Achieving

Enterprise Resilience

and

Corporate Certification

by

Combining Recovery Operations through a

Common Recovery Language and Recovery Tools,

While adhering to

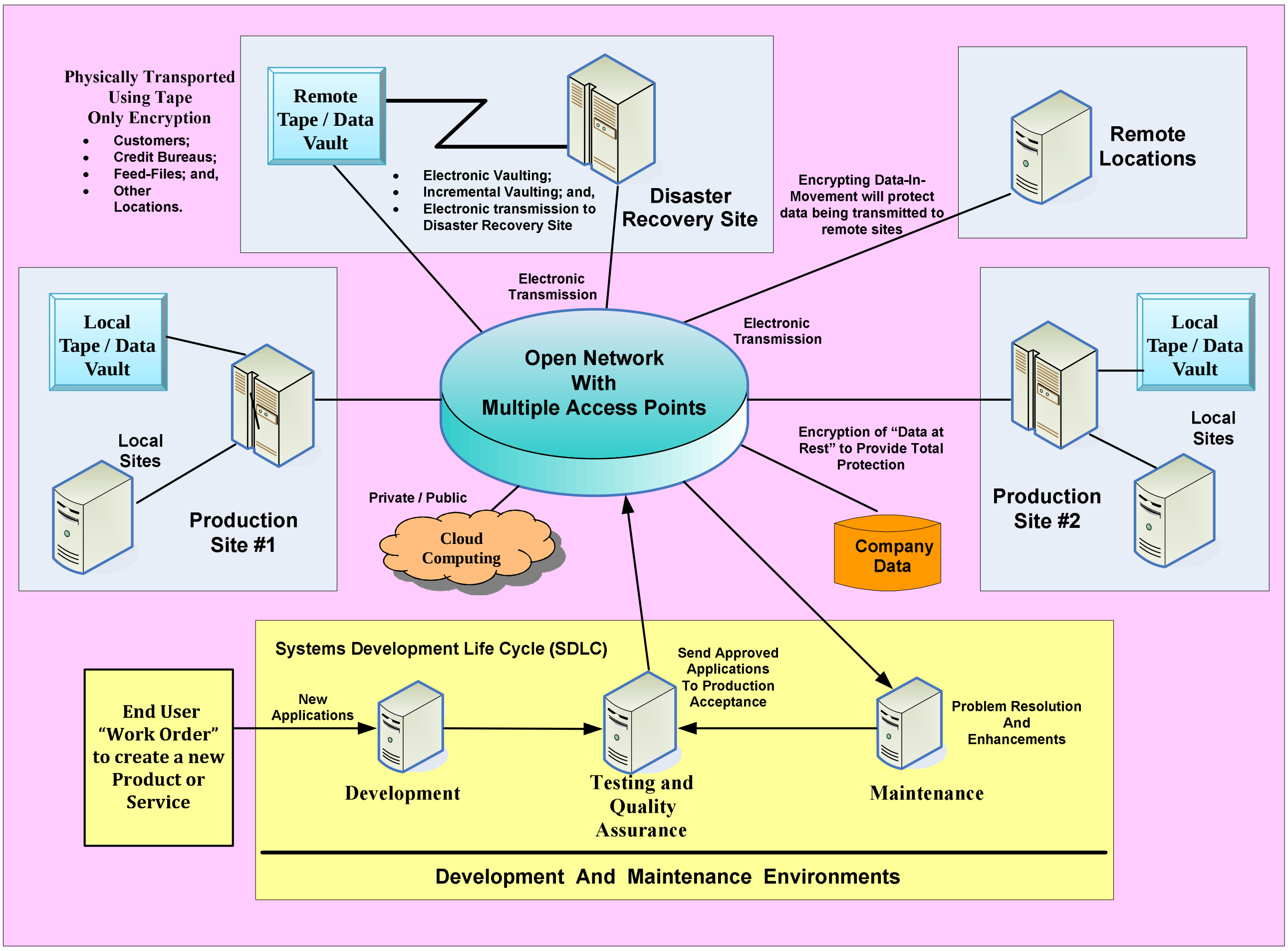
Domestic and International Certification Standards

Created by:

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

Table of Contents

Overview of the Enterprise Information Technology Environment


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

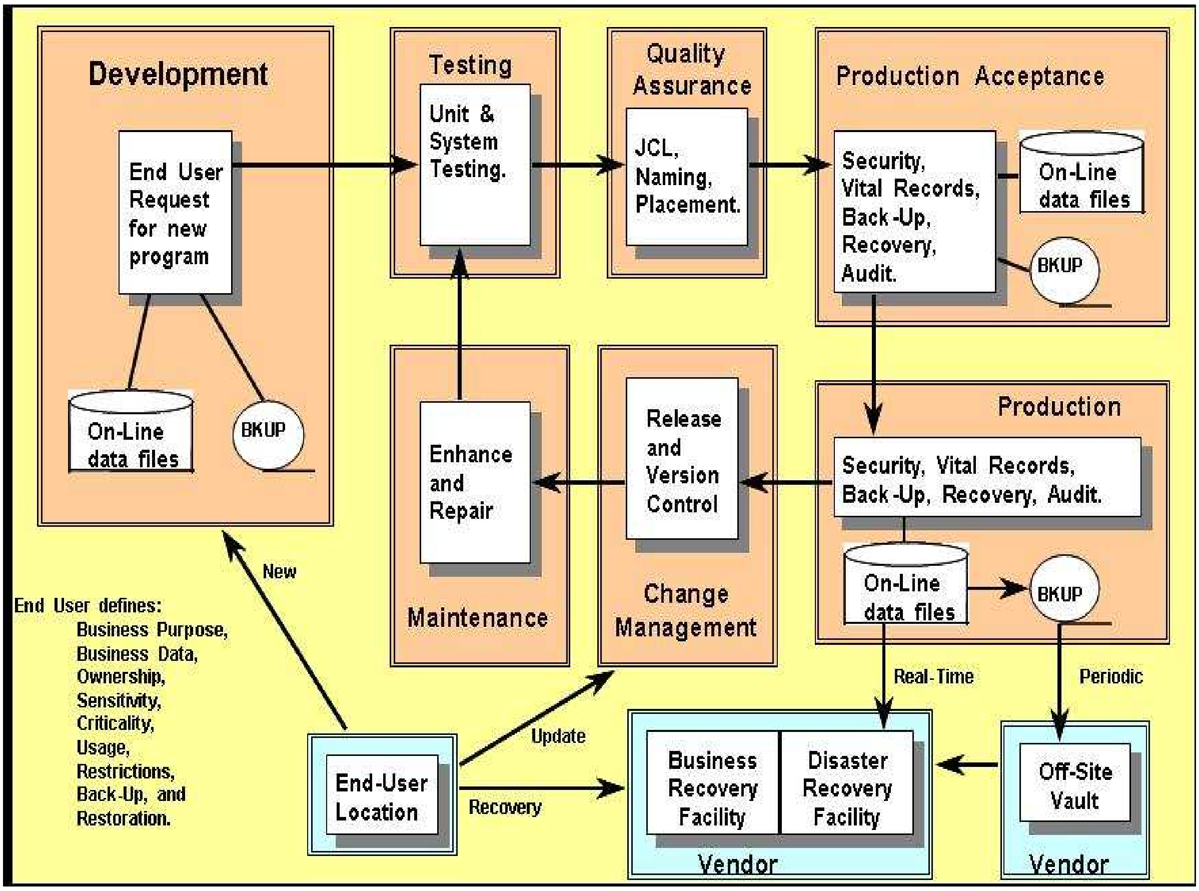
Sequence of events:

1. Applications are: Developed; Tested; reviewed by Quality Assurance; migrated to Production Acceptance where their components are placed in appropriate libraries; renamed to adhere to Production standards; and protected through IT Security, Encryption, and Library Management (including local and remote vaulting). Components are then Migrated to the Production Environment for desired scheduling and operations.

2. Real Time Electronic and Periodic Incremental Data Backups are used to protect and synchronize data across environments, while supporting automated load balancing and recovery Failover procedures.

3. The Primary Site can be recovered at the Secondary Site (Company Owned) or Recovery Site (Vendor Owned) depending on your companies desired recovery approach.

Systems Development Life Cycle (SDLC), components and flow

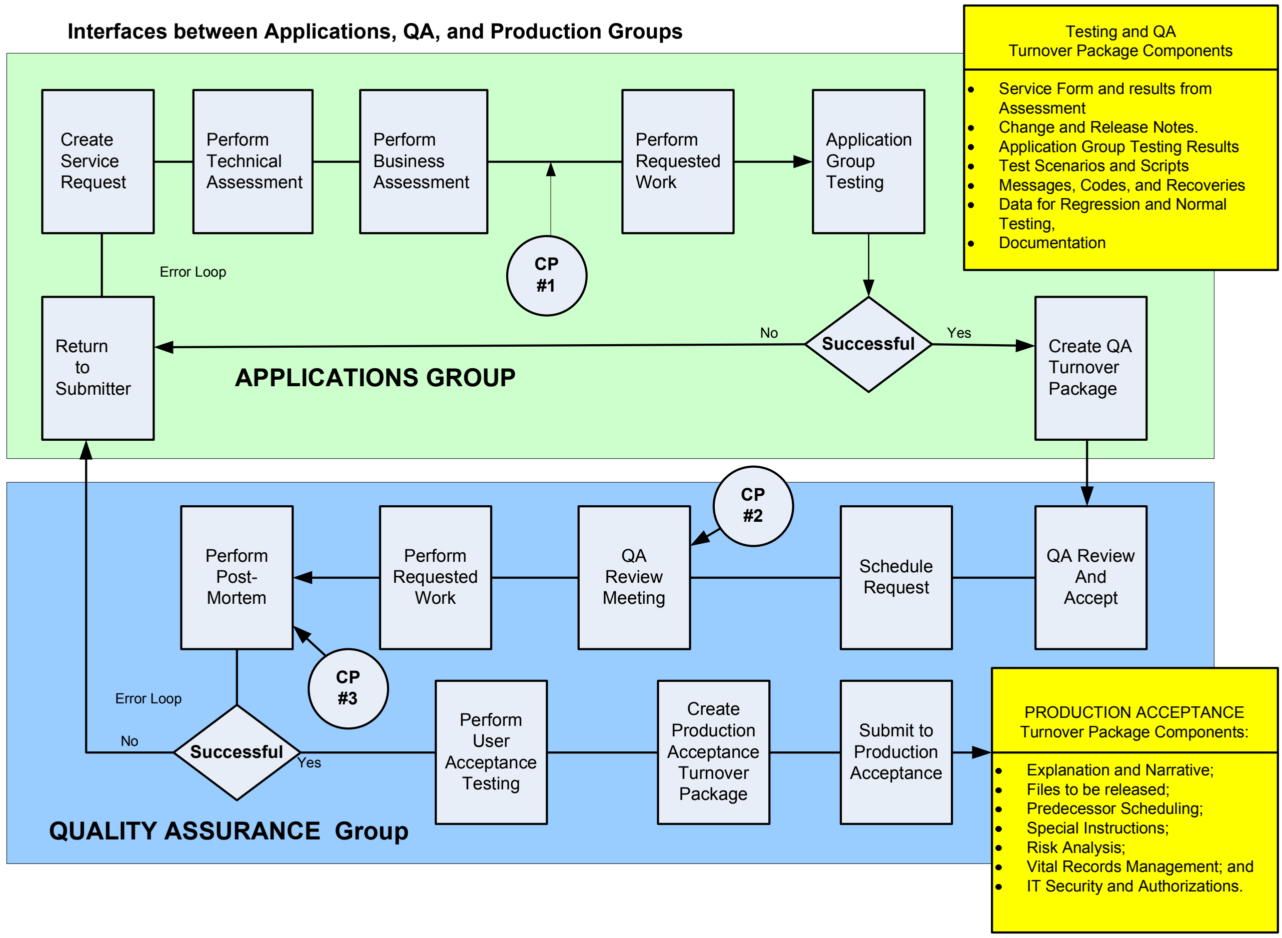


Steps involved with implementing Production Products and Services:

1. User defines Product / Service Requirements that are built by Development;
2. Testing insures proper operations, error identification and reporting, and error recovery;
3. Quality Assurance insures adherence to Standards and Procedures and company guidelines;
4. Production Acceptance moves new Product / Service into the Production Environment so that its components can be protected, named properly, and in compliance with audit and industry regulations;
5. Production implements security, vital records management, data synchronization and encryption, backup and recovery operations, support, and maintenance; and,
6. Recovery Operations are implemented to protect and safeguard IT and Business Locations.

Migrating products / services to the Production Environment

Quality Assurance and SDLC Checkpoints

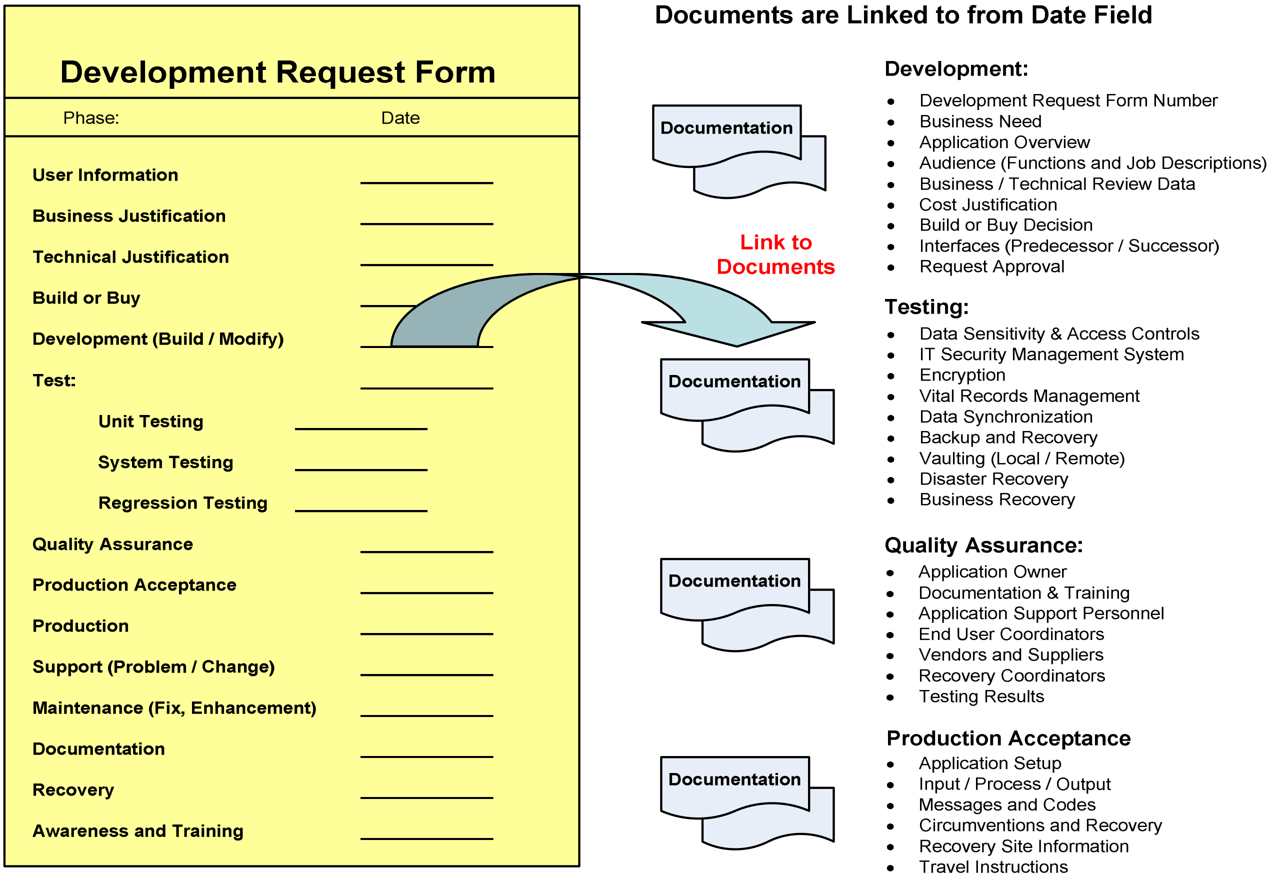

Interfaces between Applications, QA, and Production Groups
Create Service Request
Perform Technical Assessment
Perform Business Assessment
Perform Requested Work
Application Group Testing
CP #1
Error Loop
Return to Submitter
No
Successful
Yes
Create QA Turnover Package
APPLICATIONS GROUP
Testing and QA Turnover Package Components
Service Form and results from Assessment
Change and Release Notes.
Application Group Testing Results
Test Scenarios and Scripts
Messages, Codes, and Recoveries
Data for Regression and Normal Testing,
Documentation
CP #2
Perform Post-Mortem
Perform Requested Work
QA Review Meeting
Schedule Request
QA Review And Accept
CP #3
Error Loop
No
Successful
Yes
Perform User Acceptance Testing
Create Production Acceptance Turnover Package
Submit to Production Acceptance
QUALITY ASSURANCE Group
PRODUCTION ACCEPTANCE Turnover Package Components:
Explanation and Narrative;
Files to be released;
Predecessor Scheduling;
Special Instructions;
Risk Analysis;
Vital Records Management; and
IT Security and Authorizations.

Product / Service Turnover Process:

1. Client completes a Service Request that is submitted to a Technical and Business review;
2. Checkpoint #1 is used to review findings and make Build / Buy decision and strategy;
3. Development of Product / Service is completed and successfully Tested;
4. Turnover Package is submitted from Testing to QA for Review and Acceptance;
5. The Work Request is reviewed at Checkpoint #2 to determine go / no-go for performing Work Request;
6. Requested work is performed and completed;
7. A Post Mortem is performed to review success of Work Request during Checkpoint #3 meeting;
8. If Work Request fails it is returned to submitter, otherwise it moves to User Acceptance; and,
9. A Production Turnover Package is generated and submitted to Production Acceptance.

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

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

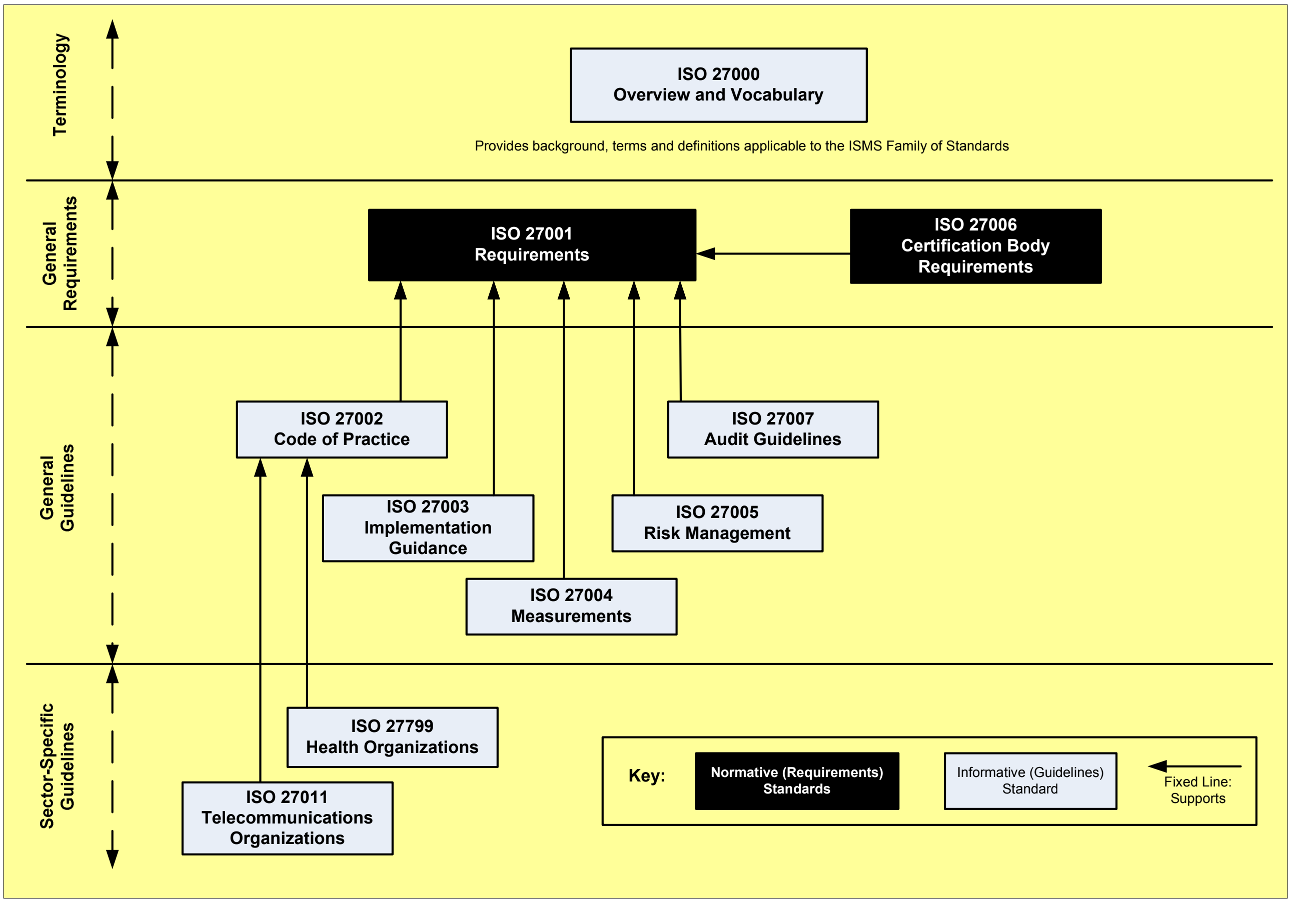
Main Documentation Menu ***Sub-Documentation Menus***

Product / Service Documentation:

1. Requestor / Owner defines Usage, Development, Operations, and Maintenance Requirements;
2. Approval to Build or Buy product / service;
3. Testing of Data Sensitivity and Access Controls through IT Security Management System;
4. Data Synchronization and Vital Records Management;
5. Backup and Recovery via Local and Remote Vaulting;
6. Full Range of Recovery Plans (Emergency, Disaster, Business, Workplace, Risk, etc.);
7. Production Acceptance instructions to set-up Product / Service for Processing;
8. Implement components into proper libraries and insure naming conventions are met;
9. Successful Completion Messages and Output Balancing instructions;
10. Error Messages and Codes, Circumventions and Recoveries, and Support Personnel; and,
11. Recovery Plans, Locations, and Travel Procedures.

Information Security Management System (ISO 27000)

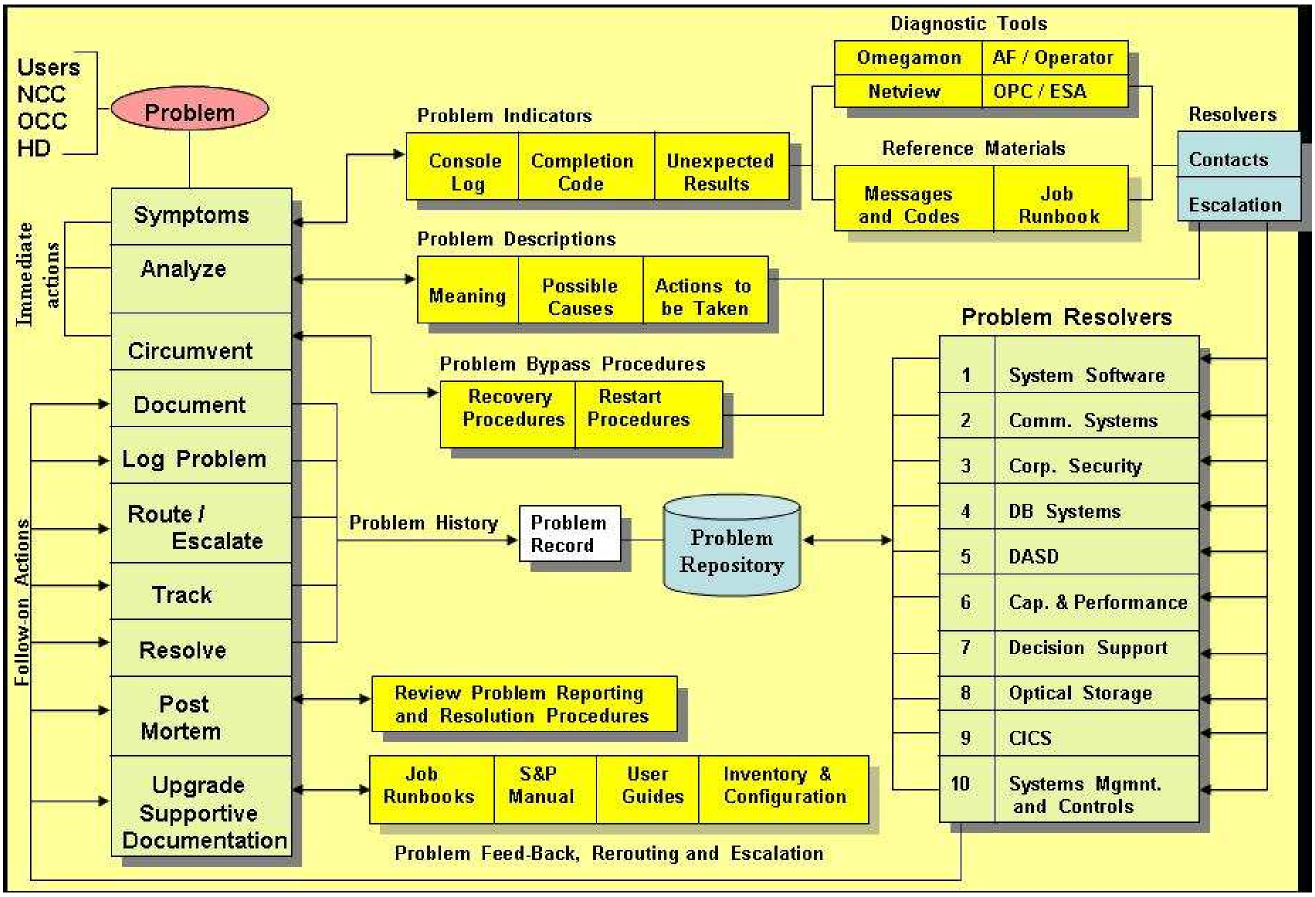
ISO 2700 Overview and Sections


Terminology
General Requirements
General Guidelines
Sector-Specific Guidelines
ISO 27000 Overview and Vocabulary
Provides background, terms and definitions applicable to the ISMS Family of Standards
ISO 27001 Requirements
ISO 27006 Certification Body Requirements
ISO 27002 Code of Practice
ISO 27007 Audit Guidelines
ISO 27003 Implementation Guidance
ISO 27005 Risk Management
ISO 27004 Measurements
ISO 27799 Health Organizations
ISO 27011 Telecommunications Organizations
Key:
Normative (Requirements) Standards
Informative (Guidelines) Standard
Fixed Line: Supports

The Information Security Management System was developed as a guideline to assist organizations implement a state-of-the-art security system that would protect information, adhere to all compliance requirements, and establish data management guidelines for best utilizing and protecting information. It consists of four sections (Terminology, General Requirements, General Guidelines, and Sector-Specific Guidelines) and contains ten modules, which are:

1. ISO 27000 – Overview and Vocabulary;
2. ISO 27001 – Requirements definitions and guidelines;
3. ISO 27002 – Code of Practices document and guidelines;
4. ISO 27003 – Implementation Guidelines;
5. ISO 27004 - Measurements guidelines and practices;
6. ISO 27005 – Risk Management guidelines and practices;
7. ISO 27006 – Audit Guidelines;
8. ISO 27799 – Health Organization guidelines and practices; and,
9. ISO 27011 – Telecommunications Organizations guidelines and procedures.

Problem Management and Circumvention Techniques



The entire Problem Life Cycle is documented above with its ten stages from Symptom Analysis through routing / escalation, tracking, resolution, and the updating of documentation and procedures resulting from a Post Mortem review. **Circumventions and Recovery Plans can be updated as a result of a Post-Mortem review**.

Tools and products used to sense, analyze, define, and respond to problems are shown. Problem Circumventions should be performed before reporting incidents to include their success / failure in the problem report. Most, if not all, of these functions are performed within ITIL in today’s environments.

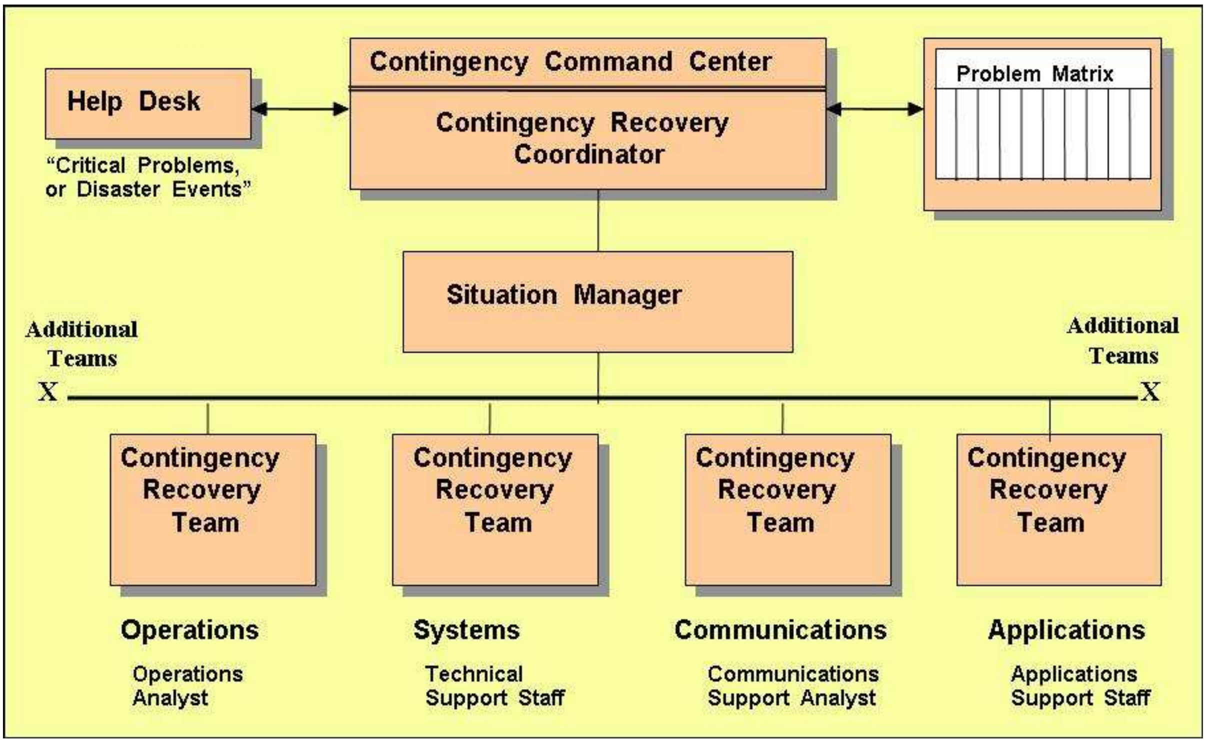
Support Levels and Escalation:

1. **Level 1 –** Analysis performed by Help Desk primary personnel based on a past occurrence of reported problem (high 90%);

2. **Level 2 –** In-house people responsible for supporting the failing component are notified and asked for problem resolution assistance; and,

3. **Level 3 –** Problem is escalated to Vendor responsible for the failing component.

Help Desk / Contingency Command Center Operations


Help Desk
"Critical Problems, or Disaster Events"
Contingency Command Center
Contingency Recovery Coordinator
Problem Matrix
Situation Manager
Additional Teams
X
Additional Teams
X
Contingency Recovery Team
Contingency Recovery Team
Contingency Recovery Team
Contingency Recovery Team
Operations
Operations Analyst
Systems
Technical Support Staff
Communications
Communications Support Analyst
Applications
Applications Support Staff

Help Desk procedures related to Recovery Operations

1. A disaster occurs as the result of a problem, and a problem is defined as a deviation from standards, so it is imperative that solid standards and procedures are developed, tested, maintained, and followed by staff and management to reduce disaster events.

2. When problems occur they are reported to the "Help Desk" whose personnel search the problem data base to see if this is a reoccurrence of a previously experienced problem (high 90% reoccurrence rate is normal).

3. Usually when a problem arises, there are circumvention procedures to follow that will restore / recover and reinitiate / restart the failing operation before problem reporting is performed;

4. Other times the problem is the result of a disaster event. When this occurs, the Help Desk attendant relates the problem to a recovery plan. He/she then activates the Recovery Plan by initiating a related "Call Tree" which notifies the Recovery Coordinator of the event. and,

5. The Contingency Recovery Coordinator notifies the "Situation Manager" responsible for the area affected by the disaster event. He/she then notifies recovery teams and they commence recovery operations in accordance to the recovery plan.

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.

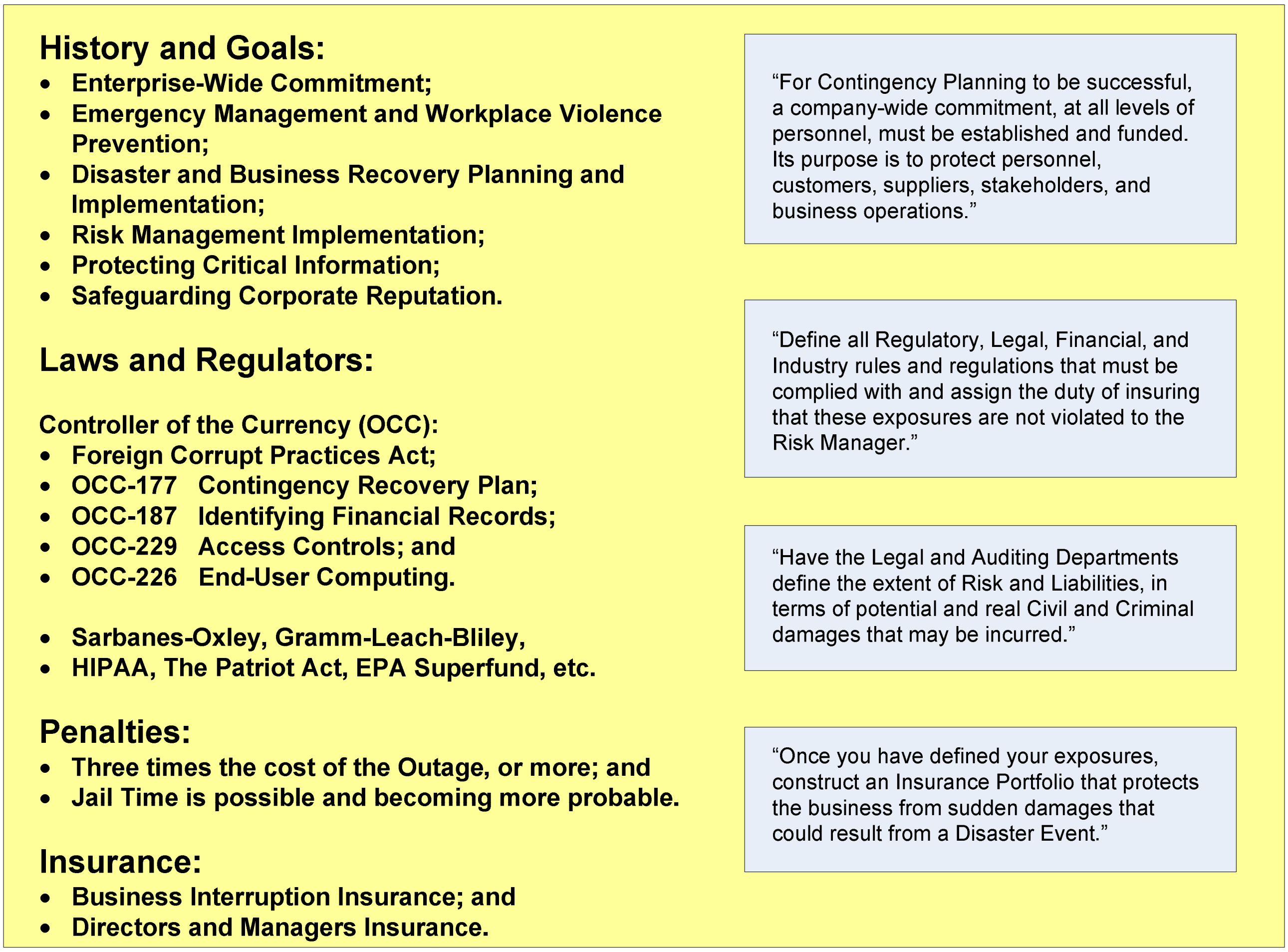
External Threats:

- Suppliers Down;
- Business Partner Down; and
- Neighboring Business Down.

Facilities:

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

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.**

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.**

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

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.**

"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."

"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."

"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."

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

Recovery Planning became a requirement when OCC-177 was issued by the Office of the Controller of the Currency. It was part of the Foreign Corrupt Practices Act that was formulated when Boeing said its financial records for a Korean deal were destroyed. Further regulations were later formulated to protect financial and compliance data from being illegally accessed or destroyed via Information Technology or Paper Document storage techniques. Because of current financial system problems and illegal business practices new laws and regulations have been, or are in the process of being, formulated.

Current trends are moving Recovery Planning towards Enterprise Resiliency and Corporate Certification that utilize "Best Practices" to achieve overall Recovery Operations via common tools and a common language to protect the entire organization world-wide. Enterprise Resiliency integrates Recovery Operations closer to the everyday tasks performed by personnel and internal control systems like SDLC, ITIL, Incident Management, and Change Management, are used to assist in this endeavor.

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;**

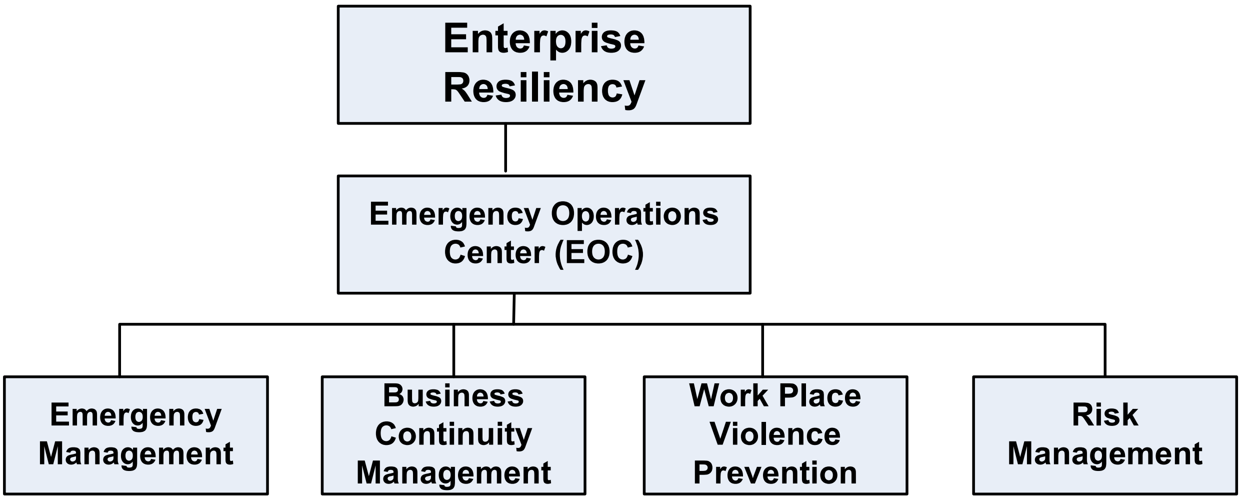
- **Working with Industry Leaders to continuously enhance recovery operations and mitigate gaps and exceptions to current practices;**

- **Achieve Compliance through Risk Management and Audit adherence;**

- **Testing and Quality Assurance; and**

- **Support and Maintenance going forward.**

What is Enterprise Resiliency?


Enterprise Resiliency
Emergency Operations Center (EOC)
Emergency Management
Business Continuity Management
Work Place Violence Prevention
Risk Management

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, etc.);**
3. **Use Best Practices tools and processes (COBIT, ITIL);**
4. **Understand 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 mitigate Gaps and Exceptions;**
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 whom;**
13. **Create / Expand Job Descriptions to direct personnel in their recovery efforts; and**
14. **Create / Update / Use Standards and Procedures, updating as changes are made.**

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.

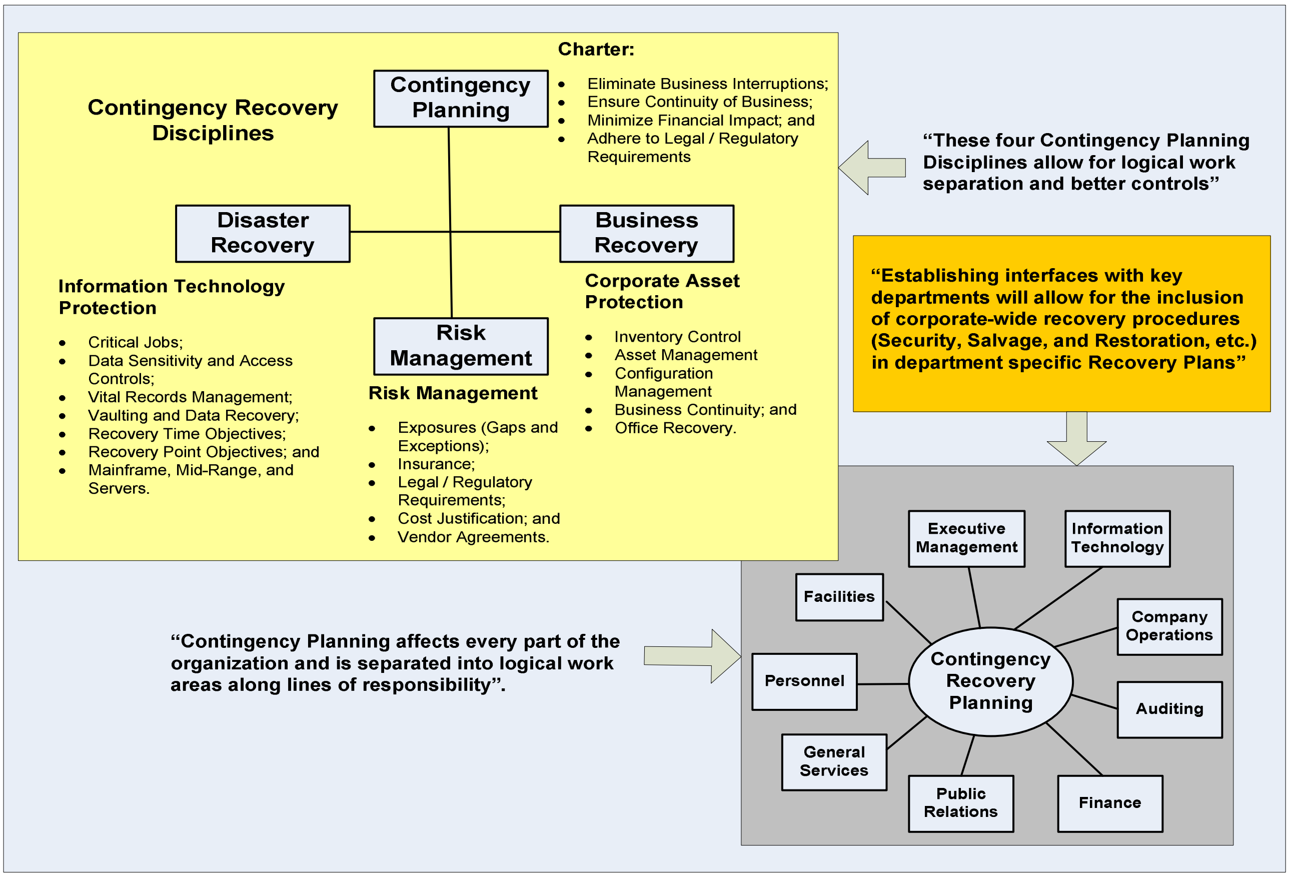
- **Workplace Violence Prevention:**
  - Security (Physical and Data) and Guards;
  - Closed Circuit Cable TV;
  - Access Controls and Card Key Systems;
  - Response Plans and Crisis Management Procedures; and
  - Employee Assistance Programs.

- **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



Charter:

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

Information Technology Protection

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

Risk Management

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

Corporate Asset Protection

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

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

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

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

1. Business Continuity Management consists of: Contingency Planning; Disaster Recovery; Business Recovery; and Risk Management (whose responsibilities are listed above).

2. Contingency Recovery Planning requires the cooperation of many, if not all, departments within a corporation.

3. Emergency Management is responsible for fire protection, internal / external personnel protection (police like), emergency operations, physical environment problems, and Hazmat conditions.

4. Once teams are established, Recovery Plans can be created, tested, and implemented. Personnel must be trained and recovery plans supported / maintained going forward.

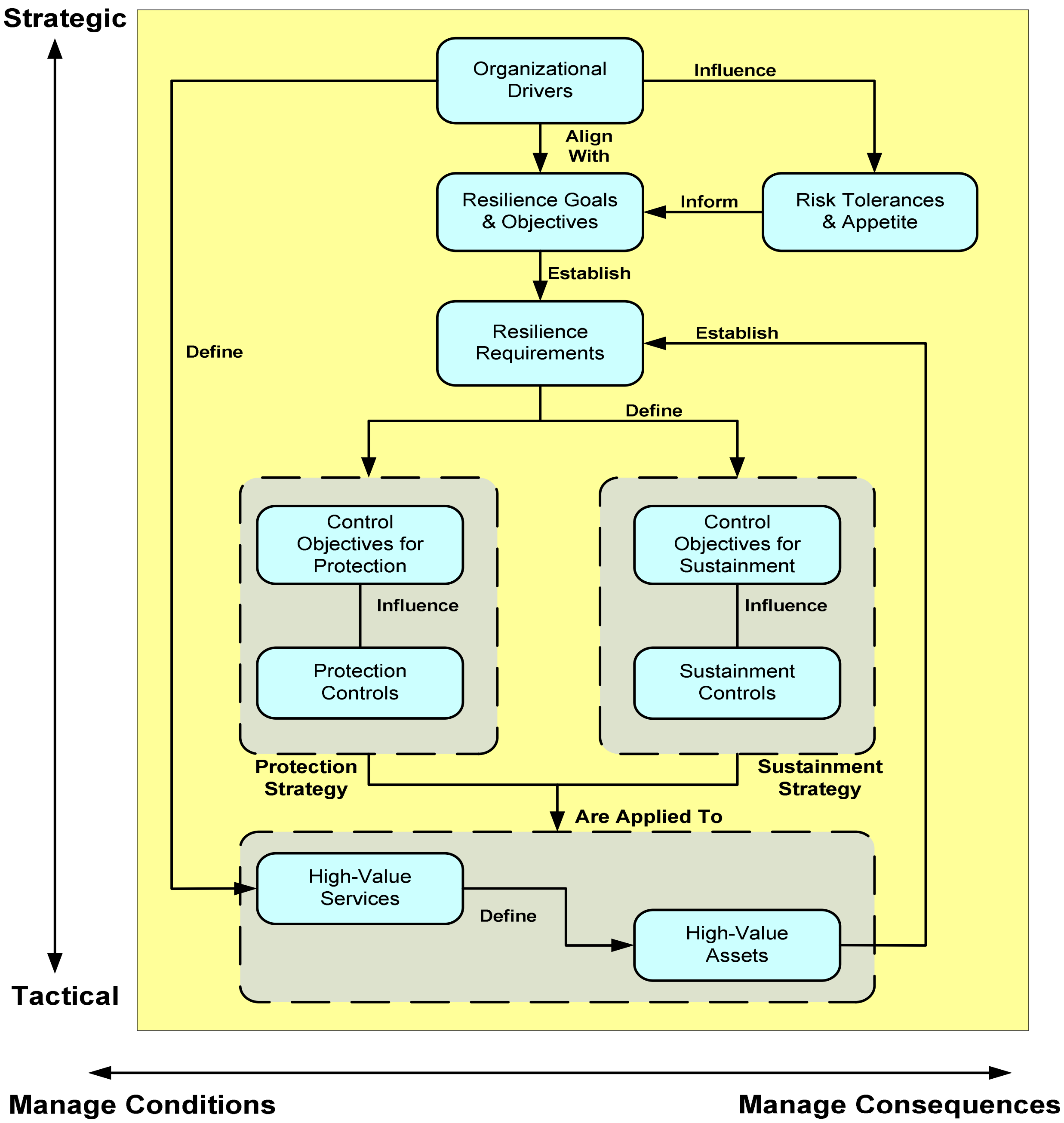
5. This can best be achieved by integrating Recovery Operations into the everyday responsibilities and functions performed by personnel, updating the Systems Development Life Cycle (SDLC), and the Change Management / Turnover process.

6. Utilizing ITIL will help achieve integration goals by adhering to company standards and procedures included in ITIL's Service Delivery and Service Support functions.

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)

CERT Resilience Management Model v1.1



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

Crisis Management, to Respond to / Control Disaster Events

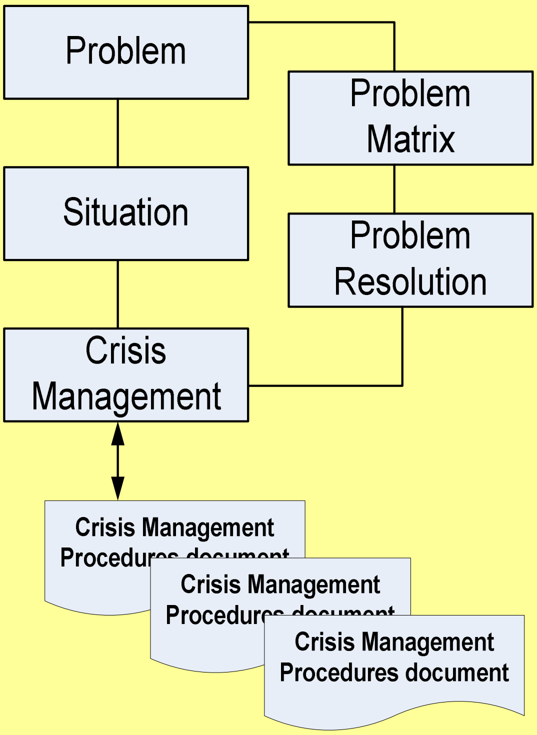
How Problems become Disasters and Controlling them through Crisis Management

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.


Problem
Problem Matrix
Situation
Problem Resolution
Crisis Management
Crisis Management Procedures document
Crisis Management Procedures document
Crisis Management Procedures document

Goals of Crisis Management

1. Define potential problem areas and their impact;
2. Develop procedures for identifying and responding to identified problem areas;
3. Document Crisis Management procedures and make personnel aware of them;
4. Test Crisis Management procedures and identify any weaknesses that should be corrected;
5. Finalize Crisis Management documentation and place into a repository;
6. Train personnel on Crisis Management concepts and procedures; and,
7. Integrate, support, and maintain Crisis Management procedures, documentation, and training.

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:

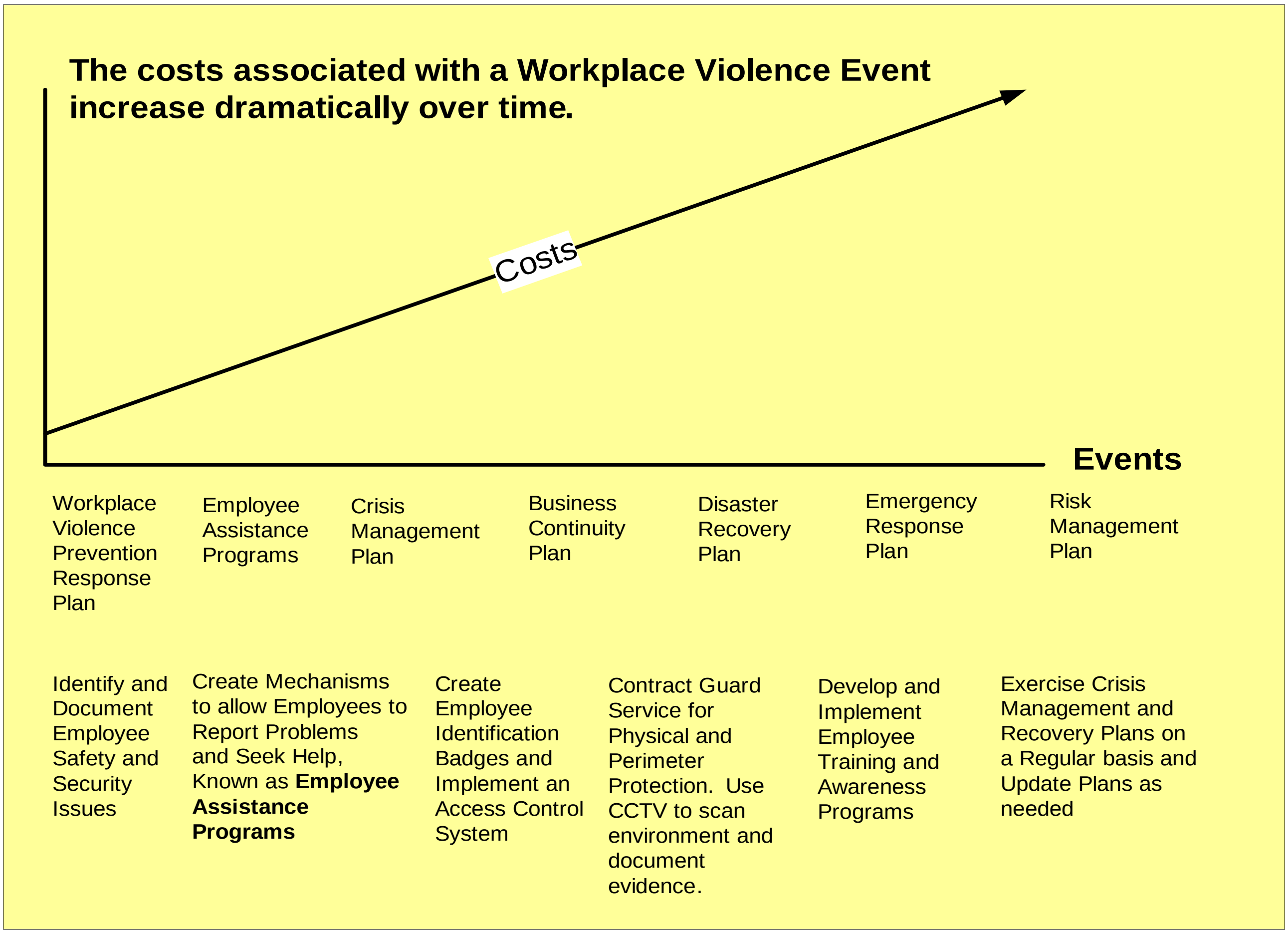
1. Comprehensive policy for Workplace Violence;
2. Train employees on Workplace Violence and its impact; and
3. Use Best Practices for Physical Security and Access Controls.

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



The costs associated with a Workplace Violence Event increase dramatically over time.

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

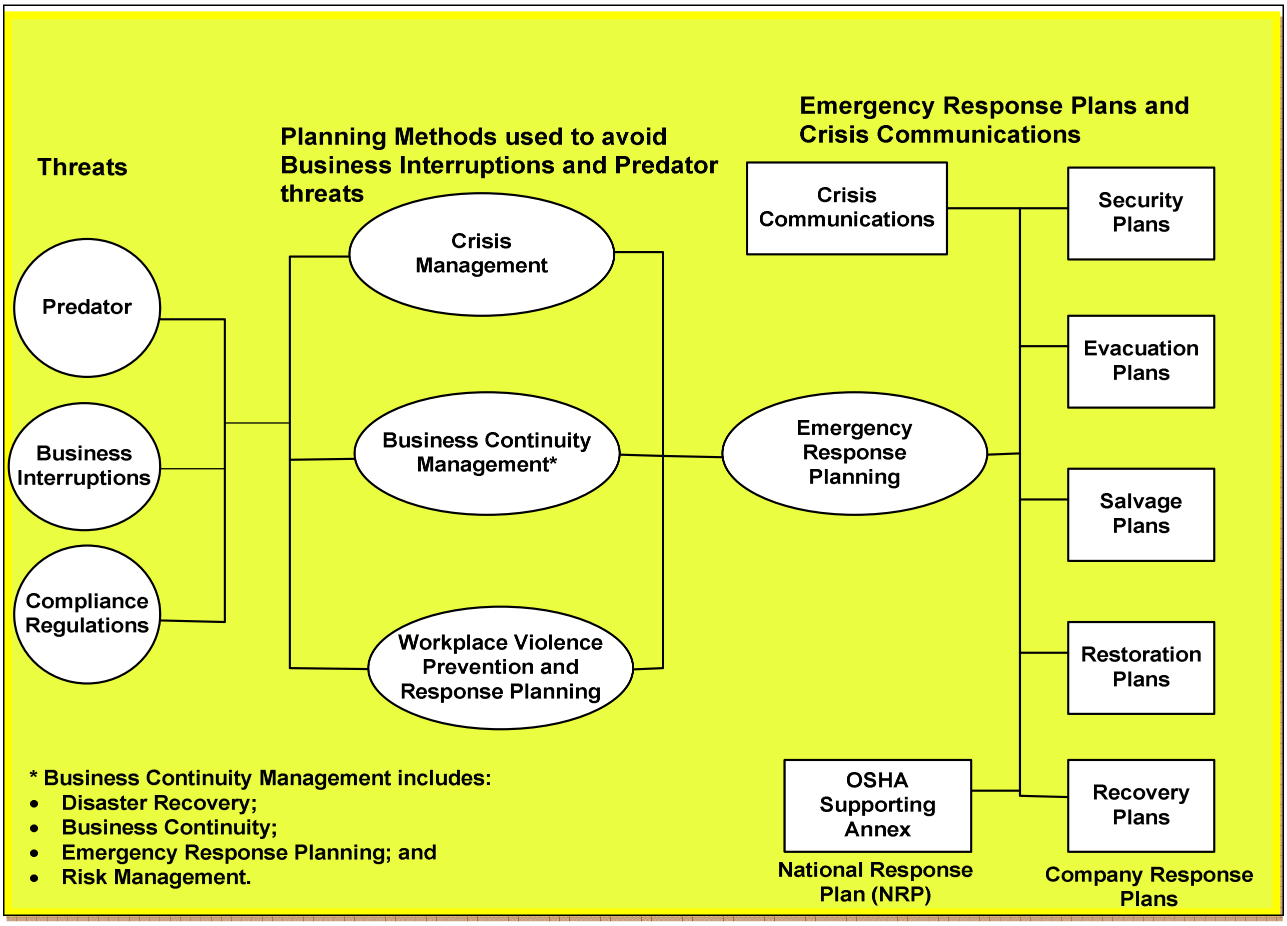
Exercise Crisis Management and Recovery Plans on a Regular basis and Update Plans as needed

The cost of Workplace Violence Prevention escalates if you neglect to implement Evacuation and Crisis Management Plans that safeguard personnel, clients, and vendors who are on your premise. Costs can be reduced by simply;

- Issuing Access Cards for a Card Key System to identify authorized personnel, vendors, and clients that are allowed access to safeguarded areas;
- Hire Physical Security Guards who would be responsible for verifying Access Cards and protecting perimeter access to locations; and
- Implement a closed circuit television system and store records for a period of time to identify violators and for evidence that can be used in prosecution.

With economic problems and layoffs increasing, Workplace Violence is expected to rise in direct proportion to the number of people who lose their jobs. This serious problem must be addressed immediately to protect personnel, keep the business operating, and to maintain the reputation of the company, while avoiding undue law suits and business interruption costs.

Target Emergency Response Environment (Logical Overview)


Threats
Planning Methods used to avoid Business Interruptions and Predator threats
Emergency Response Plans and Crisis Communications
Predator
Business Interruptions
Compliance Regulations
Crisis Management
Business Continuity Management*
Workplace Violence Prevention and Response Planning
Crisis Communications
Emergency Response Planning
Security Plans
Evacuation Plans
Salvage Plans
Restoration Plans
Recovery Plans
OSHA Supporting Annex
National Response Plan (NRP)
Company Response Plans

* Business Continuity Management includes:

- Disaster Recovery;
- Business Continuity;
- Emergency Response Planning; and
- Risk Management.

Goals:

1. Reduce Predator and Business Interruption Threats through the cooperation of all Recovery Disciplines, while maintaining Domestic and International compliance requirements;

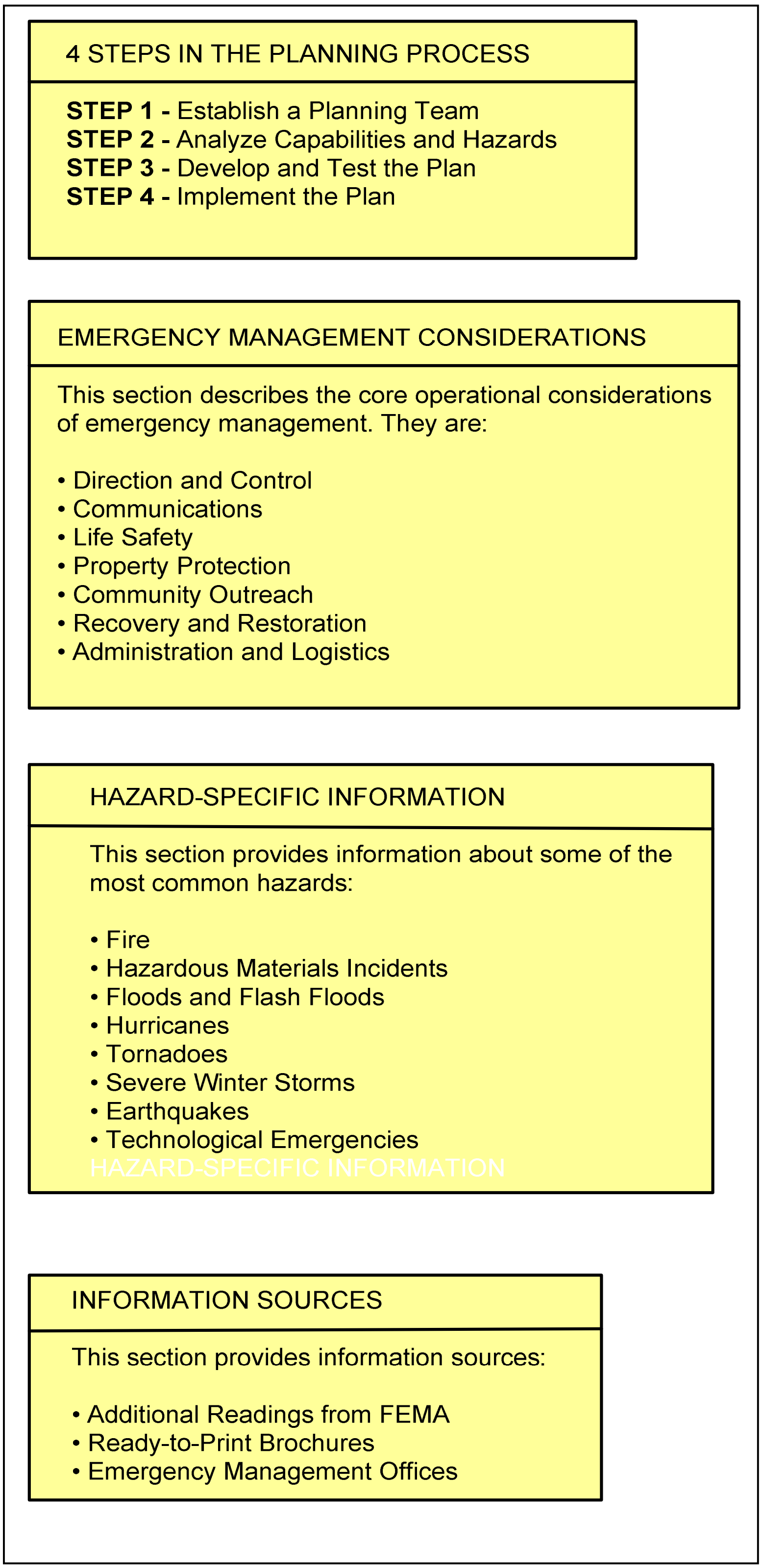
2. Implement Planning and Recovery Methods for Recovery Management, Workplace Violence Prevention, and Business Continuity Management;

3. Comply with Homeland Security, Office of Emergency Management, and National Recovery Plans (OSHA Appendix defining on-site hazardous materials) to assist First Responders;

4. Develop and Test Recovery Plans; and,

5. Implement Recovery Plans, their Support, and the Maintenance of Emergency Response Plans and Crisis Communications to best coordinate recovery operations and community outreach.

Emergency Management overview and components



4 STEPS IN THE PLANNING PROCESS

STEP 1 - Establish a Planning Team
STEP 2 - Analyze Capabilities and Hazards
STEP 3 - Develop and Test the Plan
STEP 4 - Implement the Plan

EMERGENCY MANAGEMENT CONSIDERATIONS

This section describes the core operational considerations of emergency management. They are:

- Direction and Control
- Communications
- Life Safety
- Property Protection
- Community Outreach
- Recovery and Restoration
- Administration and Logistics

HAZARD-SPECIFIC INFORMATION

This section provides information about some of the most common hazards:

- Fire
- Hazardous Materials Incidents
- Floods and Flash Floods
- Hurricanes
- Tornadoes
- Severe Winter Storms
- Earthquakes
- Technological Emergencies

HAZARD-SPECIFIC INFORMATION

INFORMATION SOURCES

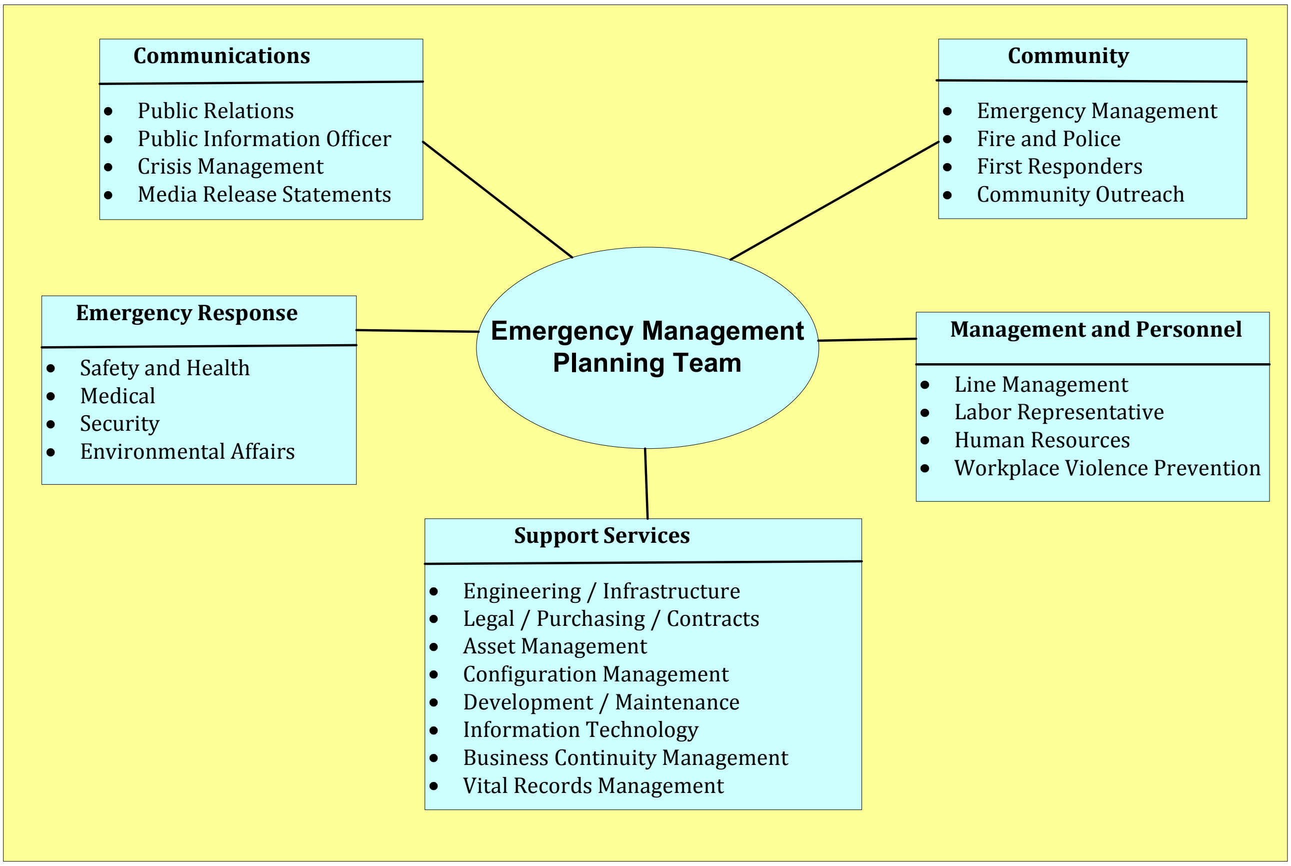
This section provides information sources:

- Additional Readings from FEMA
- Ready-to-Print Brochures
- Emergency Management Offices

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 (Local / Corporate)

1. Emergency Management Planning Team (EMPT) interfaces with many internal organizations, the surrounding community, and city / state / federal Emergency Management and OEM organizations;

2. EMPT members coordinate operations with internal / external organizations to insure that recovery plans adhere to all defined requirements and satisfy the needs of company operations;

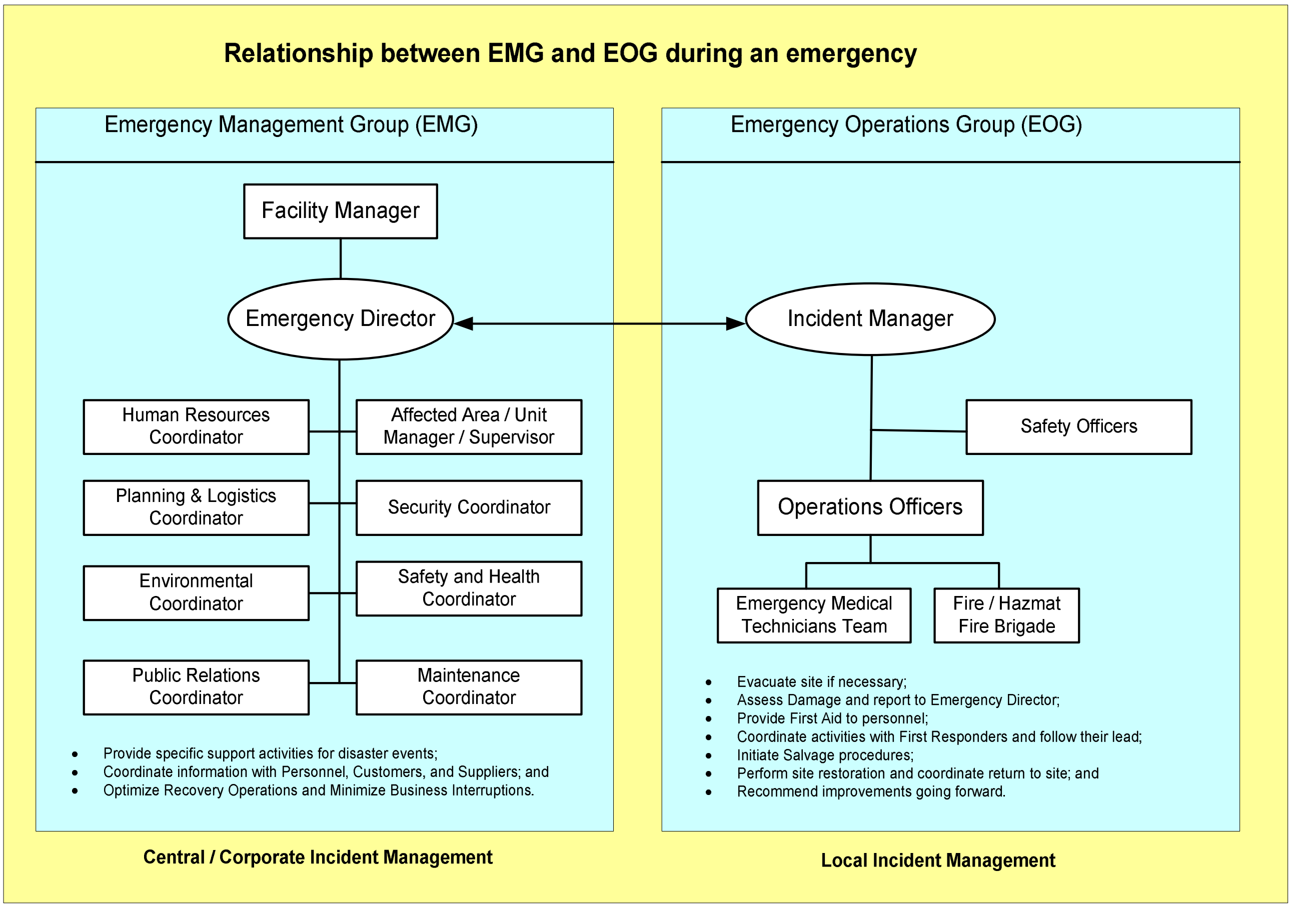
3. EMPT personnel provide a focal point for coordinating recovery operations and communications;

4. EMPT members work with community organizations and other companies within their direct or general geography (i.e., Business Parks, Community Centers, etc.);

5. The EMPT is responsible for keeping up with recovery disciplines changes and improvements and for updating procedures and awareness as necessary; and

6. The EMPT helps integrate recovery operations to comply with Version and Release Management requirements.

Emergency Management Operations Environment



Relationship between EMG and EOG during an emergency

Emergency Management Group (EMG)
Facility Manager
Emergency Director
Human Resources Coordinator
Affected Area / Unit Manager / Supervisor
Planning & Logistics Coordinator
Security Coordinator
Environmental Coordinator
Safety and Health Coordinator
Public Relations Coordinator
Maintenance Coordinator
Emergency Operations Group (EOG)
Incident Manager
Safety Officers
Operations Officers
Emergency Medical Technicians Team
Fire / Hazmat Fire Brigade

- Provide specific support activities for disaster events;
- Coordinate information with Personnel, Customers, and Suppliers; and
- Optimize Recovery Operations and Minimize Business Interruptions.

- Evacuate site if necessary;
- Assess Damage and report to Emergency Director;
- Provide First Aid to personnel;
- Coordinate activities with First Responders and follow their lead;
- Initiate Salvage procedures;
- Perform site restoration and coordinate return to site; and
- Recommend improvements going forward.

Central / Corporate Incident Management

Local Incident Management

Operations Overview

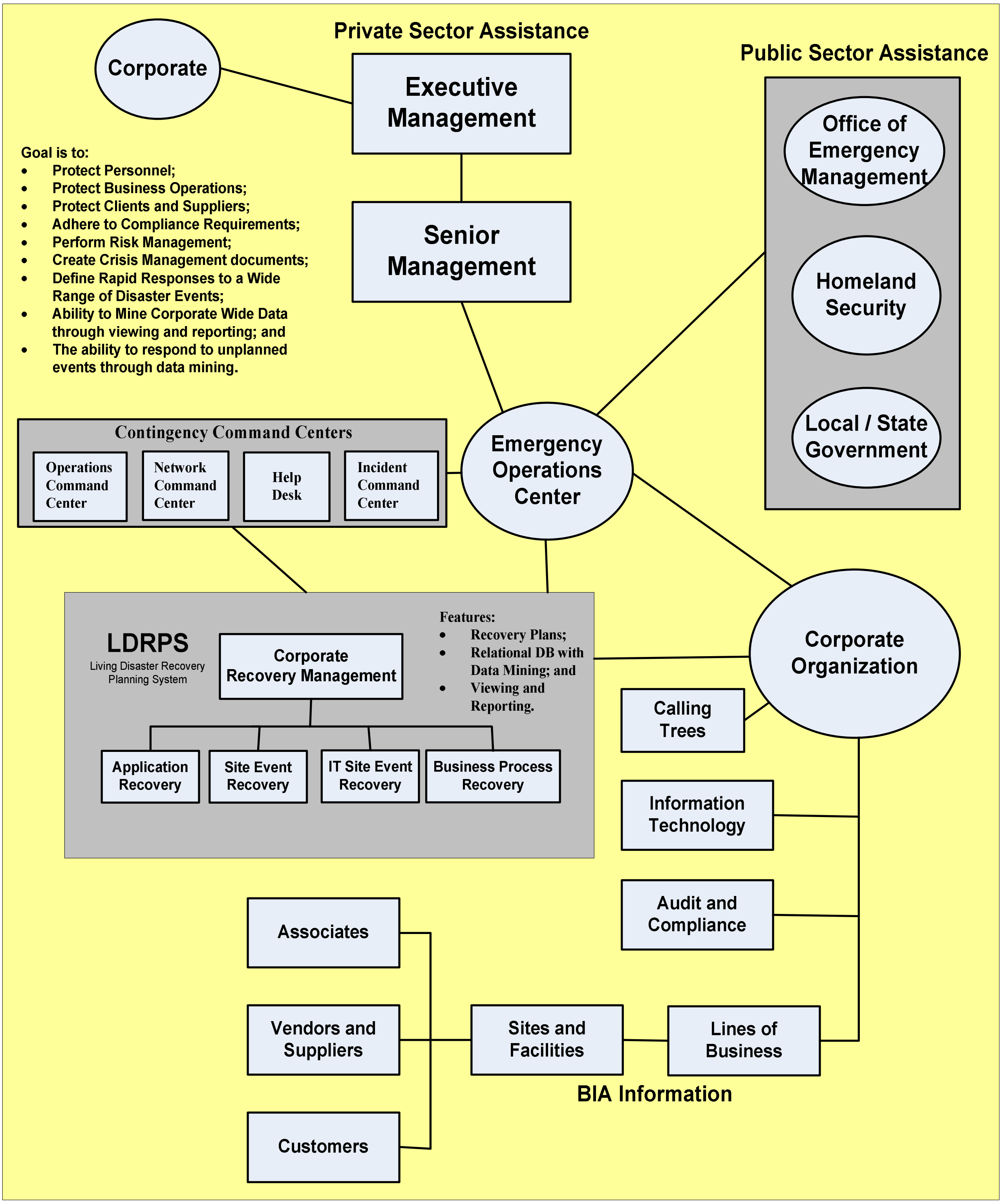
1. Incidents are investigated locally by the Incident Manager and his associates within the local Emergency Operations Group (EOG by location);

2. They report findings to the Emergency Director (EMG Corporate Location), who determines the appropriate response to the incident and dispatches response personnel to assist the Local EOG staff;

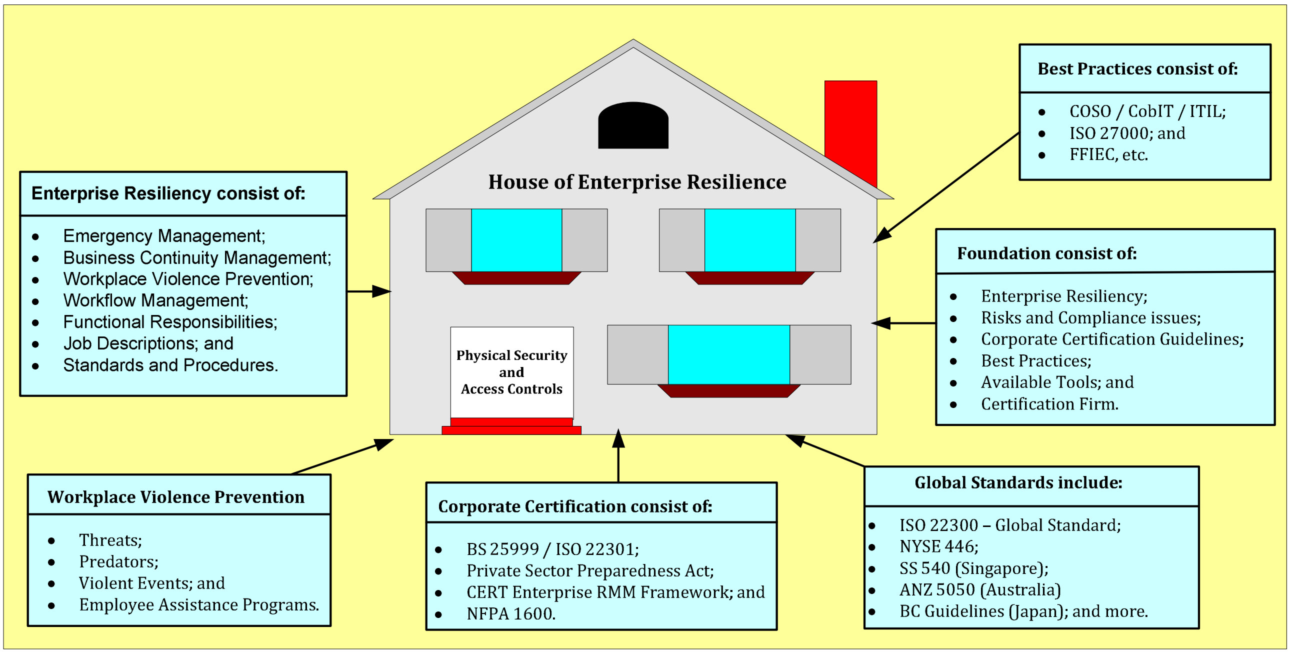
3. If the time needed to assess, salvage, and restore the damaged site is greater than recovery guidelines (or if First Responders will not allow access to the facility) then recovery plans must be activated in order to stay within Service Level Agreements and Compliance guidelines;

4. Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) are used to define time initiatives, while Recovery Time Capability (RTC) is used to determine if you can presently meet recovery objectives. If RTC is greater than RTO then improvements must be made to improve recovery responses.

Emergency Management Environmental Interfaces and Tools


Private Sector Assistance
Corporate
Executive Management
Public Sector Assistance
Office of Emergency Management
Senior Management
Homeland Security
Goal is to:
• Protect Personnel;
• Protect Business Operations;
• Protect Clients and Suppliers;
• Adhere to Compliance Requirements;
• Perform Risk Management;
• Create Crisis Management documents;
• Define Rapid Responses to a Wide Range of Disaster Events;
• Ability to Mine Corporate Wide Data through viewing and reporting; and
• The ability to respond to unplanned events through data mining.
Local / State Government
Contingency Command Centers
Operations Command Center
Network Command Center
Help Desk
Incident Command Center
Emergency Operations Center
LDRPS
Living Disaster Recovery Planning System
Corporate Recovery Management
Features:
• Recovery Plans;
• Relational DB with Data Mining; and
• Viewing and Reporting.
Corporate Organization
Calling Trees
Application Recovery
Site Event Recovery
IT Site Event Recovery
Business Process Recovery
Information Technology
Audit and Compliance
Associates
Vendors and Suppliers
Sites and Facilities
Lines of Business
BIA Information
Customers

Enterprise Resiliency must be built upon a Solid Foundation



House of Enterprise Resilience

Physical Security and Access Controls

Best Practices consist of:

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

Enterprise Resiliency consist of:

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

Foundation consist of:

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

Workplace Violence Prevention

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

Corporate Certification consist of:

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

Global Standards include:

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

Justifications for building an Enterprise Resiliency organization:

1. Enterprise Resiliency is built upon a solid foundation like a house must be;
2. Utilizing "Best Practices" like COSO, CobIT, ITIL, ISO 27000, and FFIEC Guidelines are imperative;
3. Enterprise Resiliency should combine Emergency Management, Disaster Recovery, Business Continuity, Risk Management, Workplace Violence Prevention, and Crisis Management disciplines, into a common Recovery Operation utilizing common tools and a common language, while also providing personnel with training and awareness;
4. Compliance should respond to Domestic and International guidelines and requirements, depending upon the countries that your organization does business in;
5. Recovery Management Plans should be integrating within the everyday functions performed by personnel by updating job descriptions, Standards and Procedures, and Component & Release Management, along with:
   a. Systems Development Life Cycle;
   b. Systems and Workflow Management through ITIL and other supportive tools;
   c. Product / Service validation, production operations, support, and maintenance;
   d. Recovery Plan maintenance in accordance with Version and Release Management guidelines; and,
   e. Ensuring that personnel are aware of and trained on recovery operations.
6. Provide extensive training and awareness programs to personnel and seek certifications when necessary; and
7. Seek Corporate Certification when ready.

Coso Risk Assessment Philosophy

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.

Coso Objectives and its process

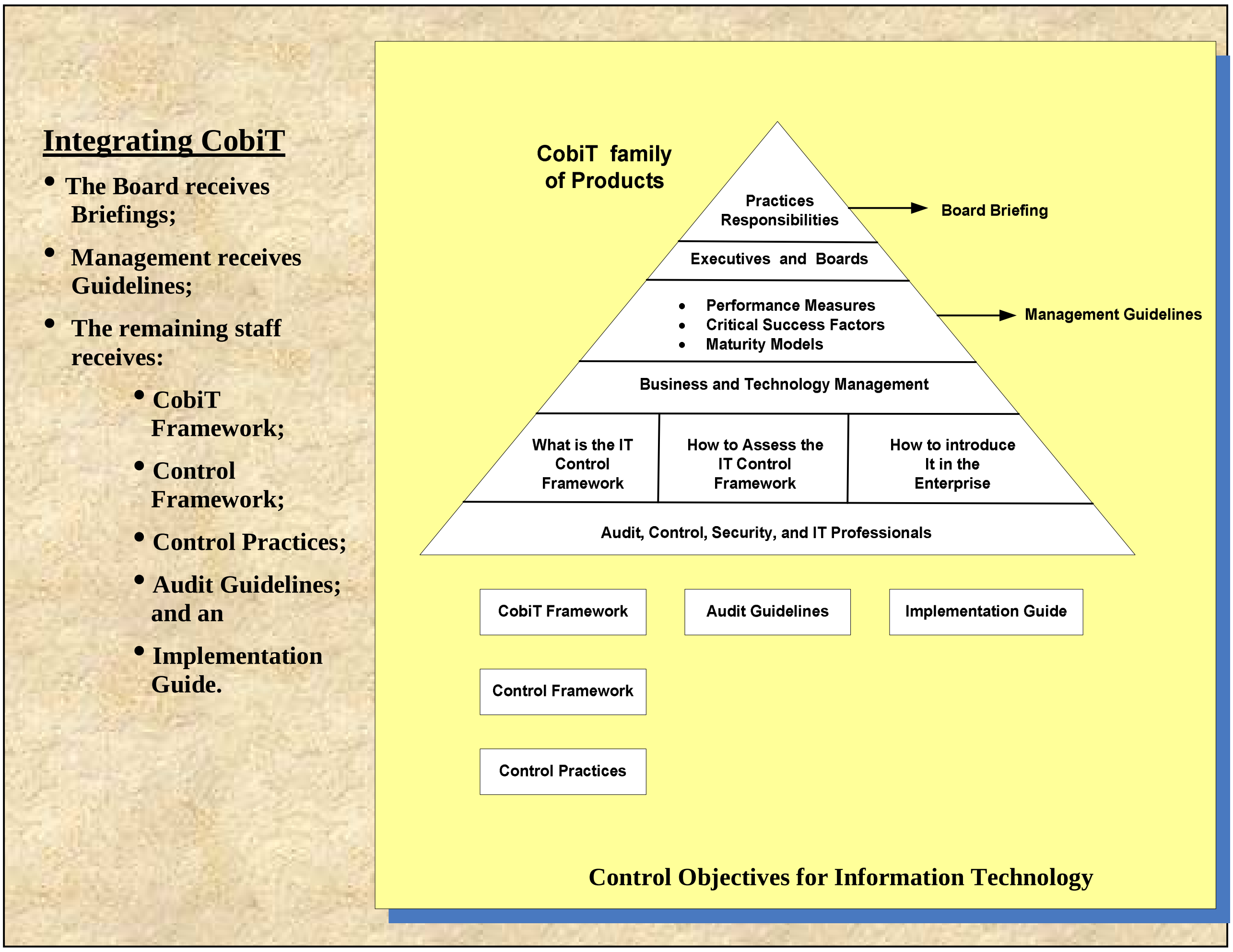
1. The above picture shows how COSO is used to identify risks, define their potential costs, and the probability of the risk;

2. It then determines how much effort and cost is associated with mitigating the risk, and how to integrate risk resolution within everyday operations by defining Job Functions and Standards and Procedures;

3. COSO ensure that best practices are not only integrated within the business but are also supported and maintained going forward; and,

4. The CERT Resilience Management Model can also help determine Risks, their Costs, the effort / cost to mitigate the Risk Gap or Exception.

CobIT Family of Products - Executive Overview



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 family of Products

Practices Responsibilities → Board Briefing

Executives and Boards

- Performance Measures
- Critical Success Factors
- Maturity Models

→ Management Guidelines

Business and Technology Management

What is the IT Control Framework

How to Assess the IT Control Framework

How to introduce It in the Enterprise

Audit, Control, Security, and IT Professionals

CobiT Framework

Audit Guidelines

Implementation Guide

Control Framework

Control Practices

Control Objectives for Information Technology

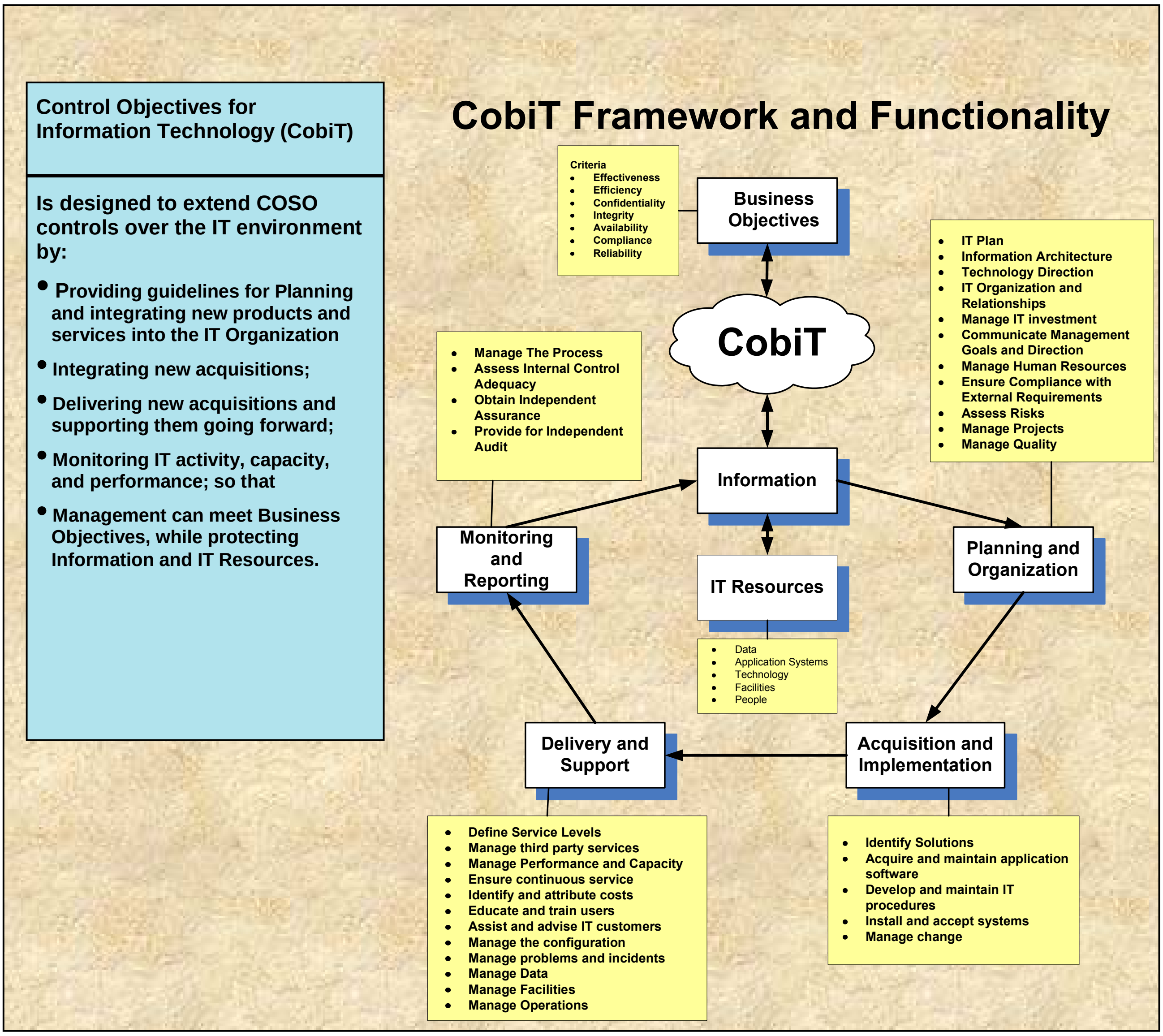
CobIT Features and Benefits include:

1. CobIT is a best practices process that helps companies integrates Business Operations within the Information Technology environment (hence CobIT). It was developed to provide all levels of personnel with the information and procedures needed to implement company products / services into the IT Production Environment.

2. CobIT also provides Control and Audit Guidelines that can be used to ensure that applications and resources are implemented in compliance with regulatory and company requirements.

3. How CobIT is integrated into an Information Technology environment is illustrated in the above picture by showing the three levels and various components that are included in the CobIT framework.

CobIT Framework – Detailed Operations



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.

CobiT Framework and Functionality

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

Business Objectives

CobiT

Information

IT Resources

- Data
- Application Systems
- Technology
- Facilities
- People

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

Planning and Organization

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

Monitoring and Reporting

Delivery and Support

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

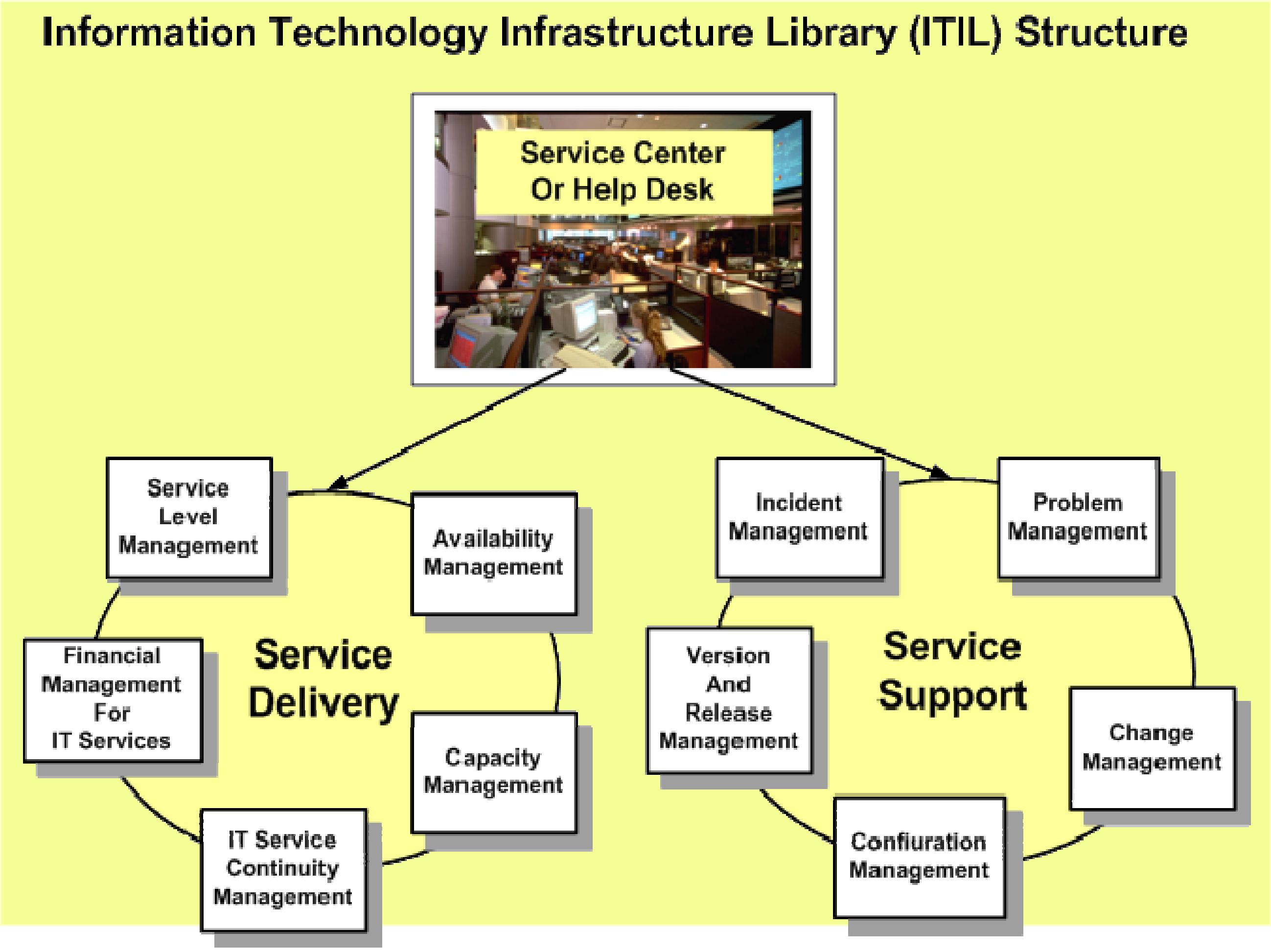
Acquisition and Implementation

- Identify Solutions
- Acquire and maintain application software
- Develop and maintain IT procedures
- Install and accept systems
- Manage change

CobIT overview

1. This picture shows how CobIT is integrated within a company's Production IT Environment;
2. Based on defined Business Objectives CobIT provides the information needed for:
   a. Planning and Organizational Placement;
   b. Acquisition and Implementation (Asset / Configuration Management);
   c. Delivery and Support (ITIL);
   d. Monitoring and Support (Capacity and Performance Systems Management); and,
   e. The need for Independent Review to validate adherence to CobIT guidelines.

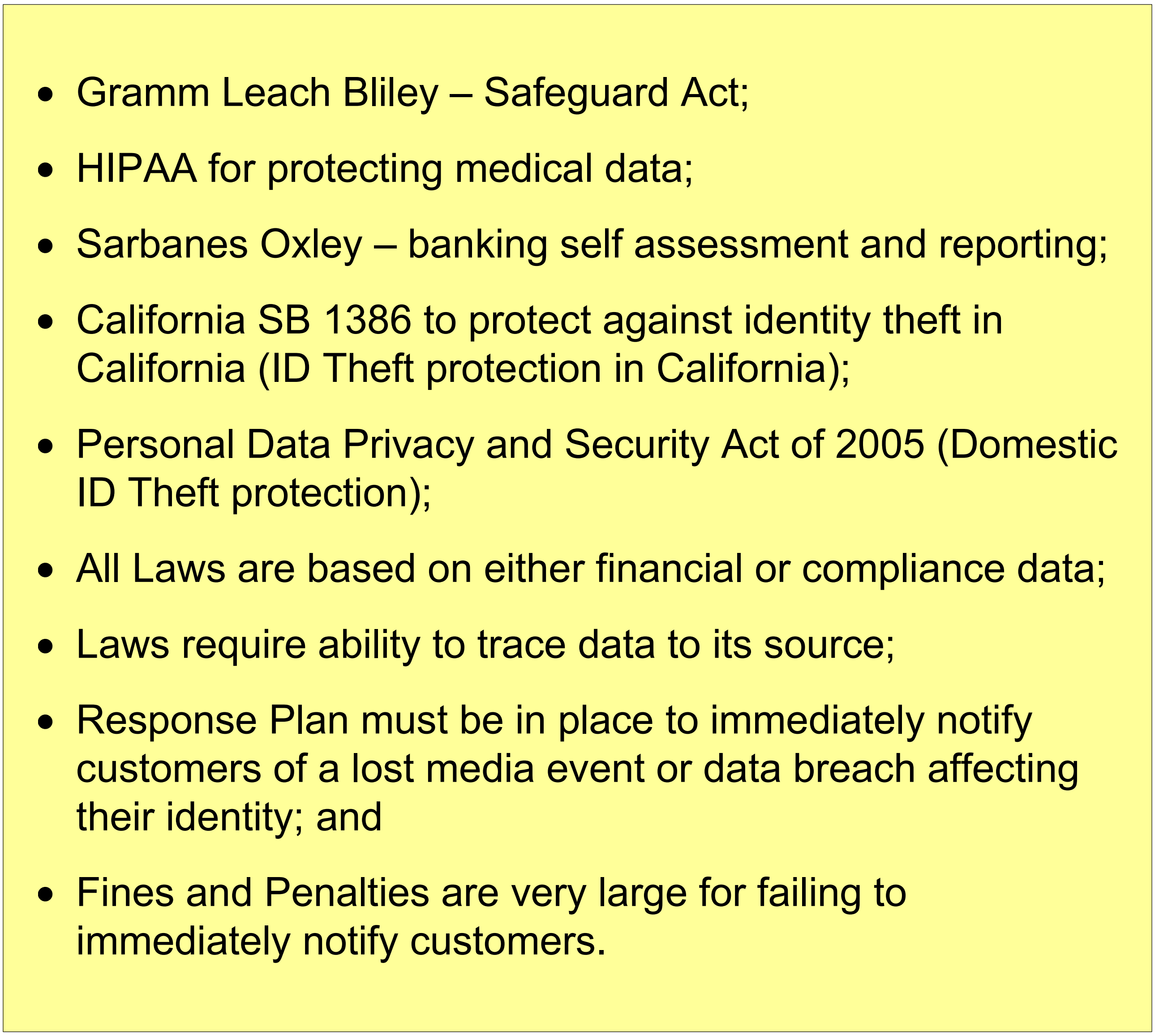
ITIL Framework - Automated Forms Management and Control



ITIL Functions, include:

1. Used to replace Forms Management and Control procedures (usually manual);
2. Service Delivery (Systems Development Life Cycle – SDLC), including:
    a. Service Level Management (Agreements / Reporting);
    b. Capacity and Performance Management;
    c. Availability Management;
    d. Financial Management; and,
    e. Business Continuity Management.
3. Services Support (Systems Management Disciplines), including:
    a. Asset and Configuration Management;
    b. Version, and Release Management; and,
    c. Incident, Problem, and Change Management.

Compliance Laws pertaining to Data Protection - Overview

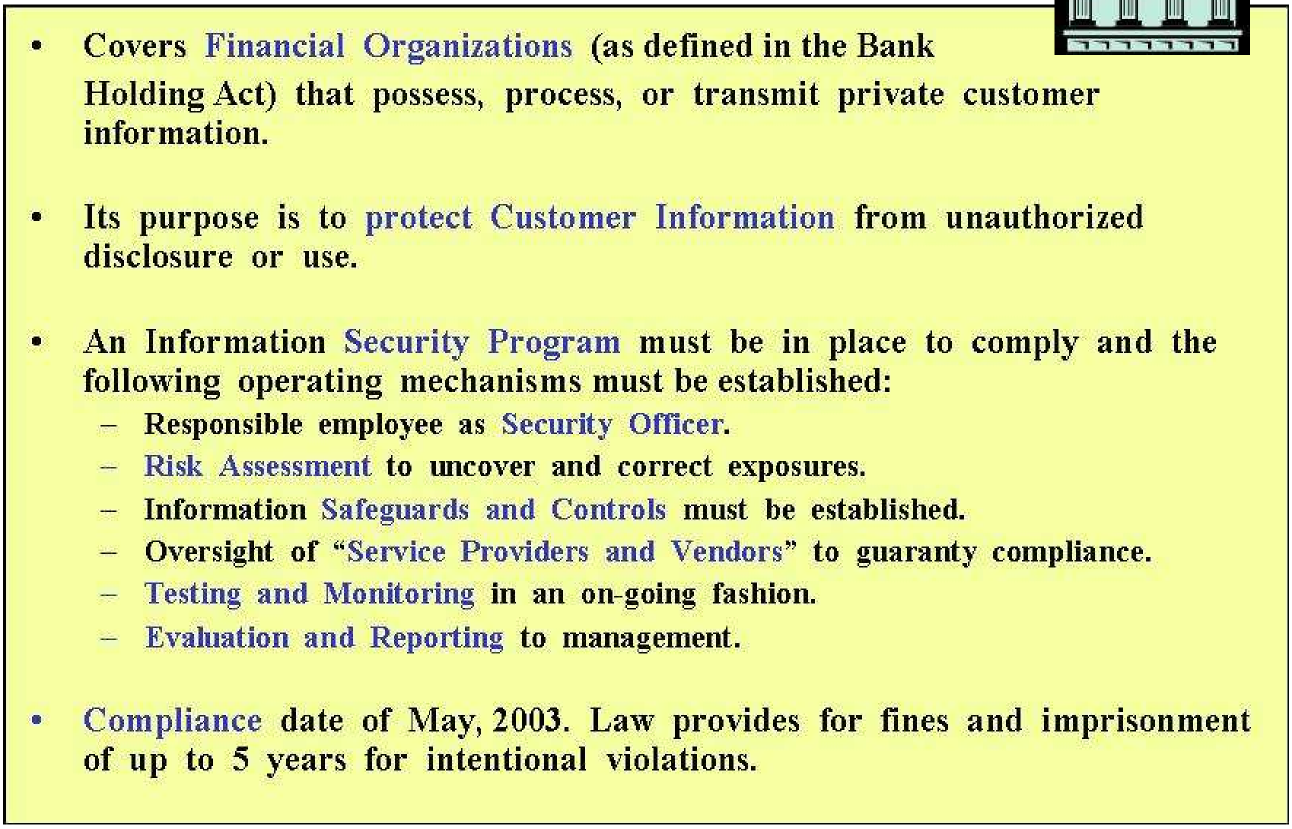


- Gramm Leach Bliley – Safeguard Act;
- HIPAA for protecting medical data;
- Sarbanes Oxley – banking self assessment and reporting;
- California SB 1386 to protect against identity theft in California (ID Theft protection in California);
- Personal Data Privacy and Security Act of 2005 (Domestic ID 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.

Additionally

1. Some of the laws governing Information Technology and Business Recovery are listed above with more details to follow. Most of these laws are based on compliance data and its protection
2. Each of the major compliance regulations, their components, and penalties are addresses in more detail in the following pages.

Graham, Leach, Bliley Act (GLB)



- 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.

GLB overview

1. To adhere to the Graham, Leach, Bliley Act (GLB) a company, must implement and maintain an in-depth IT Security program that will protect Customer Information from unauthorized access (see ISO 2700 for Information Security Management System description).

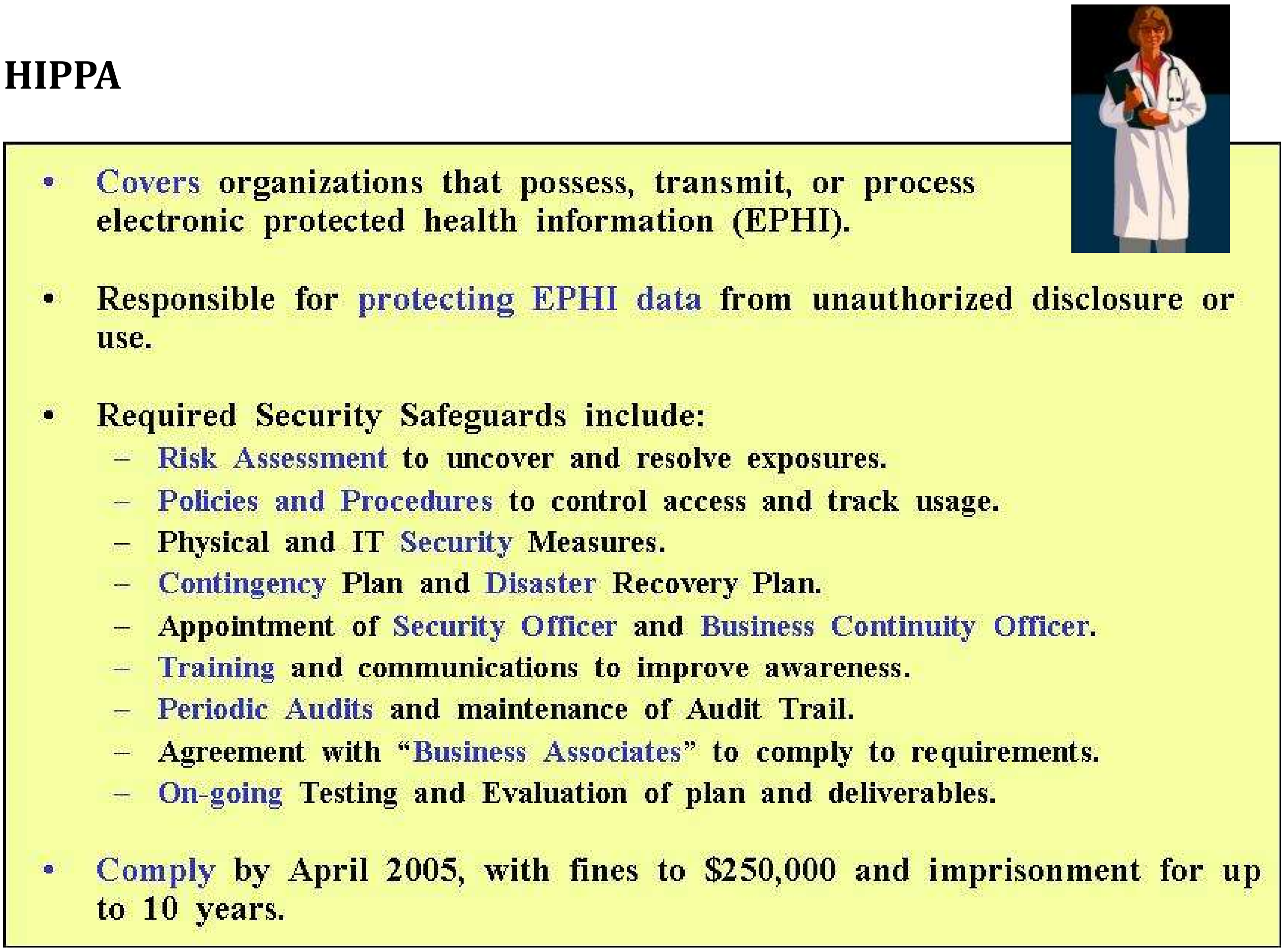
2. Its main purpose is to **stop Identify Theft** and any **unauthorized use of Customer Data**.

3. An IT Security audit is initially performed to detect where customer data is stored and how it is being protected. Any Gaps and Exceptions uncovered during this audit must be corrected to adhere to GLB;

4. IT Security Audit Trails must be maintained to document any security flaws and their correction that provides information to assist in the prosecution of violators.

5. Periodic IT Security reviews must be performed to identify improvement needs and discuss newly developed security procedures and products, with updates implemented as necessary.

HIPPA

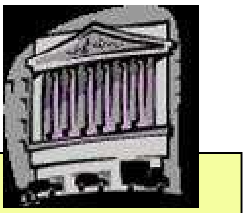


- Covers organizations that possess, transmit, or process electronic protected health information (EPHI).
- Responsible for protecting EPHI data from unauthorized disclosure or use.
- Required Security Safeguards include:
  - Risk Assessment to uncover and resolve exposures.
  - Policies and Procedures 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.

HIPPA goals

1. HIPPA was introduced to **protect personal medical information** from unauthorized access and use;
2. IT Security access control rules are created to isolate personal medical information from unauthorized access and use;
3. Security audit trails must be maintained to identify unauthorized access to personal medical information and is used to assist in the prosecution of violators;
4. Heavy fines are associated with violators of HIPPA;
5. Like GLB, HIPPA security rules and procedures are periodically reviewed to identify improvements and new procedures / products that may improve the protection of personal medical information; and,
6. These new products and procedures are implemented as deemed necessary to continually increase protection of medical information.

Sarbanes Oxley Act (SOX)



- **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).**

Sarbanes Oxley goals

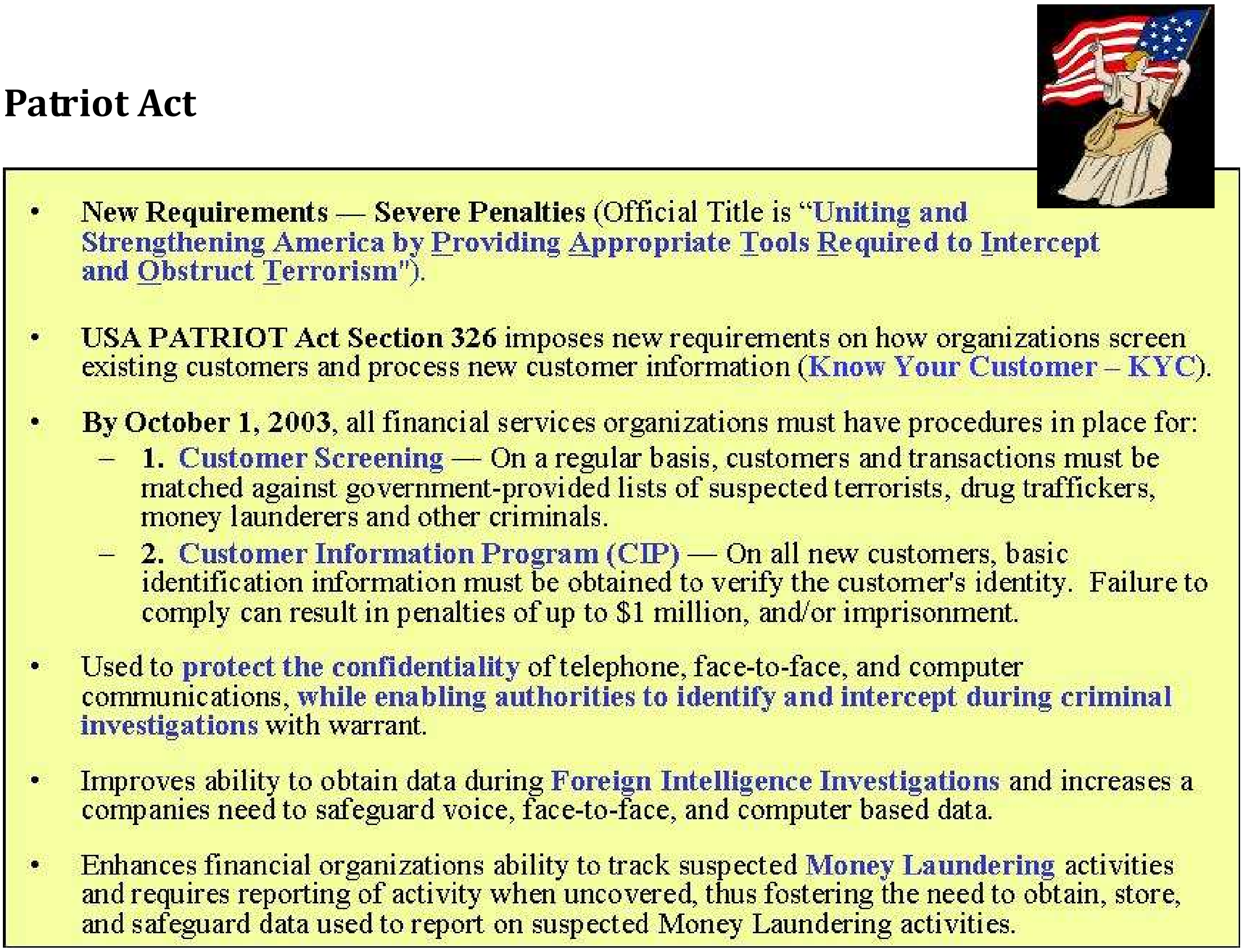
1. The Sarbanes Oxley Act was designed to **insure that corporations have current financial information available for review by auditors** and to **ensure that financial problems are addressed before they cause catastrophic problems**.

2. Its initial objective (section 302) is to define reporting requirements, then to gather all financial information into a common repository (section 404) for reporting, while eliminating security exposures (Repository can support IT Security Management).

3. The final goal of the Sarbanes Oxley Act (section 409) is to have an automated financial reporting system available for instant auditing, if necessary, and to improve financial controls.

4. More information regarding Sarbanes Oxley can be obtained through online searches, should you need to further research Sarbanes Oxley.

Patriot 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 (**Know Your Customer – KYC**).
- **By October 1, 2003**, all financial services organizations must have procedures in place 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.

Patriot Act goals

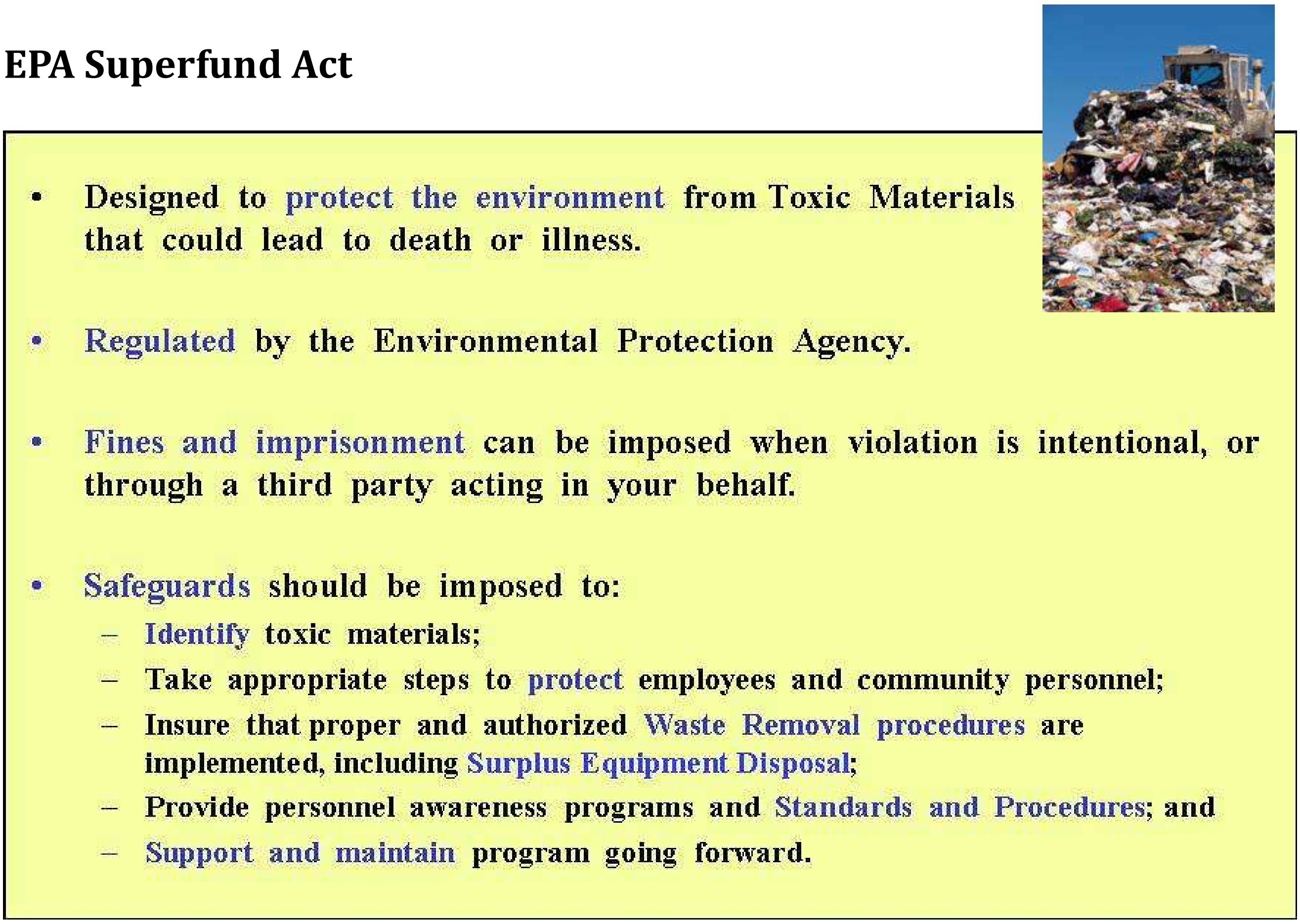
1. The Patriot Act was introduced after 9/11 to **help identify potential terrorist and their funding sources**. It directs financial organizations to first identify and validate their customers, then periodically compare their customer base to a list of know / suspected terrorist, drug traffickers, money launderers, and other criminals.

2. Other tenets of this act allows for the monitoring of communications during criminal investigations and during international communications.

3. The final section of this act allows for the monitoring of any Money Laundering activities to interrupt funding of criminal or terrorist organizations.

4. If you are the Risk Manager of a financial organization you must become familiar with the Patriot Act and adhere to its requirements or face serious criminal and civil charges.

EPA Superfund Act



- 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, including Surplus Equipment Disposal;
  - – Provide personnel awareness programs and Standards and Procedures; and
  - – Support and maintain program going forward.

EPA Super Fund goals

1. The EPA Superfund Act was designed to help **identify and clean-up toxic sites**, but has evolved to include the disposal of electronic equipment like computers, cell phones, batteries, and the like. This problem has world-wide implications because of the materials contained in computers from gold to a range of toxic materials;

2. Some computers are discarded and sent overseas for breakdown and material processing;

3. Unfortunately, the methods used to dispose of computers have resulted in poisoning and pollution on a large and dangerous scale;

4. Many companies have developed a "Total Cost of Ownership" concept for purchasing, deploying, and terminating their computer equipment;

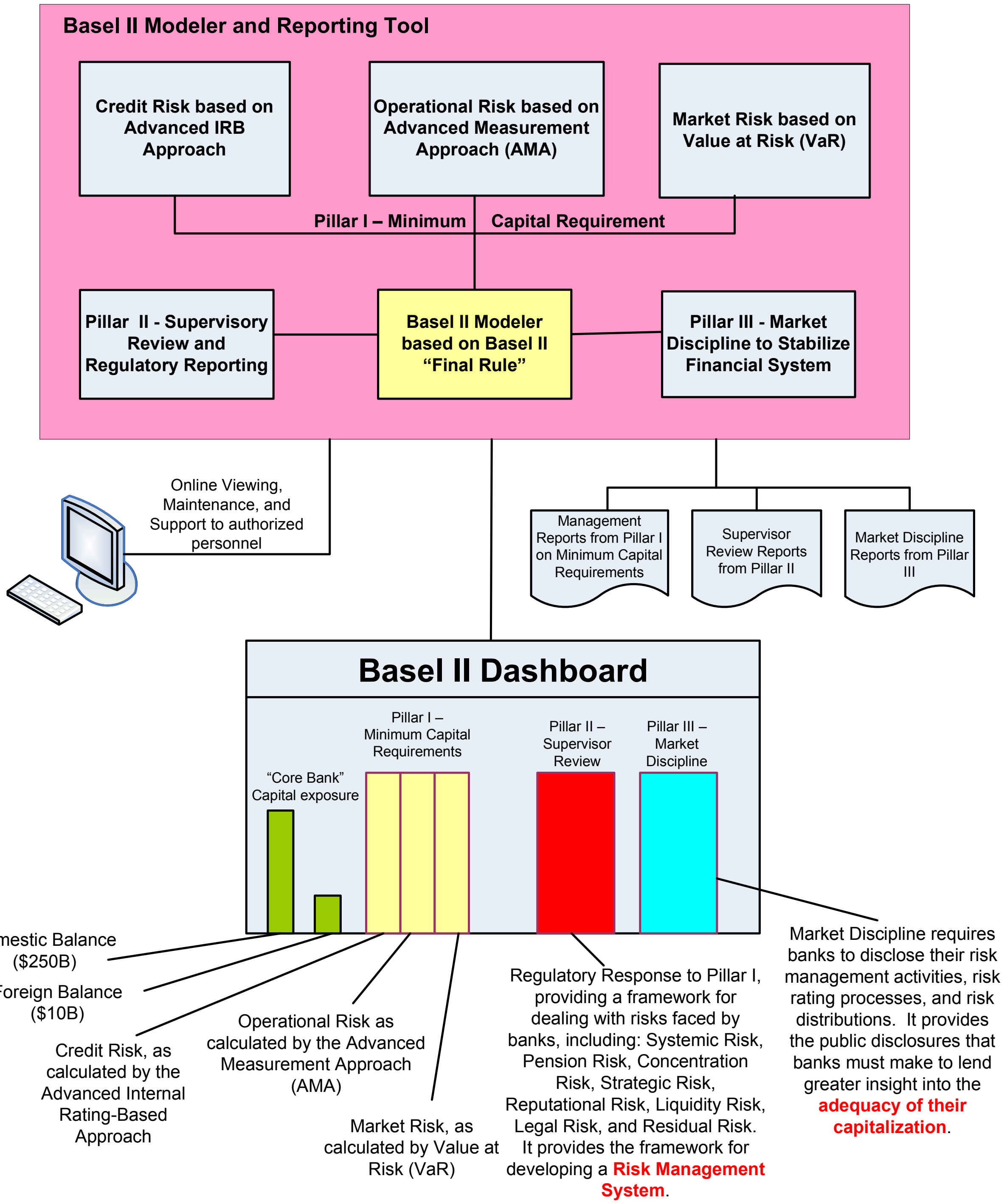
5. The vendors are responsible for supplying and disposing of computer equipment in a manner that adheres to EPA Superfund guidelines;

6. This also includes the erasing of any data from the memory of disposed or redeployed equipment thereby eliminating the chance that personal or business data would be accessed by unauthorized personnel.

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

Basel II - Overview

Basel II Modeler and Dashboard concept


Basel II Modeler and Reporting Tool
Credit Risk based on Advanced IRB Approach
Operational Risk based on Advanced Measurement Approach (AMA)
Market Risk based on Value at Risk (VaR)
Pillar I – Minimum Capital Requirement
Pillar II - Supervisory Review and Regulatory Reporting
Basel II Modeler based on Basel II "Final Rule"
Pillar III - Market Discipline to Stabilize Financial System
Online Viewing, Maintenance, and Support to authorized personnel
Management Reports from Pillar I on Minimum Capital Requirements
Supervisor Review Reports from Pillar II
Market Discipline Reports from Pillar III
Basel II Dashboard
Pillar I – Minimum Capital Requirements
Pillar II – Supervisor Review
Pillar III – Market Discipline
"Core Bank" Capital exposure
Domestic Balance ($250B)
Foreign Balance ($10B)

Credit Risk, as calculated by the Advanced Internal Rating-Based Approach

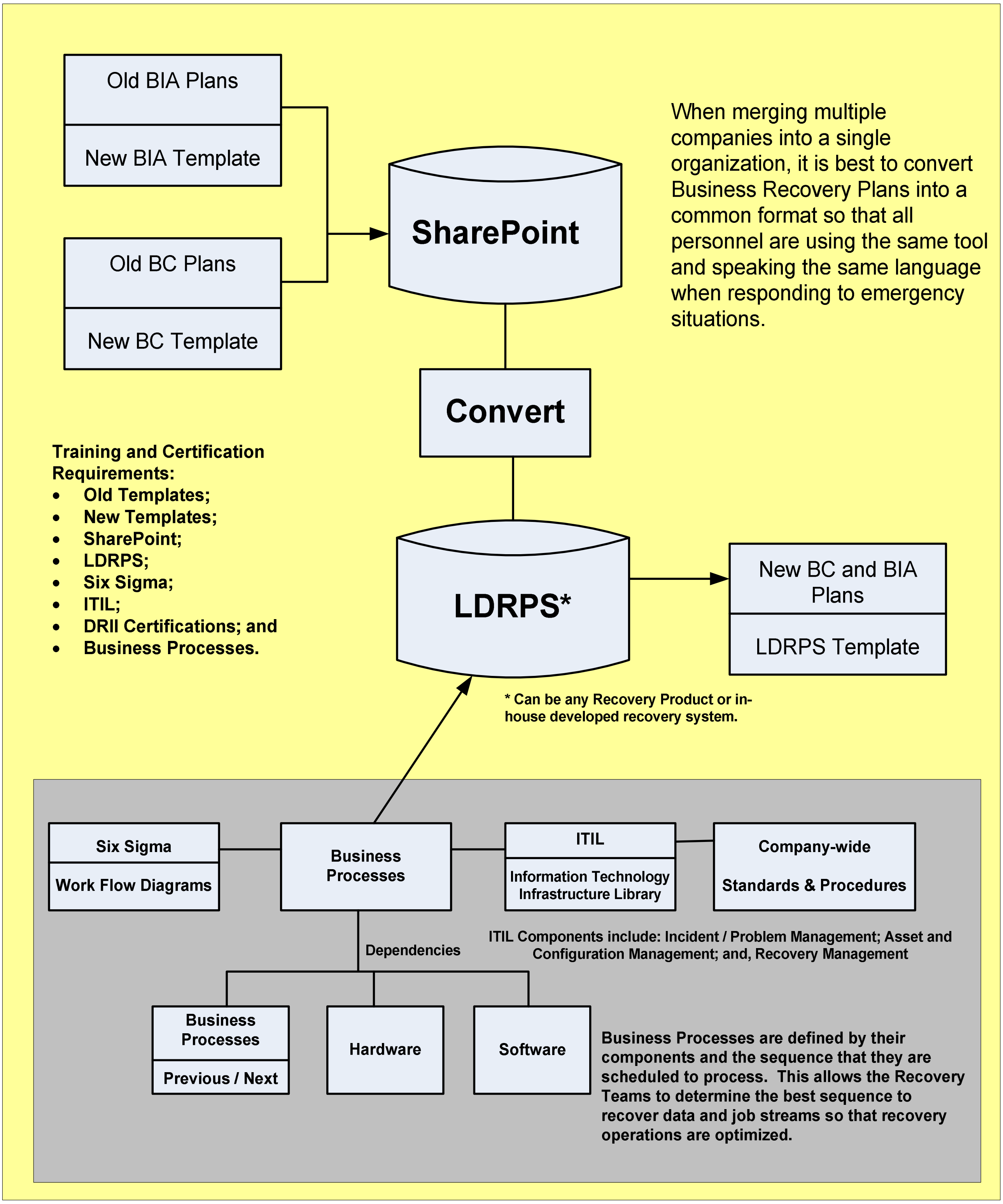
Operational Risk as calculated by the Advanced Measurement Approach (AMA)

Market Risk, as calculated by Value at Risk (VaR)

Regulatory Response to Pillar I, providing a framework for dealing with risks faced by banks, including: Systemic Risk, Pension Risk, Concentration Risk, Strategic Risk, Reputational Risk, Liquidity Risk, Legal Risk, and Residual Risk. It provides the framework for developing a **Risk Management System**.

Market Discipline requires banks to disclose their risk management activities, risk rating processes, and risk distributions. It provides the public disclosures that banks must make to lend greater insight into the **adequacy of their capitalization**.

Business Continuity Conversion and Integration



When merging multiple companies into a single organization, it is best to convert Business Recovery Plans into a common format so that all personnel are using the same tool and speaking the same language when responding to emergency situations.

Training and Certification Requirements:

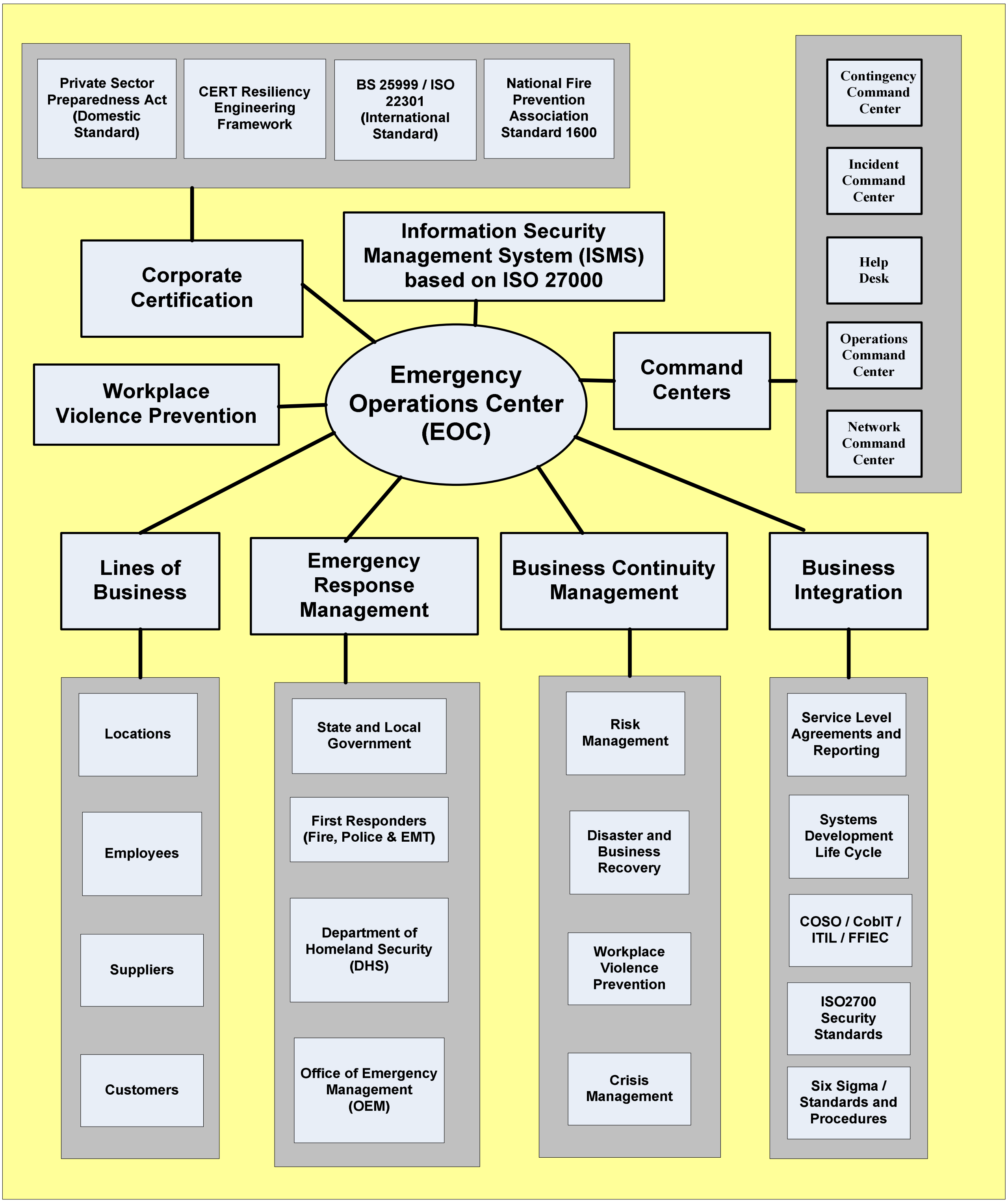
- **Old Templates;**
- **New Templates;**
- **SharePoint;**
- **LDRPS;**
- **Six Sigma;**
- **ITIL;**
- **DRII Certifications; and**
- **Business Processes.**

*** Can be any Recovery Product or in-house developed recovery system.**

ITIL Components include: Incident / Problem Management; Asset and Configuration Management; and, Recovery Management

Business Processes are defined by their components and the sequence that they are scheduled to process. This allows the Recovery Teams to determine the best sequence to recover data and job streams so that recovery operations are optimized.

Fully Integrated Recovery Operations and Disciplines (End Goal)


Private Sector Preparedness Act (Domestic Standard)
CERT Resiliency Engineering Framework
BS 25999 / ISO 22301 (International Standard)
National Fire Prevention Association Standard 1600
Contingency Command Center
Incident Command Center
Help Desk
Operations Command Center
Network Command Center
Corporate Certification
Information Security Management System (ISMS) based on ISO 27000
Workplace Violence Prevention
Emergency Operations Center (EOC)
Command Centers
Lines of Business
Emergency Response Management
Business Continuity Management
Business Integration
Locations
Employees
Suppliers
Customers
State and Local Government
First Responders (Fire, Police & EMT)
Department of Homeland Security (DHS)
Office of Emergency Management (OEM)
Risk Management
Disaster and Business Recovery
Workplace Violence Prevention
Crisis Management
Service Level Agreements and Reporting
Systems Development Life Cycle
COSO / CobIT / ITIL / FFIEC
ISO2700 Security Standards
Six Sigma / Standards and Procedures

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.