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

Abstract

- Are you utilizing your recovery personnel to achieve maximum protection?
- Have you implemented a common recovery language 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, 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 SLR/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 OEM, FEMA, Homeland Security, 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.

Topics included in this presentation

1. Business Plan (Mission, Goals & Objectives, and Risk Management;
2. IT Evolution (PC, Domains, Enterprise);
3. Systems Development Life Cycle (SDLC);
4. Data Management and Information Security Management System (ISMS);
5. Enterprise Resiliency and Corporate Certification;
6. Regulations (Domestic and International);
7. **Building Enterprise Resiliency on a solid foundation**;
8. Business Continuity and Disaster Recovery Planning for High Availability (HA) and Continuous Availability (CA) applications to achieve Zero Downtime;
9. Emergency Management;
10. Risk and Crisis Management;
11. **Laws and Regulations**;
12. Converting to a Enterprise Resiliency environment;
13. **Implementing Corporate Certification (Domestic and International)**; and,
14. **Fully Integrated** Enterprise Resiliency and Corporate Certification environment.

Layout of this presentation

A. Business Plan

- Mission Statement
- Goals and Objectives
- Risk Management

B, Direction Plan

- Building Business Recover Plans
- Certifying Application Recovery for High Availability and Continuous Availability
- IT Evolution
- SDLC
- Support and Maintenance
- Potential Risks and Threats
- Enterprise Resilience and Corporate Certification
- Risk Management Guidelines
- Crisis Management
- Workplace Violence Prevention
- Emergency Management
- Incident Management
- Emergency Operations Center (EOC)

C. Building Enterprise Resiliency

- CobIT
- ITIL
- Fully integrated Enterprise Resiliency
- Compliance Laws
  - Gramm-Leach Bliley (GLB)
  - Dodd-Frank
  - HIPAA, SOX,
  - EPA Superfund
  - Patriot Act
  - Basel II / Basel III framework
- Reporting on Compliance Adherence
- Eliminating Audit Exceptions
- **Recovery Planning**
  - BIA / BCP / EM
  - Converting to Automated Recovery Tools
  - Documentation, Awareness, and Training
- **How do we get started**

Steps to Recovery Management and Enterprise Resiliency

- **Formulate Recovery Management Charter, including:**
  - Charter, Mission Statement, Business Plan;
  - Project Plan, Goals and Objectives, Functional Requirements and Skills, Task Descriptions, Timeline;
  - Management Support, Funding, and Announcement.
- **Project Plan, Organization Structure, Job Functions;**
  - Work Flow and Systems Development Life Cycle;
  - Problem Management and Help Desk;
  - Change Management and Version and Release Management;
  - Asset and Configuration Management;
  - Access Control and Library Management;
  - Service Level Agreements (SLA) / Service Level Reporting.
- **Library Management, including:**
  - Group Drive for sharing / developing information;
  - Public Drive to house:
    - Recovery Plans and Training Materials;
    - Glossary of Terms;
    - Continuity of Business Public Documents.
- **Recovery Management Coordinators from Business Units;**
  - Subject Matter Experts supporting Business Units.
- **Selection of automated Recovery Management tool and Integration:**
  - Risk Management Assessment, Business Impact Analysis;
  - Recovery Plan creations, and Recovery Plan testing from Table-Top to Recovery Certification;
  - Mitigate any Gaps & Exceptions;
  - Mediate any Obstacles Impeding Recovery Testing;
  - Repeat Testing – Repair – Testing Cycle until Recovery Certified;
  - Repeat testing until Gold Standard is reached via Flip / Flop ability;
  - Integrate process within every functions performed by personnel.

Mission Statement:

1. Insure **Continuity of Business** and Eliminate / Reduce Business Interruptions (**Enterprise Resilience**);
2. Assure **"Corporate Certification"** by complying with Regulatory Requirements for countries that you do business in, through Risk Management and Crisis Management guidelines **(CERT / COSO)**;
3. Adhere to Service Level Agreements (**SLA**) through Service Level Reporting (**SLR**) and the use of Capacity and Performance Management procedures;
4. Implement **Enterprise-Wide Recovery Management** by combining Business Continuity Management (**BCM**), Disaster Recovery Planning (**DRP**), and Emergency Management (**EM**);
5. Utilize **"Best Practices"** to achieve **"Enterprise Resiliency" (CobIT, ITIL, etc.)**;
6. Protect personnel and achieve **physical security** through **Workplace Violence Prevention** principals, laws, and procedures;
7. Guaranty **data security** through access controls and vital records management principals and procedures within an Information Security Management System (**ISMS**) based on **ISO27000**;
8. Achieve **Failover / Failback** and data management procedures to insure **RTO, RPO**, and Continuity of Business within acceptable time lines (Dedupe, VTL, Snapshots, CDP, NSS, RecoverTrak, etc.);
9. **Integrate recovery management** procedures within the everyday functions performed by personnel as defined within their job descriptions and the Standards and Procedures Manual;
10. **Embed Recovery Management and ISMS** requirements within the Systems Development Life Cycle (SDLC) used to Develop, Test, Quality Assure, Production Acceptance / Implement, Data Management, Support and Problem Management, Incident Management, Recovery Management, Maintenance, and Version and Release Management for components and supportive documentation;
11. Develop and provide **educational awareness** and training programs to inform personnel on how best to achieve the corporate mission.

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
• Personnel (HRM and Employee Assistance)	• Vendors - Supply Chain Mgmnt. (ISO 24672 / ISO 27031)	• Clients (Products / Services) and SLA / SLR
• Locations / Infrastructure	• Community / Business / Personnel	• Lines of Business
• Physical / Data Security	• Compliance	• Recovery Management
• Optimized Operations	• Insurance	• Reputation

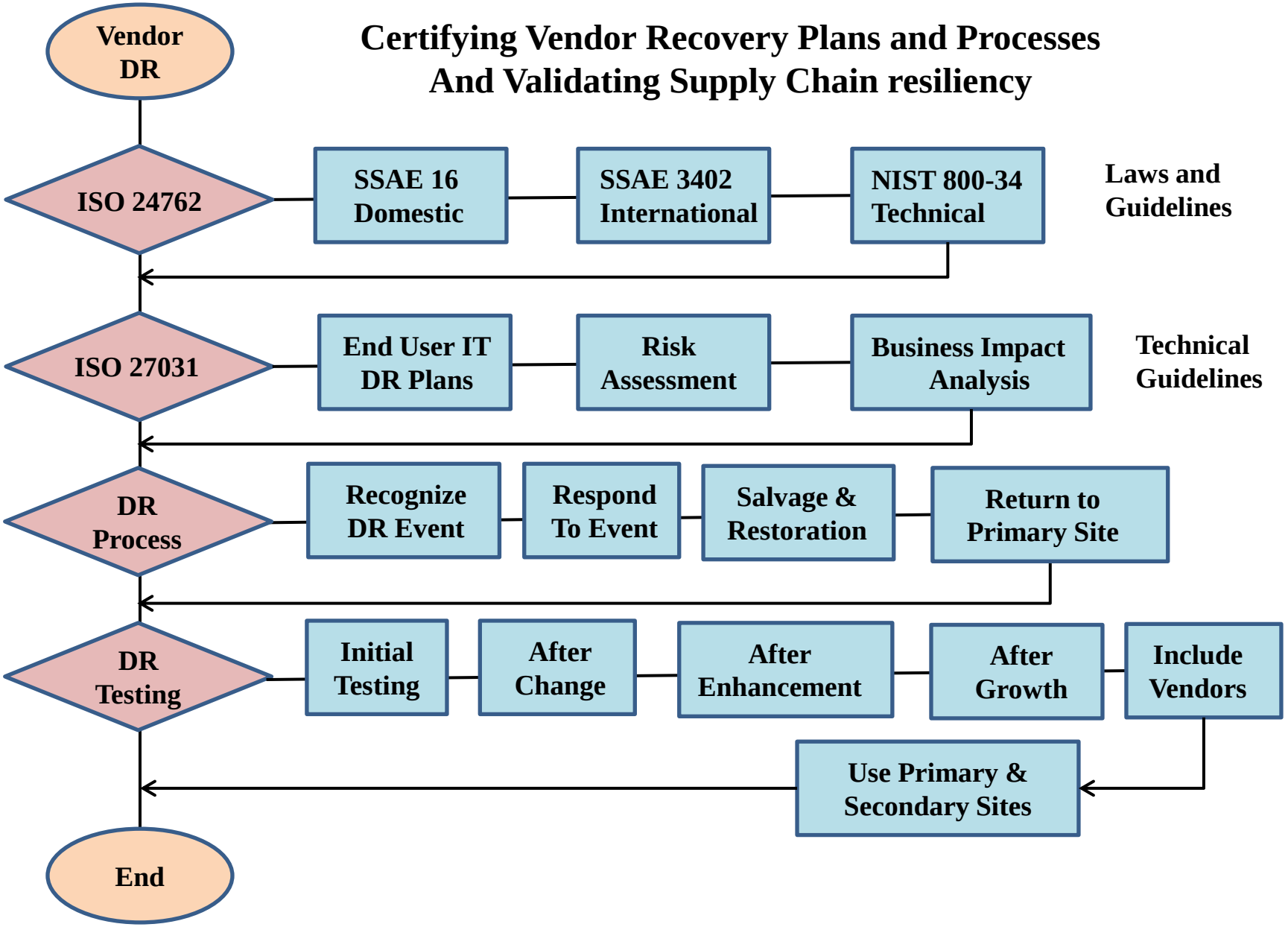
Protecting Information Technology

• 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 (Userid / Pswd)
• Vaulting, Backup, and Recovery	• Disk / File copy retrieve utilities	• RTO, RPO, RTC

Risk Management:

- Define Risk Management Process in accordance with **COSO / CERT** guidelines, including:
  - Internal Environment Review;
  - Objective Setting;
  - Event Identification;
  - Risk Assessment and Response Definitions;
  - Control Activities;
  - Information and Communications; and
  - Monitoring and Reporting.
- Define **Legal and Regulatory Requirements** (Domestic and International as needed);
- Determine OCC, Tax, and Industry **compliance requirements**;
- Perform an IT Audit / Risk Assessment to uncover **Gaps and Exceptions**;
- Define **Mitigations** and their Costs, along with data gathering and reporting guidelines;
- Calculate **cost of Mitigation against cost of Gap / Exception** to prioritize responses;
- Review **Vendor Agreements** for primary and secondary sites to eliminate / minimize **Supply Chain interruptions ISO 24762, (SSAE 16, SSAE 3402, NIST 800-34) ISO 27031**;
- Obtain **Insurance** Quotes and select appropriate insurance protection;
- **Integrate** with the everyday functions performed by personnel as outlines in their job descriptions and the Standards and Procedures Manual; and,
- Develop documentation, **awareness, and training** materials.

Example of an Automated BCP Tool - ResilienceOne


Certifying Vendor Recovery Plans and Processes
And Validating Supply Chain resiliency
Vendor DR
ISO 24762
SSAE 16 Domestic
SSAE 3402 International
NIST 800-34 Technical
Laws and Guidelines
ISO 27031
End User IT DR Plans
Risk Assessment
Business Impact Analysis
Technical Guidelines
DR Process
Recognize DR Event
Respond To Event
Salvage & Restoration
Return to Primary Site
DR Testing
Initial Testing
After Change
After Enhancement
After Growth
Include Vendors
Use Primary & Secondary Sites
End

Inventory of Assets and Applications, by location or line of business

Line of Business	Department	Business Unit	Asset ID #:	Asset Name	Availability Need	Recovery Time Expectation	Recovery Point Expectation	Recovery Time Capability	Service Recovery Expectation	Recovery Time Objective	Recovery Point Objective	Recovery Time Capability	Data Sensitivity	Access Controls	Backup Requirement	Restore Requirement	Data Corruption OK	Data Encryption
Marketing	Internet Sales	Web Site	MIW	Internet	CA .5	30 min.	1 hour	1.5 hours	30 min.	30 min.	45 min.	1.5 hours	High	Done	Hourly	10 min.	OK	Yes
	Intranet Support	Intranet	MII	Intranet	CA .5	31 min.	2 hour	1.5 hours	30 min.	30 min.	45 min.	1.5 hours	High	Done	Hourly	11 min.	OK	Yes
	Intranet Support	Help Desk	MIS	Intranet	CA .0	32 min.	3 hour	1.5 hours	30 min.	30 min.	45 min.	1.5 hours	High	Done	Hourly	12 min.	OK	Yes
	Help Desk	Support	MHS002	Internet	CA .0	33 min.	4 hour	1.5 hours	30 min.	30 min.	45 min.	1.5 hours	High	Done	Hourly	13 min.	OK	Yes
		Technology	MHT	Internet	CA .5	34 min.	5 hour	1.5 hours	30 min.	30 min.	45 min.	1.5 hours	High	Done	Hourly	14 min.	OK	Yes
		Products	MHP	Internet	CA .5	35 min.	6 hour	1.5 hours	30 min.	30 min.	45 min.	1.5 hours	High	Done	Hourly	15 min.	OK	Yes
		Services	MHS002	Internet	CA .0	36 min.	7 hour	1.5 hours	30 min.	30 min.	45 min.	1.5 hours	High	Done	Hourly	16 min.	OK	Yes
Programming	Marketing	Materials	PMM	Internet	HA 1 hr.	36 min.	7 hour	1.5 hours	30 min.	30 min.	45 min.	1.5 hours	High	Done	Hourly	16 min.	OK	Yes
	Sales	Clients	PSC	Internet	HA 1 hr.	37 min.	8 hour	1.5 hours	30 min.	30 min.	45 min.	1.5 hours	High	Done	Hourly	17 min.	OK	Yes
	Support	Applications	PSA	Computer	HA 2 hr.	38 min.	9 hour	1.5 hours	30 min.	30 min.	45 min.	1.5 hours	High	Done	Hourly	18 min.	OK	Yes
	Operations	IT	PSI	Computer	CA 1 hr.	39 min.	10 hour	1.5 hours	30 min.	30 min.	45 min.	1.5 hours	High	Done	Hourly	19 min.	OK	Yes

- Line of Business
- Department
- Business Unit
- Asset ID #: for Application, or Asset
- Asset Name
- Availability Need (Continuous Availability or High Availability by time – i.e., CA 5 is Continuous Availability within 5 minutes, or High Availability 2 hrs.)

- RTE – Recovery Time Expectation from SLA
- RPE – Recovery Point Expectation from SLA
- SRE – Service Recovery Expectation from SLA
- RTO – Recovery Time Objective from BIA
- RPO – Recovery Point Objective from BIA
- RTC – Recovery Time Capability from BIA and Testing
- Data Sensitivity from client (High, Medium, Low, etc.)
- Access Controls (Write, Read, Edit, Delete, etc.)
- Backup Requirements (1 hour – 1 day or 1 week)
- Restore Requirements (to meet RTO from BIA and RTE from SLA)
- Data Corruption OK – to confirm data validity and protection
- Data Encryption (especially for traveling data, but should cover all data)

Inventory of Assets and Applications, by supporting personnel

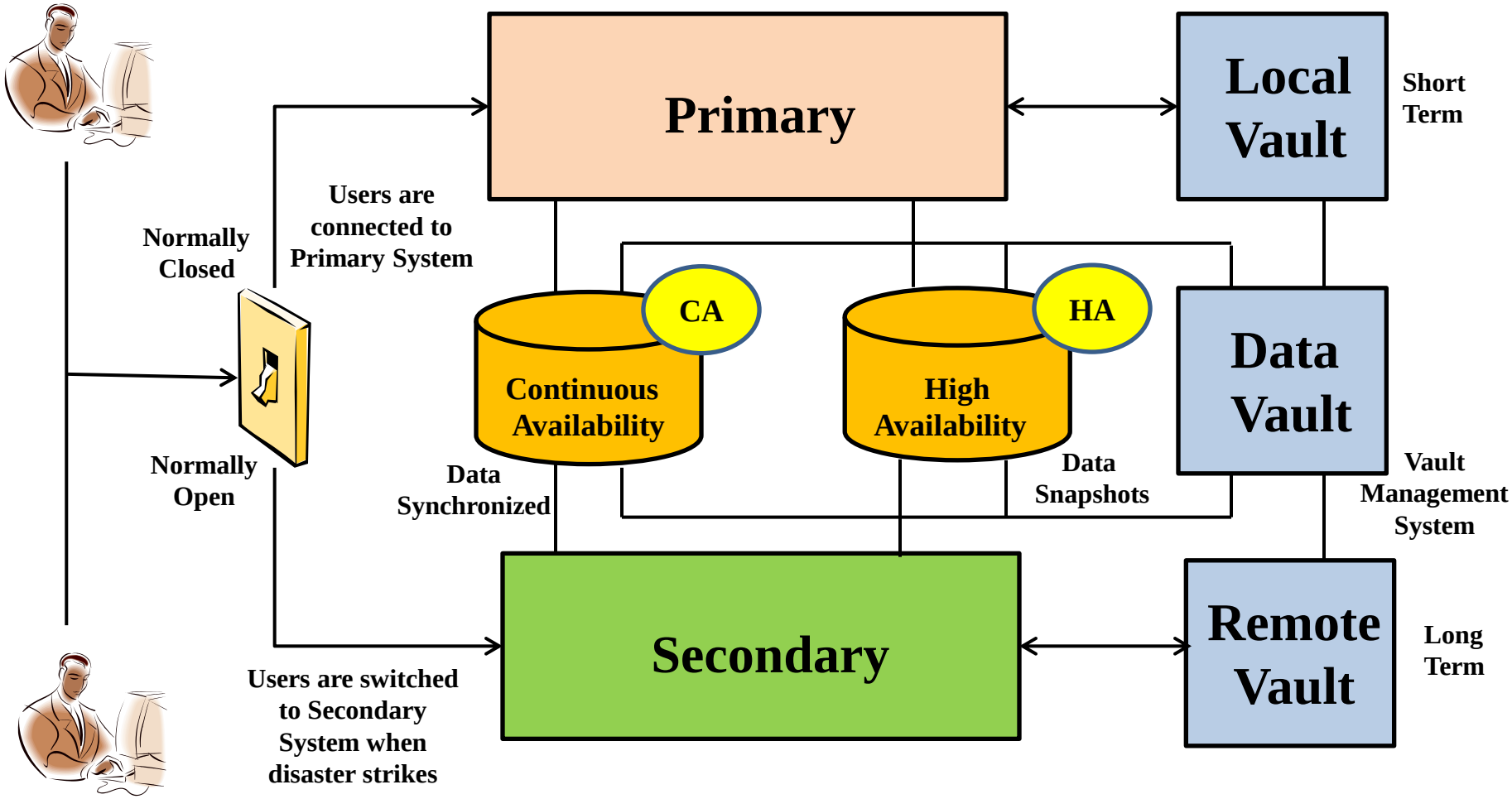
Line of Business	Department	Business Unit	Asset ID #:	Asset Name	Mainframe Systems SME	UNIX, Linus, AIX SME	Data Base SME	Programming SME	Communications SME	Infrastructure SME	Systems Architect SME	Systems Engineering SME	Meeting Schedule	Notes:	Status
Marketing	Internet Sales	Web Site	MIW	Internet	Johnson	Wright	Oracle	Java	Josephs	Holmes	Ryan	Thornton	Weekly	Discuss current sales and prospective sales	Good
	Intranet Support	Intranet	MII	Intranet	Johnson	Wright	Oracle	Java	Josephs	Holmes	Ryan	Thornton	Weekly	Discuss any Support Issues	Good
	Intranet Support	Help Desk	MIS	Intranet	Johnson	Moore	Windows	Java	Josephs	Holmes	Ryan	Thornton	Weekly	How to improve Help Desk Performance	Bad
	Help Desk	Support	MHS001	Internet	Johnson	Moore	Windows	Ruby on Rails	Josephs	Holmes	Ryan	Thornton	Bi-Weekly	How to improve Help Desk Performance	Pending
		Technology	MHT	Internet	Johnson	Moore	Windows	Ruby on Rails	Josephs	Holmes	Ryan	Thornton	Bi-Weekly	Problems, Issues, Resolutions	Good
		Products	MHP	Internet	Johnson	Moore	Windows	Ruby on Rails	Josephs	Holmes	Ryan	Thornton	Bi-Weekly	Issues, complaints, resolutions, pending	Bad
		Services	MHS002	Internet	Johnson	Moore	Windows	Ruby on Rails	Josephs	Holmes	Ryan	Thornton	Bi-Weekly	Issues, complaints, resolutions, pending	Pending
Programming	Marketing	Materials	PMM	Internet	Goldberg	Smith	SQL Server	VS Basisc	Gordon	Villa	Javier	Lewis	Monthly	New materials, updates to existing materials	Good
	Sales	Clients	PSC	Internet	Goldberg	Smith	SQL Server	Java	Gordon	Villa	Javier	Lewis	Bi-Weekly	Sales Cycle and clients progress	Good
	Support	Applications	PSA	Computer	Goldberg	Smith	SQL Server	Java	Gordon	Villa	Javier	Lewis	Weekly	Issues, complaints, resolutions, pending	Bad
	Operations	IT	PSI	Computer	Goldberg	Smith	SQL Server	Cobol	Gordon	Villa	Javier	Lewis	Weekly	Issues, complaints, resolutions, pending	Pending

Used to indicate who is assigned to build and support products and services by area. Meeting schedules are included so that updated status reports can be generated for management and participants review.

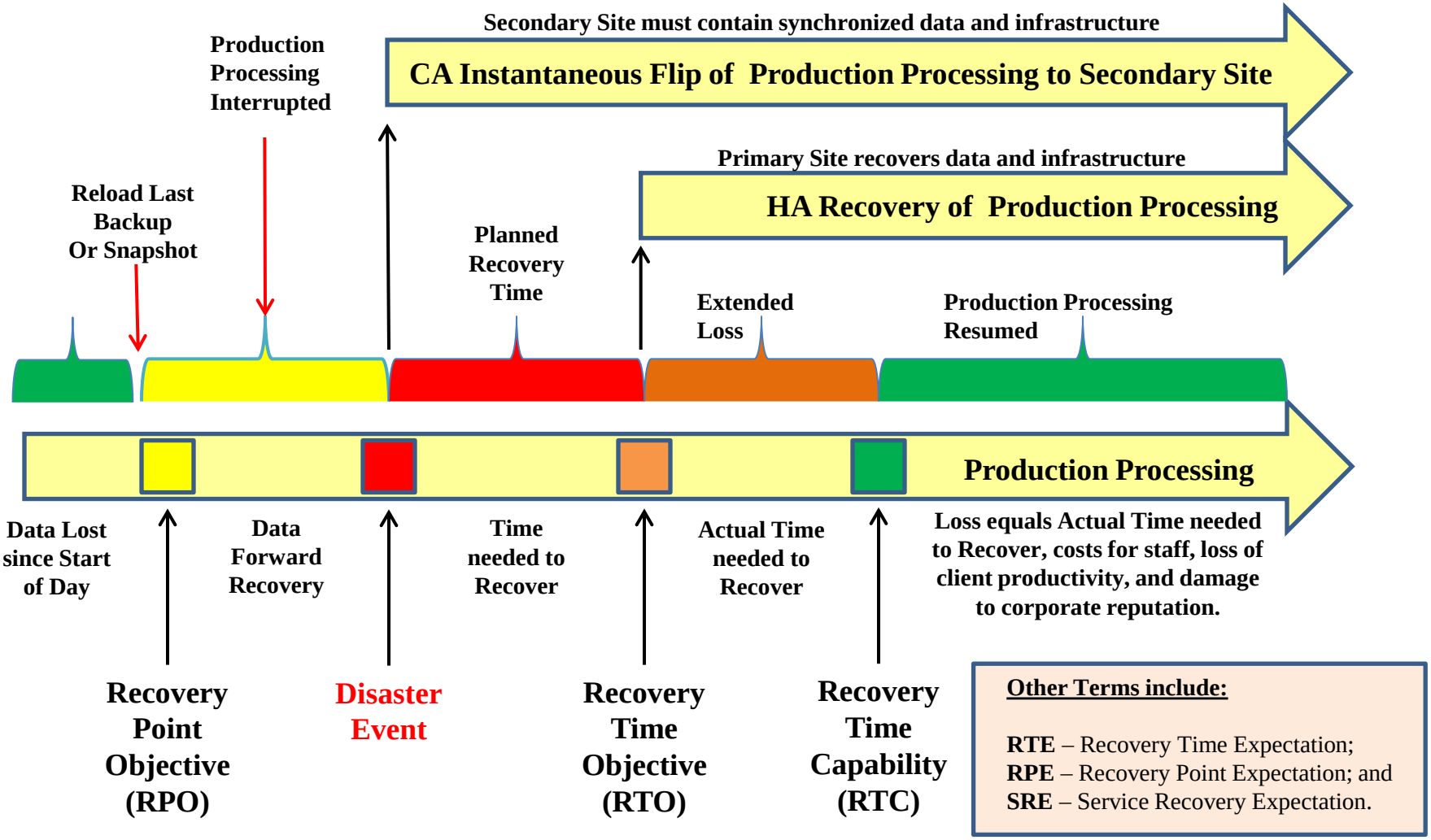
These people will have to substantiate the applications ability to recover within the RTE / RTO and for reporting Gaps & Exceptions and Obstacles impeding the applications ability to meet recovery goals.

Periodic testing is performed to insure application ability to continue to recover within time demands and that the application is in compliance. Obstacles and impediments are identified and resolved.

The Goal of Disaster Recovery with Continuous Availability (CA) and High Availability (HA)



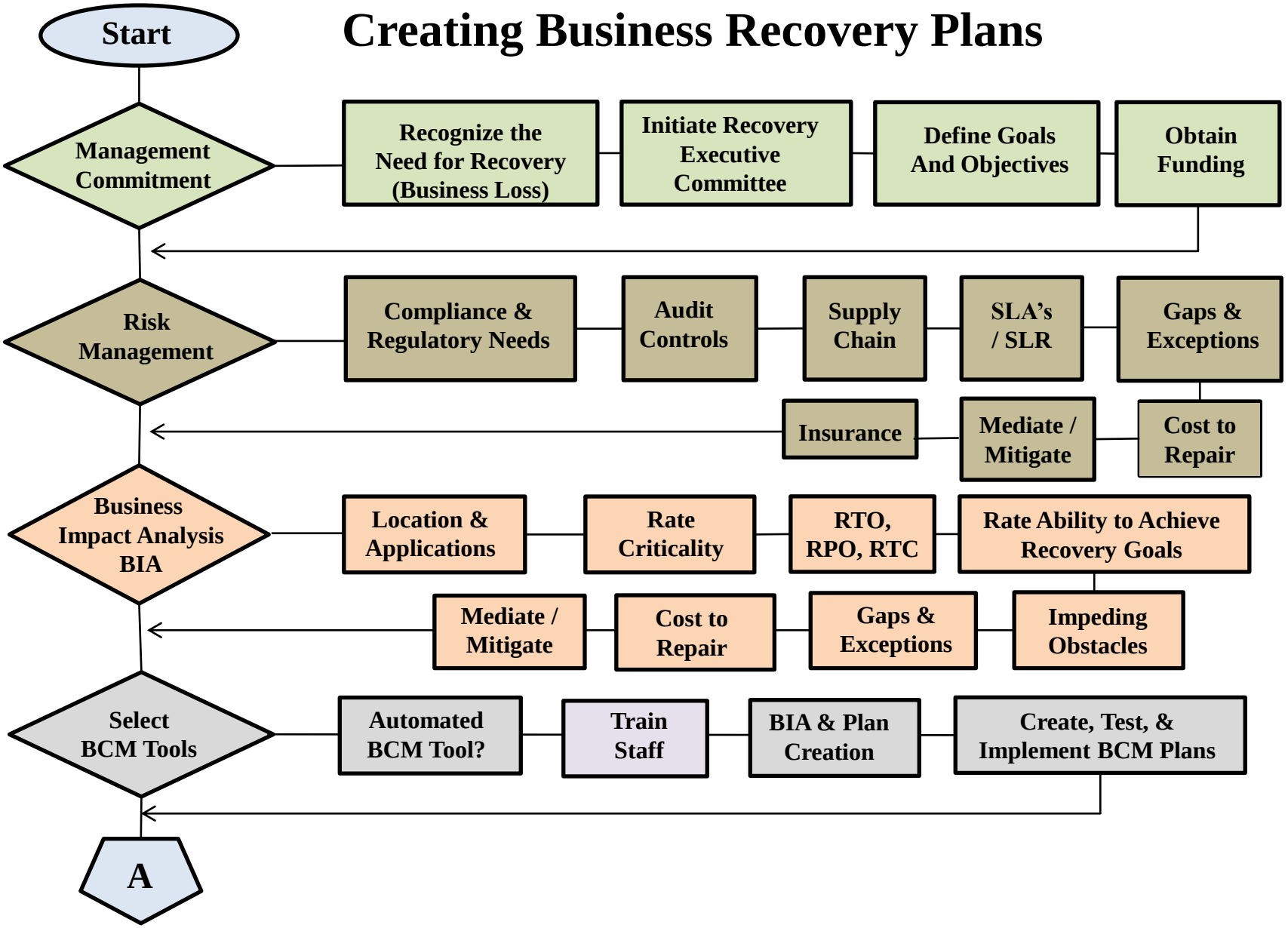
Achieving Recovery Time Objective (RTO) / Recovery Point Objective (RPO) and Recovery Time Capability (RTC)



Other Terms include:

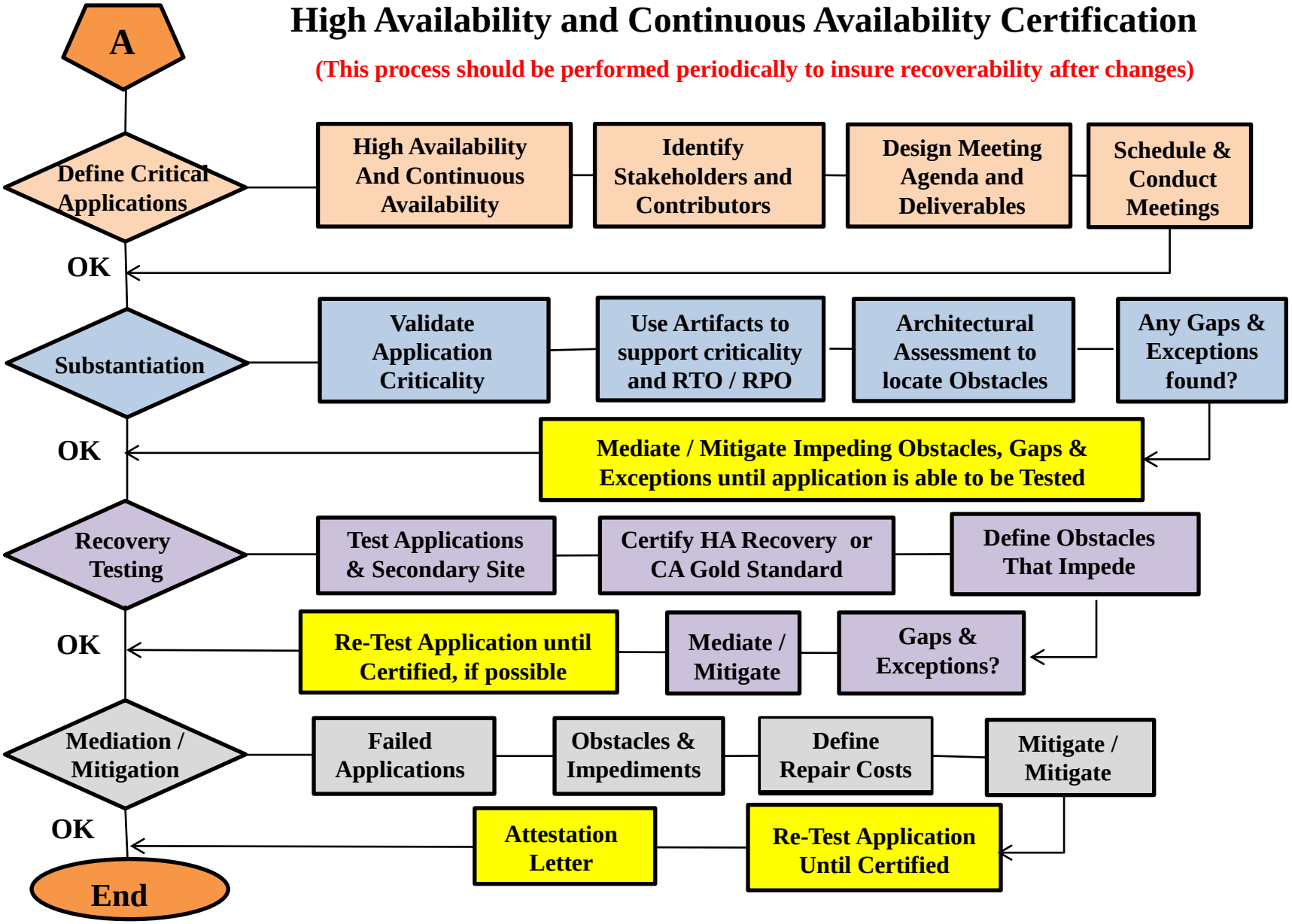
RTE – Recovery Time Expectation;
RPE – Recovery Point Expectation; and
SRE – Service Recovery Expectation.

Creating Business Recovery Plans

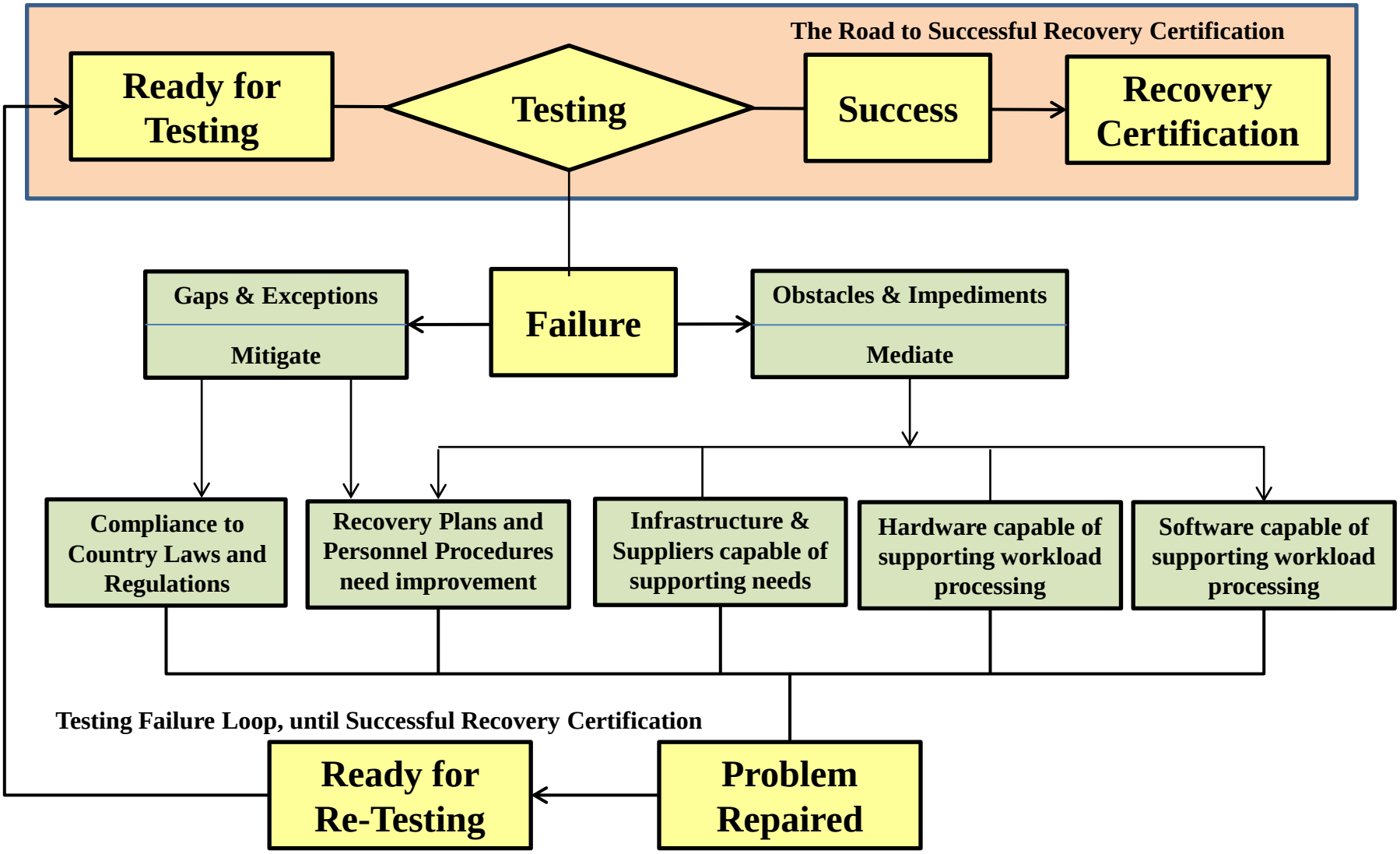


High Availability and Continuous Availability Certification

(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



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

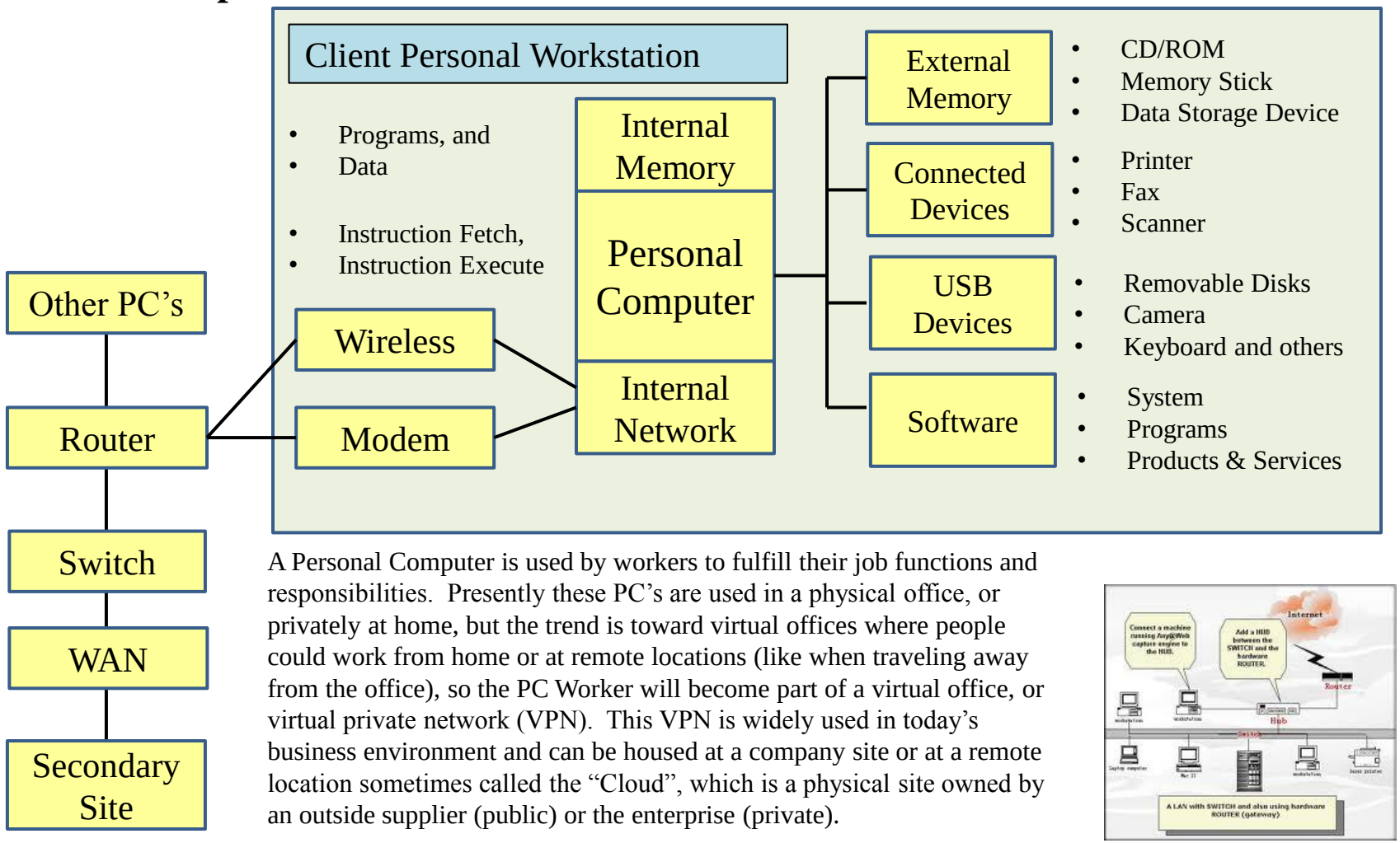
Testing & Review
- Testing
- Review
- Update
- Assurance

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

Personnel Computer environment

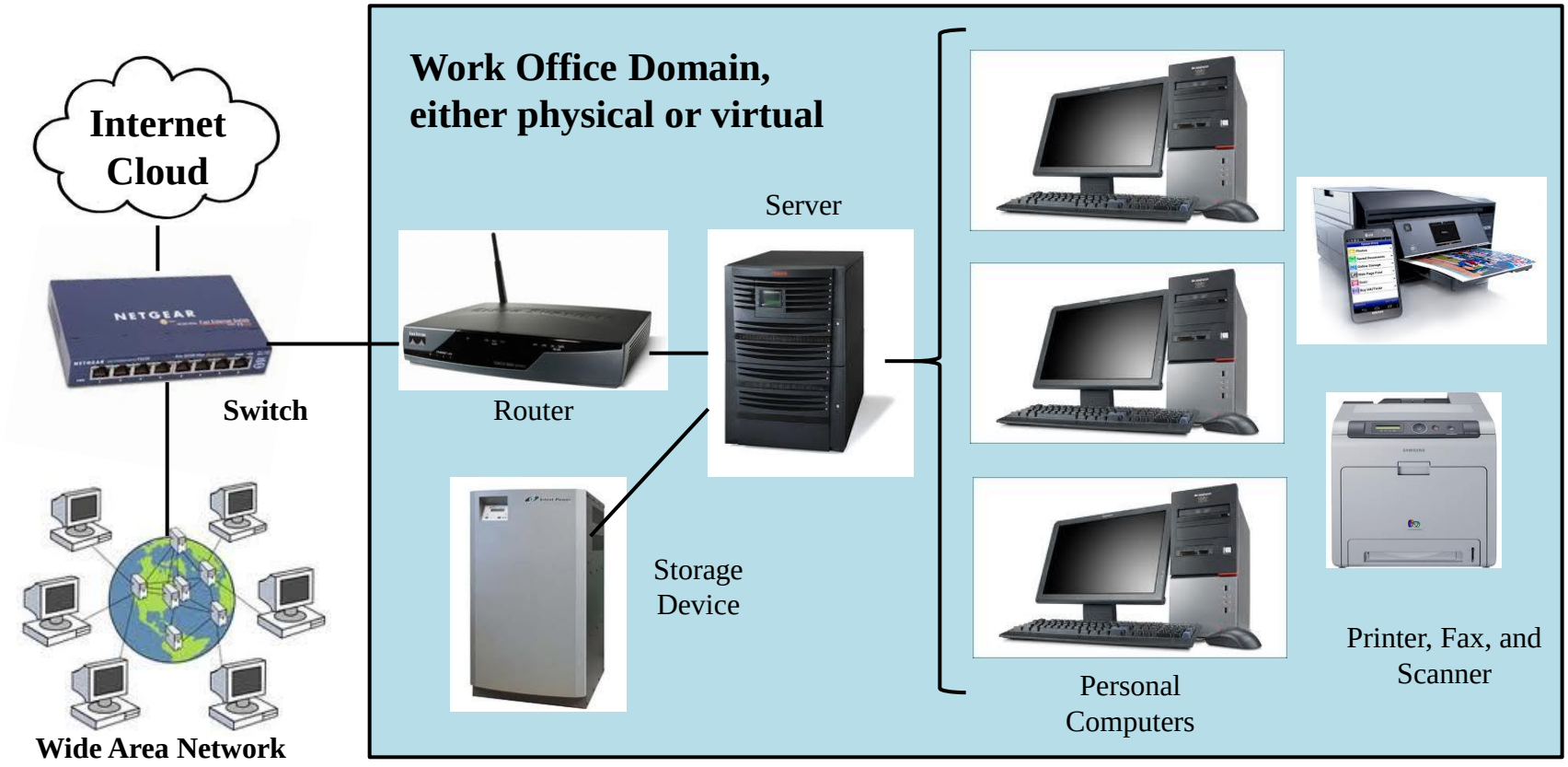


Privately owned client site or vendor owned sometimes referred to as the "Cloud".

A Personal Computer is used by workers to fulfill their job functions and responsibilities. Presently these PC's are used in a physical office, or privately at home, but the trend is toward virtual offices where people could work from home or at remote locations (like when traveling away from the office), so the PC Worker will become part of a virtual office, or virtual private network (VPN). This VPN is widely used in today's business environment and can be housed at a company site or at a remote location sometimes called the "Cloud", which is a physical site owned by an outside supplier (public) or the enterprise (private).

Programs can be stored in the server or accessed through the server, which will result in reduced costs and greater security by limiting access to authorized personnel only. This will also reduce costs for data and equipment.

Physical / Virtual Office Domains



Each Domain has a name (Domain Named Server – DNS) and contains components like PC's, printers, faxes, scanners, Storage Devices, etc.. Domains support office environments and can be either physical or virtual. Today's business model is moving from a physical to a virtual domain concept and access to the domain is migrating from the WAN to the Cloud. Clouds can be privately owned by the enterprise or owned by an outside vendor supplying services to the enterprise.

This presentation will show how products and services are created, tested, quality assured, migrated to production, supported, maintained and accessed in compliance to domestic and regulatory requirements which must be adhered to before an enterprise can do business in a country.

Target Environment

Intel Builds Dell x86 Chips for their Servers

Dell x86 Servers

IBM AIX P7 ("Watson") Systems using AIX VMware vSphere 5 and AIX Tivoli

1 million I/O per Sec.

Remote Storage

Local Storage

Double-Talk

Cisco Network Equipment for remote locations

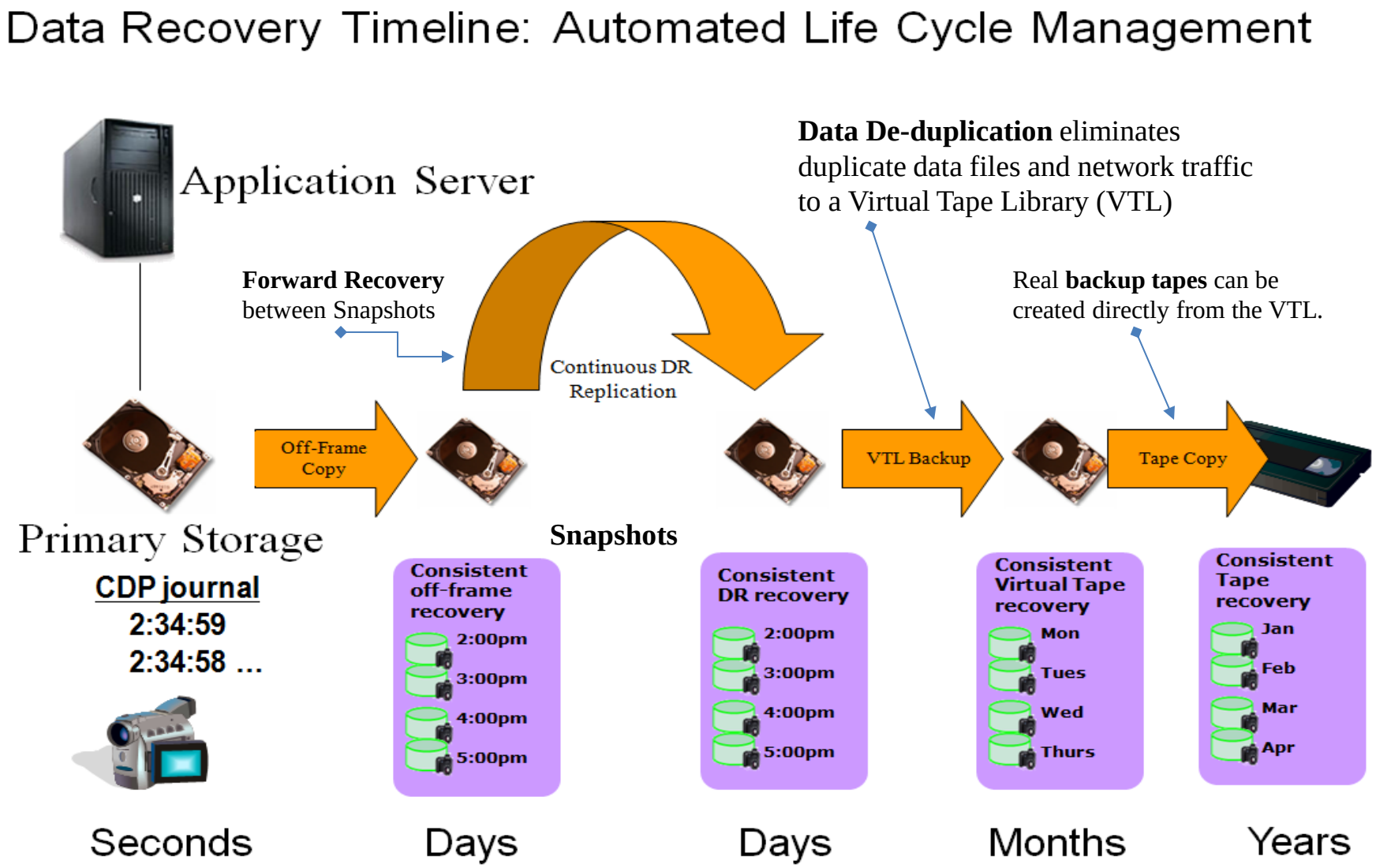
NetApp NAS to support Remote and Cloud Storage

EMC SAN, supporting 2 channels, AIX Storage Array, up to 2 TeraBytes of Local storage

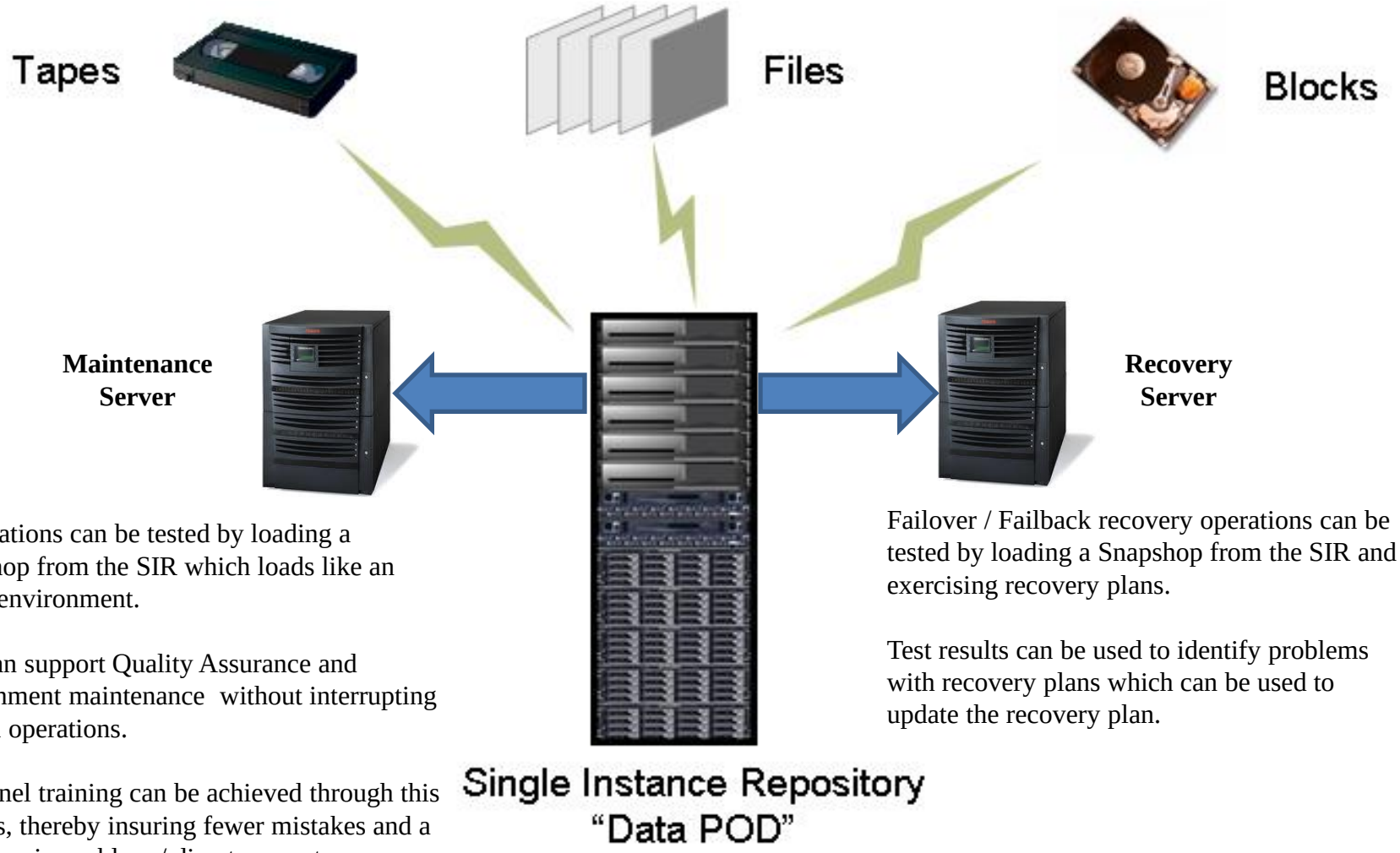
VMware vSphere 5 Software Supports :

- **vShield for Cloud Computing - security, control, and compliance.**
- **vCenter Site Recovery Manager 5.**
- **vCloud Director 5 – model and activate recovery and failover.**

Optimized Protection / Recovery Data Services



Data Protection, Maintenance, and Recovery



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

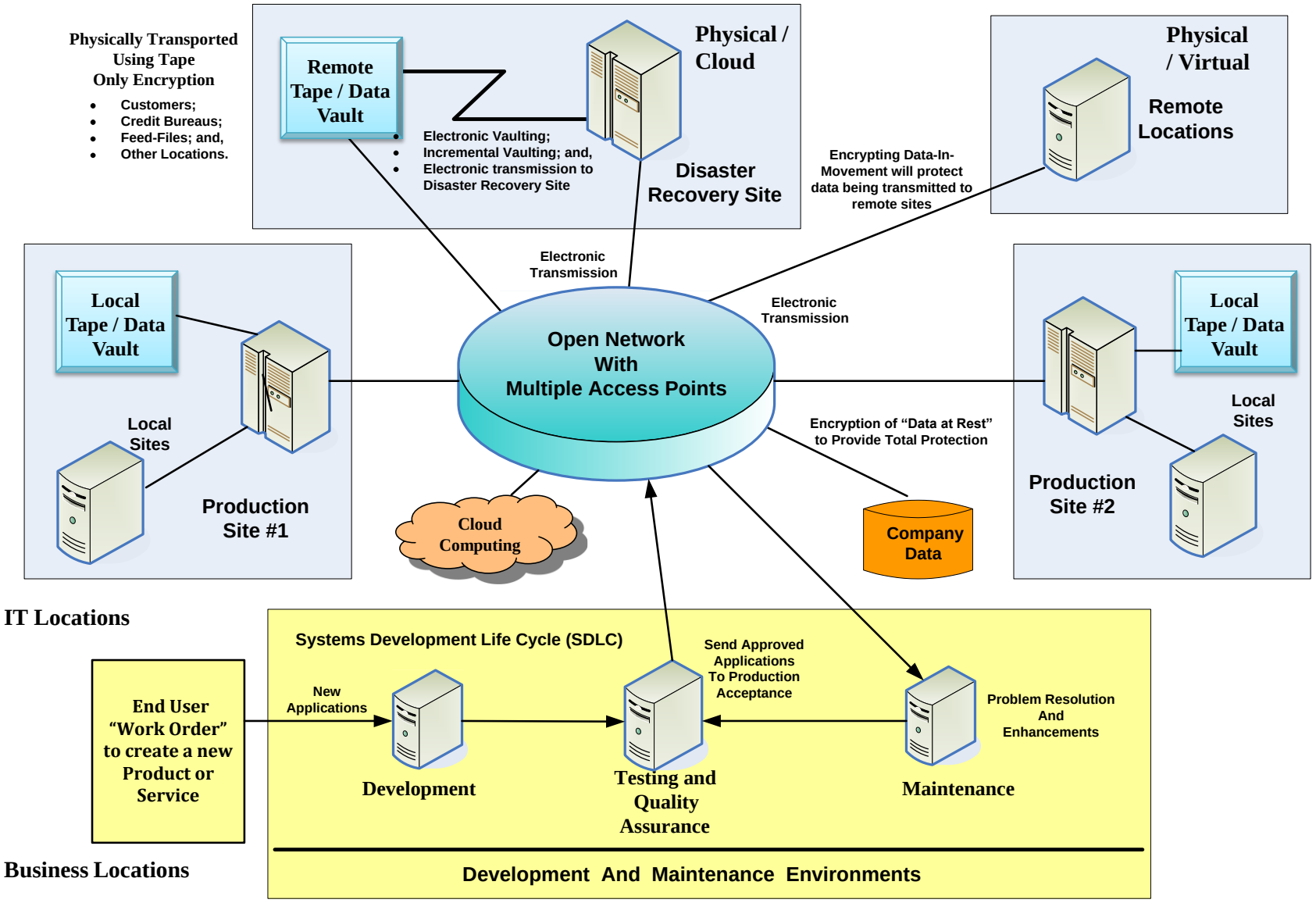
This can support Quality Assurance and environment maintenance without interrupting normal operations.

Personnel training can be achieved through this process, thereby insuring fewer mistakes and a reduction in problem / disaster events.

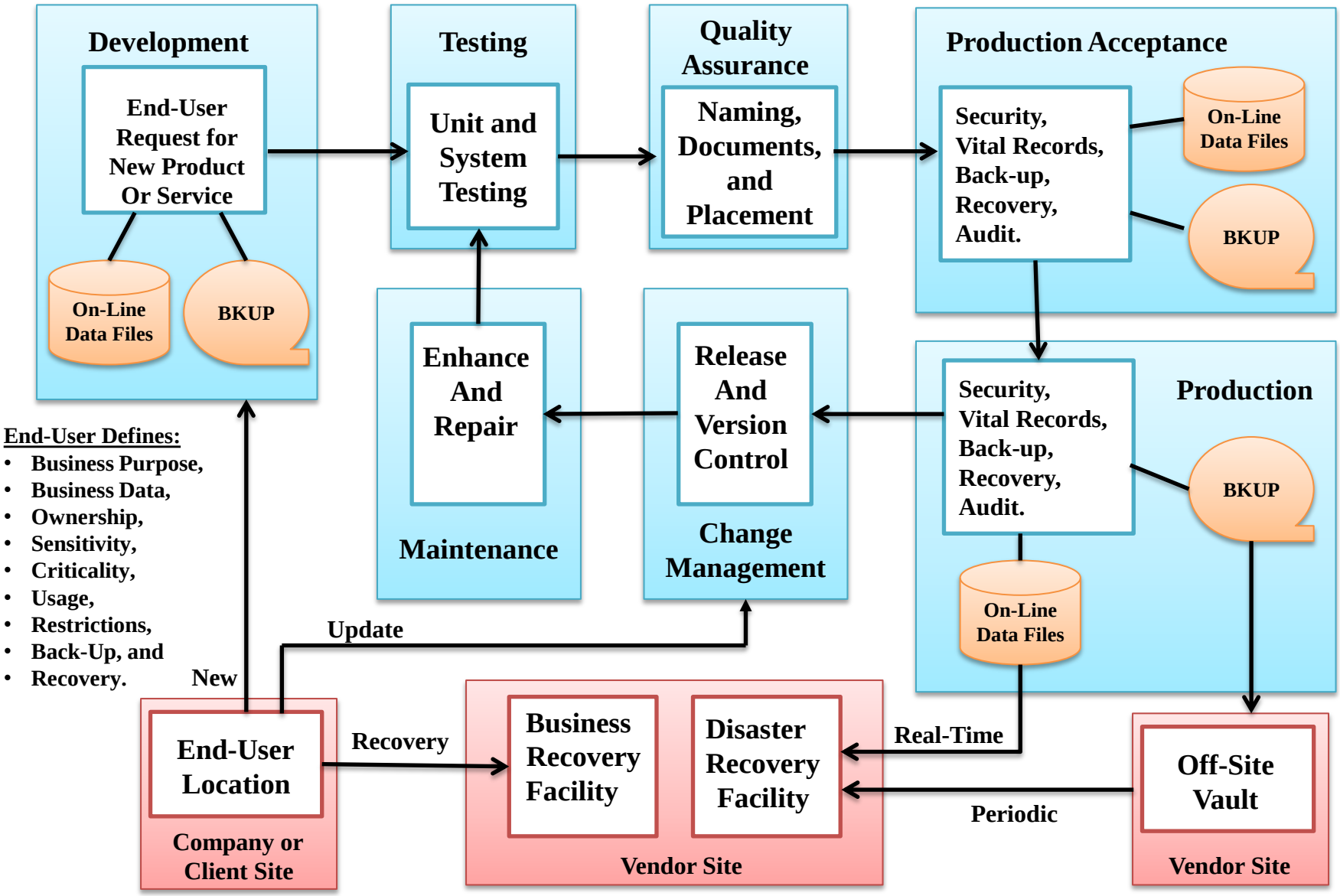
Failover / Failback recovery operations can be tested by loading a Snapshop from the SIR and exercising recovery plans.

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

Overview of the Enterprise Information Technology Environment

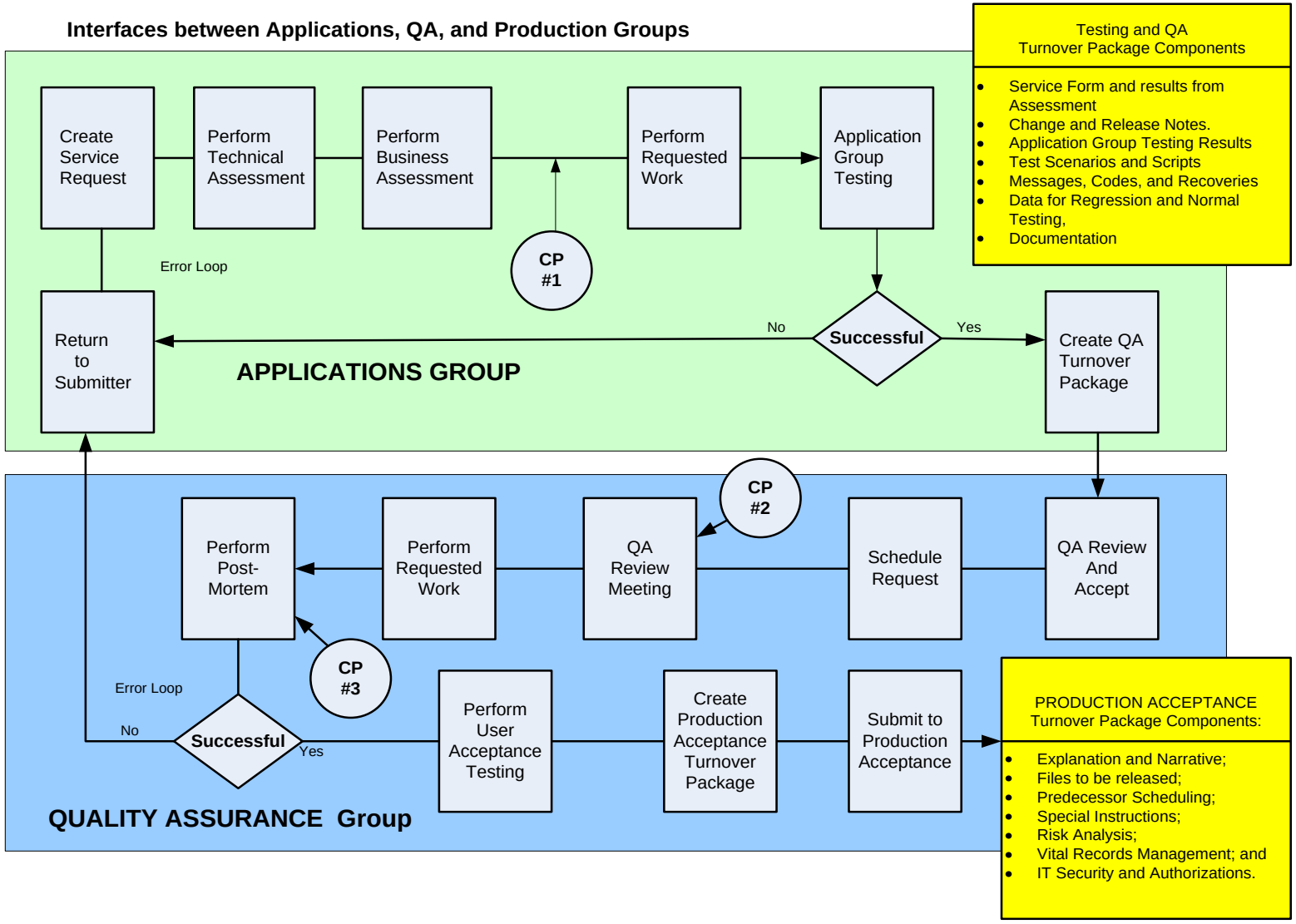


Systems Development Life Cycle (SDLC), Components and flow



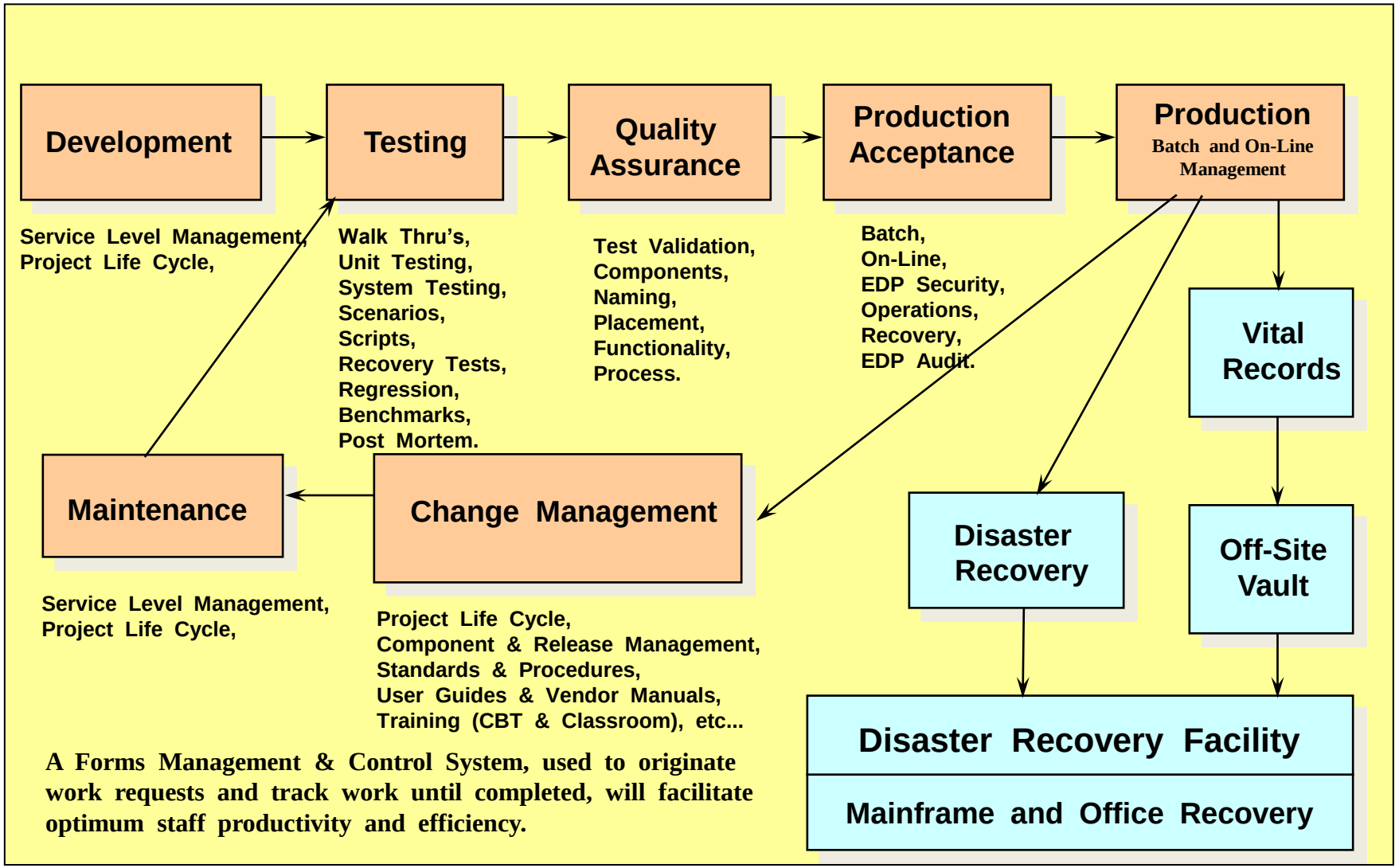
Migrating products / services to the Production Environment

Quality Assurance and SDLC Checkpoints



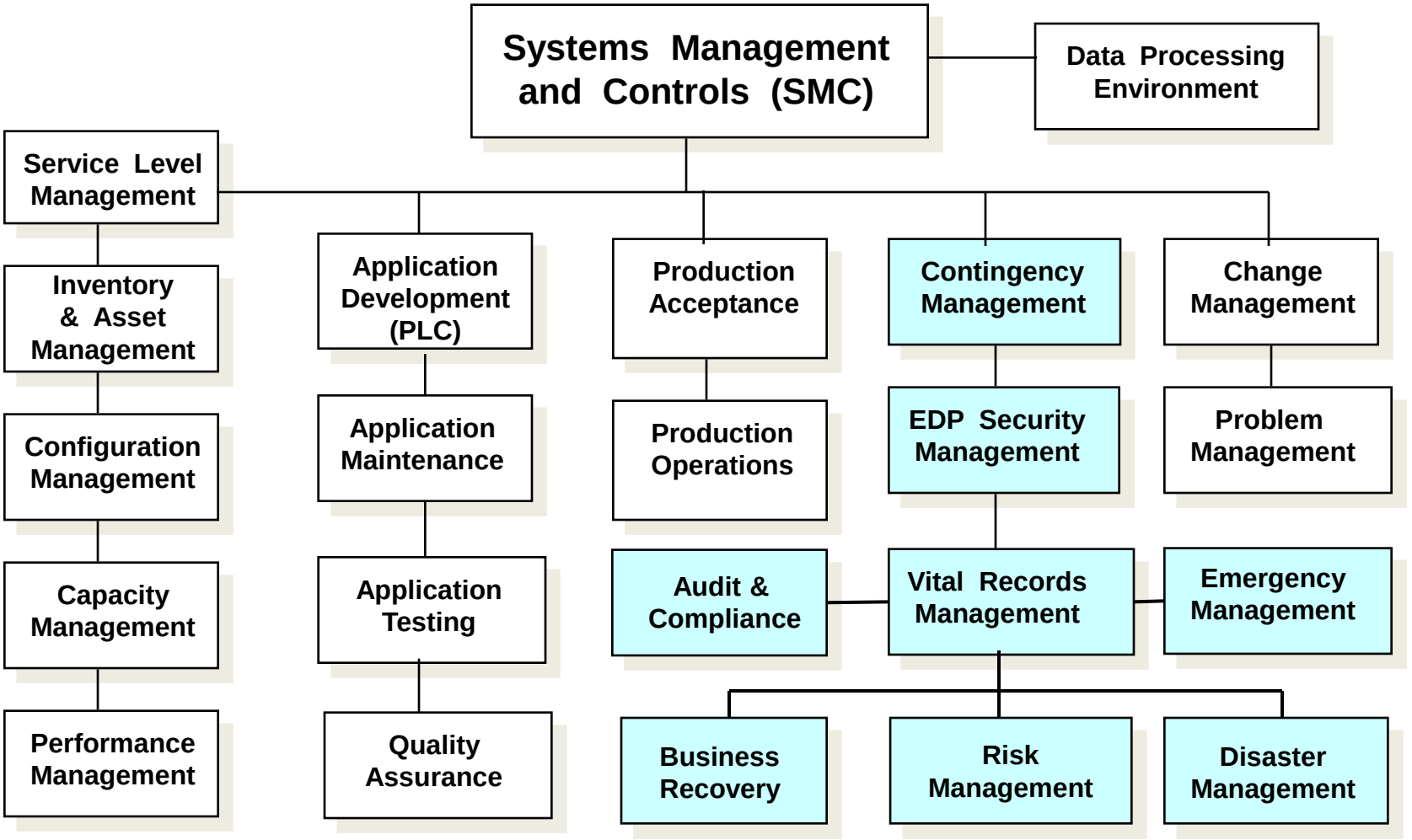
Systems Management Controls and Workflow

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



A Forms Management & Control System, used to originate work requests and track work until completed, will facilitate optimum staff productivity and efficiency.

Systems Management Organization



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:

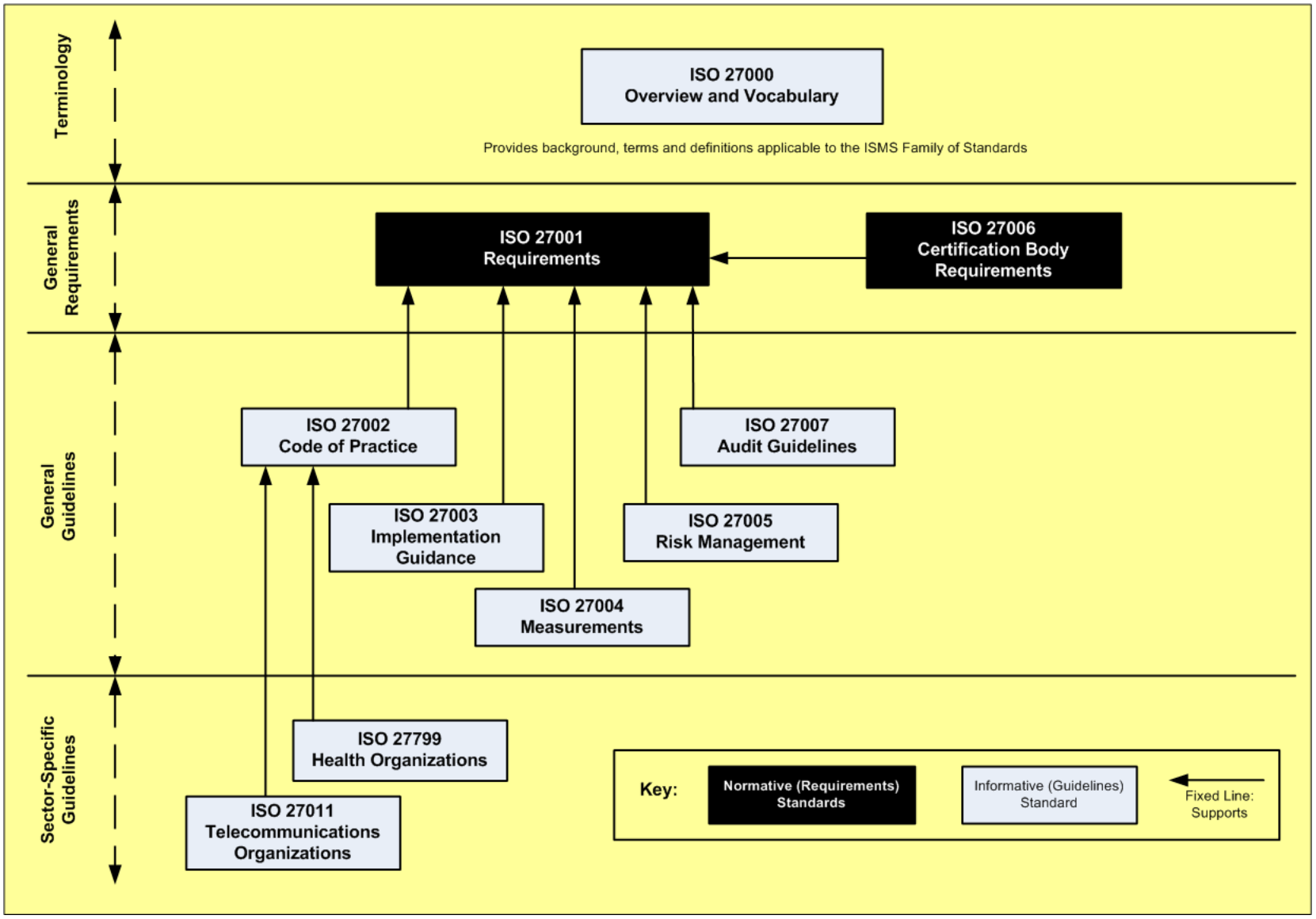
User Name: _____ User Division: _____ User Identifier _____
Work Order #: _____ Date: _____ For: _____

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: **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: $ _____

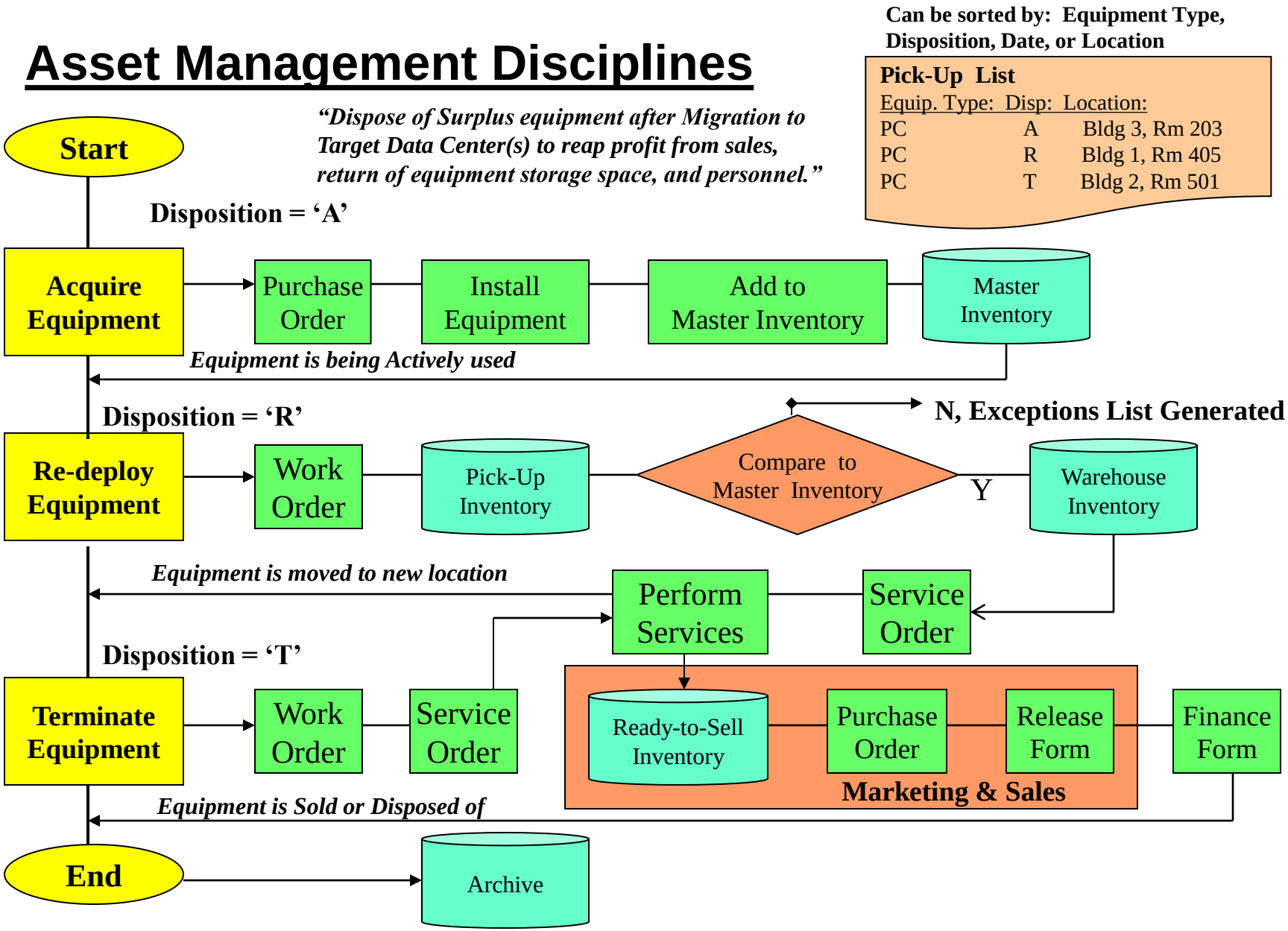
Total Cost: $ _____

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.

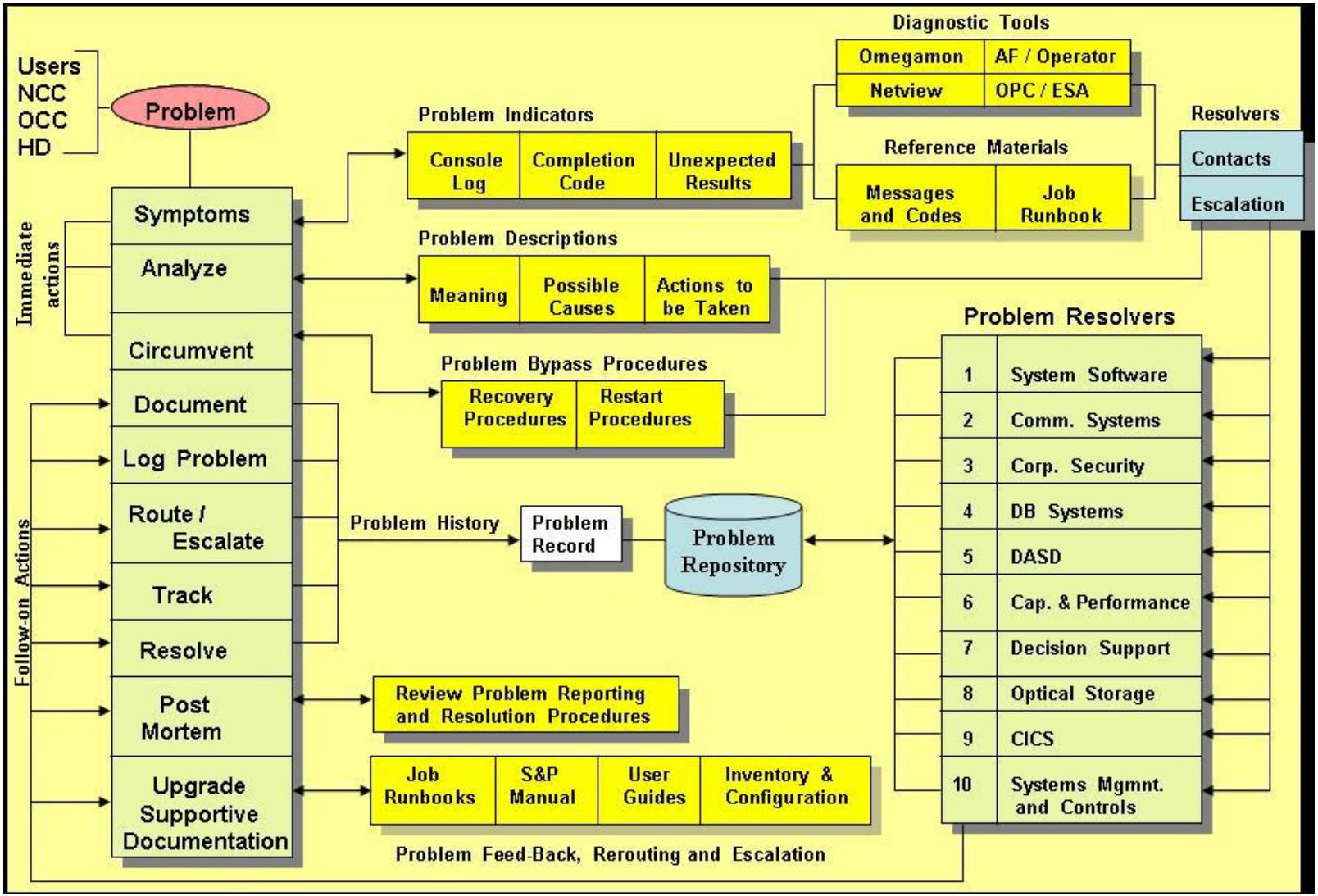
ISO 2700 Overview and Sections



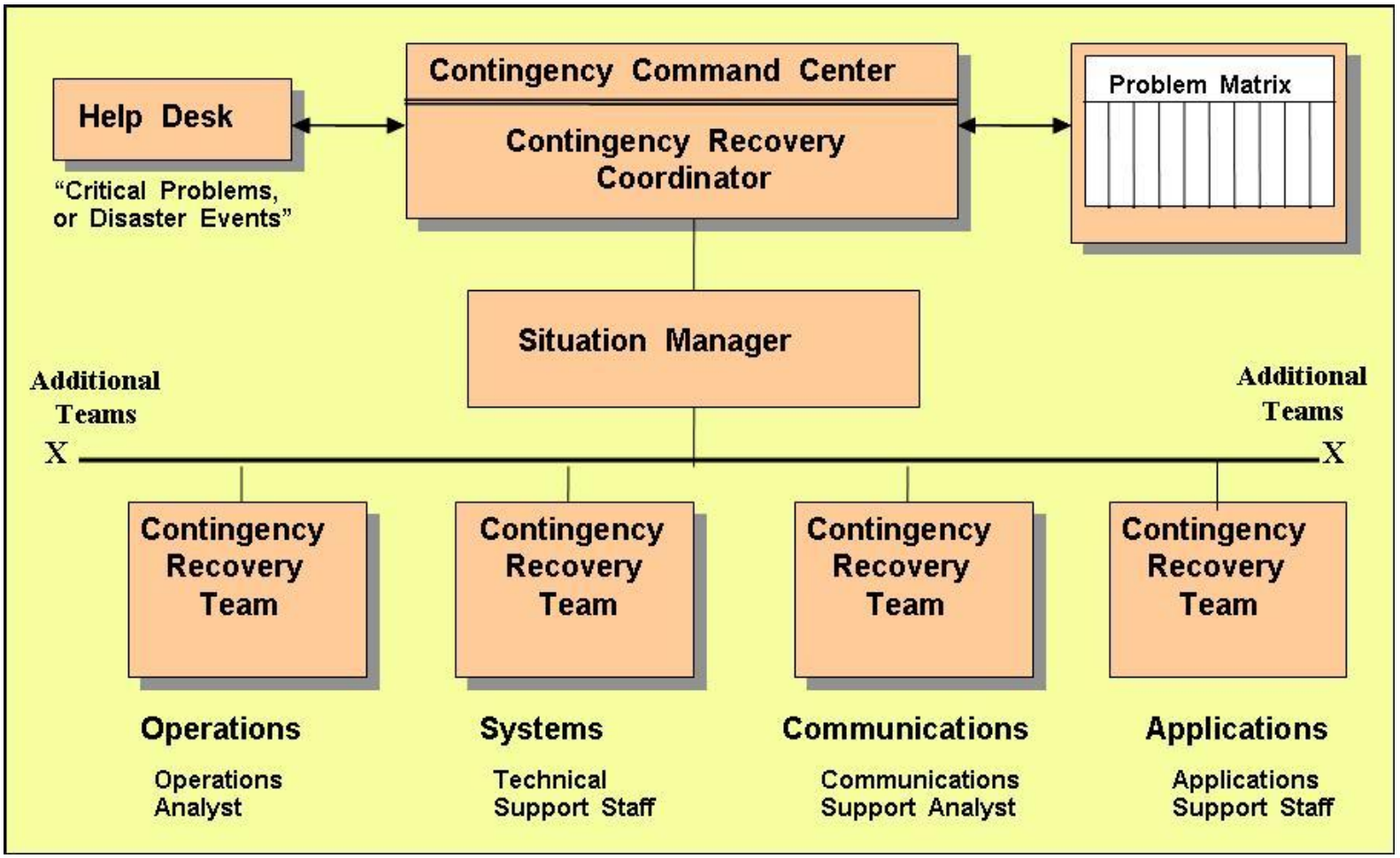
Asset Management Disciplines



Problem Management and Circumvention Techniques



Help Desk / Contingency Command Center Operations



Problems are reported to Help Desk who compare critical problems to Problem Matrix and Select Recovery Plan then call Situation Manager who assembles necessary Recovery Teams to respond to critical problems and disaster events. Lessons learned are used to update recovery procedures.

The Potential Risks and Threats facing a Corporation

Malicious Activity:
- Fraud, Theft, and Blackmail;
- Sabotage, Workplace Violence; and
- Terrorism.

Natural Disasters:
- Fire;
- Floods and other Water Damage;
- Avian, Swine, or other Epidemic / Pandemic occurrence;
- Severe Weather;
- Air Contaminants; and
- Hazardous Chemical Spills.

Technical Disasters:
- Communications;
- Power Failures;
- Data Failure;
- Backup and Storage System Failure;
- Equipment and Software Failure; and
- Transportation System Failure.

External Threats:
- Suppliers Down;
- Business Partner Down; and
- Neighboring Business Down.

Facilities:
- HVAC – Heating, Ventilation, and Air Conditioning;
- Emergency Power / Uninterrupted Power; and
- Recovery Site unavailable.

Recovery Management plans for loss of a location, service, vendor, or personnel due to a disaster event.

Disasters can render unusable / un-accessible specific resources (like a building) due to: flooding; water damage; inclement weather; transportation outage; power outage; or many other situations. Rather than write specific recovery plans for each event that could render a building un-accessible, a single plan for loss of a building can be written and incorporated into the crisis management plan associated with the specific disaster event causing the need to evacuate a building.

Disasters result from problems and problems are the result of a deviation from standards. By making sure your standards and procedures are correct and maintained you will reduce disaster events. These procedures should be included in the SDLC, Maintenance, and Change Control process.

Working with the community will allow recovery managers to become good neighbors, build relationships with other recovery managers, and keep aware of situations outside of their control.

Working with governmental agencies like FEMA , OEM, and Homeland Security will help recovery managers to stay current with compliance needs and recovery planning trends.

Laws and Regulations Justifying the Need for a Recovery Plan

History and Goals:

- **Enterprise-Wide Commitment;**
- **Emergency Management and Workplace Violence Prevention;**
- **Disaster and Business Recovery Planning and Implementation;**
- **Risk Management Implementation;**
- **Protecting Critical Information;**
- **Safeguarding Corporate Reputation.**

"For Contingency Planning to be successful, a company-wide commitment, at all levels of personnel, must be established and funded. Its purpose is to protect personnel, customers, suppliers, stakeholders, and business operations."

Laws and Regulators:

Controller of the Currency (OCC):

- **Foreign Corrupt Practices Act;**
- **OCC-177 Contingency Recovery Plan;**
- **OCC-187 Identifying Financial Records;**
- **OCC-229 Access Controls; and**
- **OCC-226 End-User Computing.**

"Define all Regulatory, Legal, Financial, and Industry rules and regulations that must be complied with and assign the duty of insuring that these exposures are not violated to the Risk Manager."

- **Sarbanes-Oxley, Gramm-Leach-Bliley,**
- **HIPAA, The Patriot Act, EPA Superfund, etc.**

"Have the Legal and Auditing Departments define the extent of Risk and Liabilities, in terms of potential and real Civil and Criminal damages that may be incurred."

Penalties:

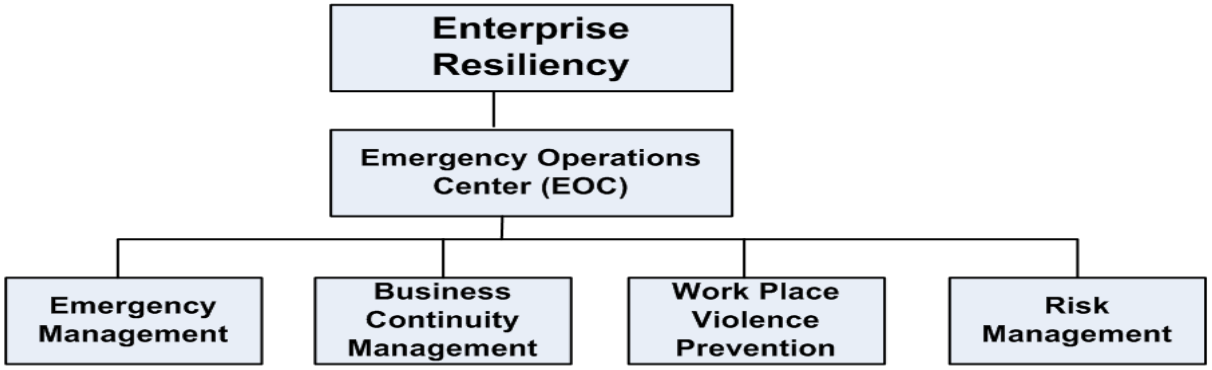
- **Three times the cost of the Outage, or more; and**
- **Jail Time is possible and becoming more probable.**

Insurance:

- **Business Interruption Insurance; and**
- **Directors and Managers Insurance.**

"Once you have defined your exposures, construct an Insurance Portfolio that protects the business from sudden damages that could result from a Disaster Event."

What is Enterprise Resiliency



The goal of Enterprise Resiliency is to combine the four recovery disciplines of Emergency Management, Business Continuity Management, Workplace Violence Prevention, and Risk Management into a cohesive recovery management discipline with a common language and common tools. By following this path, Recovery Personnel will learn all recovery disciplines making them better able to identify and respond to disaster events by utilizing the common language, tools, and a common set of Standards and Procedures (optimized Communications).

The Road to Enterprise Resiliency Includes (steps to follow):

1. Define Risks (Natural, Man-Made, Use CERT RMM and COSO for direction);
2. Determine Compliance Requirements (see GLB, HIPPA, SOX, Patriot Act, EPA Superfund);
3. Use Best Practices tools and processes (COBIT, ITIL);
4. Understand road to Corporate Certification Guidelines (DRII, BCI);
5. Locate Certification Firms / Organizations (Training the Trainers is in process now);
6. Develop a Business Plan and create a Management Commitment within Project Initiation Directive defining Scope and Commitment;
7. Perform Risk Assessment / BIA to define current Risks their costs and your ability to respond to Risks;
8. Build Business Recovery Plans for offices and business locations;
9. Build Disaster Recovery Plans for data centers and IT Infrastructure;
10. Build Emergency Recovery Plans to protect against Fire, Floods, Physical Protection, and First Responder;
11. Build Workplace Violence Prevention Plans to protect locations and personnel;
12. Defined Functional Responsibilities to determine what must be done and by who;
13. Create / Expand Job Descriptions to direct personnel in the recovery efforts; and
14. Create / Update / Use Standards and Procedures, updating as changes are made.

Why Implement Enterprise Resiliency and Corporate Certification?

The Problem

- Coordinating Recovery Operations for all disciplines;
- Better safeguard personnel, clients, suppliers, and business operations;
- Improving problem response times and reducing outage times;
- Developing a common Recovery Language and Toolset throughout the enterprise;
- Adhering to Compliance requirements;
- Insuring clients and suppliers that recovery operations are optimized;
- Complying with Domestic and International Recovery Guidelines; and
- Gaining Corporate Certification for Recovery Operation.

The Solution:

Develop Enterprise Resiliency Operation, including:

- Emergency and Risk Management;
- Business Continuity / Disaster Recovery Management / Crisis Management; and,
- Workplace Violence Prevention.

Gain Corporate Certification by adhering to industry guidelines, including:

- BS 25999 / ISO 22301 (international);
- Private Sector Preparedness Act (domestic);
- National Fire Prevention Association 1600;
- Certification Firms / Organizations to verify compliance and recovery practices; and,
- Certify Recovery Personnel via DRII or BCI training / testing.

Use Best Practices to achieve goals, including:

- COSO;
- CobIT;
- ITIL;
- ISO 27000;
- Six Sigma; and,
- FFIEC.

Integrating Enterprise Resiliency throughout the Corporation, including;

- Business Operations, Client Support, and Supplier Support;
- System Development Life Cycle, Change Management, and Functional Responsibilities;
- Resiliency Documentation, Awareness, and Training;
- Functional Responsibilities, Job Descriptions, Standards and Procedures Manual; and,
- Corporate-Wide Compliance and Recovery Operations.

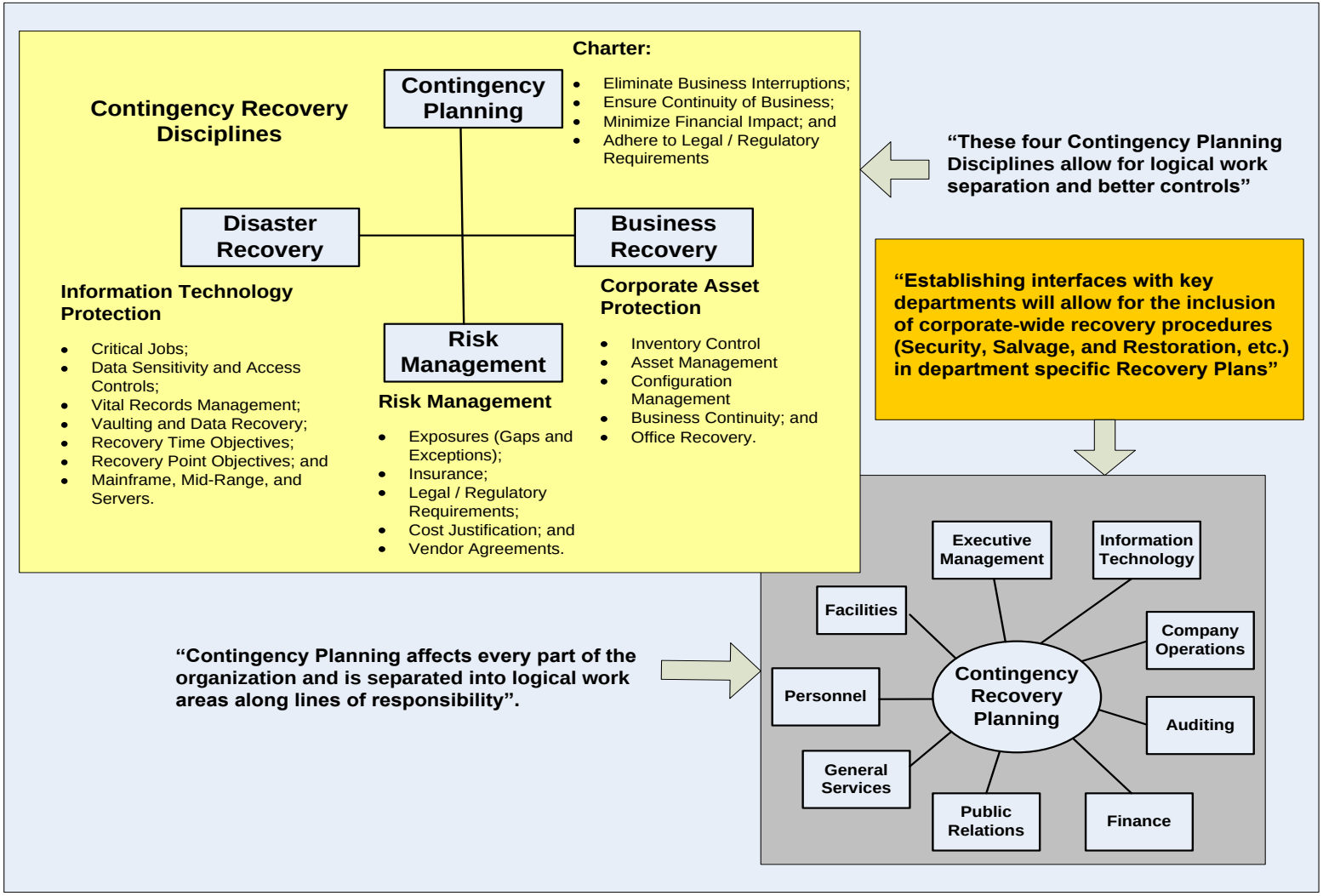
The Goal of Combining Recovery Operations

- **Desire to most rapidly and efficiently respond to encountered disaster events, or other emergencies by merging Emergency Management, Business Continuity, Disaster Recovery, and Workplace Violence Prevention:**
- **Best approach to protecting Employees, Customers, Suppliers, and Business Operations:**
- **Ensuring the Reputation and Integrity of the Organization;**
- **Combining many Lines of Business into a cohesive recovery structure with a common set of objectives, templates, tools, and a common language;**
- **Ensuring that your recovery environment meets and exceeds industry Best Practices;**
- **Utilization of Automated Tools;**
- **Integration of Best Practices like COSO, CobIT, ITIL, Six Sigma, ISO 27000, and FFIEC to optimize personnel performance, Standards and Procedures;**
- **Certify the business recovery environment and its components;**
- **Staffing, Training and Certifying Recovery Personnel;**
- **Integration with the Corporation, Customers, and Suppliers;**
- **Interfacing with First Responders, Government, and the Community;**
- **Working with Industry Leaders to continuously enhance recovery operations and mitigate gaps and exceptions to current practices;**
- **Achieve Compliance through Risk Management and Audit adherence;**
- **Testing and Quality Assurance; and**
- **Support and Maintenance going forward.**

What is Emergency Management and Corporate Certification?

- **Emergency Management Preparedness:**
  - First Responders (Fire / Police, / EMT, etc.);
  - Emergency Operations Center (EOC);
  - Department of Homeland Security (DHS); and
  - Office of Emergency Management (OEM).
- **Business Recovery Management:**
  - Business Recovery;
  - Disaster Recovery;
  - Risk Management; and
  - Crisis Management.
- **Workplace Violence Prevention:**
  - Security (Physical and Data) and Guards;
  - Closed Circuit Cable TV;
  - Access Controls and Card Key Systems;
  - Response Plans and Crisis Management Procedures; and
  - Employee Assistance Programs.
- **Supportive Agencies:**
  - Disaster Recovery Institute International (DRII);
  - Business Continuity Institute (BCI);
  - Contingency Planning Exchange; and
  - Association of Contingency Planners.
- **Supportive Tools:**
  - Recovery Planner RPX;
  - Living Disaster Recovery Planning System (LDRPS);
  - Six Sigma or Workflow Management;
  - Information Technology Infrastructure Library (ITIL);
  - Company Standards and Procedures; and
  - Training and Awareness services.
- **Corporate Business Resiliency Certification:**
  - Private Sector Preparedness Act (PL 110-53 Title IX Section 524);
  - National Fire Prevention Association Standard 1600; and
  - BS25999 / ISO 22301 International Standard;
  - FFIEC.

Business Continuity Management Disciplines and Integration



Crisis Management, to Respond to / Control Disaster Events

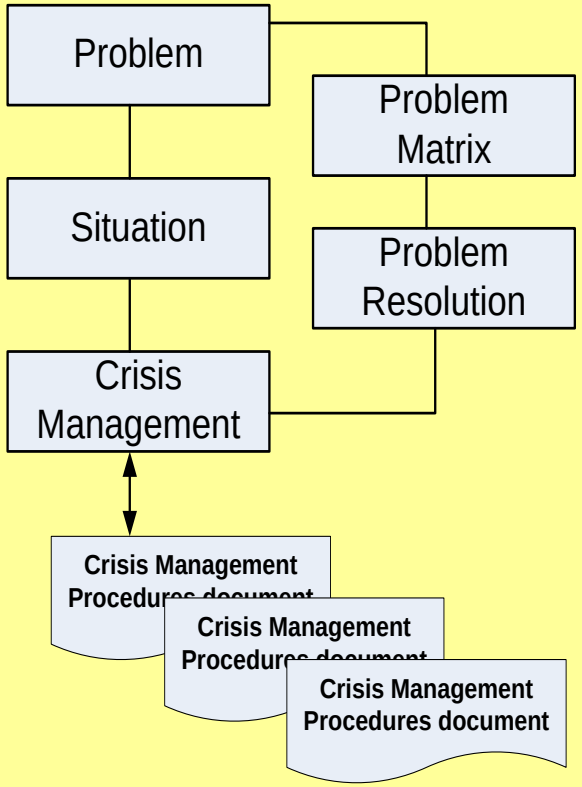
How Problems become Disasters and Controlling them through Crisis Management

When a problem arises and there are no formal procedures to direct Operations personnel in the analysis and repair of the problem, then a situation can occur that may lead to a potential crisis.

Compounding a problem by taking unnecessary actions can lead to a prolonged outage, which can effect the ability to meet deadlines. This additional scheduling problem may result in a situation which can lead to a crisis as well.

An example of this would be when a Data Check on a Hard Disc Storage device occurs and there are no back-up copies of the information. This problem would create a prolonged outage, because the data contents on volume would have to be recreated. Additionally, if multiple jobs are dependent upon the failed Volume the effect of the problem will be even greater. This type of crisis situation could very easily be avoided by insuring that all Data Volumes have back-up copies stored in the local vault, so that restores can be provided. An additional copy of the Data Volume should also be stored in an off-site vault if the data is critical. In today's IT environment, real-time and/ or incremental data backups are commonplace.

The goal of Crisis Management is to determine which problem types can occur and their impact. To then develop recovery plans and instruction that direct personnel to take appropriate actions when problems occur that would eliminate a crisis situation from arising. It is based on preparation and not response.



NYS Workplace Violence Prevention Act

June 7, 2006 – Article 27-6 of Labor Law

Employers must perform a Workplace Evaluation or Risk Assessment at each worksite to develop and implement programs to prevent and minimize workplace violence.

Commonly referred to as "Standard of Care" and the OSHA "General Duty Law" which must be in place to avoid, or limit, law suites. It consists of:

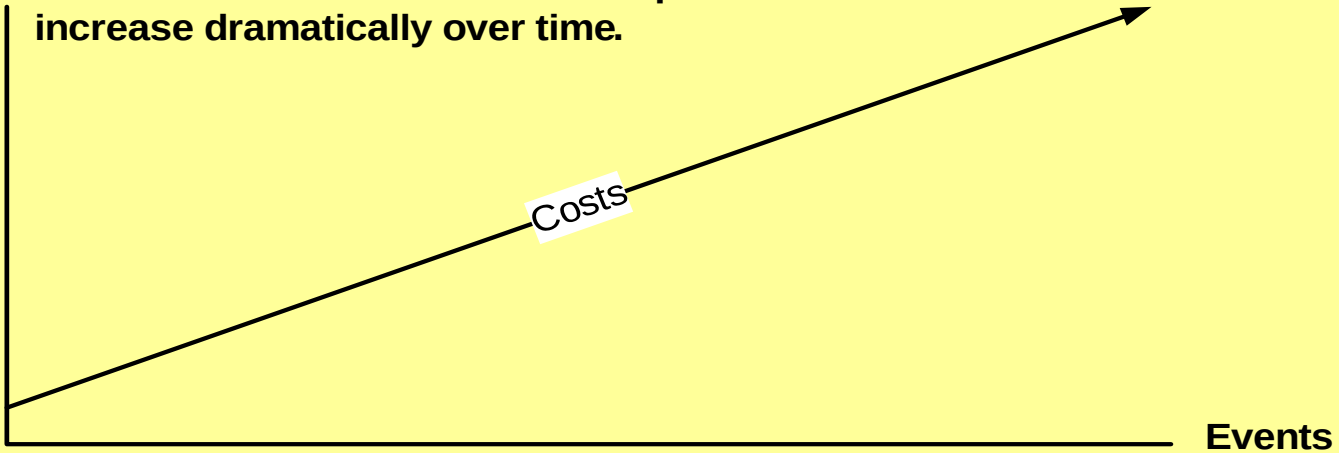
1. Comprehensive policy for Workplace Violence;
2. Train employees on Workplace Violence and its impact; and
3. Use Best Practices for Physical Security and Access Controls.

Why Workplace Violence occurs and most likely reason for offence:

- Number one cause is loss of job or perceived loss of job;
- Presently being addressed REACTIVELY, but should become PROACTIVE;
- Corporate culture must first accept importance of having a Workplace Violence policy that is embraced and backed by Executive Management;
- "Duty to Warn" - if a threat is made to a person, then they must be informed of the threat and a company must investigate any violent acts in a potential hire's background.
- Average Jury award for Sexual Abuse if $78K, while average award for Workplace Violence is $2.1 million – with 2.1 million incident a year, 5,500 events a day, and 17 homicides a week.
- Survey found that business dropped 15% for 250 days after event. Onsite security costs $25K with all costs totaling $250K / year.
- Offender Profile consisted of:

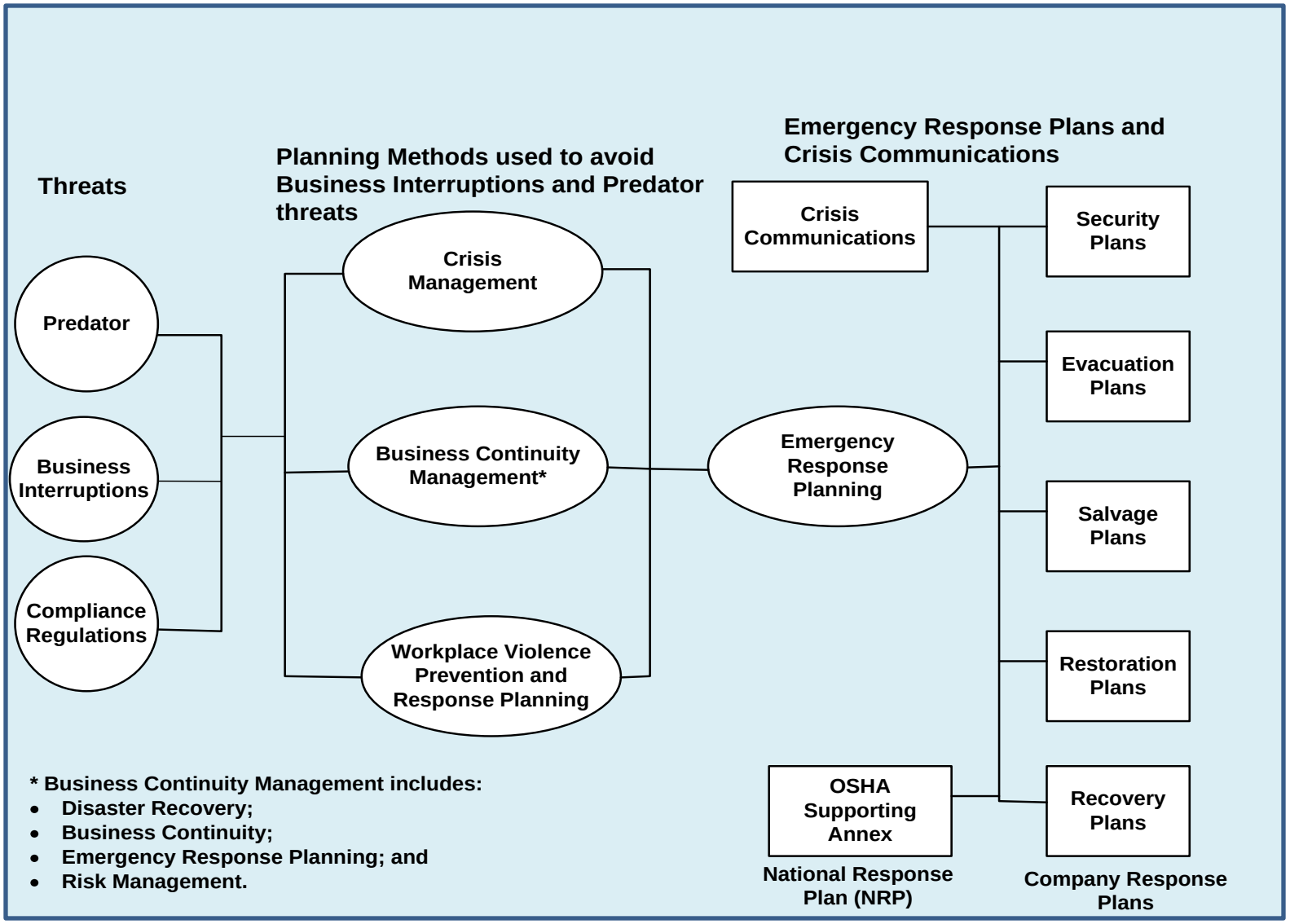
1. Loner (age 26-40) who was made fun of, teased, and abused by workmates;
2. Cultural change has promoted Gun usage;
3. Their identify is made up of their job, so if you fire them they are losing their Identify / Lifestyle and will respond violently.
4. Instead of Workplace Violence, perpetrator may use computer virus, arson, or other methods to damage / ruin business;
5. Hiring tests can be used to identify potential Workplace Violence perpetrators;
6. Does not take criticism well and does not like people in authority;
7. Employee Assistance Programs can be developed to help cope with personal life crisis and avoid Workplace Violence situation – a range of these programs should be developed and made available to the staff and their family.

The Costs of Workplace Violence

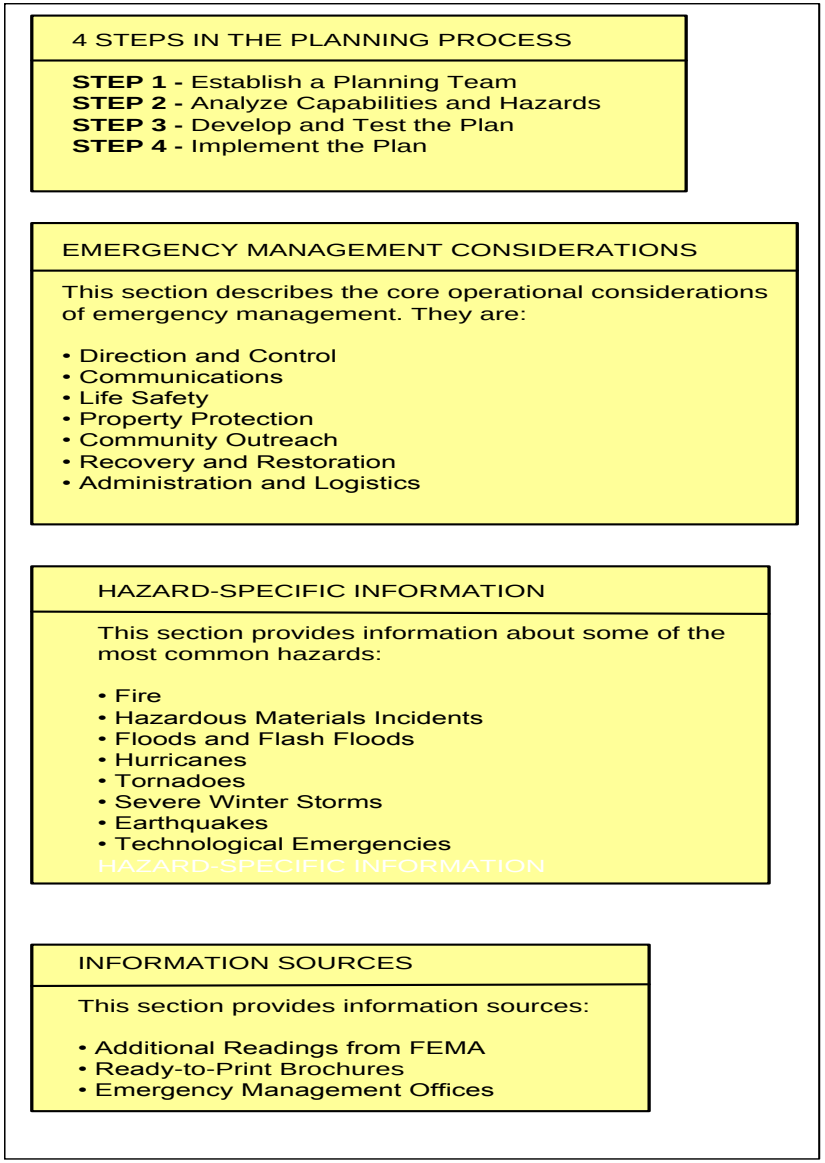


Workplace Violence Prevention Response Plan	Employee Assistance Programs	Crisis Management Plan	Business Continuity Plan	Disaster Recovery Plan	Emergency Response Plan	Risk Management Plan
Identify and Document Employee Safety and Security Issues	Create Mechanisms to allow Employees to Report Problems and Seek Help, Known as **Employee Assistance Programs**	Create Employee Identification Badges and Implement an Access Control System	Contract Guard Service for Physical and Perimeter Protection. Use CCTV to scan environment and document evidence.	Develop and Implement Employee Training and Awareness Programs	Exercise Crisis Management and Recovery Plans on a Regular basis and Update Plans as needed	

Target Emergency Response Environment (Logical Overview)



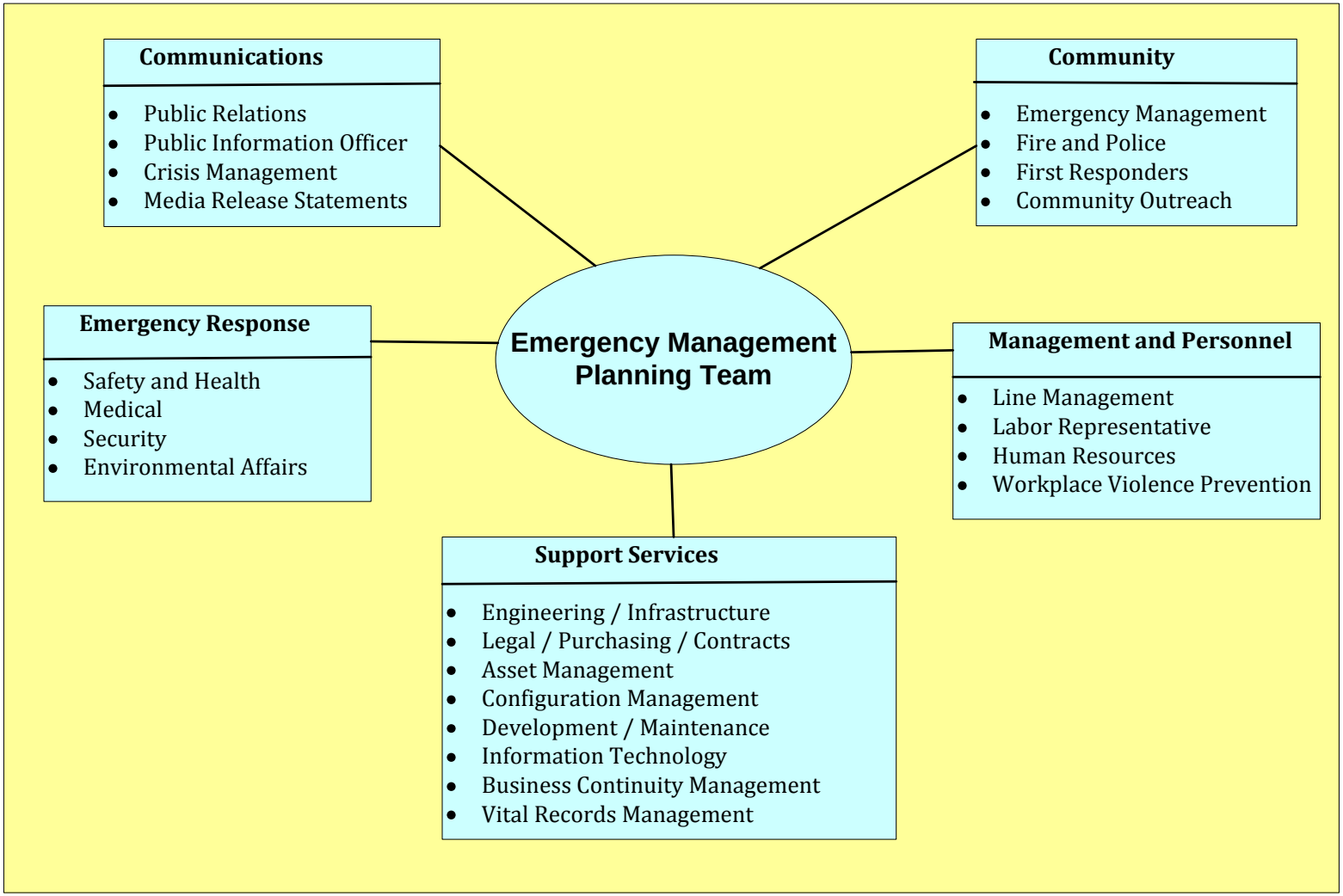
Emergency Management overview and components



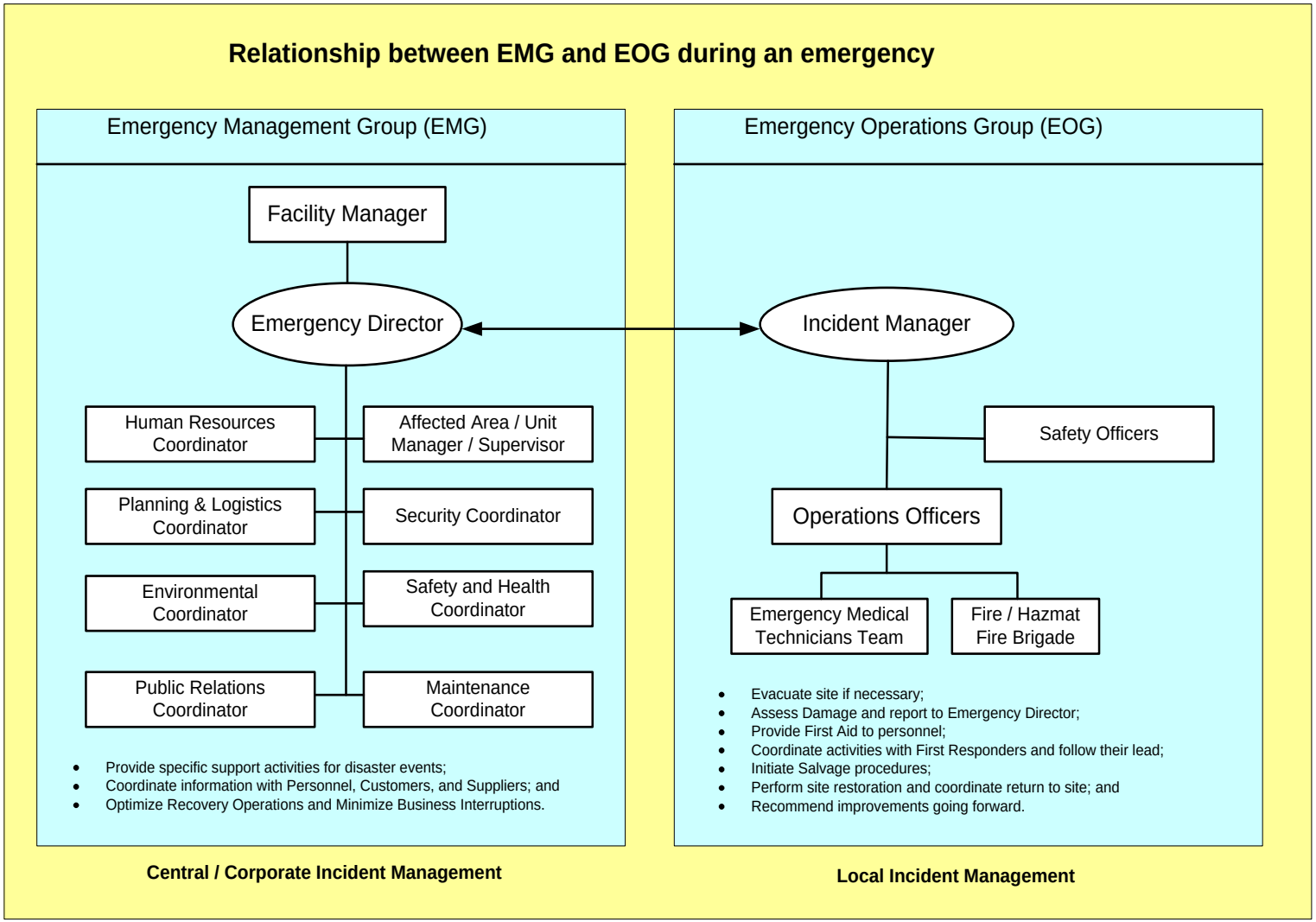
Emergency Management is established and procedures are generated through the following process:

1. Define the EM Planning process, its Scope, and Team members;
2. Release a Project Initiation Executive Memo defining EM Goals, its Priority, and that Executive Management is behind the development of EM and associated procedures;
3. EM team will develop project plan containing EM Considerations and planned direction, with time line, costs, deliverables, and resource requirements;
4. Management is provided with Executive Presentation and Written Report on EM Direction and Plan, so that Approval can be received and any concerns corrected before moving forward;
5. EM develops procedures, trains personnel, and tests prototype action plans;
6. Corrections and updates are created based on Lessons Learned;
7. EM Trial Project(s) are performed and reviewed;
8. EM procedures and documentation is finalized and approved; and
9. EM is Rolled Out to entire company and people trained.

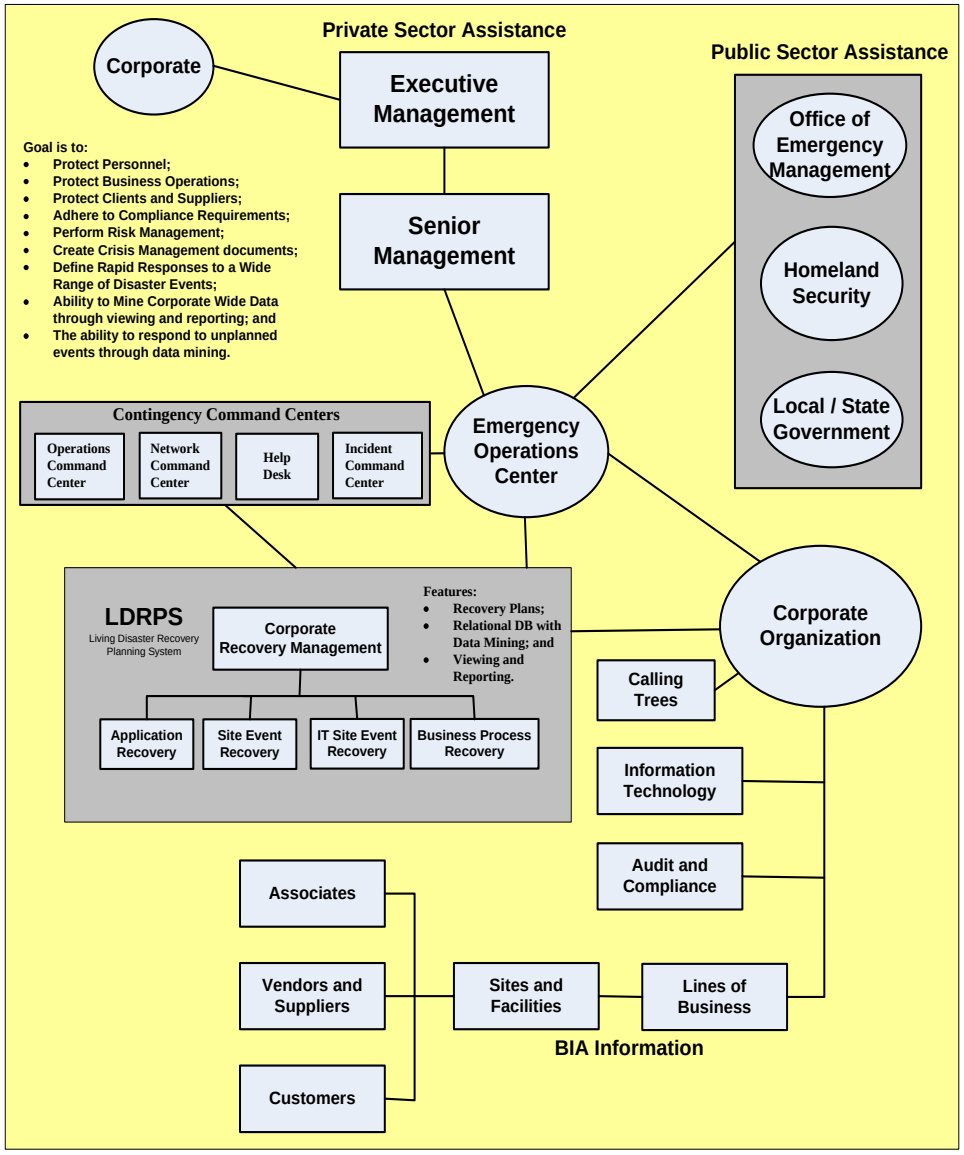
Emergency Management Planning Team Interfaces



Emergency Management Operations Environment, with Incident Management interface between remote locations and headquarters



Current Emergency Operations Center (EOC) Environmental Interfaces and Tools



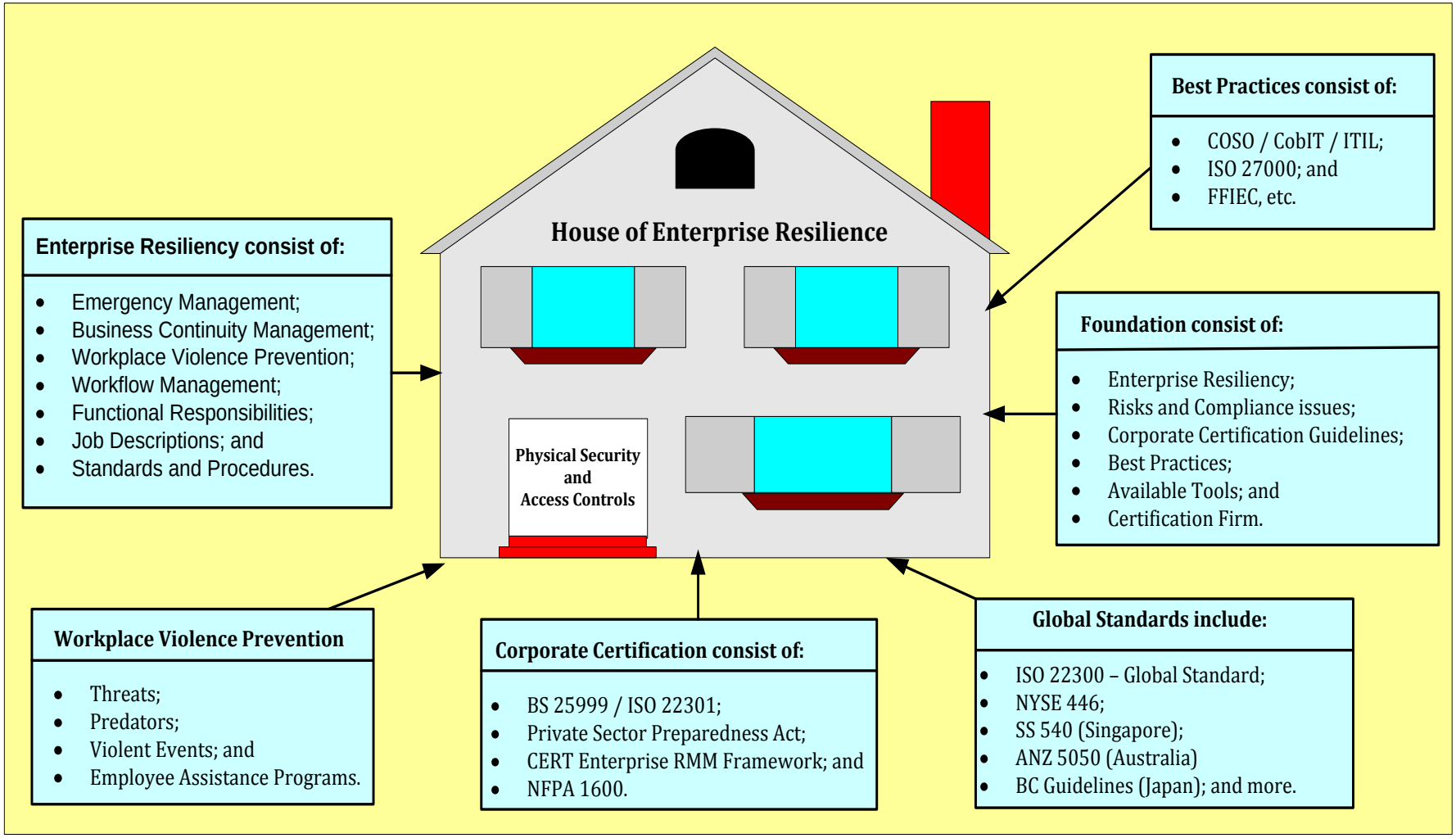
Currently corporate management directs executive management to develop a disaster response group, resulting in the creation of an Emergency Operations Center (EOC) which is presently manned by personnel with First Responder backgrounds (Fire, Police, Government backgrounds).

Incorporating Business Recovery Planning (loss of an office) with Disaster Recovery (loss of an Information Technology service) will elevate the EOC to be better prepared to respond to disaster events. Coordination with the Public Sector Assistance functions and internal Command Centers will provide the EOC with better and more current information.

Use of automated tools will speed recovery operations, and knowledge of the Corporate Organization will make it easier to communicate disaster and recovery information to company personnel so that a better recovery response can be taken and personnel will be more aware of what is happening.

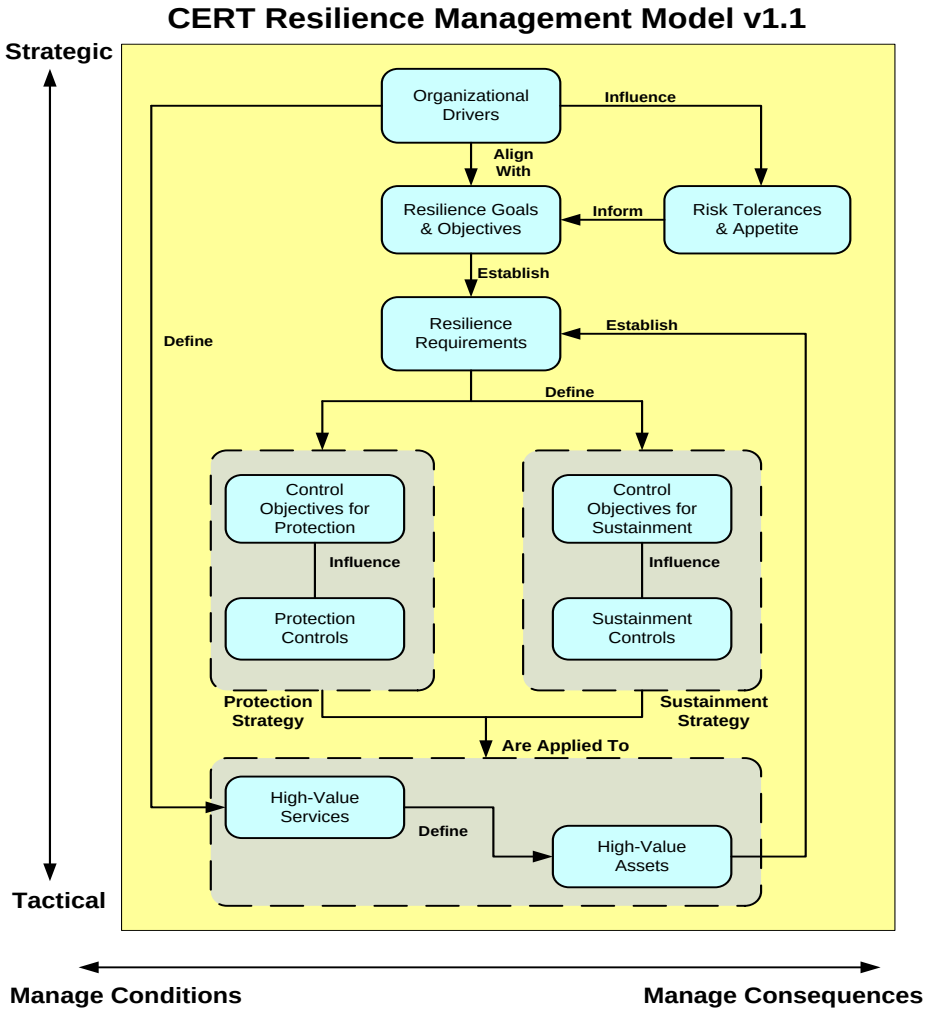
Communications with neighbors and the media will help maintain the corporate reputation and may assist in recovery operations. Consider the use of Social Media to support communications.

Enterprise Resiliency must be built upon a Solid Foundation



Risk Management via CERT Resilience Management Model (RMM)

The goal of Resiliency (Risk) Management is to determine Risk Exposures and the company's desire to mitigate all uncovered Gaps and Exceptions due to costs and abilities (see below)



Source: Caralli, Richard; Allen, Julia; White, David; CERT Resilience Management Model (RMM): A Maturity Model for Managing Operational Resilience (SEI Series in Software Engineering). Addison-Wesley 2010
CERT is defined as: Computer Energy Readiness Team

Risks can include:

- Natural Disasters;
- Compliance;
- Disaster Event;
- Business Reputation;
- Personnel Failures;
- Supply Chain;
- Infrastructure;
- Maintenance Schedule;
- Production Deadlines;
- Service Level Agreements;
- Regional Disaster;
- Community / Building Loss;
- Workplace Violence and Active Shooter;
- Data and Physical Security; and
- Personnel Training and Awareness.

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.

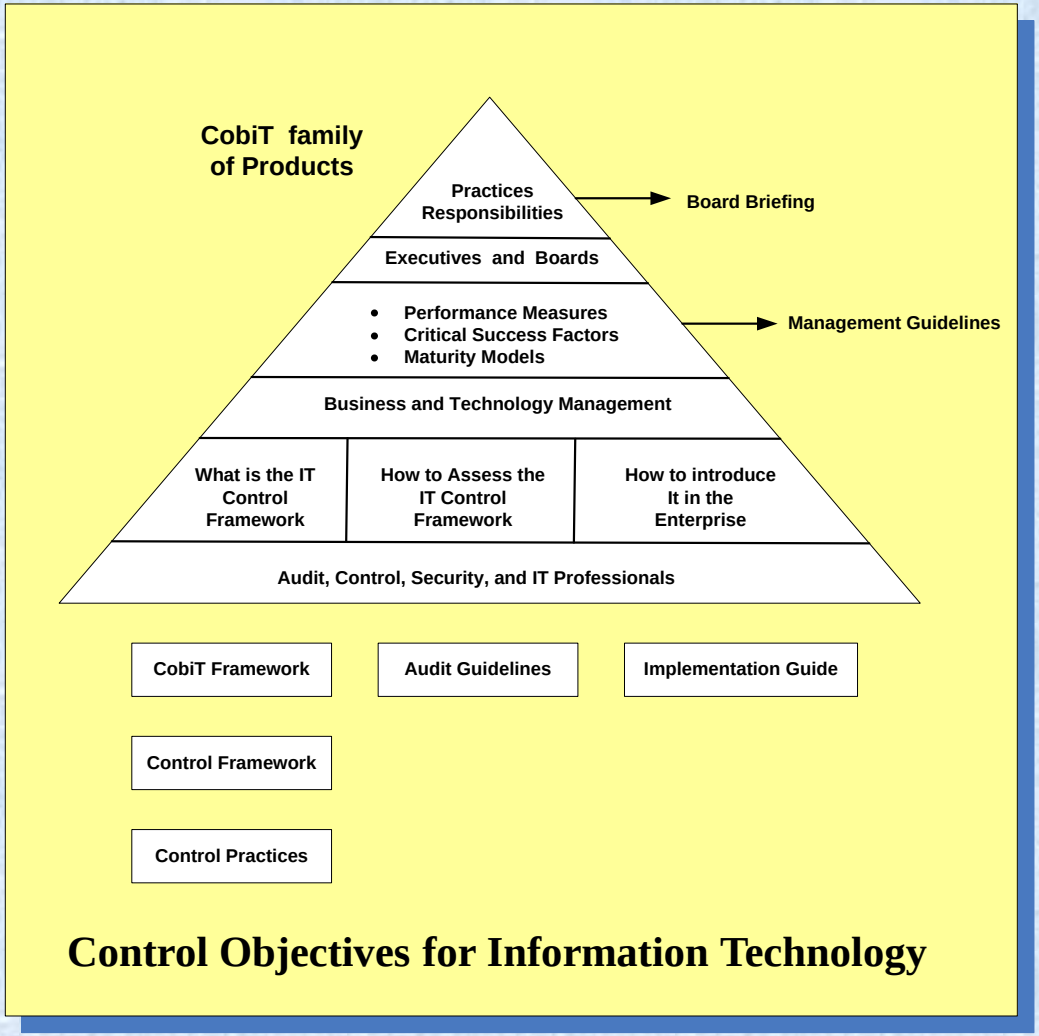
Implementation of Standards and Procedures guidelines associated with Risk Assessment to guaranty compliance to laws and regulations.

Employee awareness training, support, and maintenance going forward.

CobiT Family of Products

Integrating CobiT

- The Board receives Briefings;
- Management receives Guidelines;
- The remaining staff receives:
  - CobiT Framework;
  - Control Framework;
  - Control Practices;
  - Audit Guidelines; and an
  - Implementation Guide.

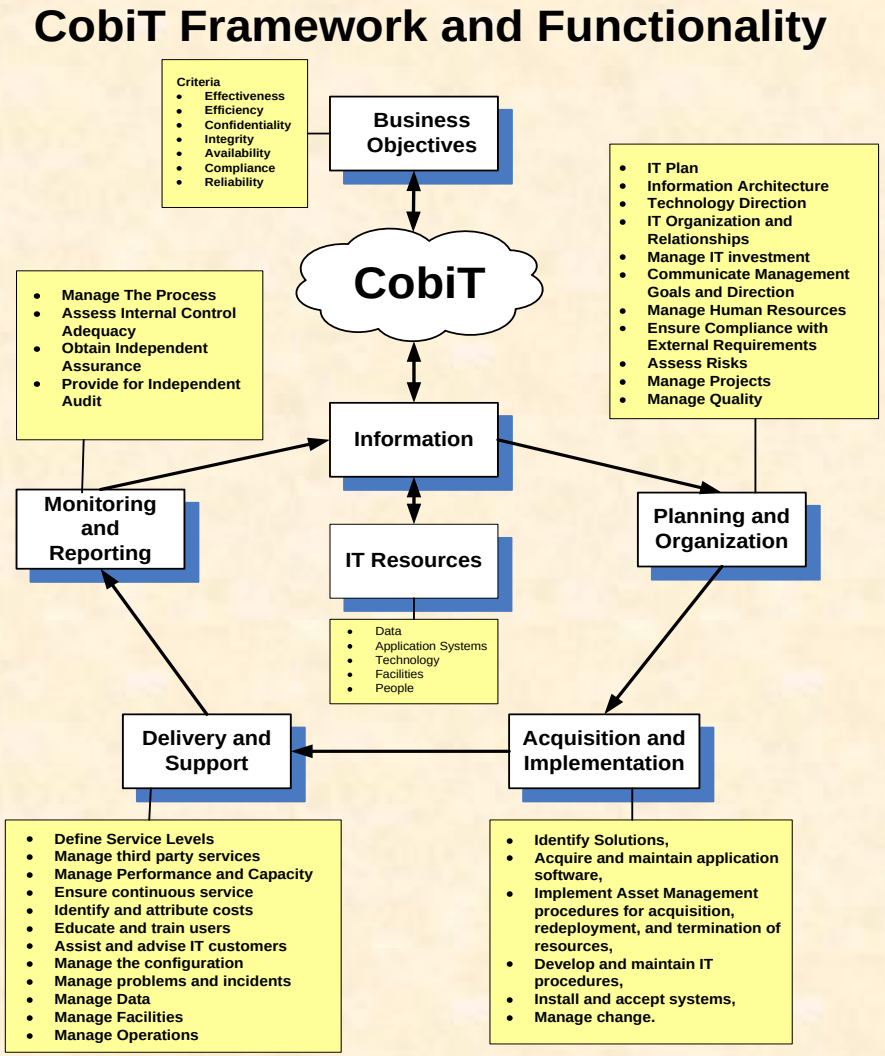


CobiT Framework

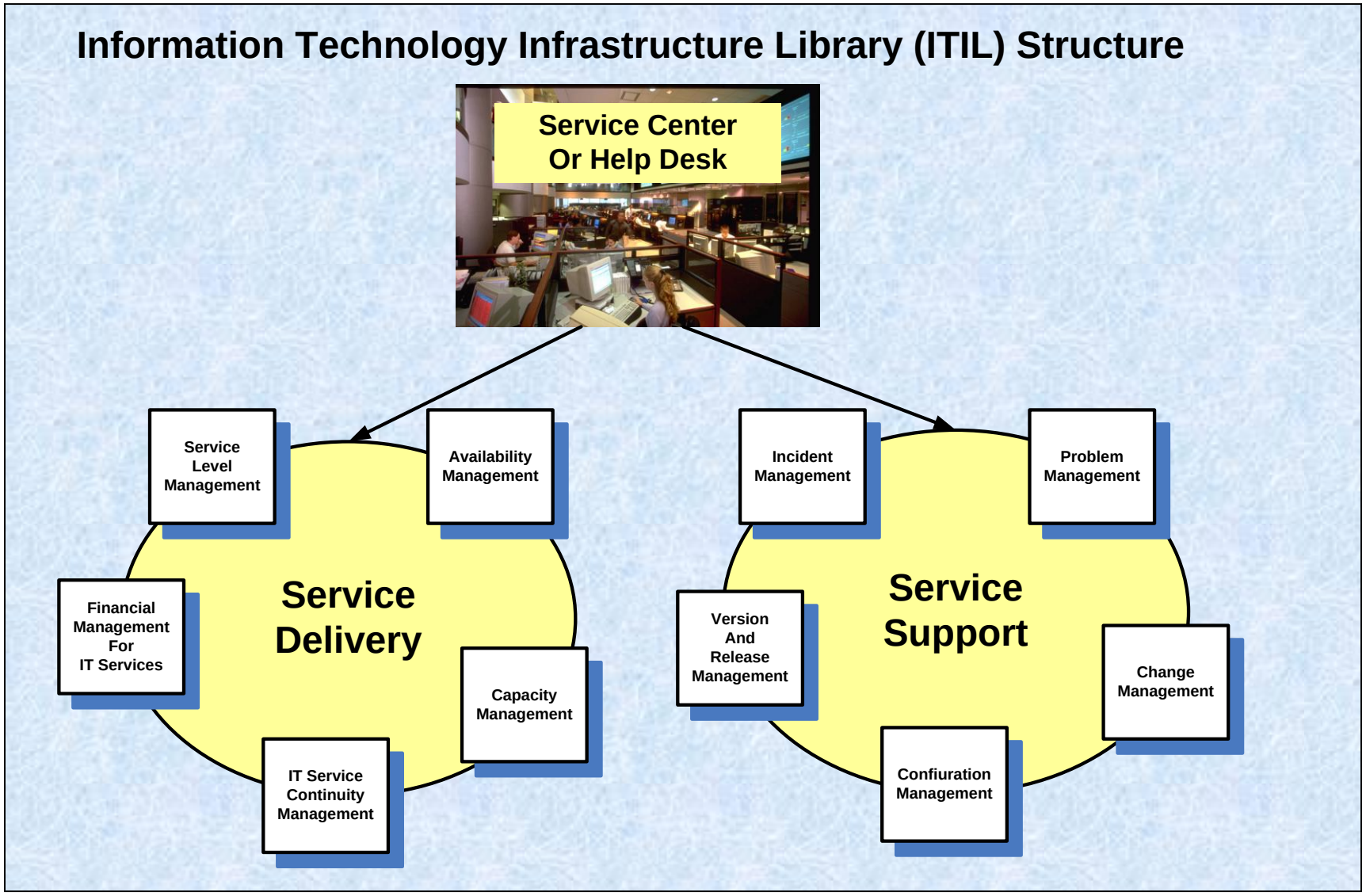
Control Objectives for Information Technology (CobiT)

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 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 Framework v2



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

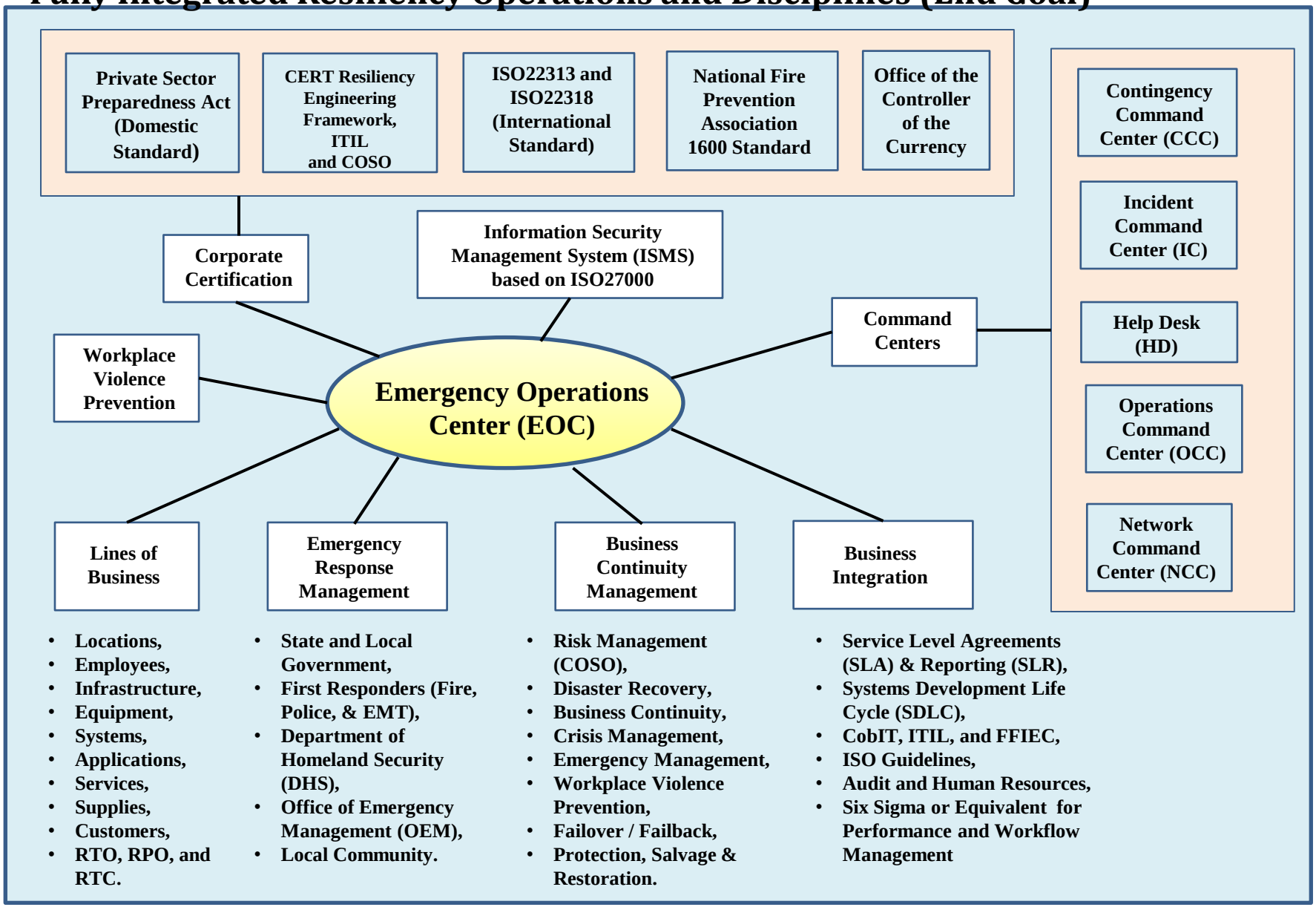
1. Service Strategy
- Service Portfolio Management (available Services and Products)
- Financial Management (PO, WO, A/R, A/P, G/L, Taxes and Treasury)

2. Service Design
- Service Catalogue Management
- Service Level Management (SLA / SLR)
- Risk Management (CERT / COSO)
- Capacity 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

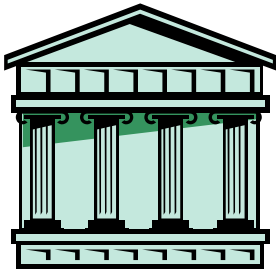
Fully Integrated Resiliency Operations and Disciplines (End Goal)



Compliance Laws pertaining to Data Protection - Overview

- Gramm Leach Bliley – Safeguard Act;
- HIPAA for protecting medical data;
- Sarbanes Oxley – banking self assessment and reporting;
- California SB 1386 to protect against identity theft in California (ID Theft protection in California);
- Personal Data Privacy and Security Act of 2005 (Domestic ID Theft protection);
- All Laws are based on either financial or compliance data;
- Laws require ability to trace data to its source;
- Response Plan must be in place to immediately notify customers of a lost media event or data breach affecting their identity; and
- Fines and Penalties are very large for failing to immediately notify customers.

Gramm-Leach-Bliley



- Covers Financial Organizations (as defined in the Bank Holding Act) that possess, process, or transmit private customer information.
- Its purpose is to protect Customer Information from unauthorized disclosure or use.
- An Information Security Program must be in place to comply and the following operating mechanisms must be established:
  - Responsible employee as Security Officer.
  - Risk Assessment to uncover and correct exposures.
  - Information Safeguards and Controls must be established.
  - Oversight of "Service Providers and Vendors" to guaranty compliance.
  - Testing and Monitoring in an on-going fashion.
  - Evaluation and Reporting to management.
- Compliance date of May, 2003. Law provides for fines and imprisonment of up to 5 years for intentional violations.

Dodd–Frank Wall Street Reform and Consumer Protection Act (Overview)

1, The consolidation of regulatory agencies, elimination of the national thrift charter, and new oversight council to evaluate systemic risk;

2. Comprehensive regulation of financial markets, including increased transparency of derivatives (bringing them onto exchanges);

3. Consumer protection reforms including a new consumer protection agency and uniform standards for "plain vanilla" products as well as strengthened investor protection;

4. Tools for financial crises, including a "resolution regime" complementing the existing Federal Deposit Insurance Corporation (FDIC) authority to allow for orderly winding down of bankrupt firms, and including a proposal that the Federal Reserve (the "Fed") receive authorization from the Treasury for extensions of credit in "unusual or exigent circumstances";

5. Various measures aimed at increasing international standards and cooperation including proposals related to improved accounting and tightened regulation of credit rating agencies.

Provisions:

1. Title I - Financial Stability
2. Title II – Orderly Liquidation Authority
3. Title III – Transfer of Powers to the Comptroller, the FDIC, and the Fed
4. Title IV – Regulation of Advisers to Hedge Funds and Others
5. Title V – Insurance
6. Title VI – Improvements to Regulation
7. Title VII – Wall Street Transparency and Accountability
8. Title VIII – Payment, Clearing and Settlement Supervision
9. Title IX – Investor Protections and Improvements to the Regulation of Securities
10. Title X – Bureau of Consumer Financial Protection
11. Title XI – Federal Reserve System Provisions
    a. Governance and oversight
    b. Standards, Plans & reports, and off-balance-sheet activities
12. Title XII – Improving Access to Mainstream Financial Institutions
13. Title XIII – Pay It Back Act
14. Title XIV – Mortgage Reform and Anti-Predatory Lending Act
    a. Property Appraisal Requirements
15. Title XV – Miscellaneous Provisions.
    a. Restriction on U.S. Approval of Loans issued by International Monetary Fund
    b. Disclosures on Conflict Materials in or Near the Democratic Republic of the Congo
    c. Reporting on Mine Safety
    d. Reporting on Payments by Oil, Gas and Minerals in Acquisition of Licenses
    e. Study on Effectiveness of Inspectors General
    f. Study on Core Deposits and Brokered Deposits
16. Title XVI – Section 1256 Contracts

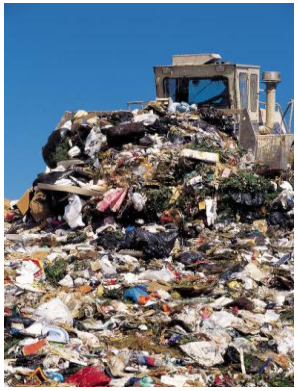
HIPAA

- **Covers organizations that possess, transmit, or process electronic protected health information (EPHI).**
- **Responsible for protecting EPHI data from unauthorized disclosure or use.**
- **Required Security Safeguards include:**
  - **Risk Assessment to uncover and resolve exposures.**
  - **Policies and Procedures to control access and track usage.**
  - **Physical and IT Security Measures.**
  - **Contingency Plan and Disaster Recovery Plan.**
  - **Appointment of Security Officer and Business Continuity Officer.**
  - **Training and communications to improve awareness.**
  - **Periodic Audits and maintenance of Audit Trail.**
  - **Agreement with "Business Associates" to comply to requirements.**
  - **On-going Testing and Evaluation of plan and deliverables.**
- **Comply by April 2005, with fines to $250,000 and imprisonment for up to 10 years.**

Sarbanes-Oxley Act

- Requires companies to perform quarterly self-assessments of risks to business processes that affect financial reporting and to attest to findings on an annual basis (CFO and CEO, possibly CIO too). Section 302 requires "Signing Officer" to design reports for compliance submission.
- Section 404 requires that technology personnel develop and implement means for protecting critical financial data (data security, back-up and recovery, business continuity planning, and disaster recovery), because loss of data is not acceptable.
- Section 409 will require "Real-Time Reporting" of financial data, thus creating the need for new Standards and Procedures and perhaps re-engineering of functions to better comply with the Law.
- Companies must devise "Checks and Balances" to guaranty that those people creating functions (like programmers) are not the person responsible for validating the functions operation (rather a separate checker must validate function).
- Checks and Balances prohibit big 4 accounting firms from performing Risk Assessment because they are the ones performing audit (Conflict of Interest).
- Penalties can include fines as high as $5 million and imprisonment can be for as long as 20 years for deliberate violation.

EPA and Superfund



- Designed to protect the environment from Toxic Materials that could lead to death or illness.
- Regulated by the Environmental Protection Agency.
- Fines and imprisonment can be imposed when violation is intentional, or through a third party acting in your behalf.
- Safeguards should be imposed to:
  - Identify toxic materials,
  - Take appropriate steps to protect employees and community personnel,
  - Insure that proper and authorized Waste Removal procedures are implemented,
  - Provide personnel awareness programs and Standards and Procedures,
  - Support and maintain program going forward.

SSAE Controls (Domestic, International, and old)

Domestic

International

Old

One of the most effective ways a service organization can communicate about its controls is through a "***Statement on Standards for Attestation Engagements*" – SSAE** Service Auditor's Report. There are two types of Service Auditor's Reports: Type I and Type II.

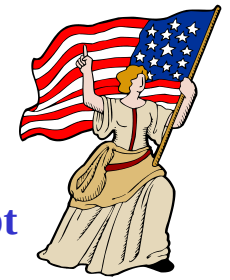
A **Type I** report describes the service organization's controls at a specific point in, while a **Type II** report not only includes the service organization's description of controls, but also includes detailed testing of the service organization's controls over a minimum six month period. The contents of each type of report is described in the following table:

Report Contents	Type I	Type II
1. Independent service auditor's report - SSAE (i.e. opinion)	Included	Included
2. Service organization's description of its system (including controls).	Included	Included
3. Information provided by the independent service auditor; includes a description of the service auditor's tests of operating effectiveness and the results of those tests	Optional	Included
4. Other information provided by the service organization (e.g. glossary of terms).	Optional	Included

In a **Type I** report, the service auditor will express an opinion and report on the subject matter provided by the management of the service organization as to: **(1)** whether the service organization's description of its system fairly presents the service organization's system that was designed and implemented as of a specific date; and **(2)** whether the control objectives stated in management's description of the service organization's system were suitably designed to achieve those control objectives - also as of a specified date.

In a **Type II** report, the service auditor will express an opinion and report on the subject matter provided by the management of the service organization as to: **(1)** whether the service organization's description of its system fairly presents the service organization's system that was designed and implemented during a specified period; **(2)** whether the control objectives stated in management's description of the service organization's system were suitably designed throughout the specified period to achieve control objectives; and **(3)** whether the controls related to the control objectives stated in management's description of the service organization's system operated effectively throughout the specified period to achieve those control objectives.

Patriots Act

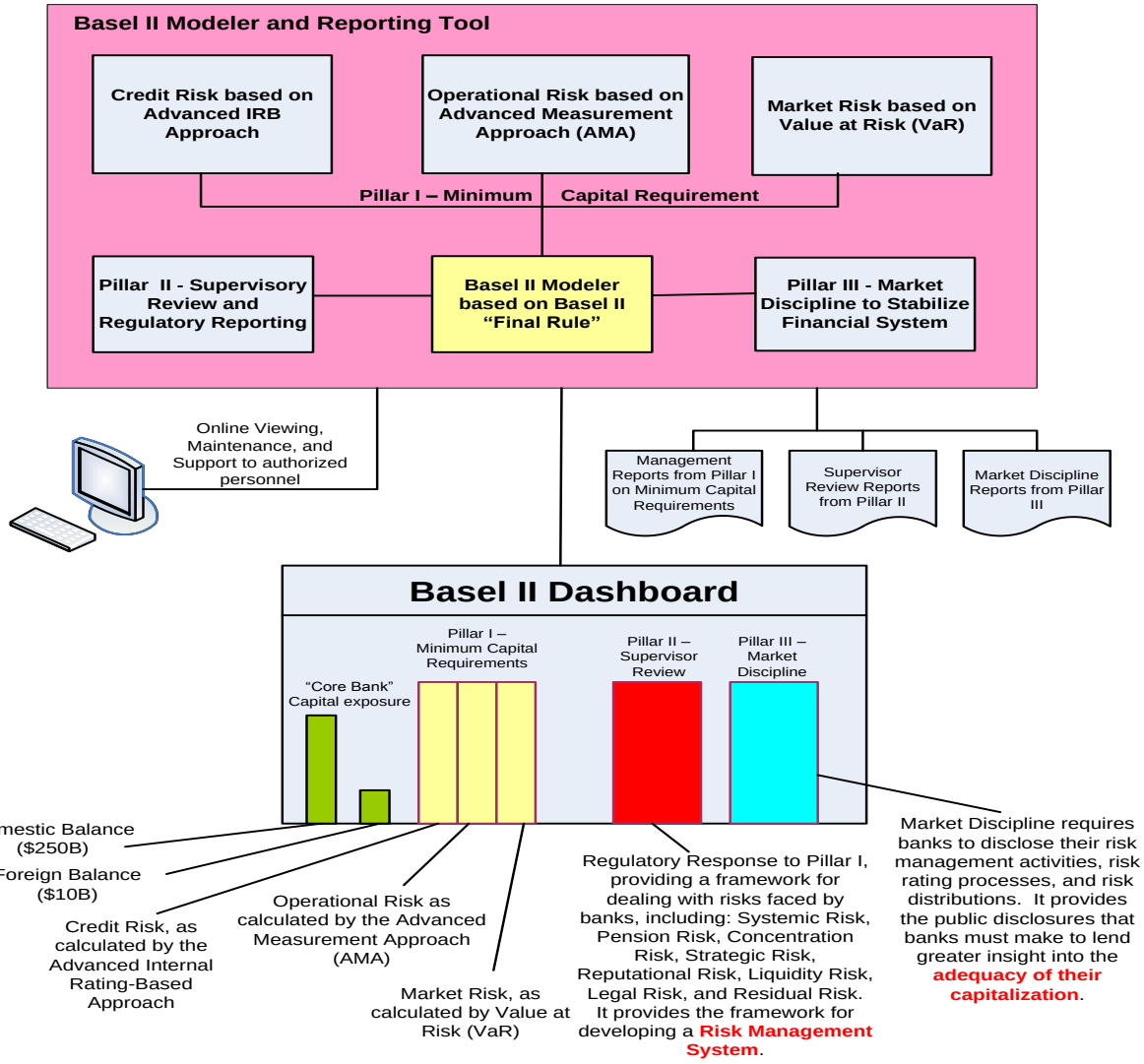


- **New Requirements — Severe Penalties** (Official Title is "**Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism**").
- **USA PATRIOT Act Section 326** imposes new requirements on how organizations screen existing customers and process new customer information.
- **By October 1, 2003**, all financial services organizations must have in place procedures for:
  - **1. Customer Screening** — On a regular basis, customers and transactions must be matched against government-provided lists of suspected terrorists, drug traffickers, money launderers and other criminals.
  - **2. Customer Information Program (CIP)** — On all new customers, basic identification information must be obtained to verify the customer's identity. Failure to comply can result in penalties of up to $1 million, and/or imprisonment.
- Used to **protect the confidentiality** of telephone, face-to-face, and computer communications, **while enabling authorities to identify and intercept during criminal investigations** with warrant.
- Improves ability to obtain data during **Foreign Intelligence Investigations** and increases a companies need to safeguard voice, face-to-face, and computer based data.
- Enhances financial organizations ability to track suspected **Money Laundering** activities and requires reporting of activity when uncovered, thus fostering the need to obtain, store, and safeguard data used to report on suspected Money Laundering activities.

Basel II - Overview

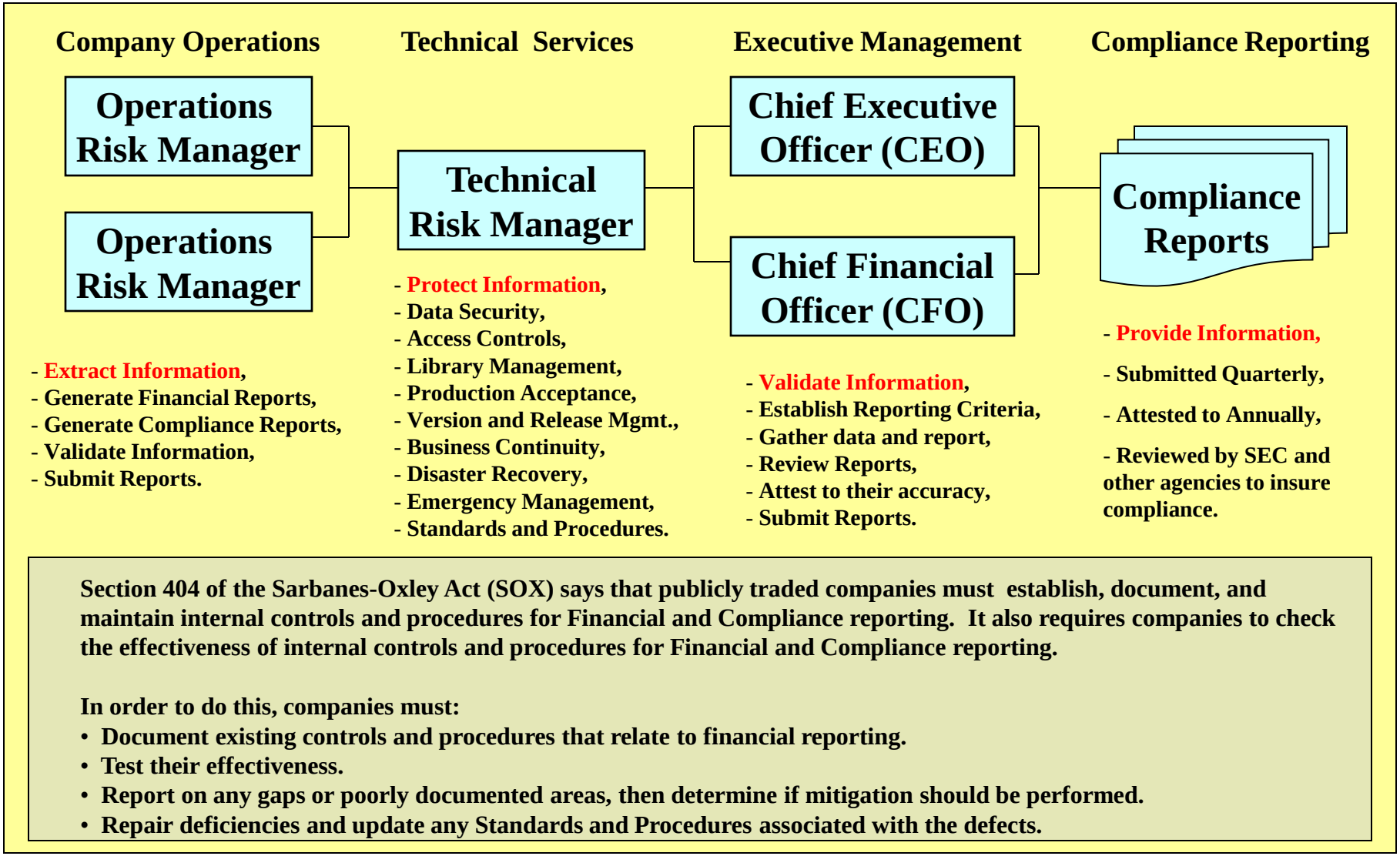
Basel II Modeler and Dashboard concept

Legend:
IRB – Internal Rating-Based Approach;
AMA – Advanced Measurement Approach; and,
VaR – Value at Risk approach.



Basel III is an updated version of Basel II that is awaiting approval.

How reporting is accomplished

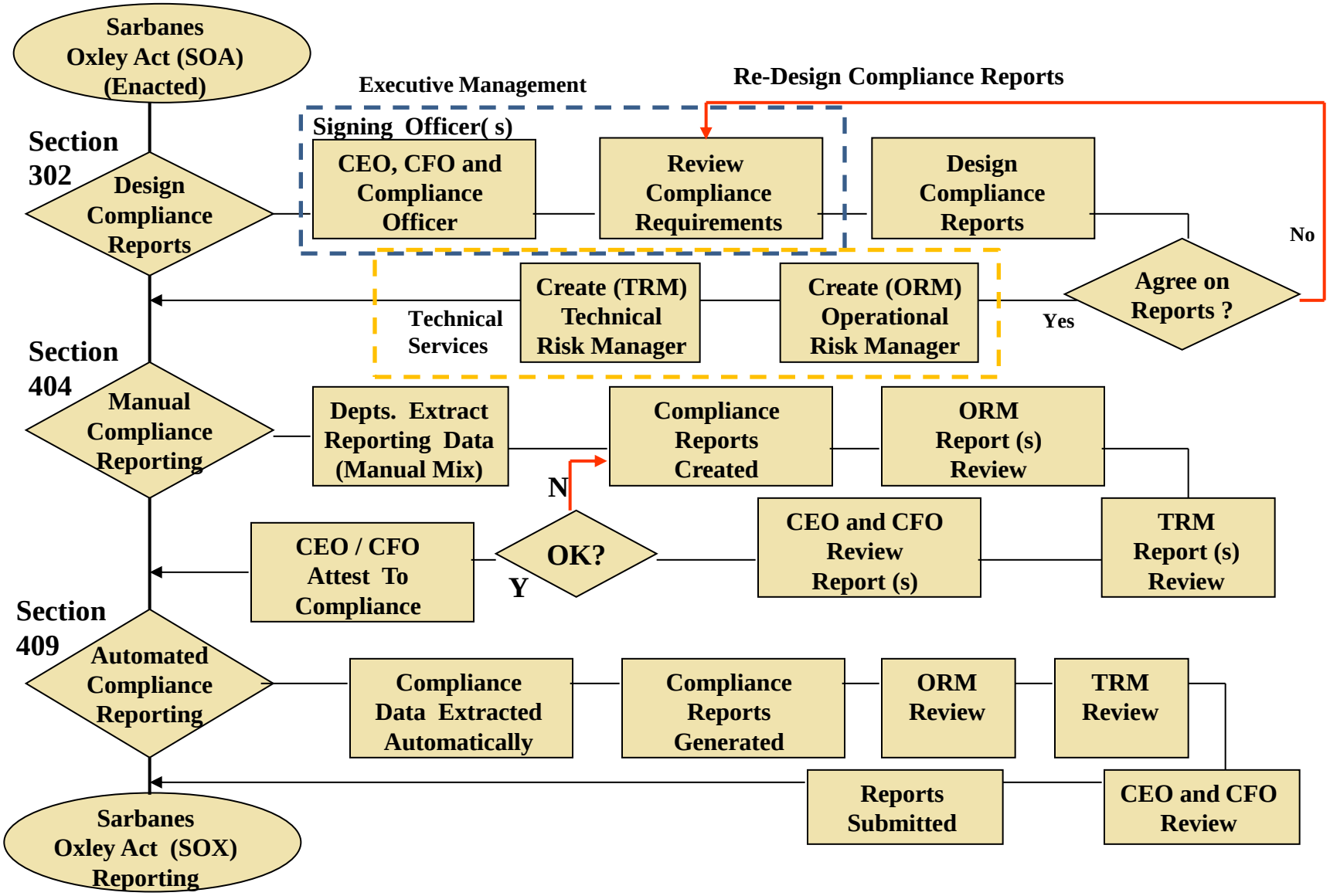


Section 404 of the Sarbanes-Oxley Act (SOX) says that publicly traded companies must establish, document, and maintain internal controls and procedures for Financial and Compliance reporting. It also requires companies to check the effectiveness of internal controls and procedures for Financial and Compliance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

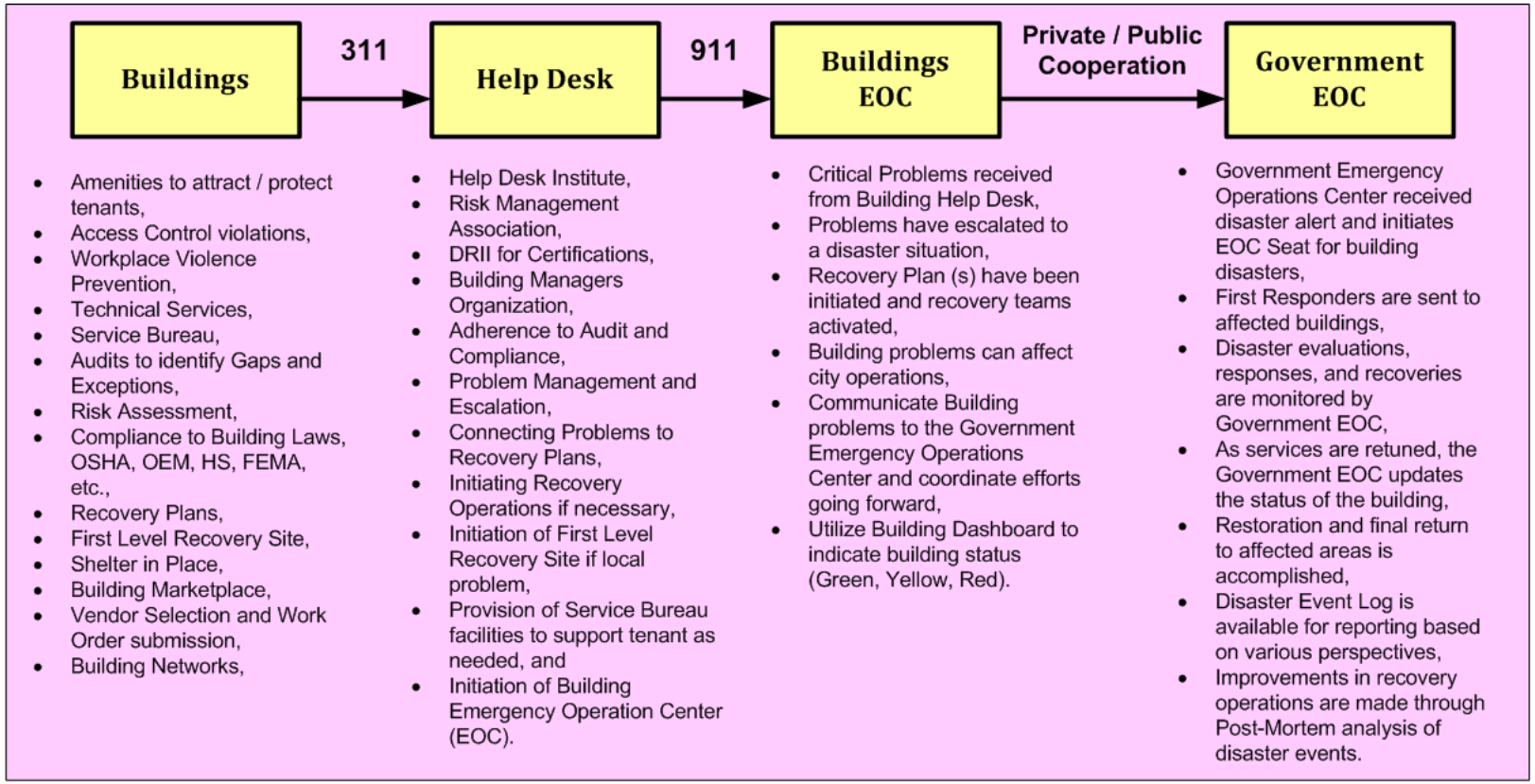
In order to do this, companies must:

- **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.**

Creating Compliance Reports



Building Services, Help Desk, and Emergency Operation Center coordination



Strategy:

- Improved Tenant Safety,
- Sell as a Service,
- Insurance benefits,
- Assessment to uncover problems and recommend solutions.

Relationships:

- Disaster Recovery Institute International,
- Help Desk Institute,
- NYC OEM EOC, and
- Risk Management Institute..

Benefits:

- Employee Certifications,
- Building Managers Organization,
- Public / Private sector cooperation,
- Safeguarded building that is in compliance with laws and regulations.

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?**
  - **What form is it in (Excel, Database, manual, fax, email, etc.)**
  - **Who has access to it and how can they impact data (create, edit, use, convert, etc.)**
- **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 data and facilities.**
- **Utilize existing Standards and Procedures to duplicate process and identify errors.**
- **Examine the available Employee Awareness and Education programs.**

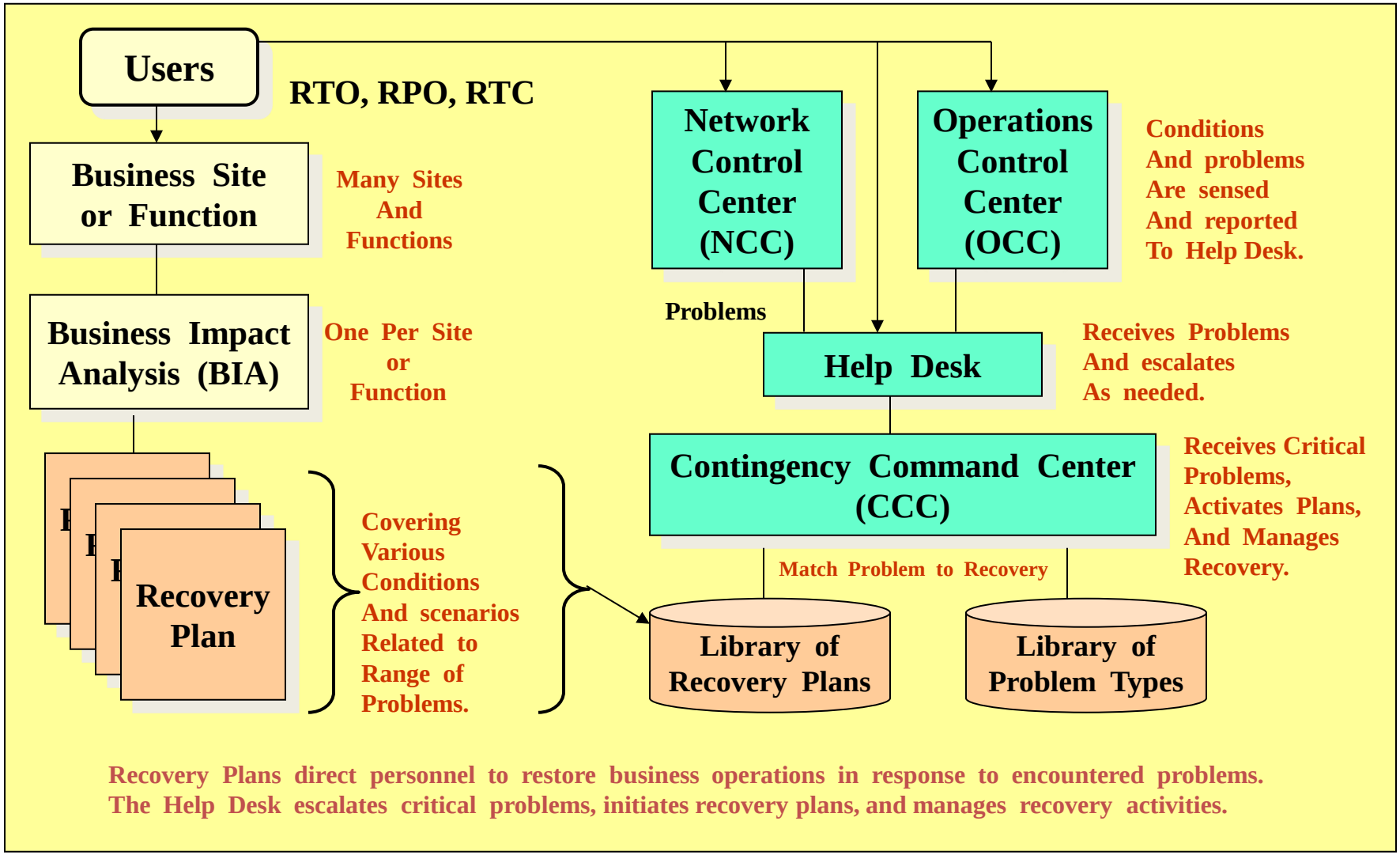
As a result of this study, it will be possible to identify weaknesses and develop procedures to overcome the weaknesses, thereby improving efficiency and productivity.

Strategies for Eliminating Audit Exceptions

- Review of Compliance Requirements (Business and Industry)
- Data Sensitivity, EDP Security and Vital Records Management,
- Eliminate Data Corruption and Certify HA / CA Application recovery,
- Production Acceptance, Quality Control and Project Life Cycle,
- Utilizing Automated Tools,
- Elimination of Single-Point-Of-Failure concerns,
- Inventory / Asset Management,
- Problem and Crisis Management,
- Work-Flow automation through Re-Engineering processes,
- Training and Awareness programs.

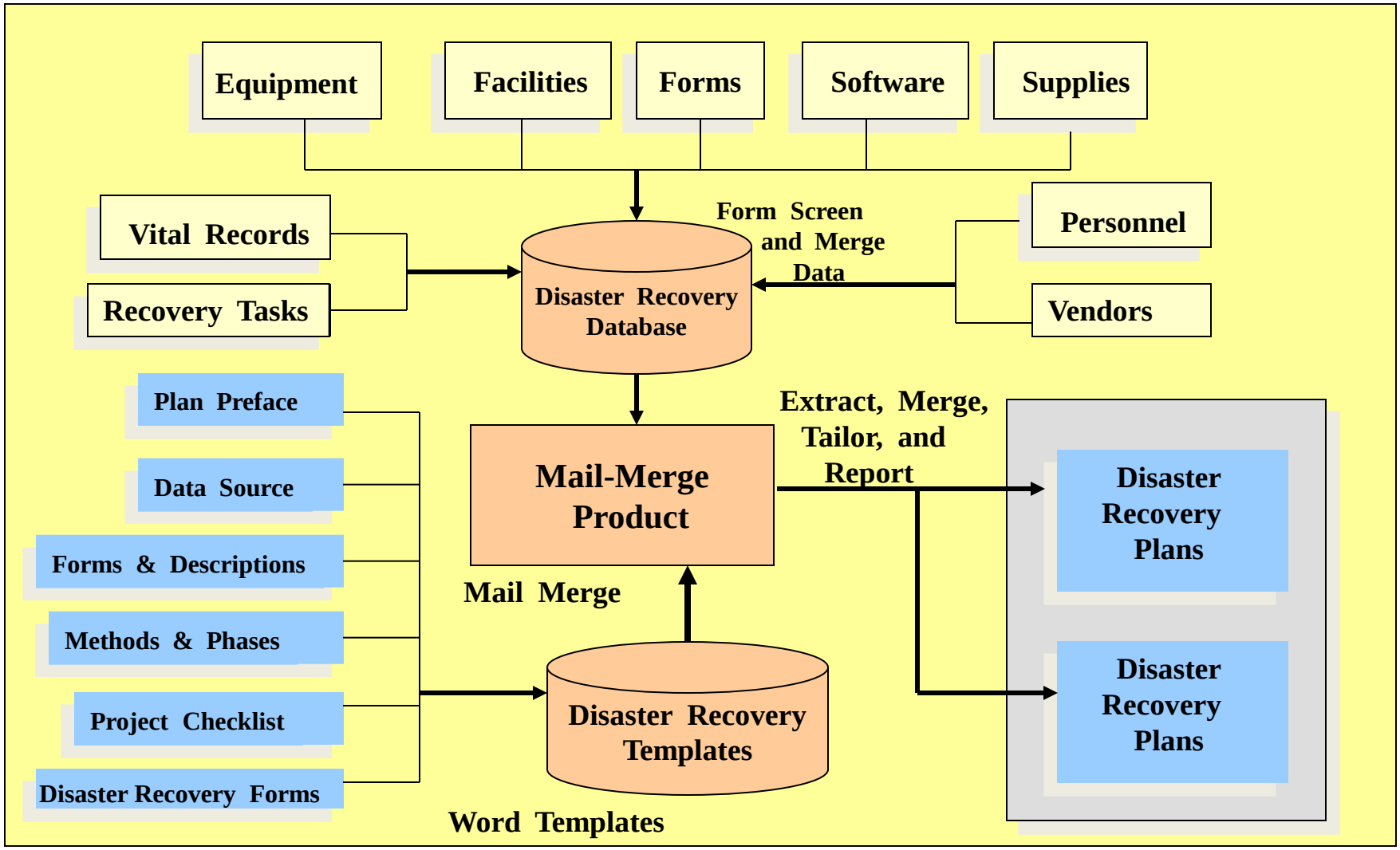
Overview of Business Continuity Planning and BIA's

Recovery Time Objective (RTO), Recovery Point Objective (RPO), and Recovery Time Capability (RTC) are found via BIA

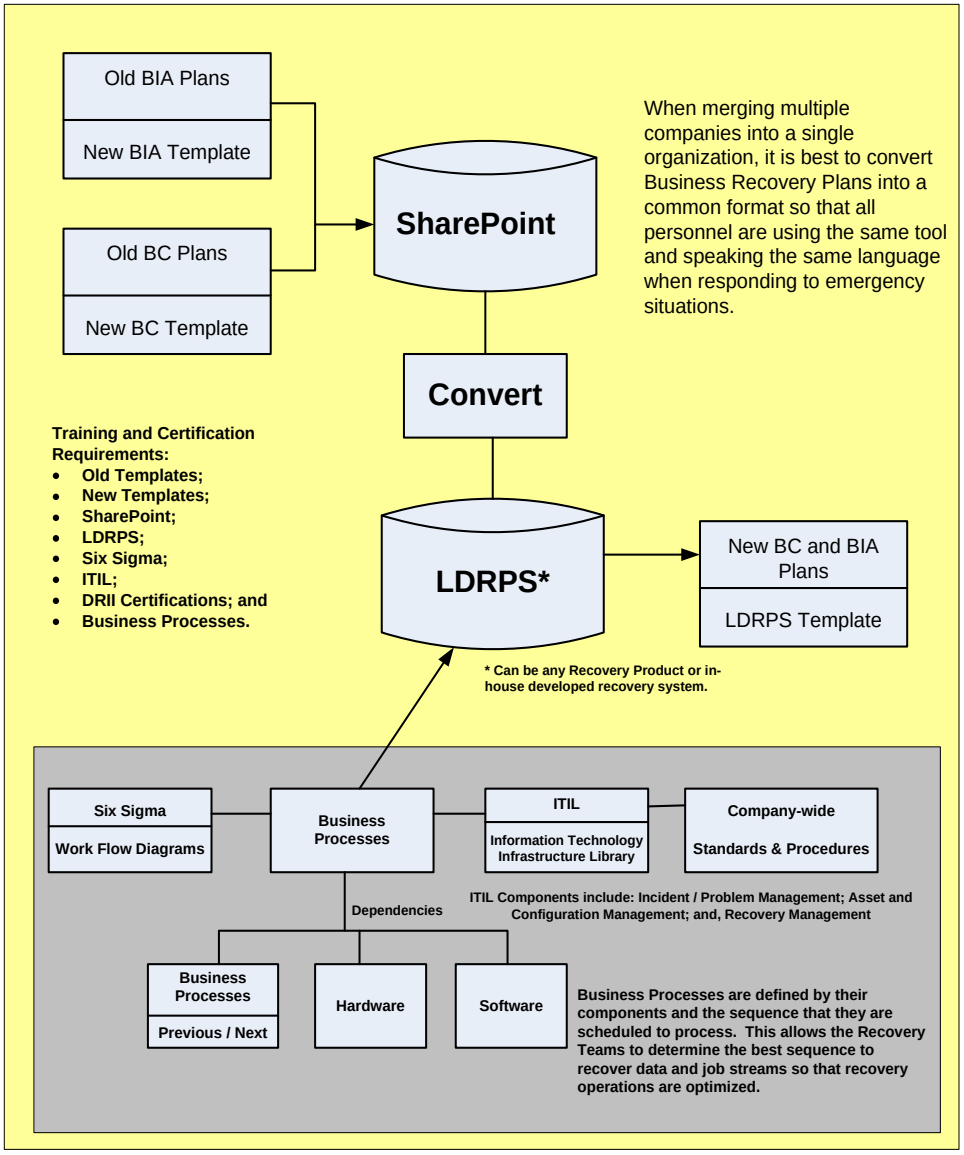


Recovery Plans direct personnel to restore business operations in response to encountered problems. The Help Desk escalates critical problems, initiates recovery plans, and manages recovery activities.

Disaster Recovery Plan Data Sources and Output Generation



Business Continuity Conversion and Integration

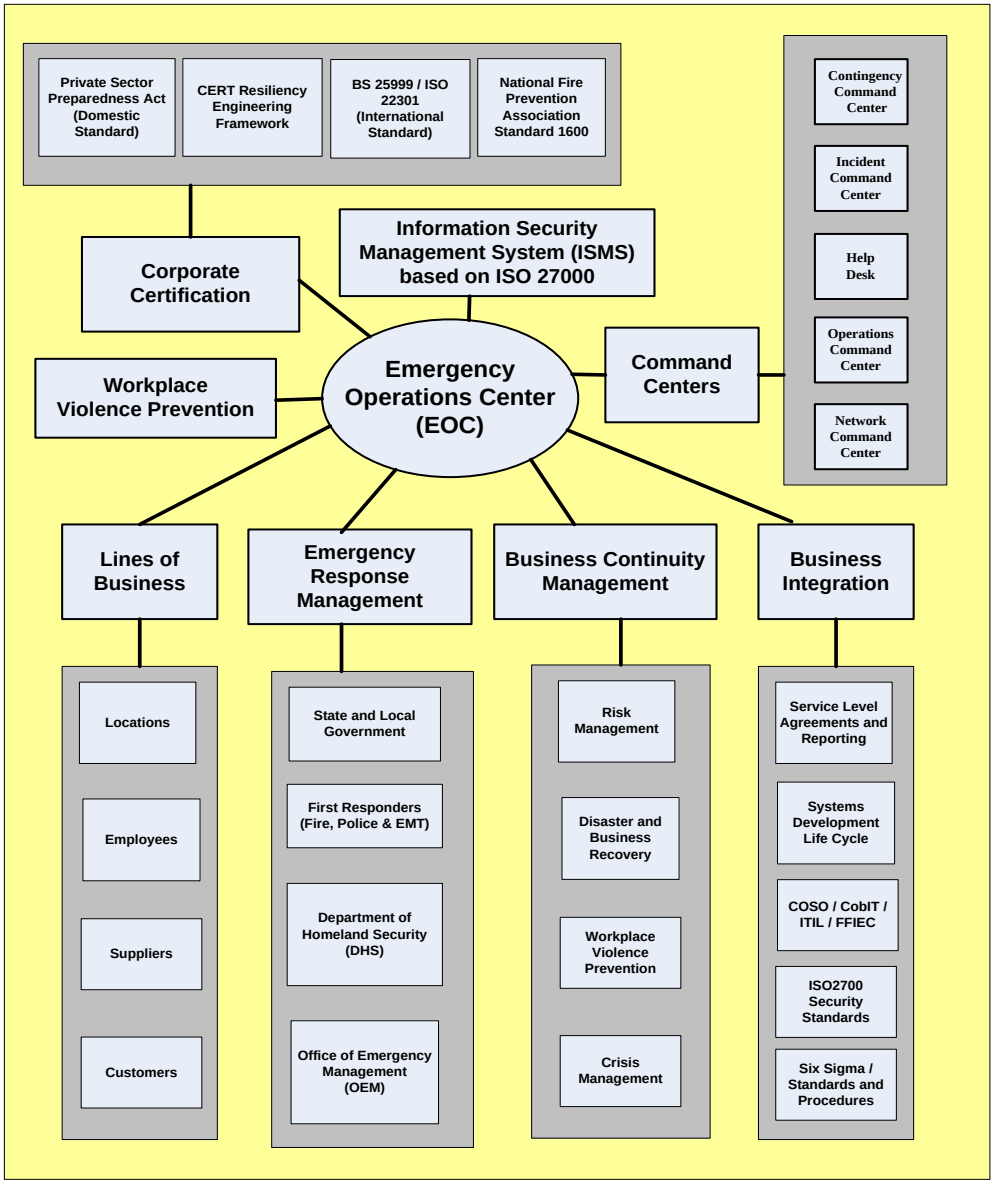


Paper based recovery plans are extremely hard to create and maintain, taking a lot of personnel time and effort which can be error prone and very costly.

Converting to an automated recovery planning product (like Living Disaster Recovery Planning System – LDRPS, or eBRP) will speed the creation of recovery plans and make it much easier to maintain them. The cost of an automated tool should be easily off-set by the reduction in personnel effort and costs.

Incorporating the automated recovery tool within the business process will integrate recovery operations into the everyday functions performed by personnel. For example, should an employee leave the organization part of their exit planning would include determining their recovery team function and triggering their replacement on the team by notifying the team leader and directing them to locate and train a replacement.

Fully Integrated Recovery Operations and Disciplines (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 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.

How to get started

Review existing Recovery Operations, including:

- Emergency Management Preparedness;
- Business Continuity Management;
- Workplace Violence Prevention; and
- Enterprise Security Operations (Physical and Data).

Evaluate Command Centers and how they interact with Recovery Operations, including:

- Emergency Operations Center (EOC);
- Incident Command Center (ICC);
- Help Desk (HD);
- Network Command Center (NCC); and
- Operations Command Cente (OCC)r.

Define Company Lines of Business (LOB), including;

- Business Functions, Products, and Services provided;
- Locations and Personnel;
- Customers and Suppliers;
- Applications and Business Processes; and
- Existing Evacuation, Crisis Management, and Recovery Operations.

Document Integration Requirements, including:

- Service Level Agreements (SLA) and Service Level Reporting (SLR);
- Systems Development Life Cycle (SDLC) and Workflow Management;
- Best Practices tools and procedures, including: COSO, COBIT, ITIL;
- Ensure adherence to Regulatory Requirements to insure compliance; and
- Define Functional Responsibilities, Job Descriptions, and Standards and Procedures.

Create Business Plan, including:

- Mission Statement;
- Goals and Objectives;
- Assumptions;
- Scope and Deliverables;
- Detailed Project Plan;
- Gain Management Acceptance through Report and Presentation of Findings;
- Establish Schedule of Events and Assign Personnel to Tasks;
- Define Functional Responsibilities, Job Descriptions, and Standards and Procedures to be followed going forward;
- Train and Certify Personnel in Recovery Operations; and
- Monitor, Report, Improve, Validate; Roll-Out; Train; and Implement.