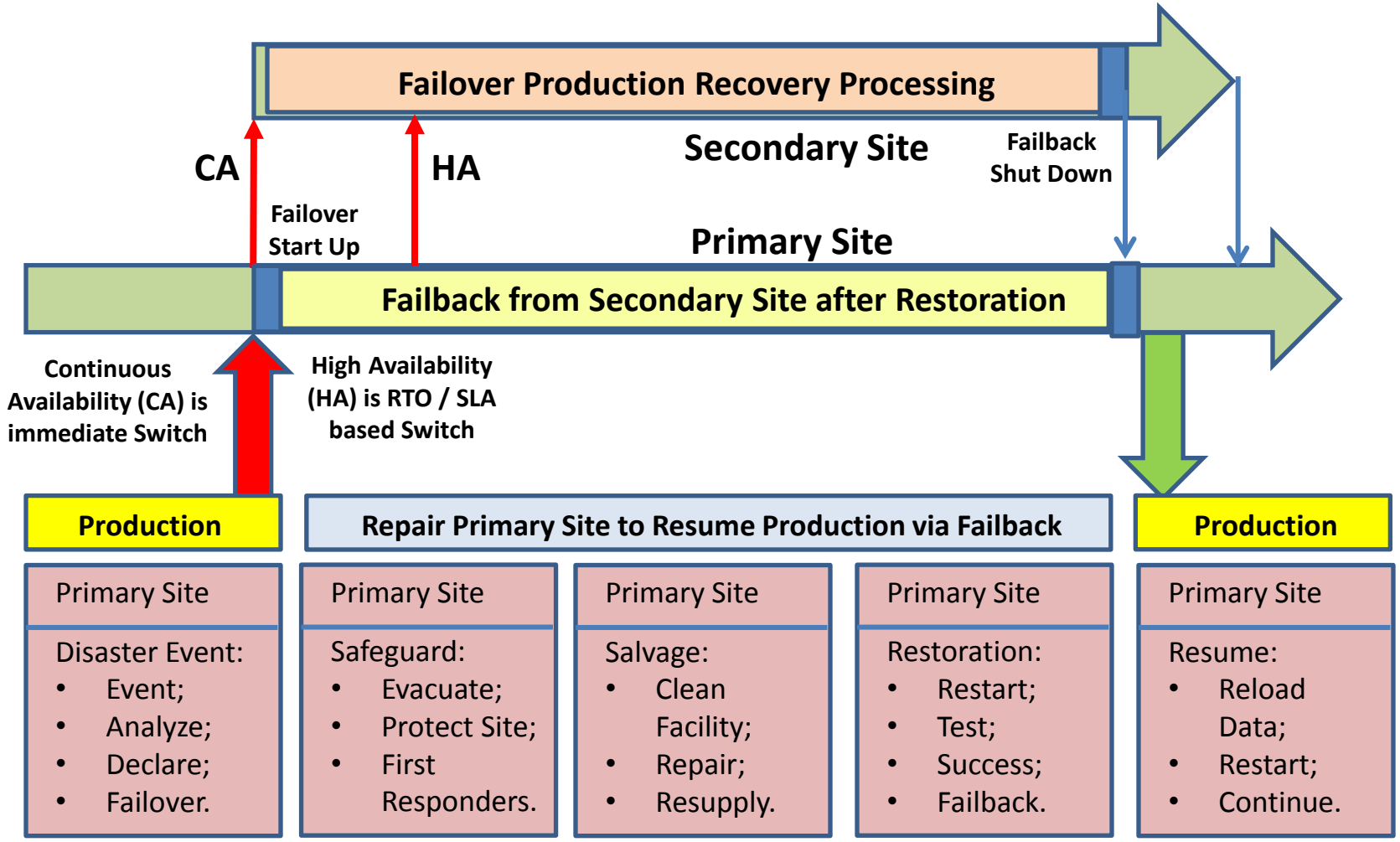


Enterprise Resiliency and Corporate Certification



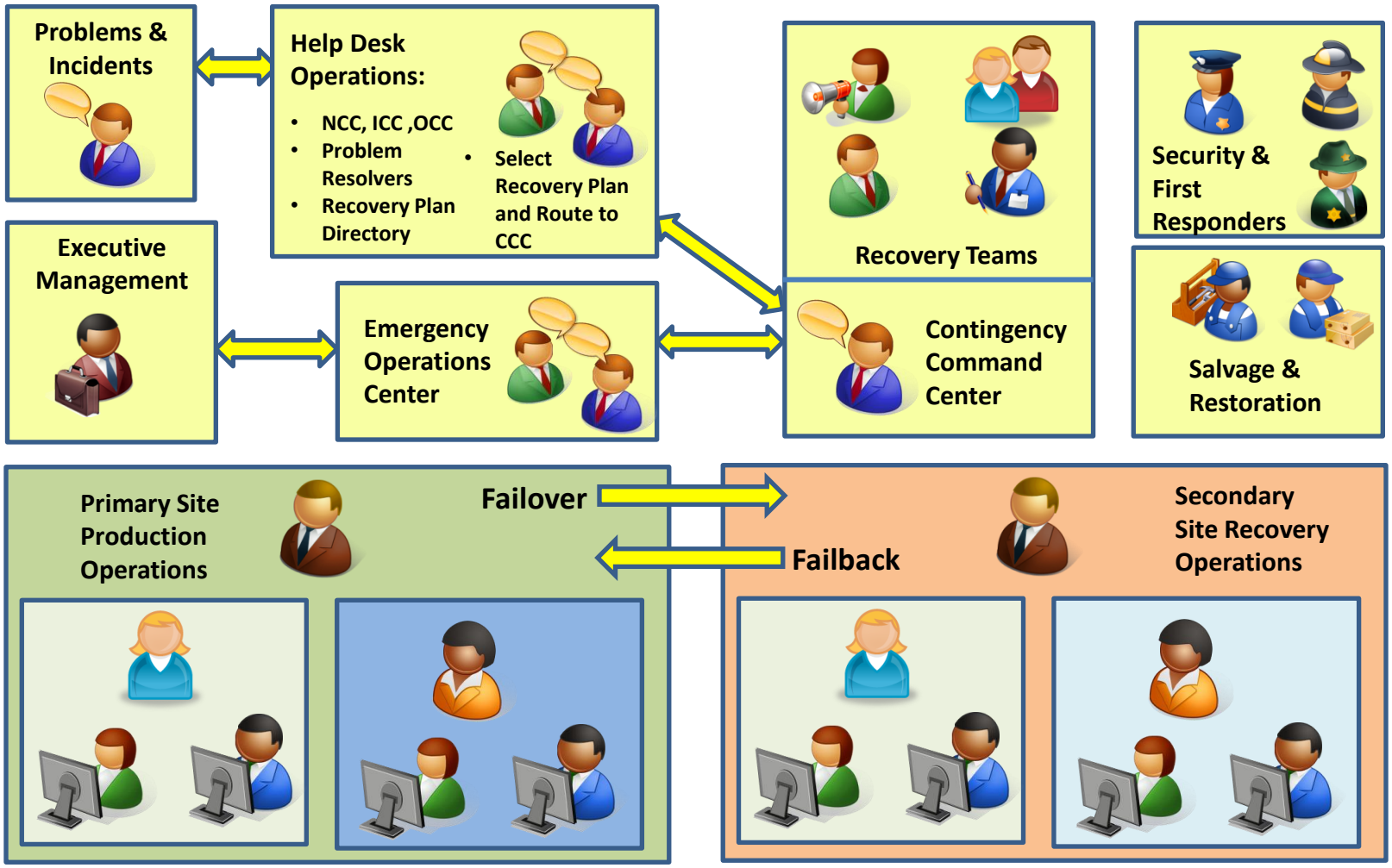
Lifecycle of a Disaster Event (Why we create Recovery Plans)

"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"



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."



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**) and Client Contracts;
4. Guaranty **Data Security and Recovery (RTO** / **RPO)** objectives;
5. **Protect Personnel** through Physical Security and a Workplace Safety;
6. Utilize **"Best Practices"** to achieve goals;
7. Achieve "**Zero Downtime**" through "**Certified Recovery"** via Failover / Failback for HA (High Availability) applications and Flip / Flop for "**Gold Standard Certification"** of CA (Continuous Availability) applications;
8. **Integrate Enterprise Resiliency and Corporate Certification World-Wide;**
9. **Update Documentation** and adhere to **Version and Release Management;**
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** and **Business Impact Analysis** 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 Specific Risks;
- Develop documentation, **awareness, and training** materials; and
- Provide **Support and Maintenance** going forward.

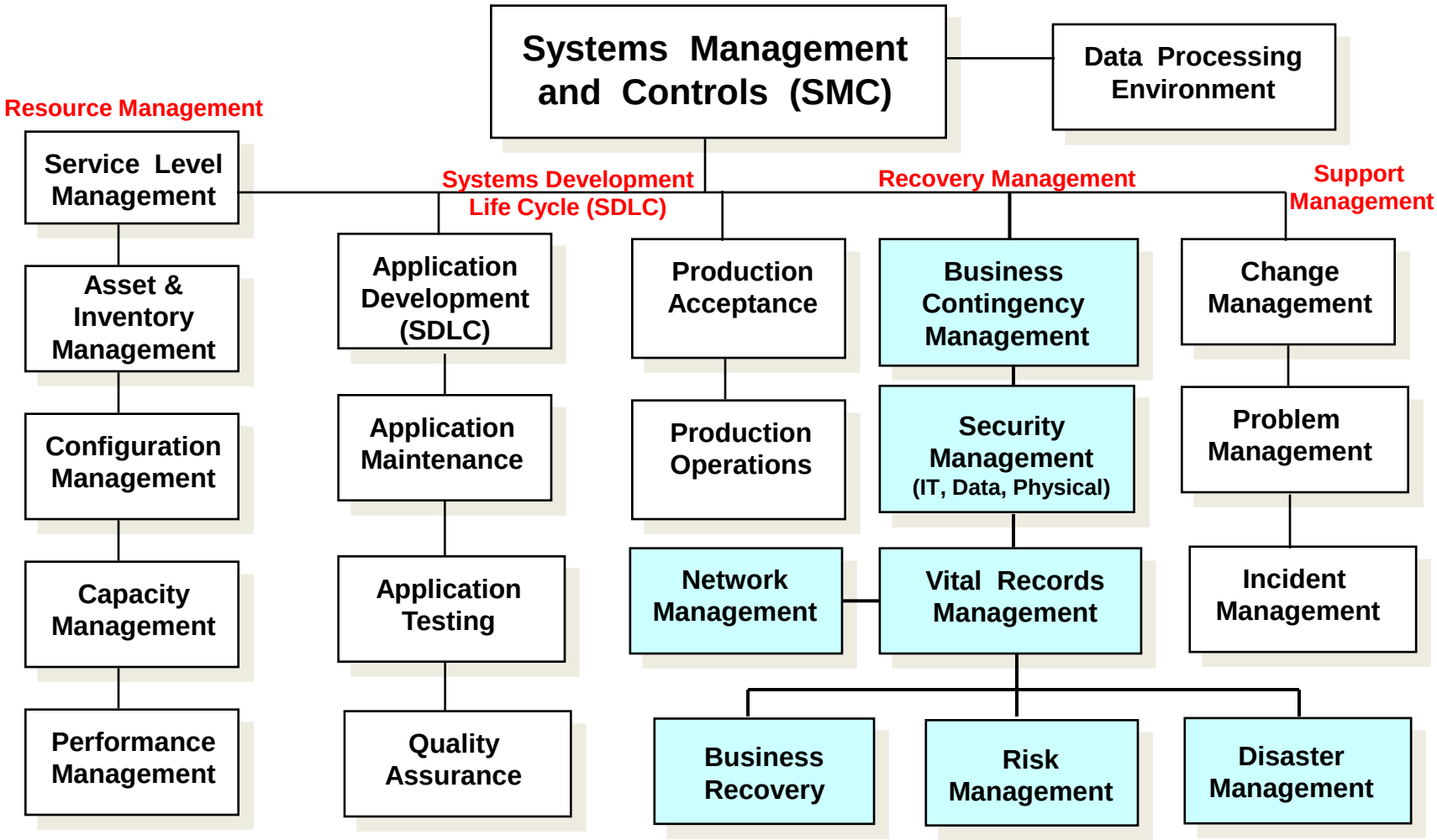
Establishing the Recovery Management process

- Formulate Recovery Management Business Plan and obtain strong Management Support to implement and maintain the recovery management process;
- Identify Stakeholders and Participants, form teams and orientate personnel;
- Develop a Project Plan, with resources, delivery dates, costs, and reporting;
- Define Recovery 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;
- Provide documentation, training, and awareness on recovery plans;
- Create, Test, Certify, and Implement Recovery Plans;
- Integrate Recovery Management, fully document, and Train Staff; and,
- Support and Maintain Recovery Management going forward.

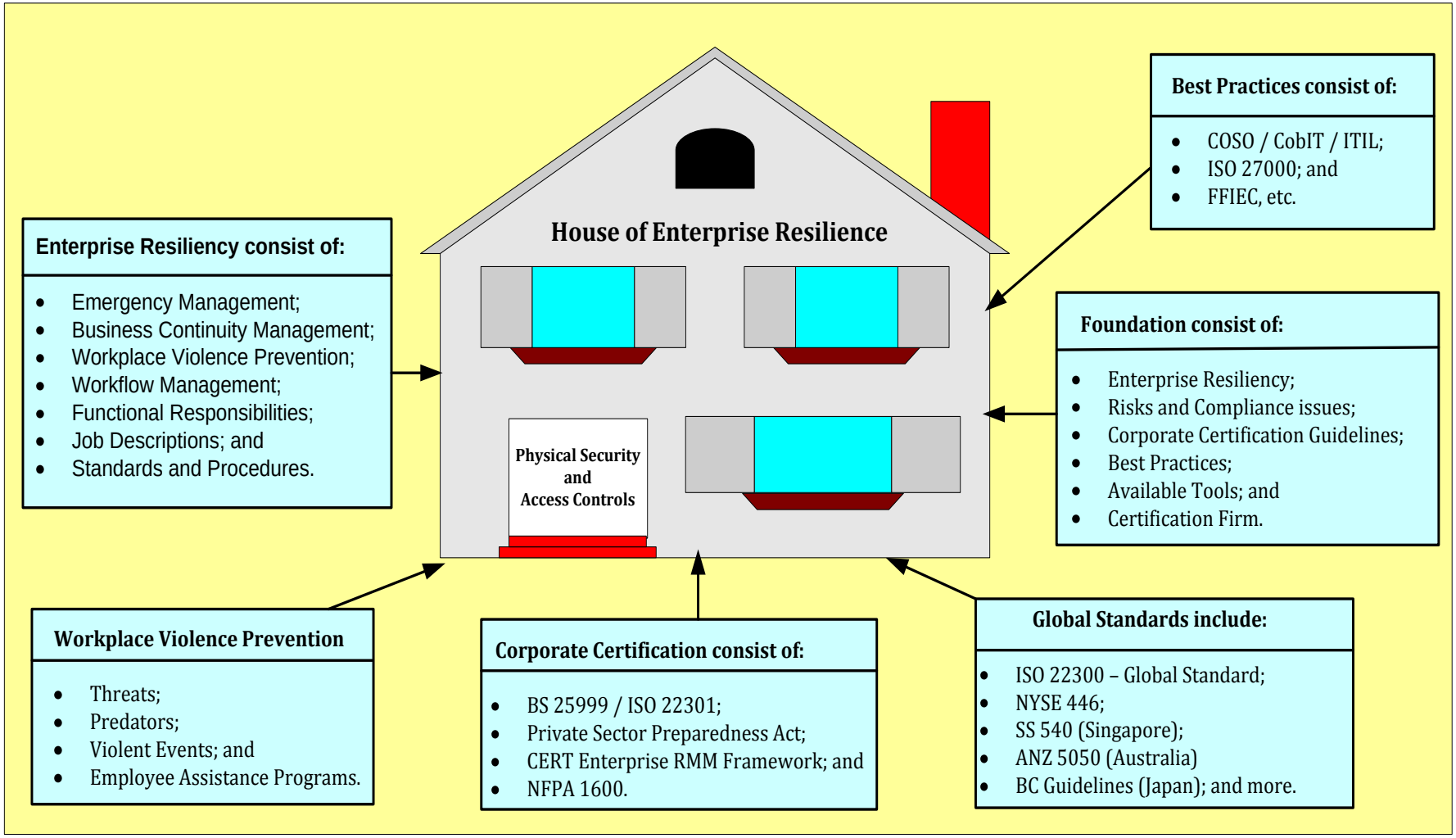
Achieving Enterprise Resiliency and Corporate Certification

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; and,
9. Provide ongoing Support and Maintenance.

Systems Management Organization



Enterprise Resiliency must be built upon a Solid Foundation



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.

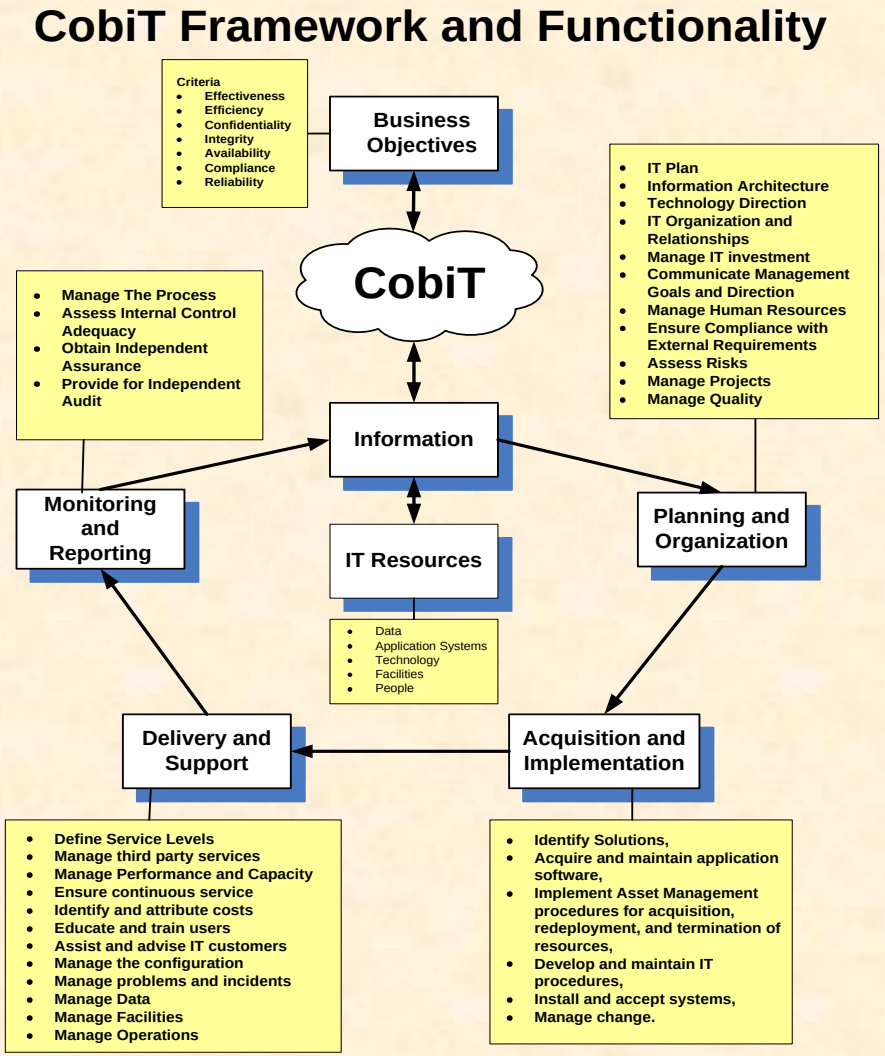
Employee awareness training, support, and maintenance going forward.

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.



ITIL V3 Overview

Information
Technology
Infrastructure
Library (**ITIL**)

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)

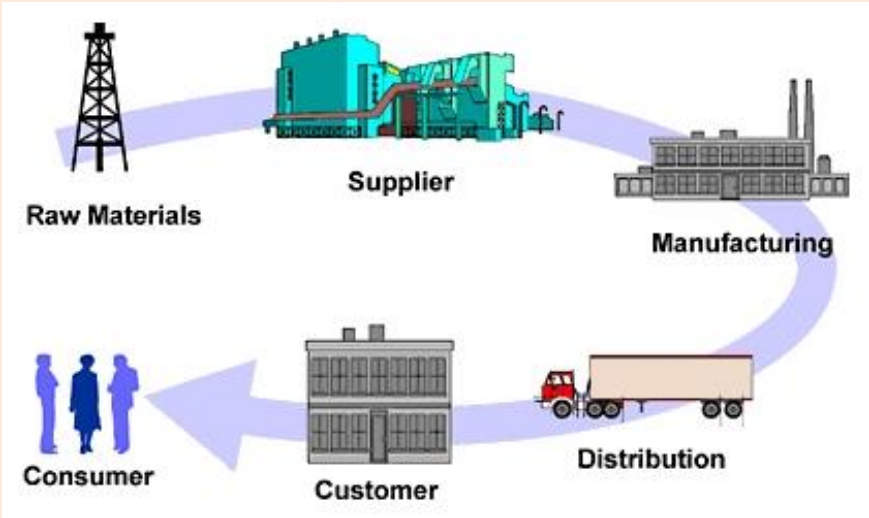
2. **Service Design**
   - Service Catalogue Management
   - Service Level Management (**SLA / SLR**)
   - Risk Management (**CERT / COSO**)
   - Capacity and Performance Management
   - Availability Management (**SLA / SLR**)
   - IT Service Continuity Management **(BCM)**
   - Information Security 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

Supply Chain Management Physical Environment

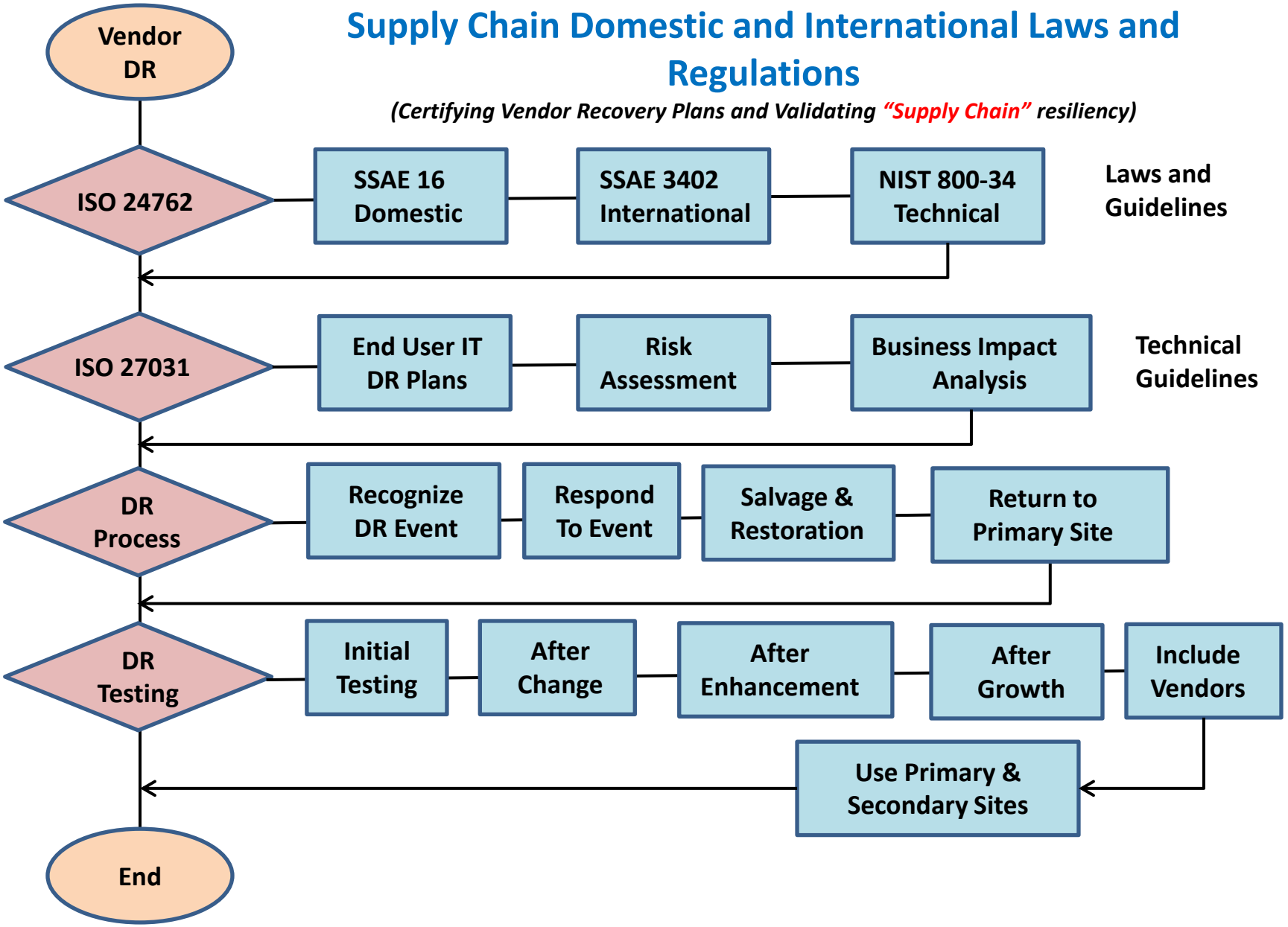
- Supply Chain has international connections where raw materials are collected and manufacturing achieved.
- Materials are transported to domestic market via ships, planes, and other means.
- Materials are delivered to suppliers and distributors who then deliver products to end clients.
- End client must be informed of supply chain interruptions so that alternative suppliers can be obtained.



- Customer must have secondary plans to address the loss of raw materials, suppliers, manufacturing, distribution, and delivery to customer locations.
- If disasters occur that require customer to mover to secondary site, then supplier must be able to continue to supply materials at the same rate as the original site.
- All "Single-Points-Of-Failures" in Supply Chain must be identified and alternatives created to protect business continuation.
- National and International laws and regulations help achieve supply chain protection.

Supply Chain Domestic and International Laws and Regulations

(Certifying Vendor Recovery Plans and Validating "Supply Chain" resiliency)



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?

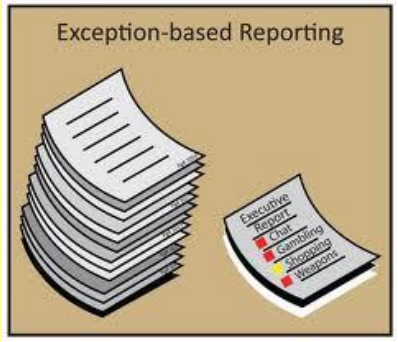
Laws and Regulations concentrate on the VALIDITY of PROVIDED DATA, so we start with a review of how sensitive data is described, created, protected, and used, including:

- **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.

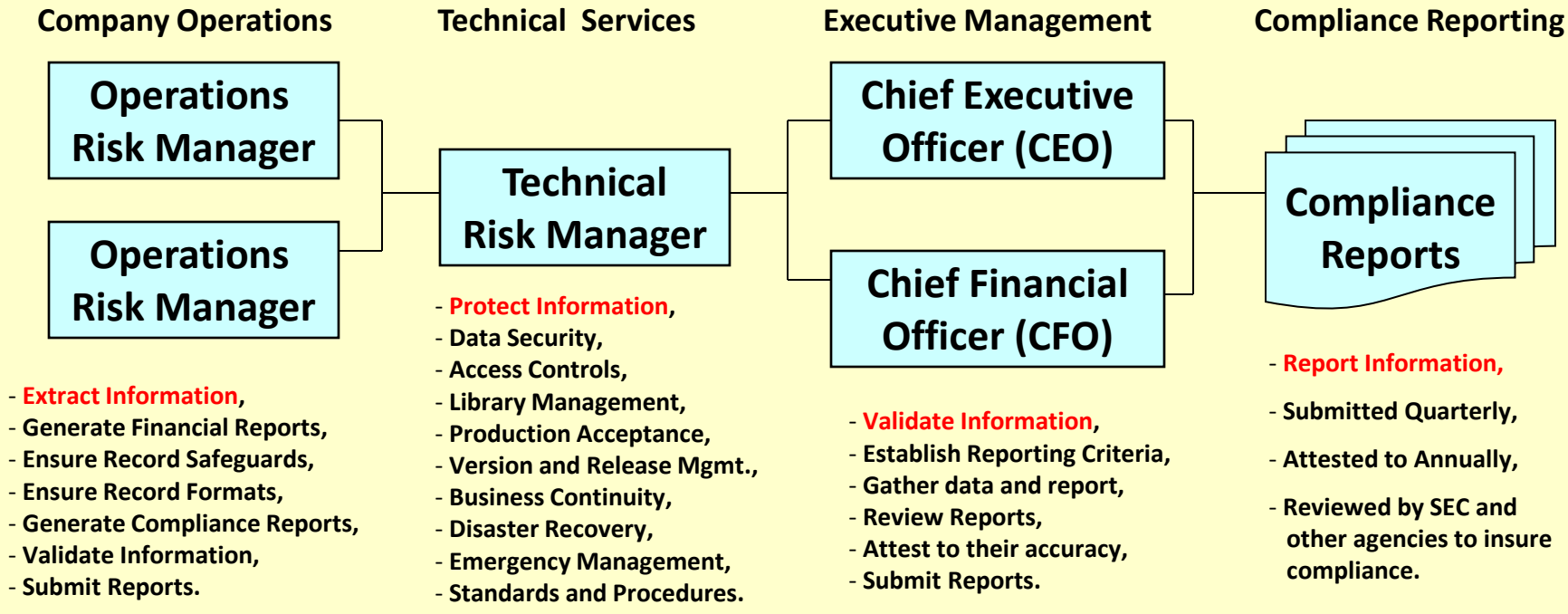
Strategies for Eliminating Audit Exceptions

- 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.

How reporting is accomplished

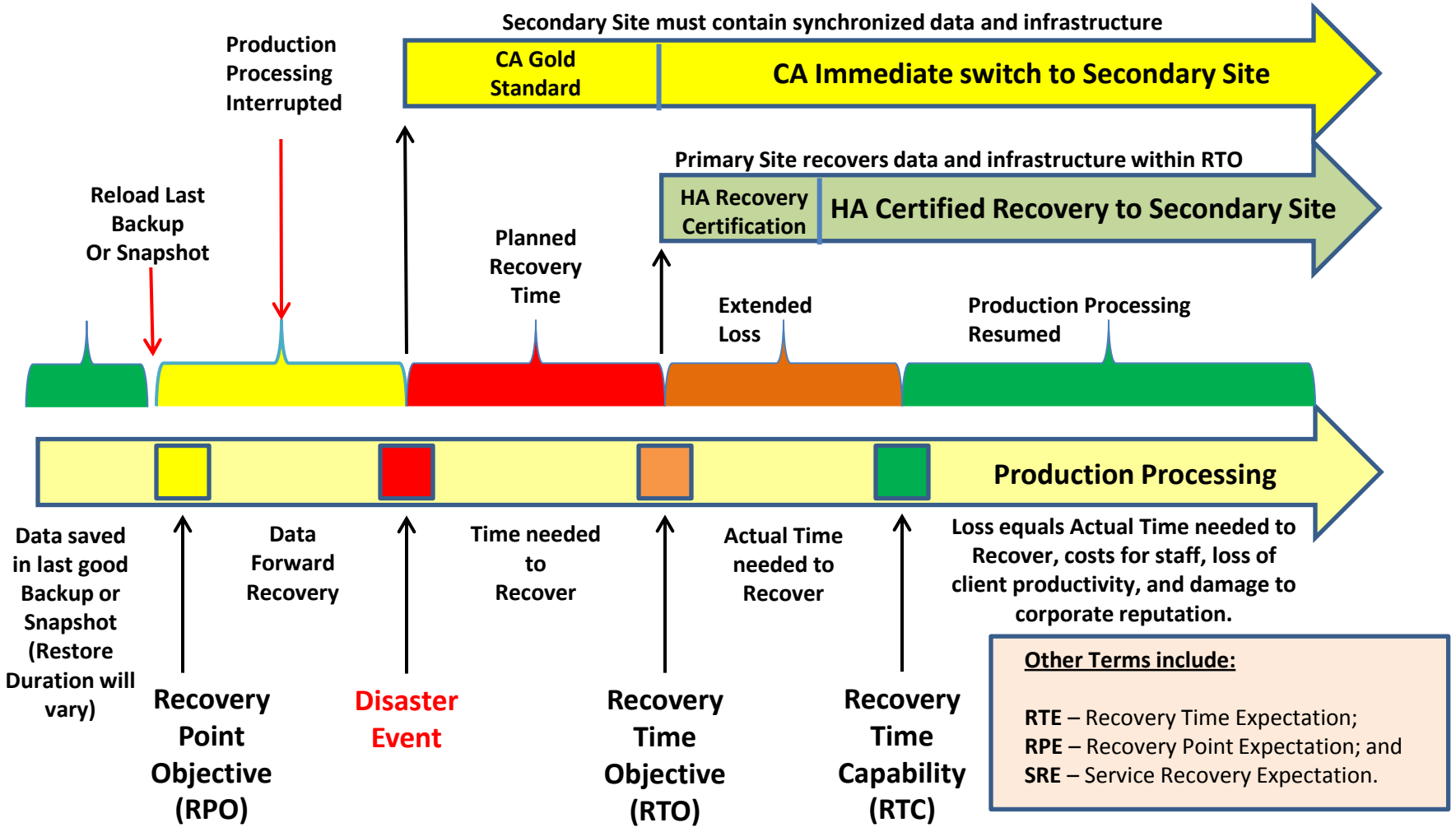


Section 404 of the Sarbanes-Oxley Act (SOX) says that publicly traded companies must establish, document, and maintain internal controls and procedures for Financial and Compliance reporting. It also requires companies to check the effectiveness of internal controls and procedures for Financial and Compliance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

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



Optimized Data Protection / Recovery 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

Continuous DR Replication

Real **backup tapes** can be created directly from the VTL.

Off-Frame Copy

VTL Backup

Tape Copy

Primary Storage

CDP journal

2:34:59

2:34:58 ...

Snapshots

Consistent off-frame recovery
- 2:00pm
- 3:00pm
- 4:00pm
- 5:00pm

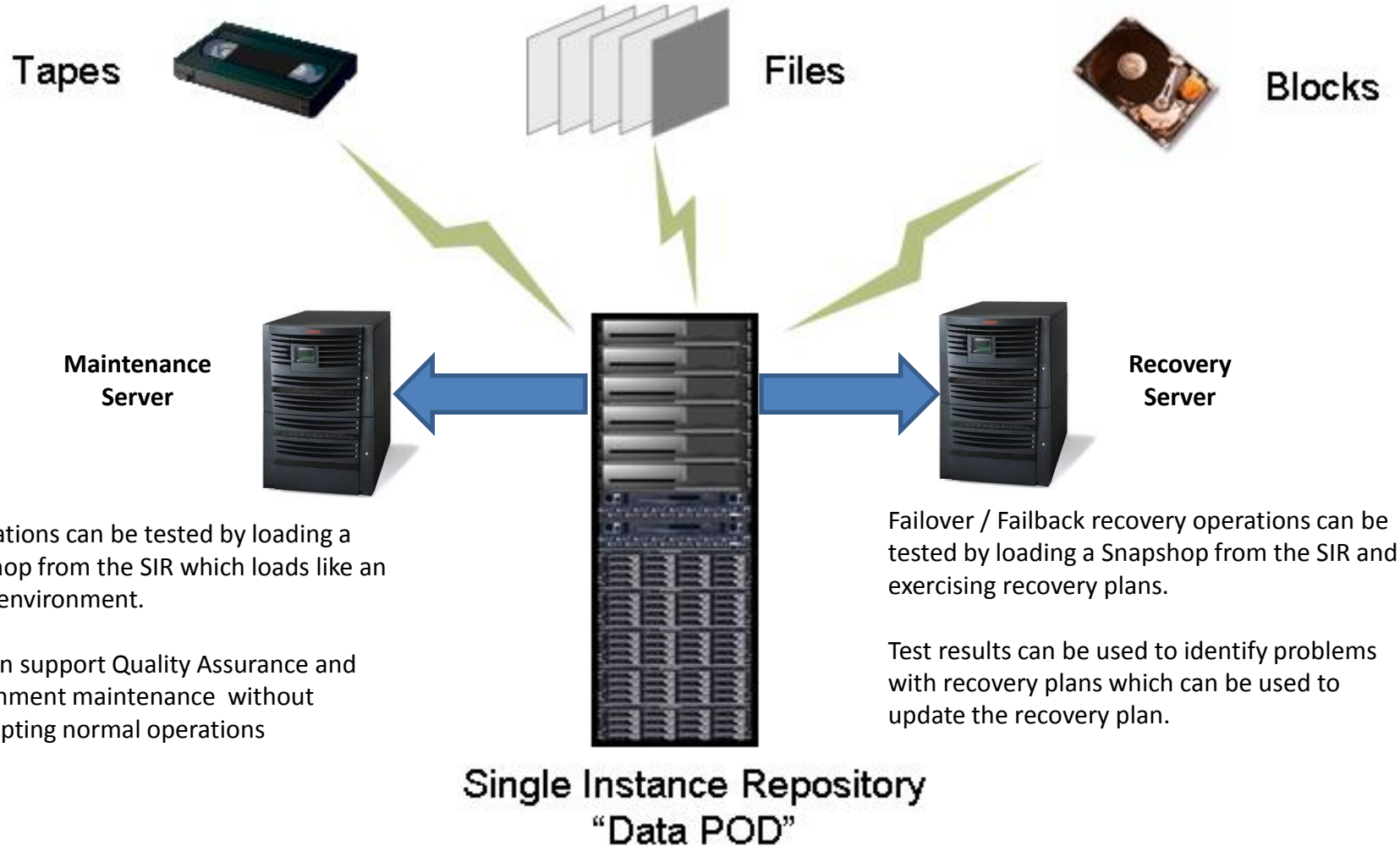
Consistent DR recovery
- 2:00pm
- 3:00pm
- 4:00pm
- 5:00pm

Consistent Virtual Tape recovery
- Mon
- Tues
- Wed
- Thurs

Consistent Tape recovery
- Jan
- Feb
- Mar
- Apr

Seconds | Days | Days | Months | Years

Data Protection, Maintenance, and Recovery



Applications can be tested by loading a Snapshop from the SIR which loads like an active environment.

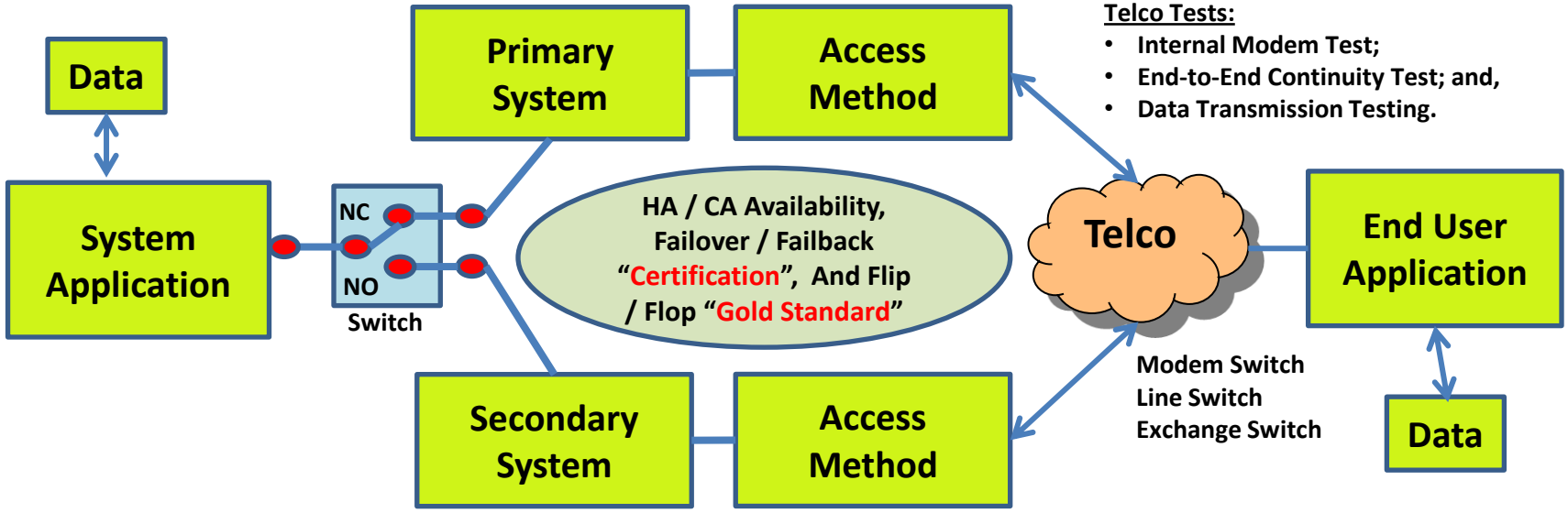
This can support Quality Assurance and environment maintenance without interrupting normal operations

Failover / Failback recovery operations can be tested by loading a Snapshop from the SIR and exercising recovery plans.

Test results can be used to identify problems with recovery plans which can be used to update the recovery plan.

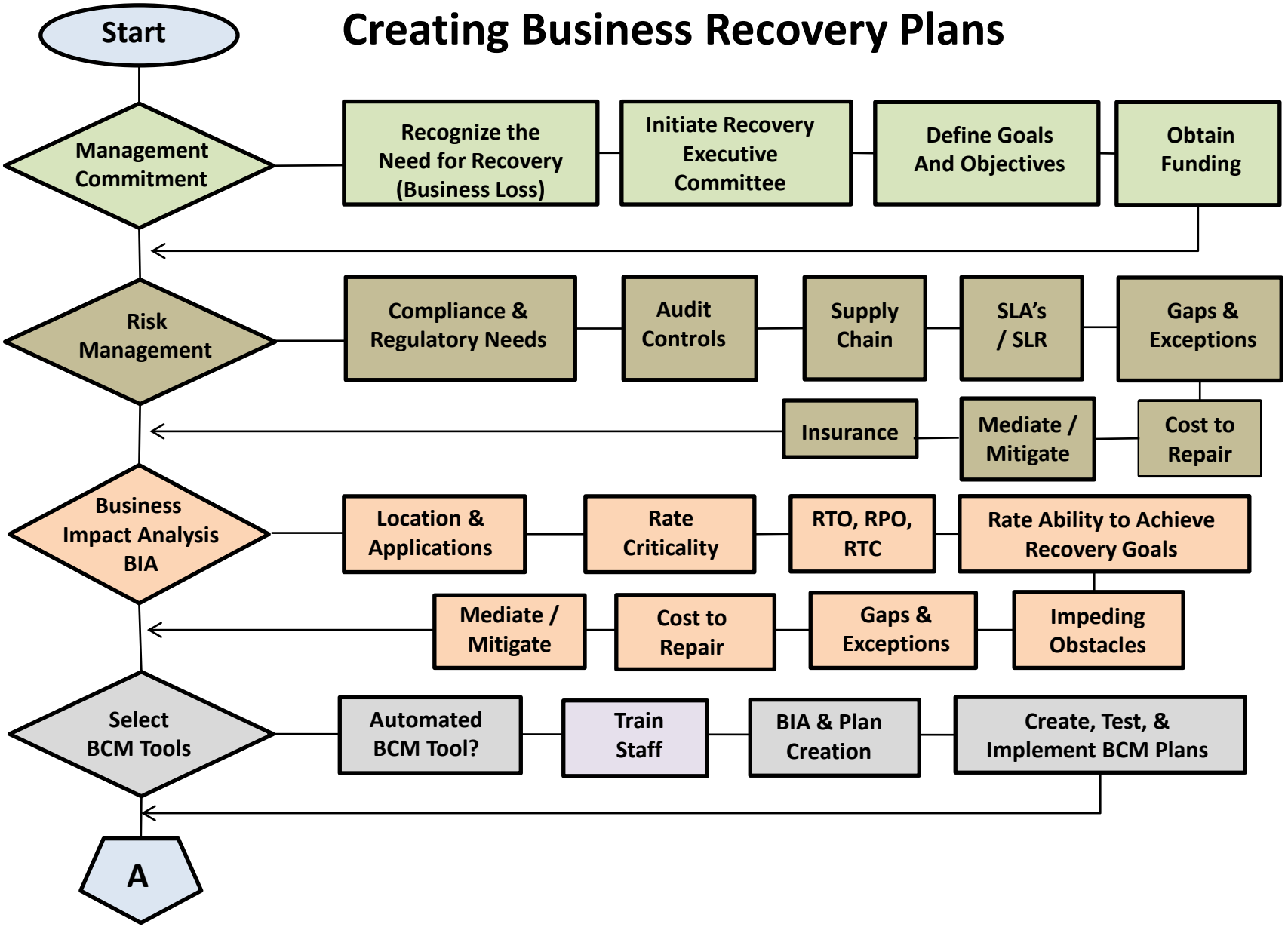
Store and Forward concept for safe data transmission / reception and achieving "Zero Downtime"

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.



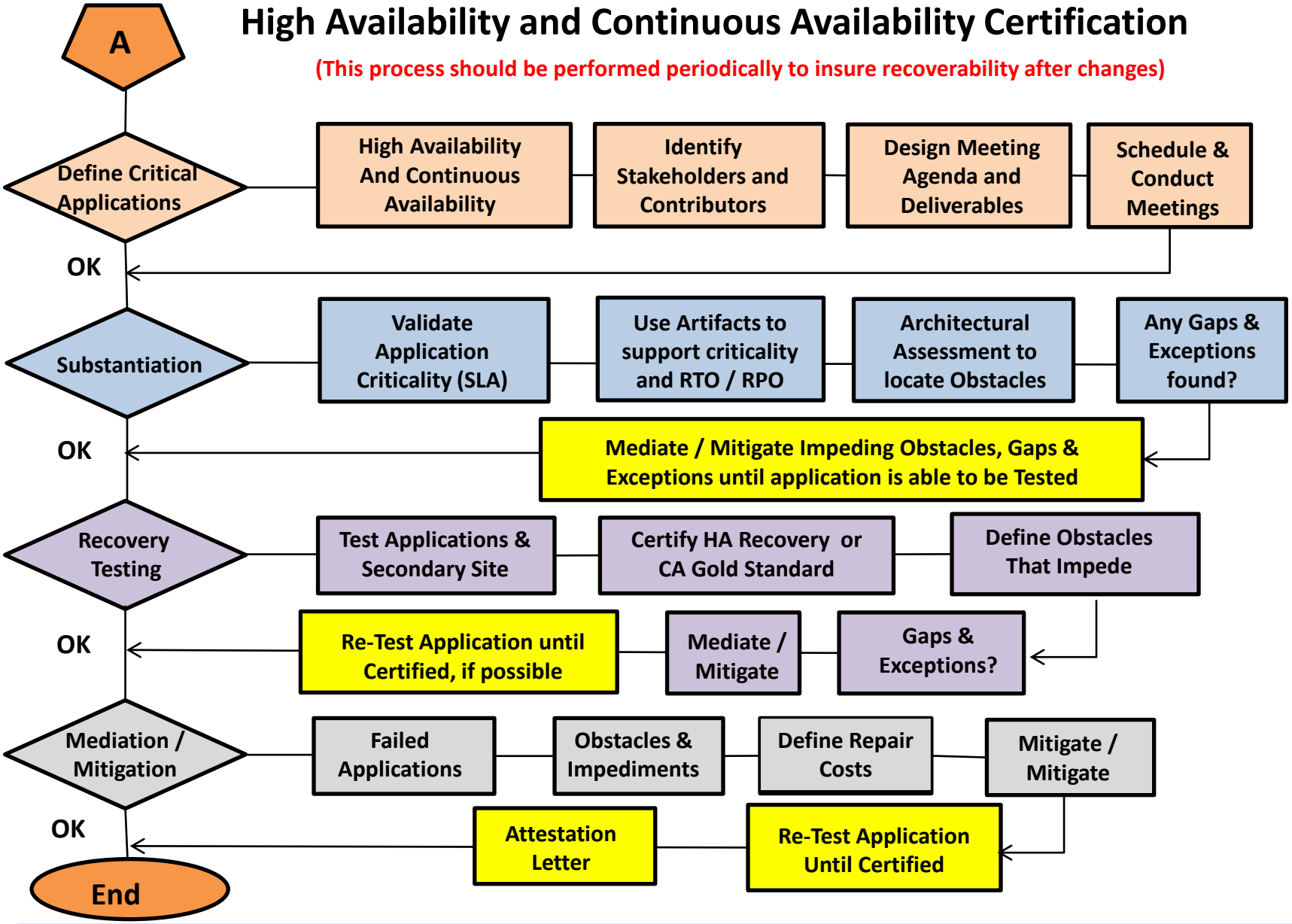
"**Zero Downtime**" can be achieved through "**Recovery Certification**" for HA Applications and "**Gold Standard Recovery Certification**" for CA Applications. Using the "**Store and Forward**" concepts shown here and eliminating any "**Single Points of Failure**" will help you achieve the goals.

Creating Business Recovery Plans

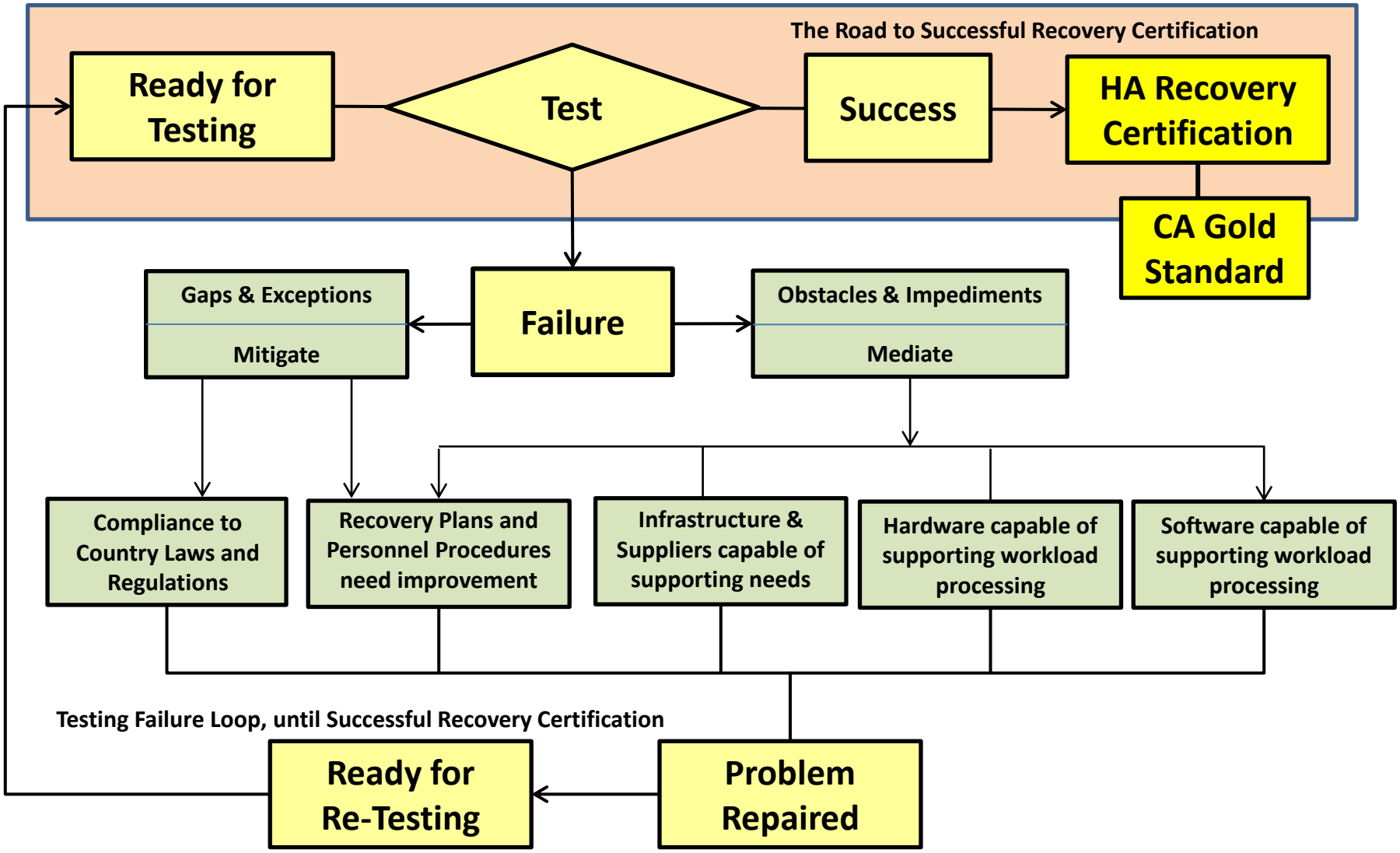


High Availability and Continuous Availability Certification

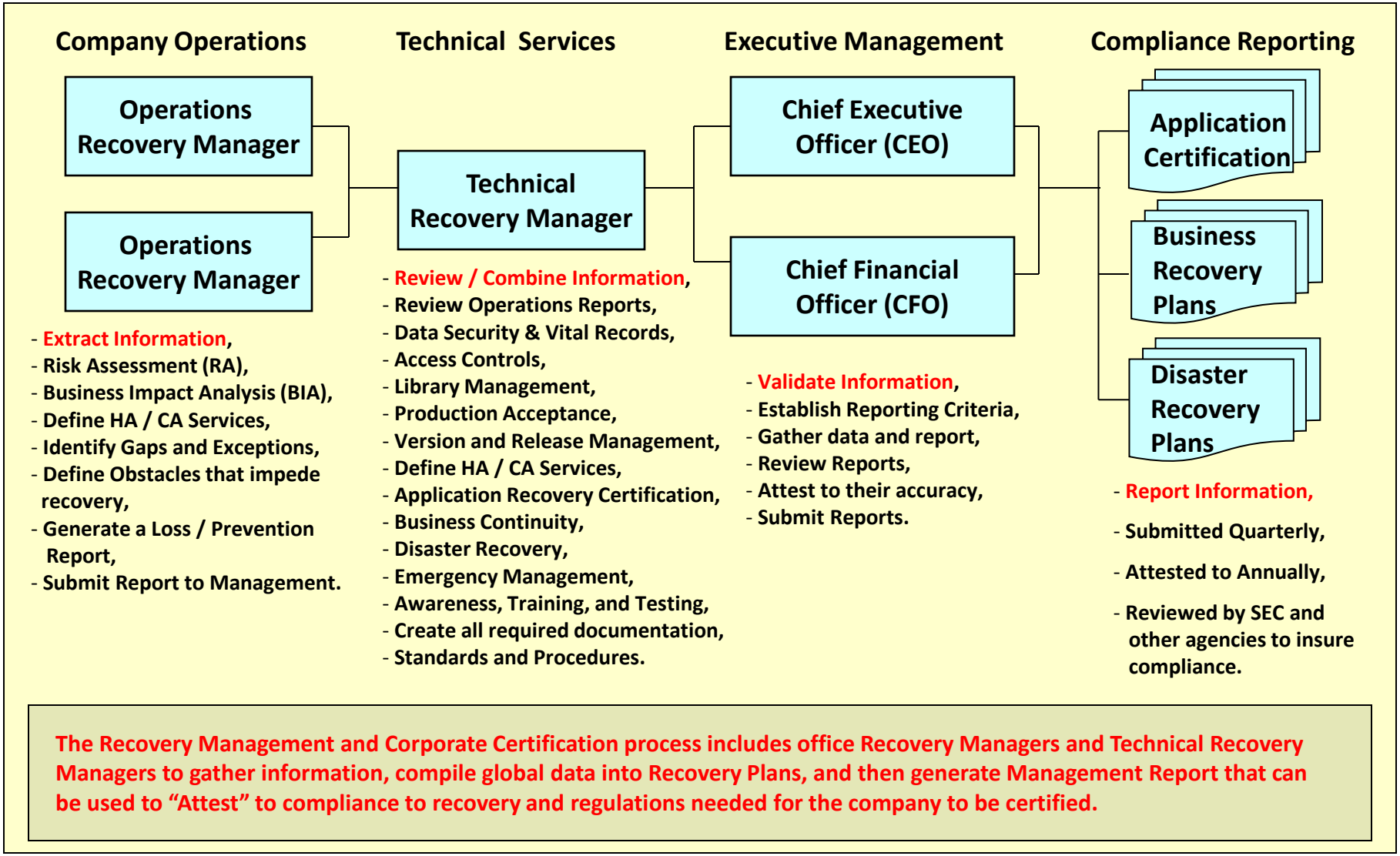
(This process should be performed periodically to insure recoverability after changes)



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

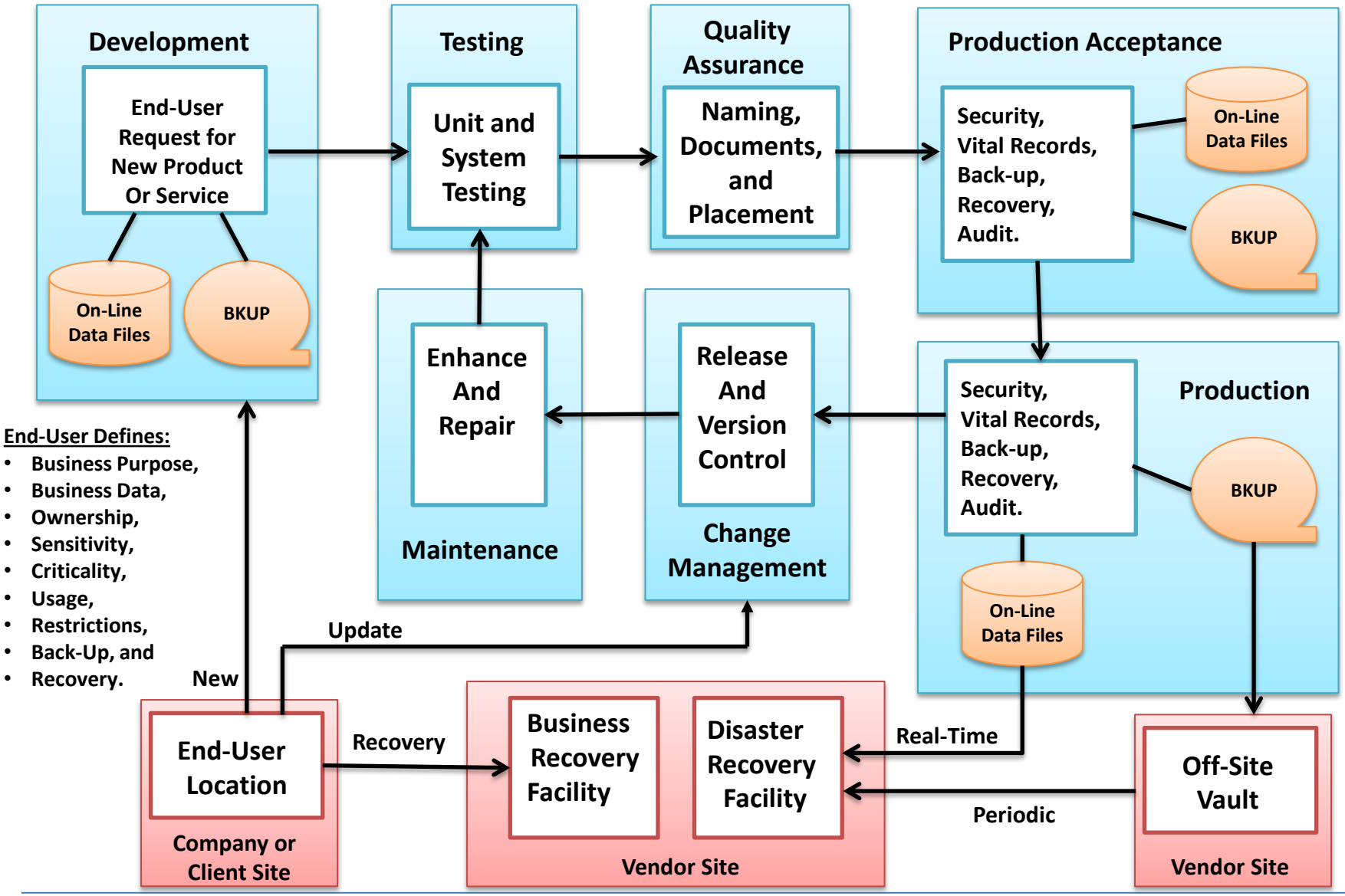


Reporting on Recovery and Certification



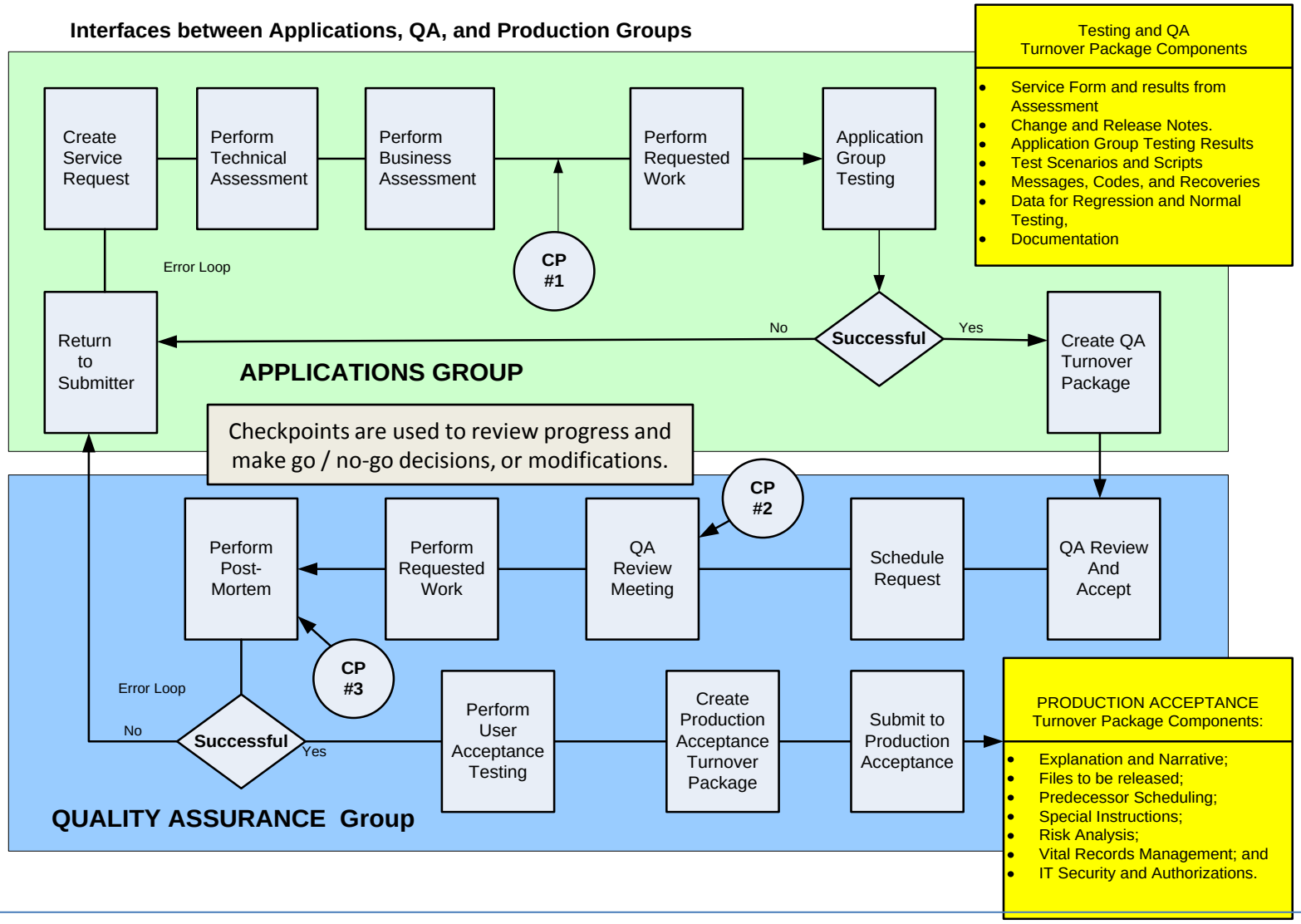
The Recovery Management and Corporate Certification process includes office Recovery Managers and Technical Recovery Managers to gather information, compile global data into Recovery Plans, and then generate Management Report that can be used to "Attest" to compliance to recovery and regulations needed for the company to be certified.

Systems Development Life Cycle (SDLC), Components and flow



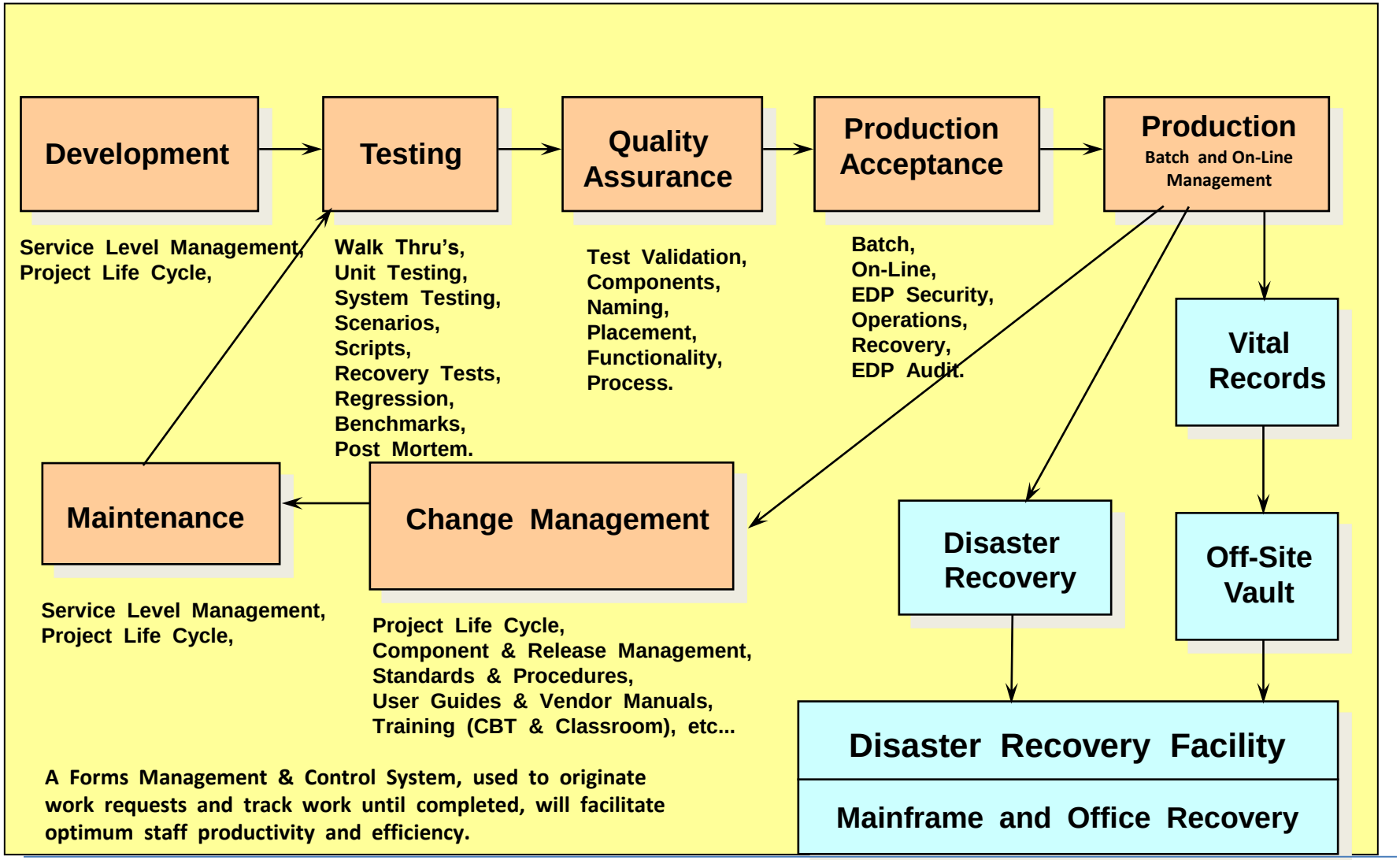
Migrating products / services to the Production Environment

Quality Assurance and SDLC Checkpoints



Systems Management Controls and Workflow

Service Level Reporting, Capacity Management, Performance Management, Problem Management, Inventory Management, Configuration Management.



Job Documentation Requirements and Forms Automation

New Product / Service Development Request Form Life Cycle

Development Request Form

Phase: Date

- User Information _____
- Business Justification _____
- Technical Justification _____
- Build or Buy _____
- Development (Build / Modify) _____
- Test: _____
  - Unit Testing _____
  - System Testing _____
  - Regression Testing _____
- Quality Assurance _____
- Production Acceptance _____
- Production _____
- Support (Problem / Change) _____
- Maintenance (Fix, Enhancement) _____
- Documentation _____
- Recovery _____
- Awareness and Training _____

Documents are Linked to from Date Field

Link to Documents

Documentation

Documentation

Documentation

Documentation

Development:

- Development Request Form Number
- Business Need
- Application Overview
- Audience (Functions and Job Descriptions)
- Business / Technical Review Data
- Cost Justification
- Build or Buy Decision
- Interfaces (Predecessor / Successor)
- Request Approval

Testing:

- Data Sensitivity & Access Controls
- IT Security Management System
- Encryption
- Vital Records Management
- Data Synchronization
- Backup and Recovery
- Vaulting (Local / Remote)
- Disaster Recovery
- Business Recovery

Quality Assurance:

- Application Owner
- Documentation & Training
- Application Support Personnel
- End User Coordinators
- Vendors and Suppliers
- Recovery Coordinators
- Testing Results

Production Acceptance

- Application Setup
- Input / Process / Output
- Messages and Codes
- Circumventions and Recovery
- Recovery Site Information
- Travel Instructions

Main Documentation Menu ***Sub-Documentation Menus***

Information Accounting and Charge-Back System Concept

By utilizing Work Order (WO) and Purchase Order (PO) concepts, it is possible to track and bill clients for their use of Information Technology services associated with development and maintenance services. This concept is presented below:

User Name: _____ User Division: _____ User Identifier _____
Work Order #: _____ Date: _____ For: _____

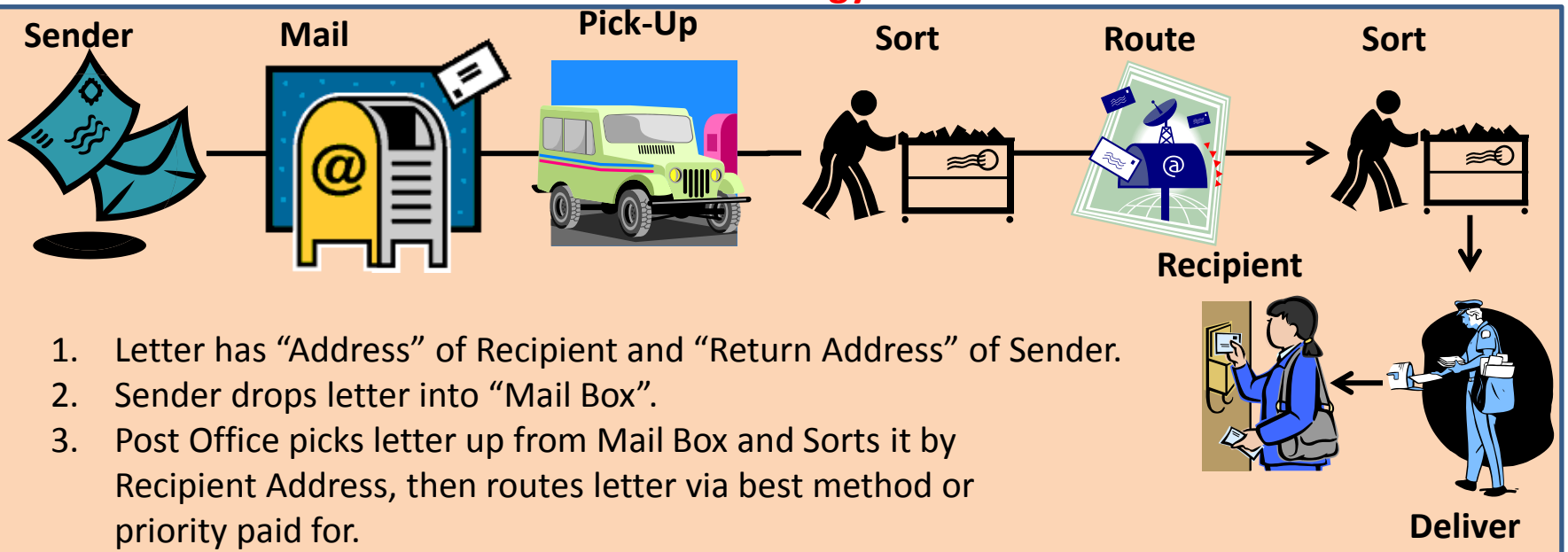
PO for: **Development**	Cost: $ _____
PO for: **Testing**	Cost: $ _____
PO for: **Quality Assurance**	Cost: $ _____
PO for: **Production Acceptance**	Costs $ _____
PO for: **Production (on-going)**	Cost: $ _____
PO for: **Vital Records Management**	Cost: $ _____
PO for: **Asset Management (Acquisition, Redeployment, Termination)**	Cost: $ _____
PO for: **Inventory and Configuration Management**	Cost: $ _____
PO for: **Information and Security Management**	Cost: $ _____
PO for: **Safe Workplace Violence Prevention**	Cost: $ _____
PO for: **Recovery Management**	Cost: $ _____
PO for: **Documentation and Training**	Cost: $ _____
PO for: **Support and Problem Management**	Cost: $ _____
PO for: **Change Management**	Cost: $ _____
PO for: **Version and Release Management**	Cost: $ _____

Total Cost: $ _____

Bill can be generated via Forms Management, Time Accounting, or Flat Cost for Services. This system can be used to predict costs for future projects and help control expenses and personnel time management.

Existing Post Office Mail Pick-up and Delivery System

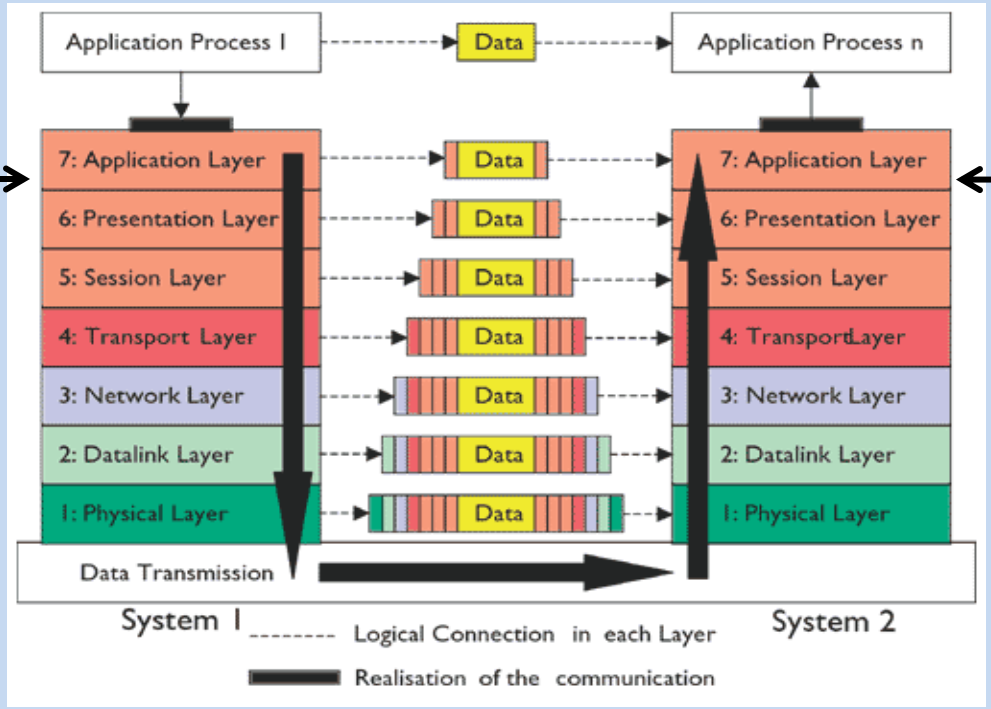
An IT Analogy



1. Letter has "Address" of Recipient and "Return Address" of Sender.
2. Sender drops letter into "Mail Box".
3. Post Office picks letter up from Mail Box and Sorts it by Recipient Address, then routes letter via best method or priority paid for.
4. Letter is resorted at Recipient Post Office and placed into Postman's Route Bag.
5. Postman delivers letter to recipient.
6. Letter is "Returned to Sender" if address is incorrect or refused by Recipient.
7. This example is used as the foundation for the Internet and the Internet Protocol (IP) being used.
8. Internet is currently transitioning from IPv4 (Internet of Things) to IPv6 (Internet of Everything) because IPv4 is running out of addresses (2>32 = 4.3 Billion Addresses, IPv6 2>128 = Unlimited Addresses). This will support more addresses than there are atoms on earth, so you can expect machines of all types to have IP Addresses.

Internet Protocol (IP) Delivery System (Local / Remote)

Sender posts / receives data from Internet via 7 Level Internet Service Communications method.



Internet Protocol (IP) provides a sending and receiving address. IPv4 has 4.3 Billion addresses, which are almost gone, while IPv6 has unlimited Addresses.

Logical Layer

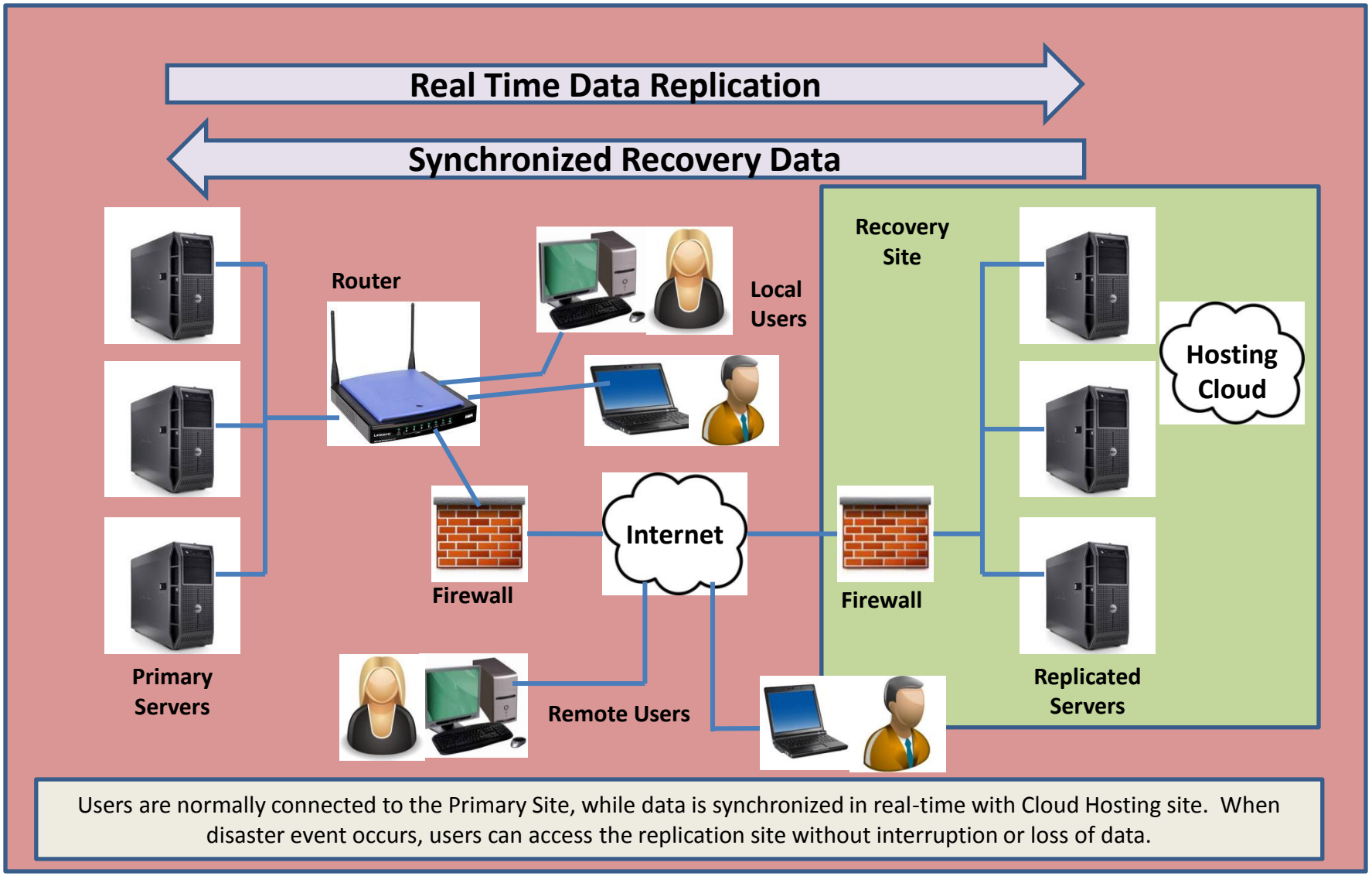
Sender Mail → **Pick-Up** → **Sort** → **Route** → **Sort** → **Deliver** → **Recipient**

From PC to Application Layer (1)

From Application Layer (1) through Presentation Layer (2), Session Layer (3), and Transportation Layer (4) for delivery to receiving site. Process is repeated until message has been successfully sent and received. This is a "Handshaking" operation where Data Packets are sent to receiving site and acknowledged as successfully received (ACK) or not (NAK). Failures are retransmitted until received successfully or an error notification is posted (Layer 5-7).

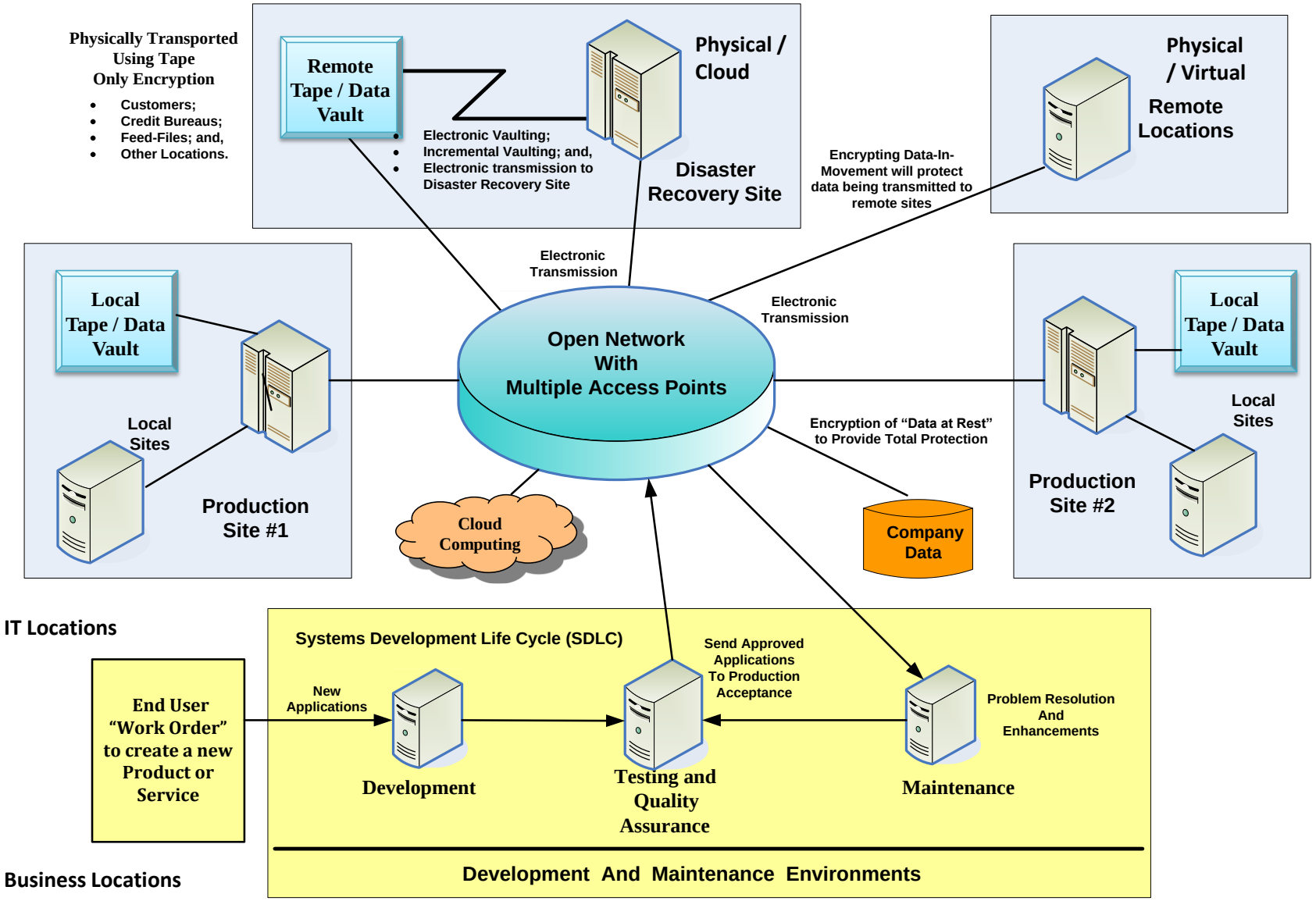
Physical Layer

Data Synchronization and Recovery Operations using Cloud Based Hosting



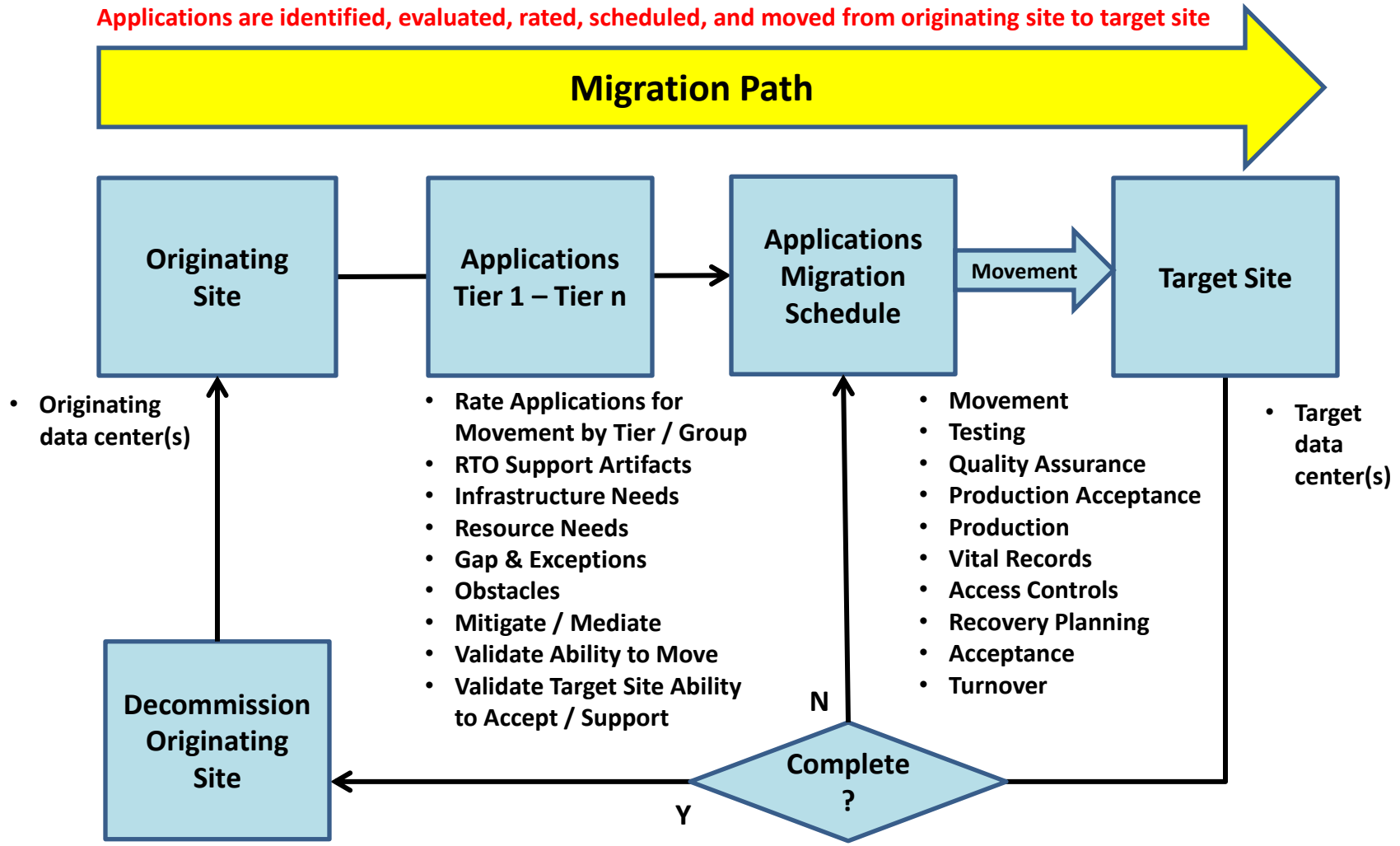
Users are normally connected to the Primary Site, while data is synchronized in real-time with Cloud Hosting site. When disaster event occurs, users can access the replication site without interruption or loss of data.

Overview of the Enterprise Information Technology Environment



Migration Pathway and Goals

(Can apply to Site Consolidations or Recovery Site migrations)



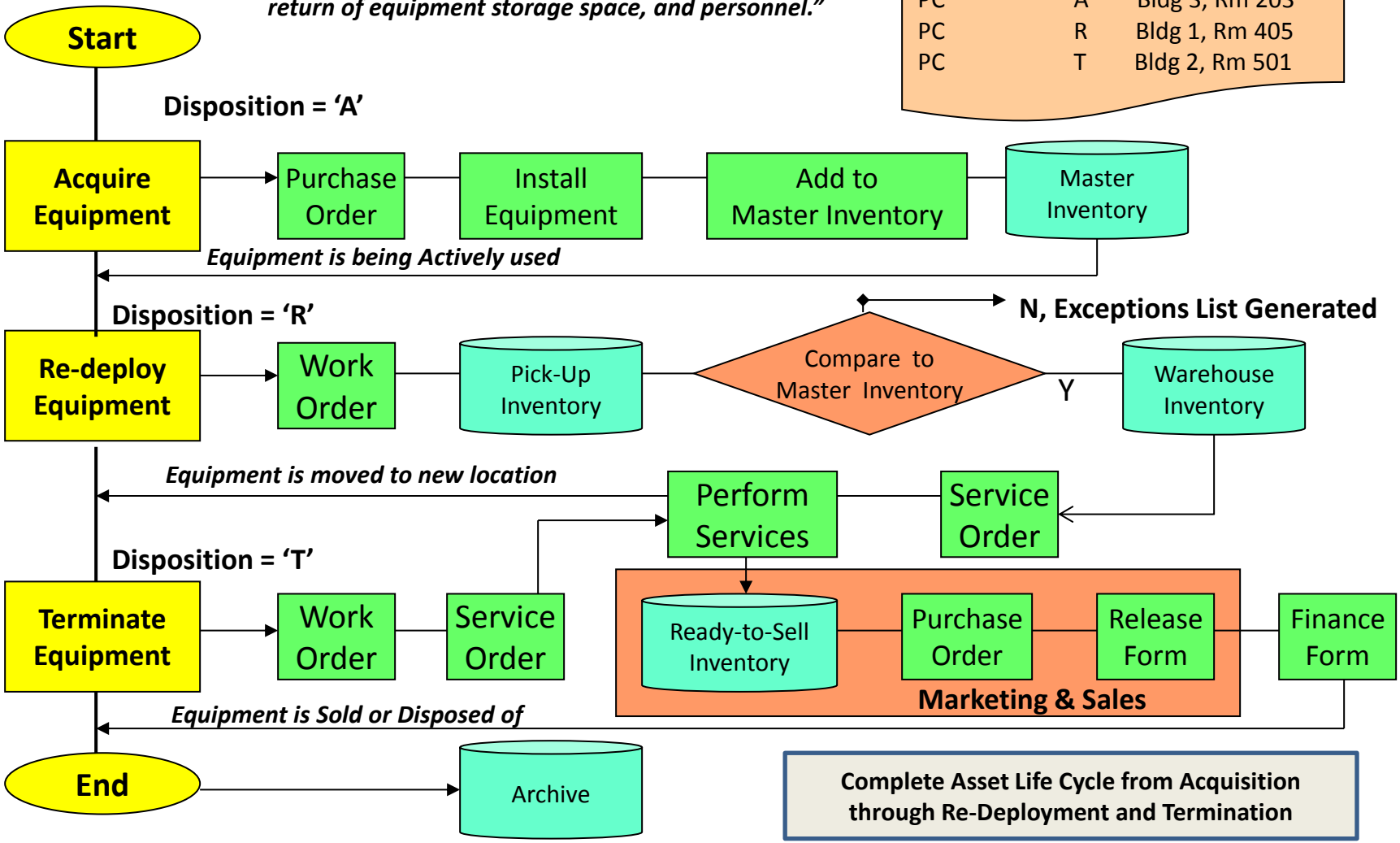
Asset Management Disciplines

Can be sorted by: Equipment Type, Disposition, Date, or Location

"Dispose of Surplus equipment after Migration to Target Data Center(s) to reap profit from sales, return of equipment storage space, and personnel."

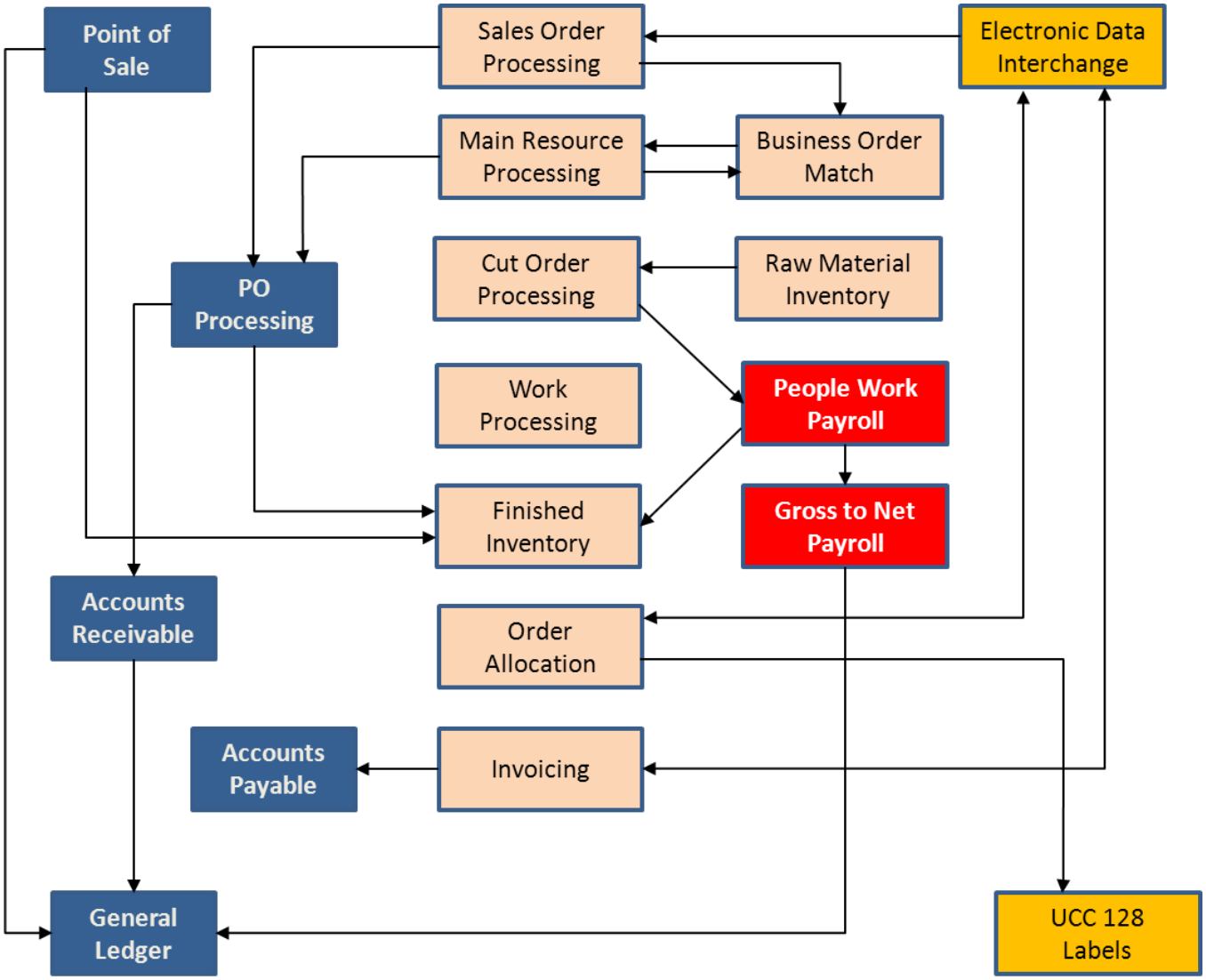
Pick-Up List

Equip. Type:	Disp:	Location:
PC	A	Bldg 3, Rm 203
PC	R	Bldg 1, Rm 405
PC	T	Bldg 2, Rm 501

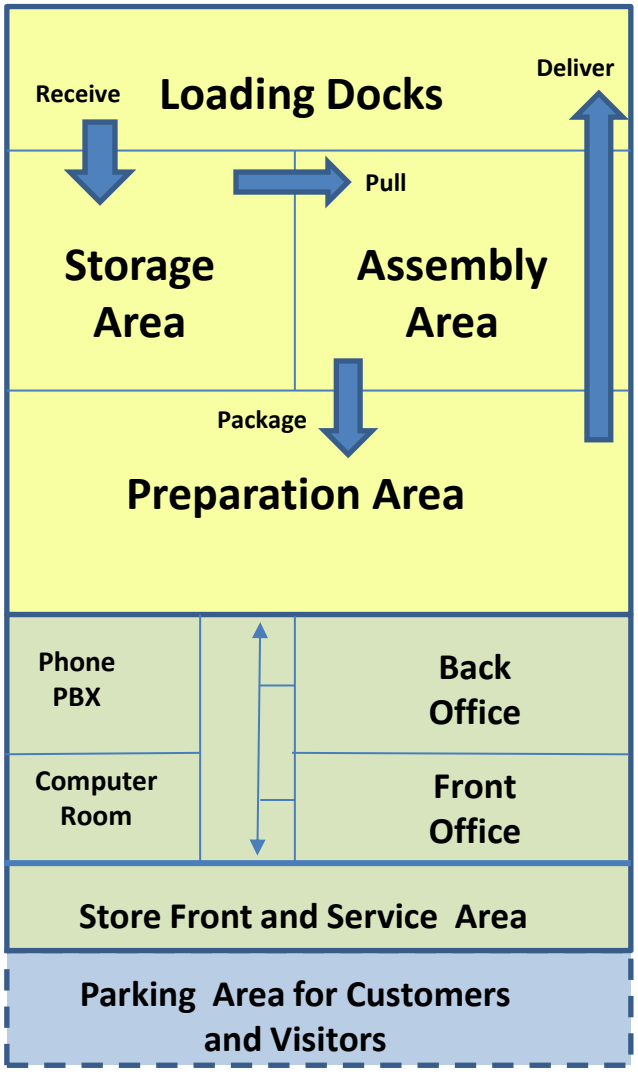


Complete Asset Life Cycle from Acquisition through Re-Deployment and Termination

Inventory Management System Process



Warehouse and Distribution Facility



The Warehouse and Distribution Facility is responsible for accepting orders from customers, assembling goods for delivery, scheduling deliveries, and tracking order fulfillment from start to end. The Loading Dock accepts Supplier / Vendor shipments and produces deliveries for Customers. Products are validated, labeled, and placed in the Storage Area for Assembly and Delivery Preparation to satisfy Customer orders.

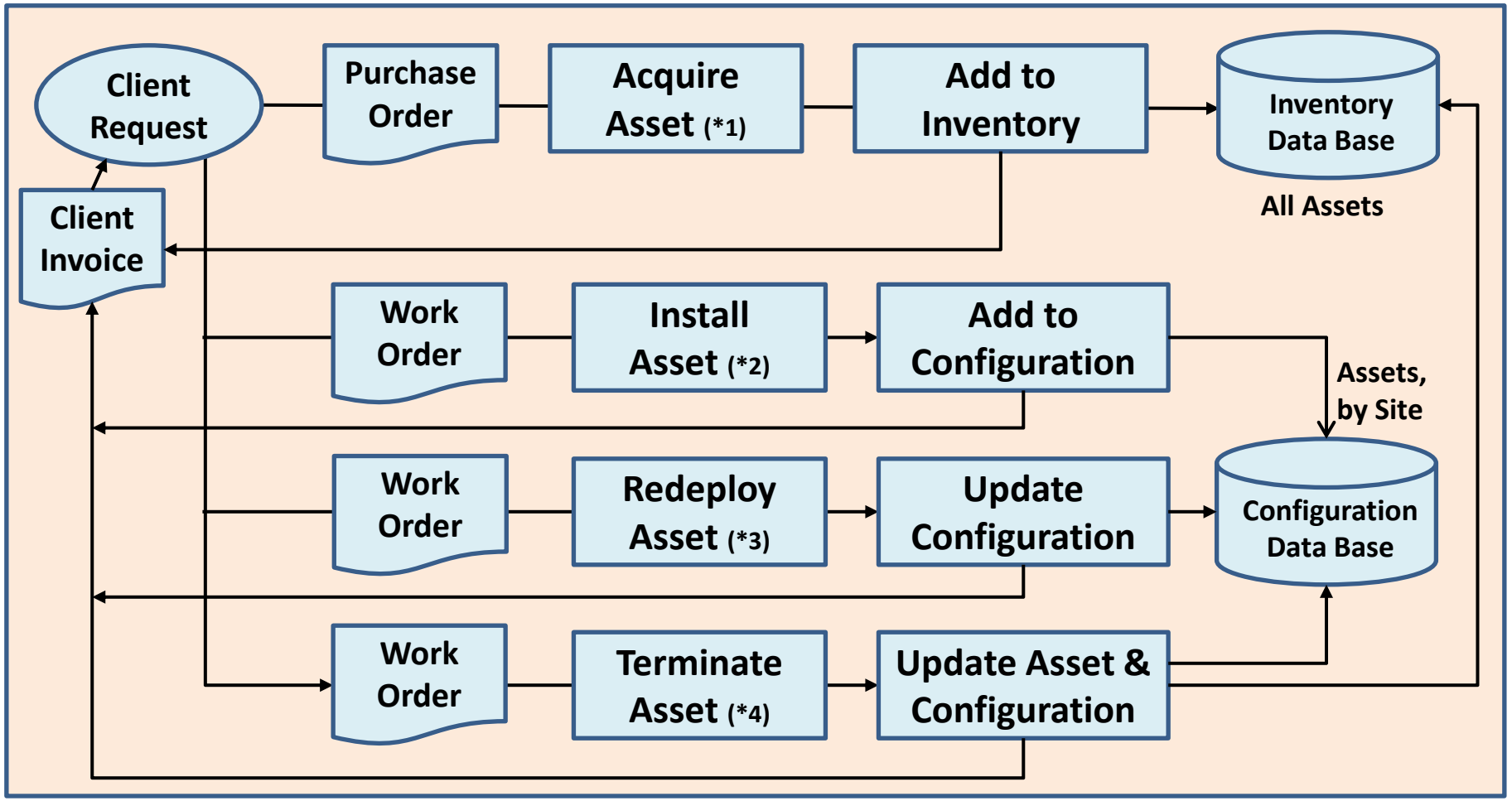
Accounting accepts Work Orders, issues Purchase Orders to Suppliers and Vendors, Accepts Delivered Goods and Places them into the Storage Area for Assembly and Delivery Preparation to Clients.

Accounting tracks Work Orders and Purchase Orders, along with Personnel Hours used to Prepare Deliveries and Transportation Costs. Once Complied, an Invoice is sent to the Customer along with the Delivery of Ordered Goods. The Fulfillment Process is tracked using the Accounts Receivable (A/R), Accounts Payable (A/P), and General Ledger (G/L) process. Time and Expenses are tracked to report on the efficiency of responding to customer orders and improvements are made as deemed necessary to speed delivery, cut costs, and generally improve profit margins.

The Back Office and Front Office is supported through a Computer System and Private Branch Exchange (PBX) phone system that supports: order entry and tracking; and communications between company, customer, supplier, and vendor personnel.

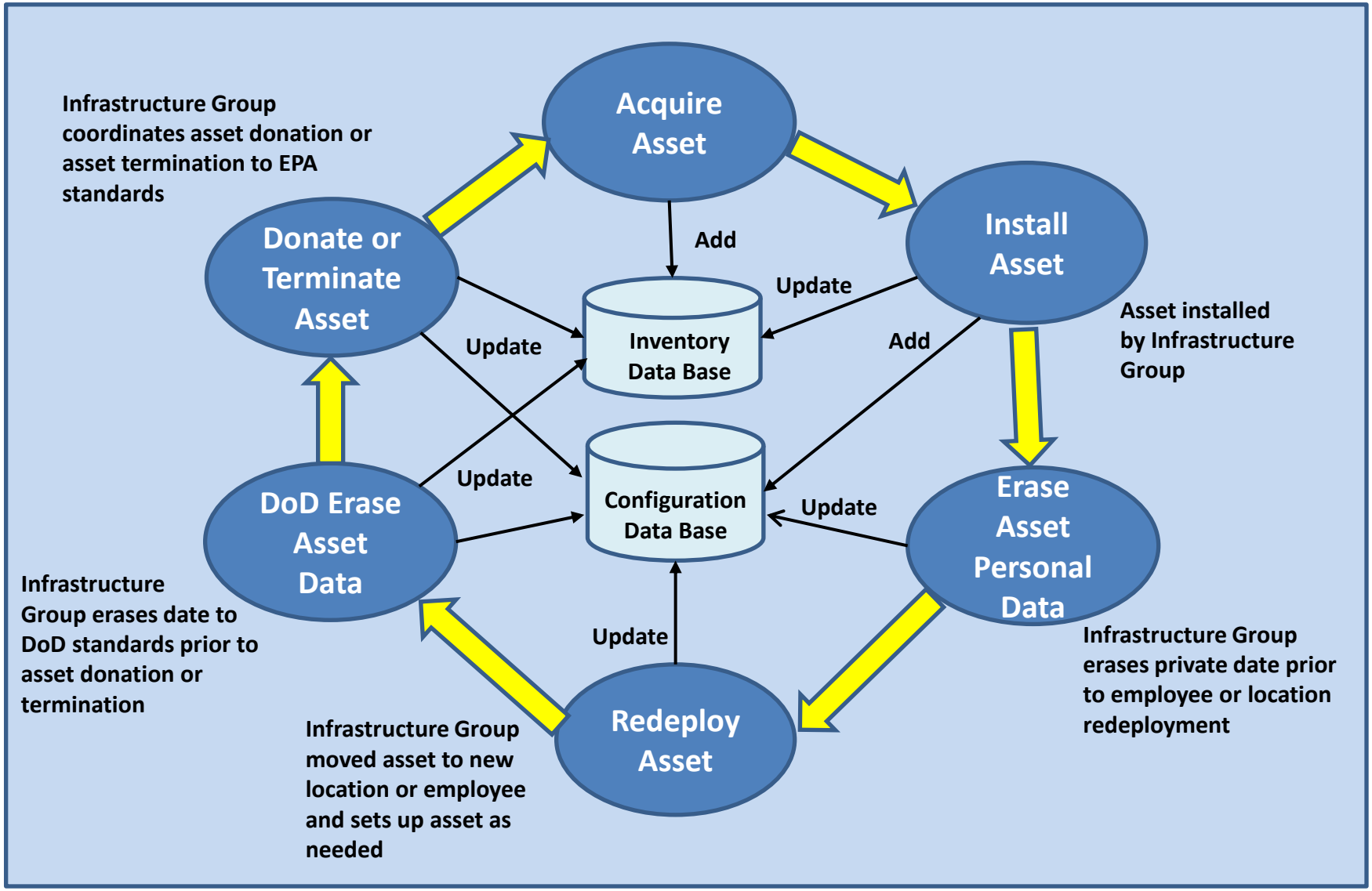
In some cases, a Store Front for private purchases is included in the facility with Parking provided for Customers and Visitors.

Inventory Management Environment

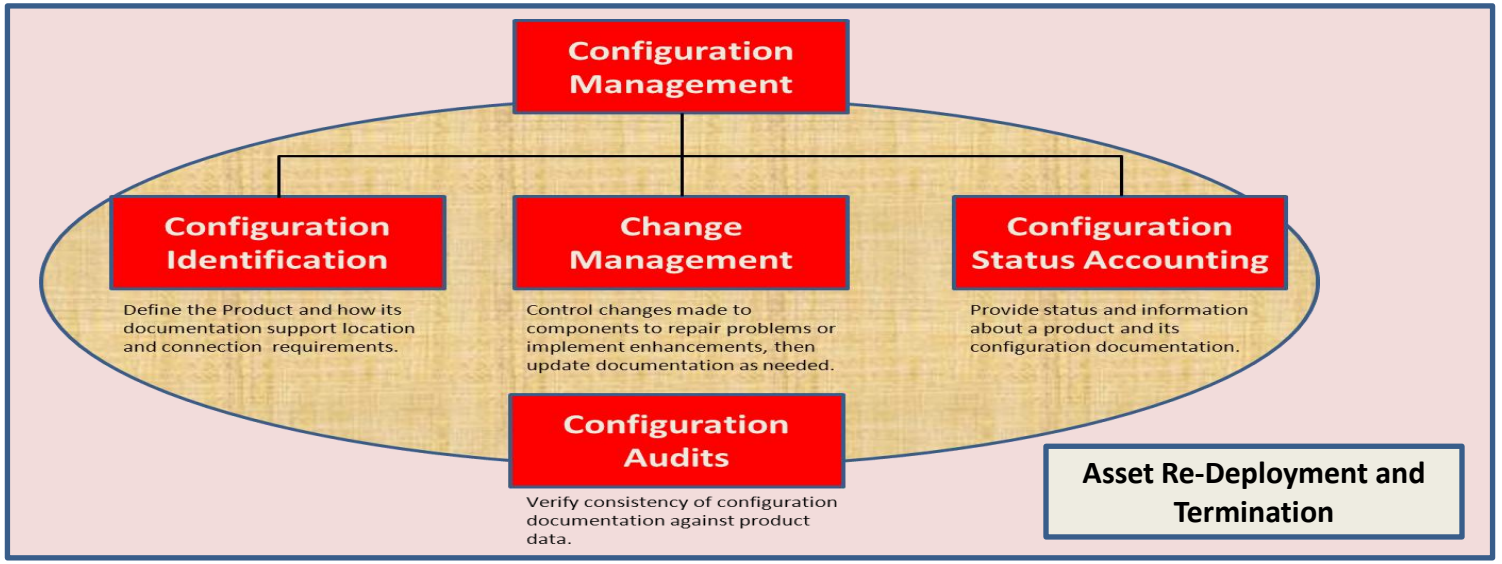


*1 – Purchased Equipment as per guidelines (Leased, Owned, Rented, Type, and Vendor).
*2 – Infrastructure Group schedules and installed Asset.
*3 – Assets are moved from one location to another or reassigned to staff with work performed by the Infrastructure Group.
*4 – Asset are terminated and data erased in accordance to DoD data erasure standards, then equipment is disposed or or donated in accordance to EPA guidelines and requirements.

Inventory Management Life Cycle

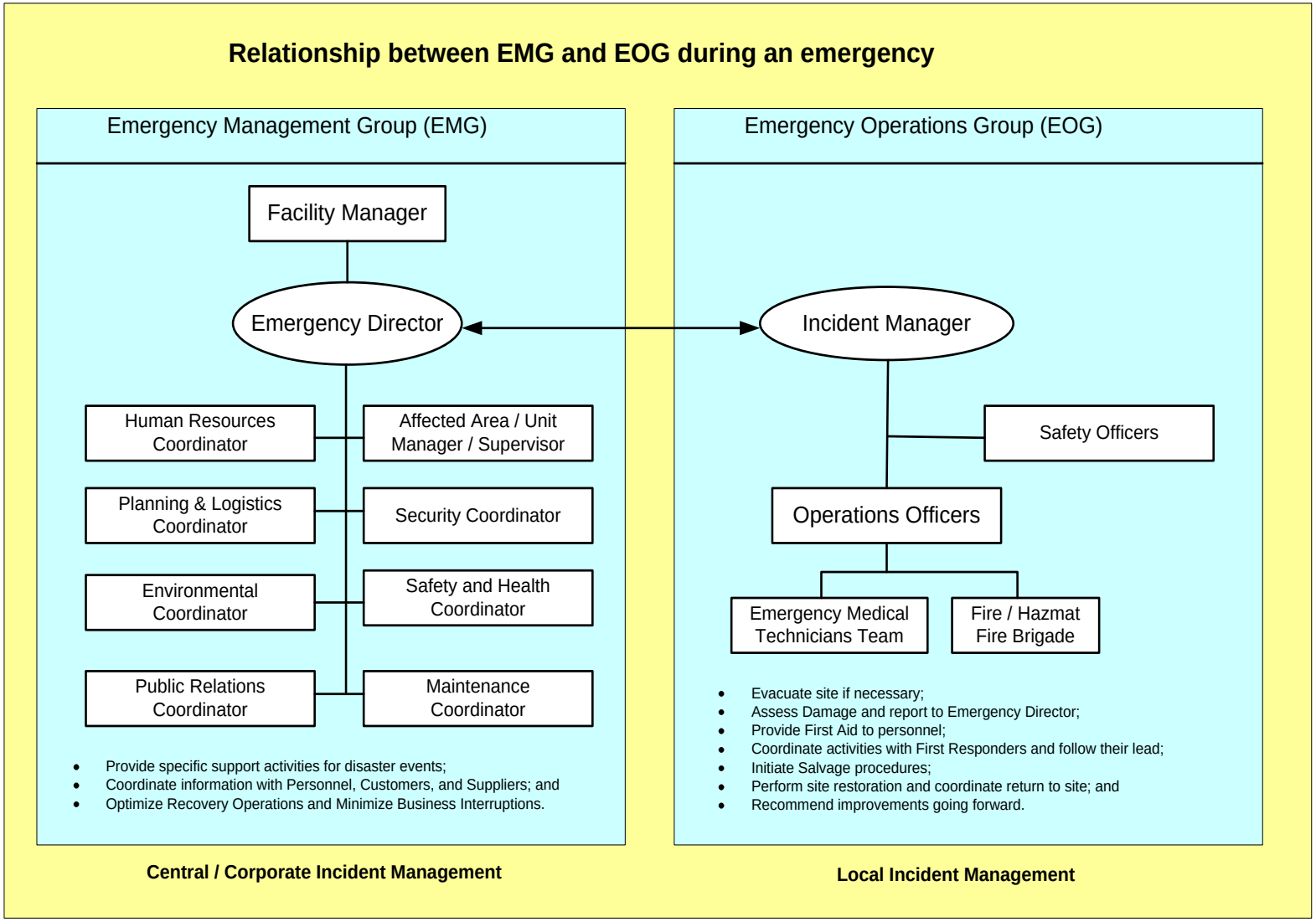


Configuration Management Environment

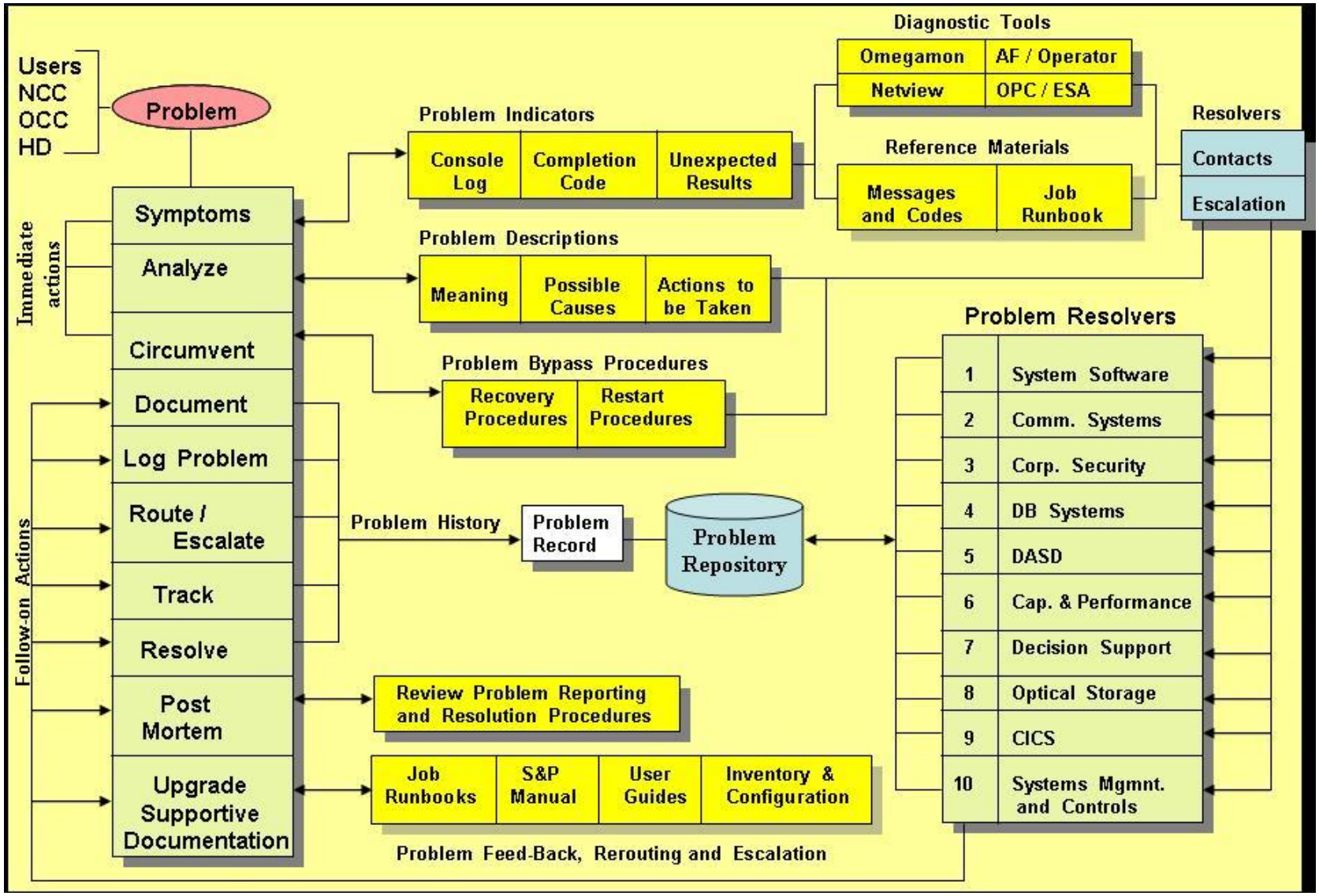


- **Assets are assigned to systems called configurations to support business functions & operations.**
- **Assets must be installed by Facilities Management personnel, who develop a schedule to move, or update, assets as deployment dictates (this process may take days to achieve).**
- **Assets are changed by Facilities Management to support new enhancements and repair problems.**
- **Assets are identified in an inventory and their status is maintained for viewing by support personnel and management (history, engineering changes, problem repairs, enhancements, etc.).**
- **Single-Point-Of-Failure of components are identified and alternate paths created for protection from outage and recovery purposes..**
- **Periodic audits of assets are conducted.**
- **Assets have a lifecycle and are changed / replaced periodically to support new needs and technology advancements (usually of a four-to-five year basis).**
- **Financial profiles of assets are maintained so that management can decide upon the most economical manner to utilize assets (i.e., long-term = buy or lease, short-term = rent, etc.)**

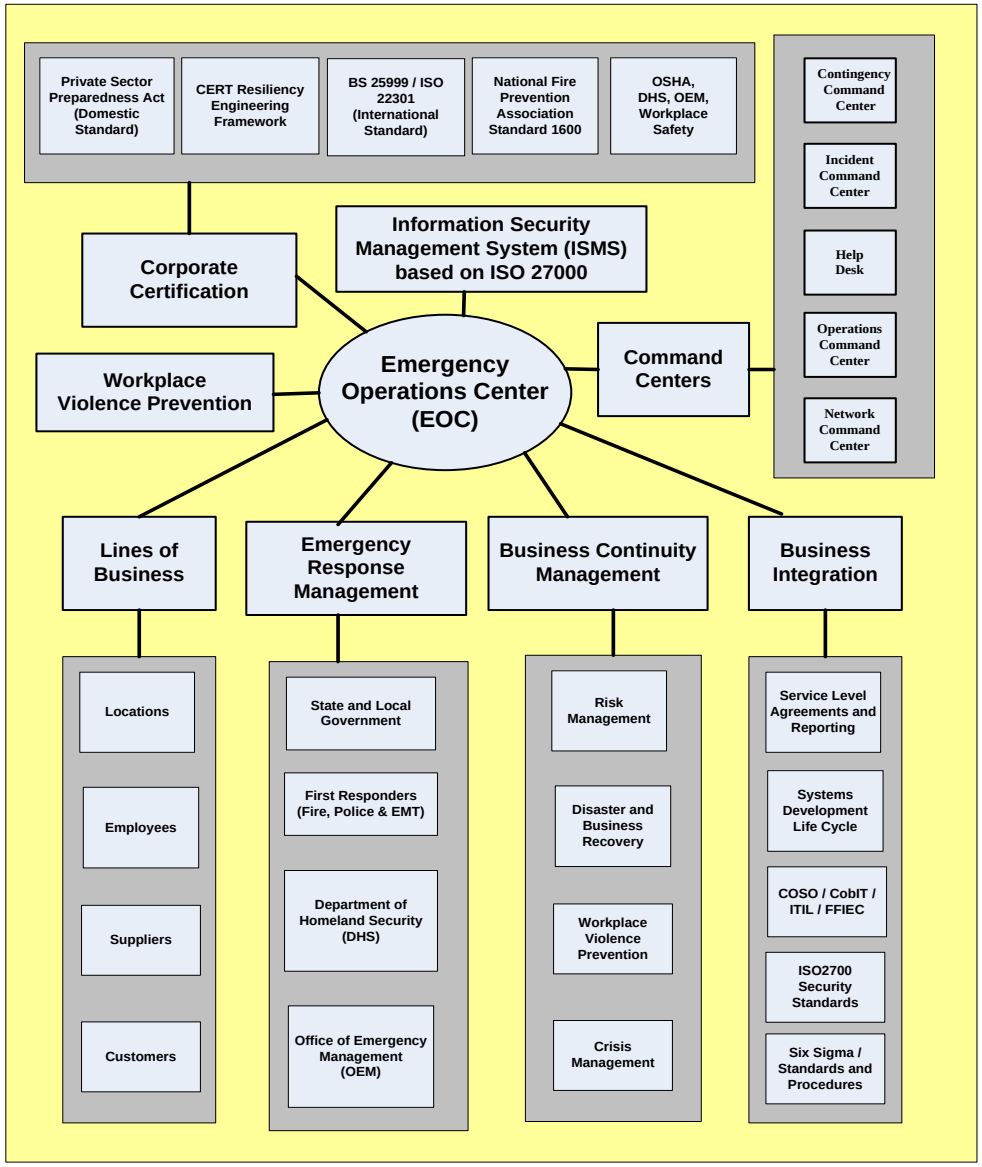
Incident / Emergency Management Operations Environment



Problem Management and Circumvention Techniques



Fully Integrated Recovery Operations and Disciplines (Physical End Goal)



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.

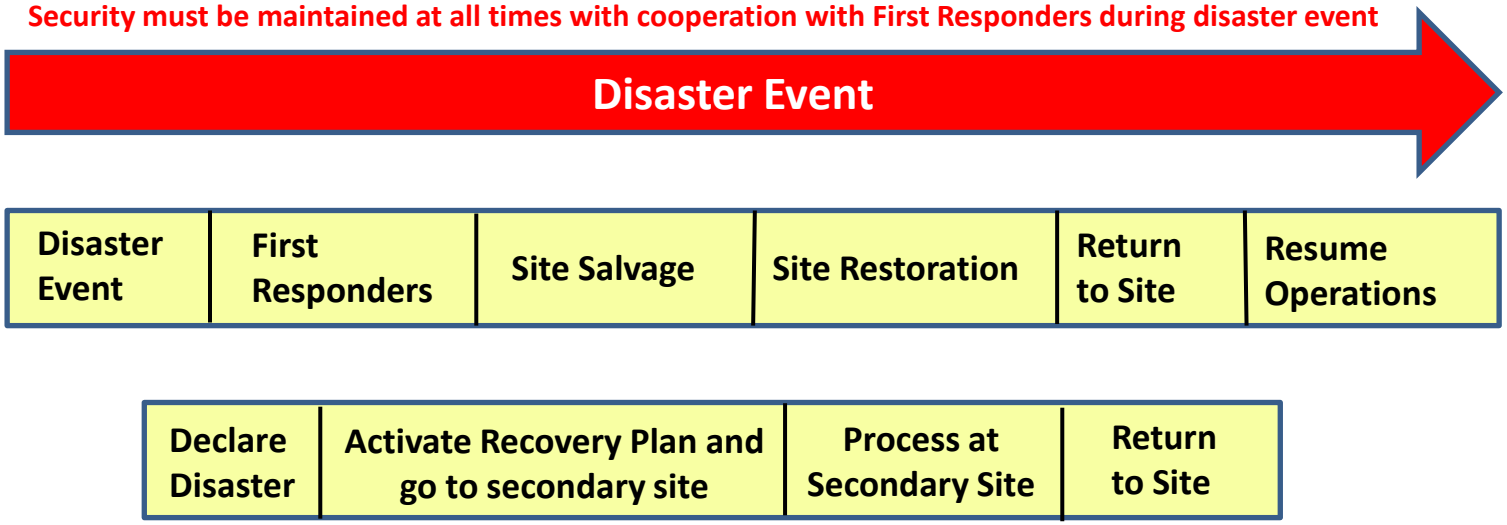
Workplace Violence Prevention and **Information Security** is adhered to by implementing guidelines to protect personnel and data by following the latest guidelines related to these topics.

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 are identified and connections provided to the EOC so that communications and coordination can be achieved in the most 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.

Responding to Disaster Events



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.

Additional considerations include Insurance and Claim Processing, media communications, and coordination with government organizations and companies near your facility that may be affected by the disaster event.

Being a good neighbor is important to protect your reputation and show good will.

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

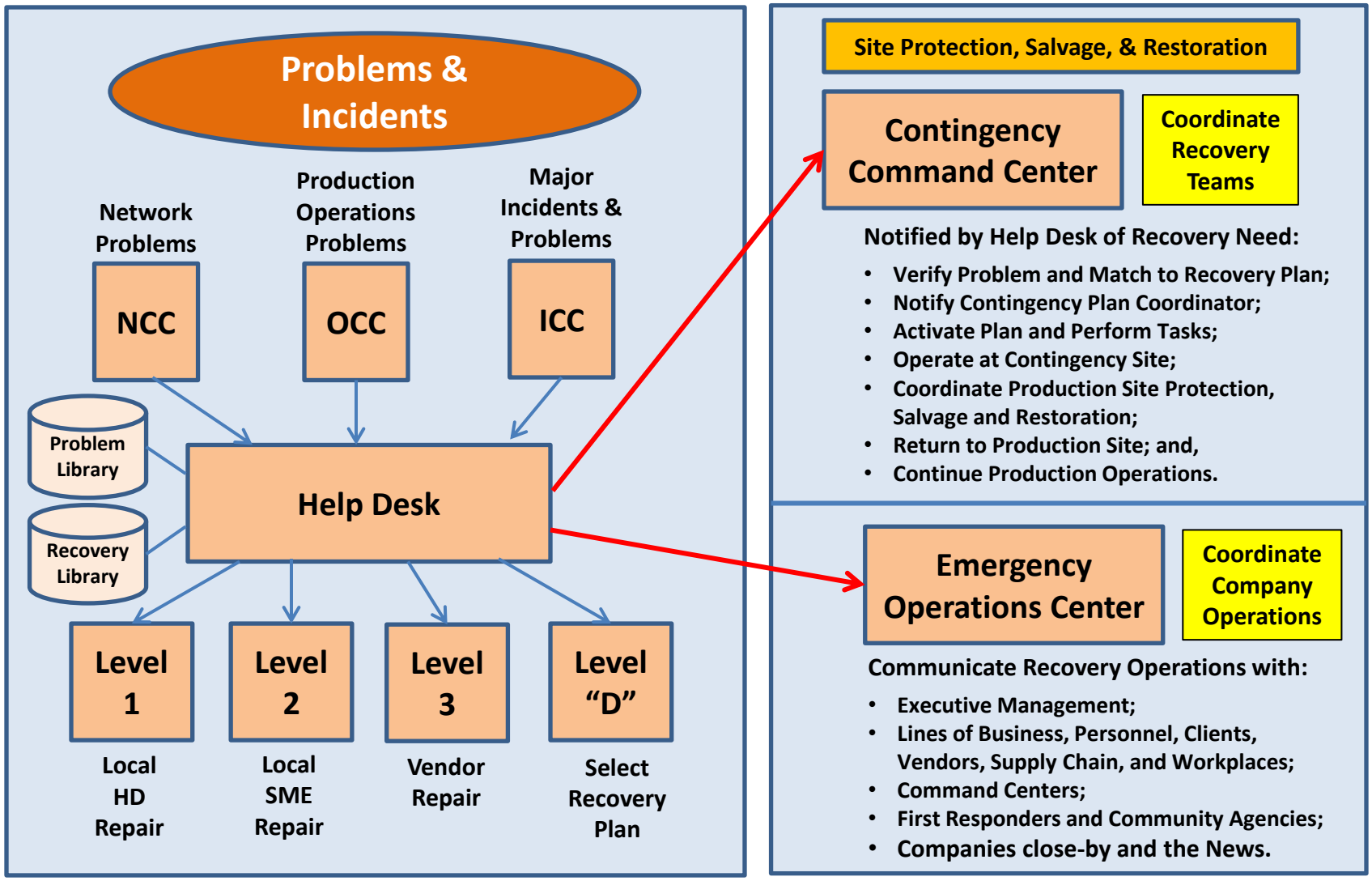
Primary Site Recovery Plan:

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

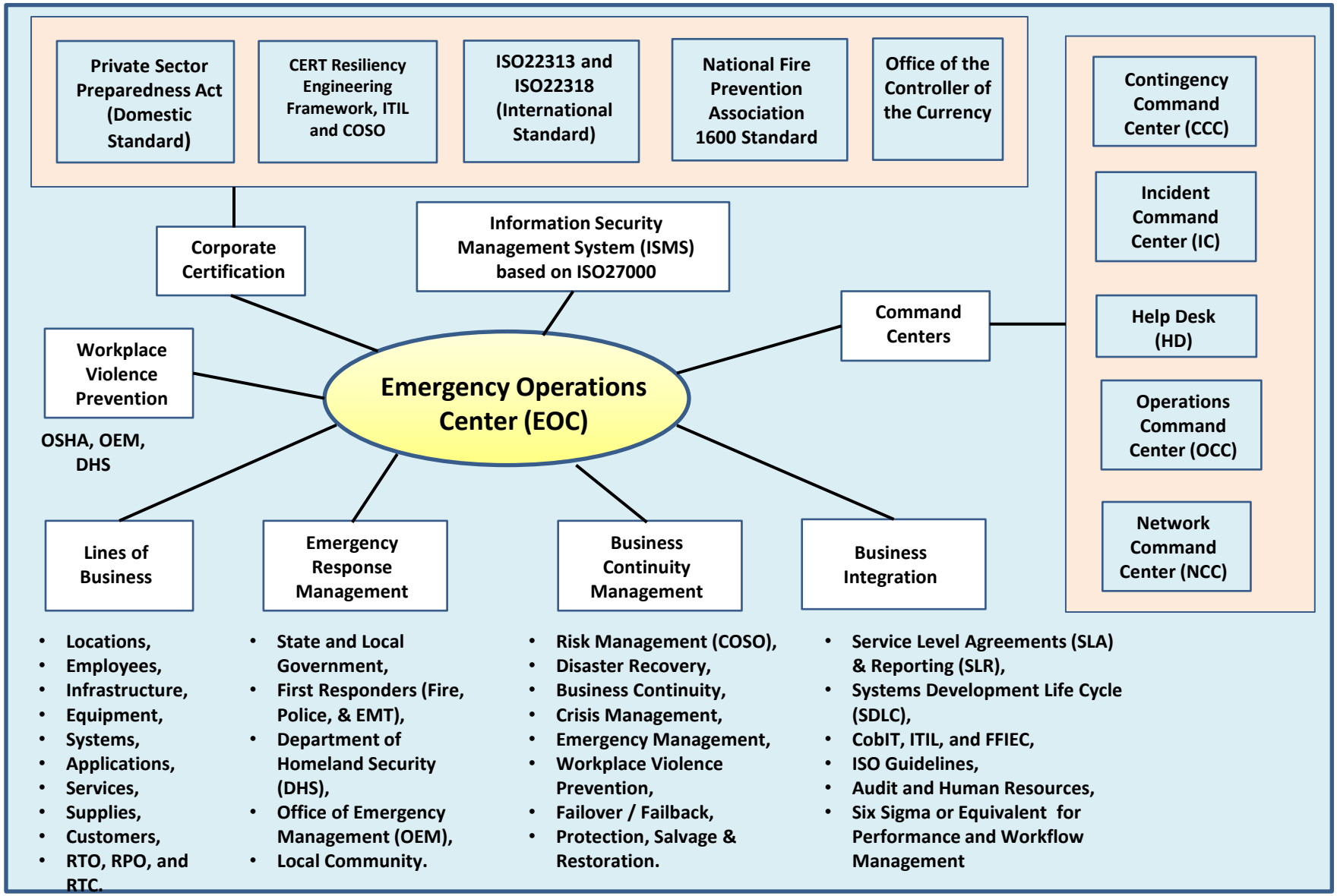
Alternate Site Recovery Plan:

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

Activating and Coordinating Disaster Recovery Plans



Fully Integrated Resiliency Operations and Disciplines (Logical End Goal)



Conclusions

- **Enterprise Resiliency and Corporate Certification will build an efficient and safeguarded environment that best supports continued business operations and the company reputation.**
- **Many people are involved with planning and implementing, so awareness is high and training can be easily achieved.**
- **A well trained and loyal staff will best support retention and recruitment of personnel and clients, while supporting future growth and an industry reputation as an excellent company.**
- **SLA / SLR and Client Contract management will be more easily achieved, thereby producing a happier client and support for future growth through references.**
- **Use of "Best Practices" will better guaranty success, while protecting management's decision to implement a state-of-the-art production, compliant, and recoverable environment.**
- **Use of the latest Data Management technology will support recovery time requirements, while allowing for off-line testing of maintenance and recovery operations.**
- **Integration of Systems Management, Workflow Management, and a Charge-Back System will provide monitor and control over costs, while developing a repository or accomplished work that can be referenced when planning similar projects.**
- **Integration of the Emergency Operations Center (EOC) with Command Centers, Lines of Business, and Recovery Operations will enhance the information provided to Executive Management and allow them to better communicate with clients and assist with expediting resumption of business operations.**

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.