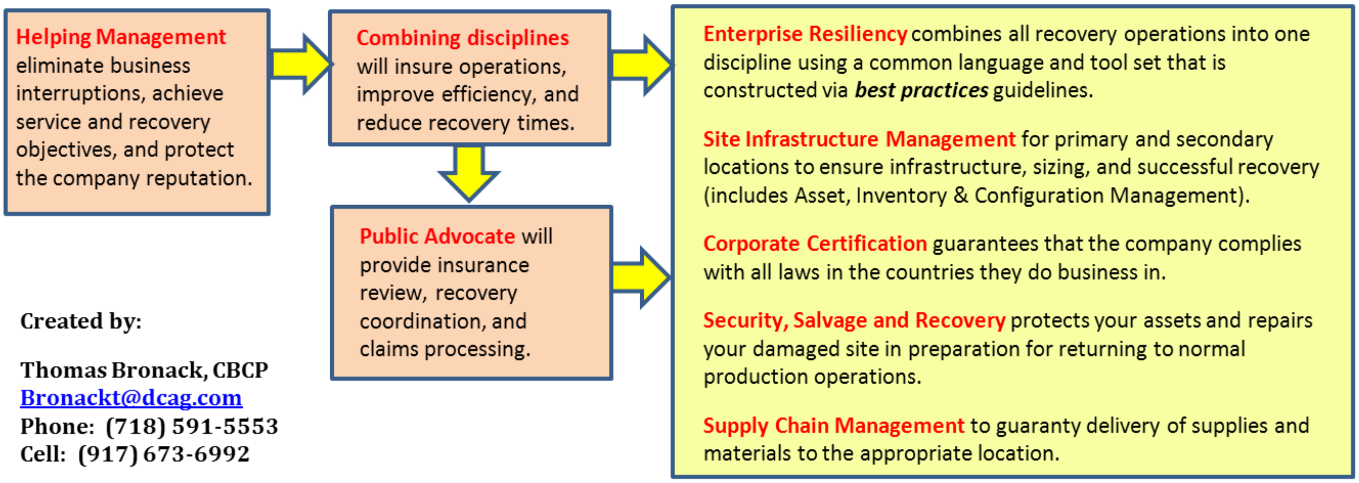
Achieving Enterprise Resiliency And Corporate Certification

DCAG
Service Offering

By

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



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

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

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

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

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

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

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

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

Created by:

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

The following article was created to explain how a company can achieve more effective recovery and compliance through Enterprise Resiliency and Corporate Certification. It is intended to provide a solid foundation upon which your company can achieve an optimized, safeguarded, and compliant environment for both business and Information Technology locations. As a result of these efforts the company and its personnel will positively enhance their reputation.

Companies following the directions outlined in this paper will improve production and recovery operations, ensured the company reputation, and generally achieved a higher degree of business operations with fewer interruptions. Additionally, the staff will be better trained, have a higher degree or morale, and the company will achieve a higher rate of retention for people and business clients (both present and prospective).

Table of Contents:

Contents

What is Enterprise Resiliency and Corporate Certification

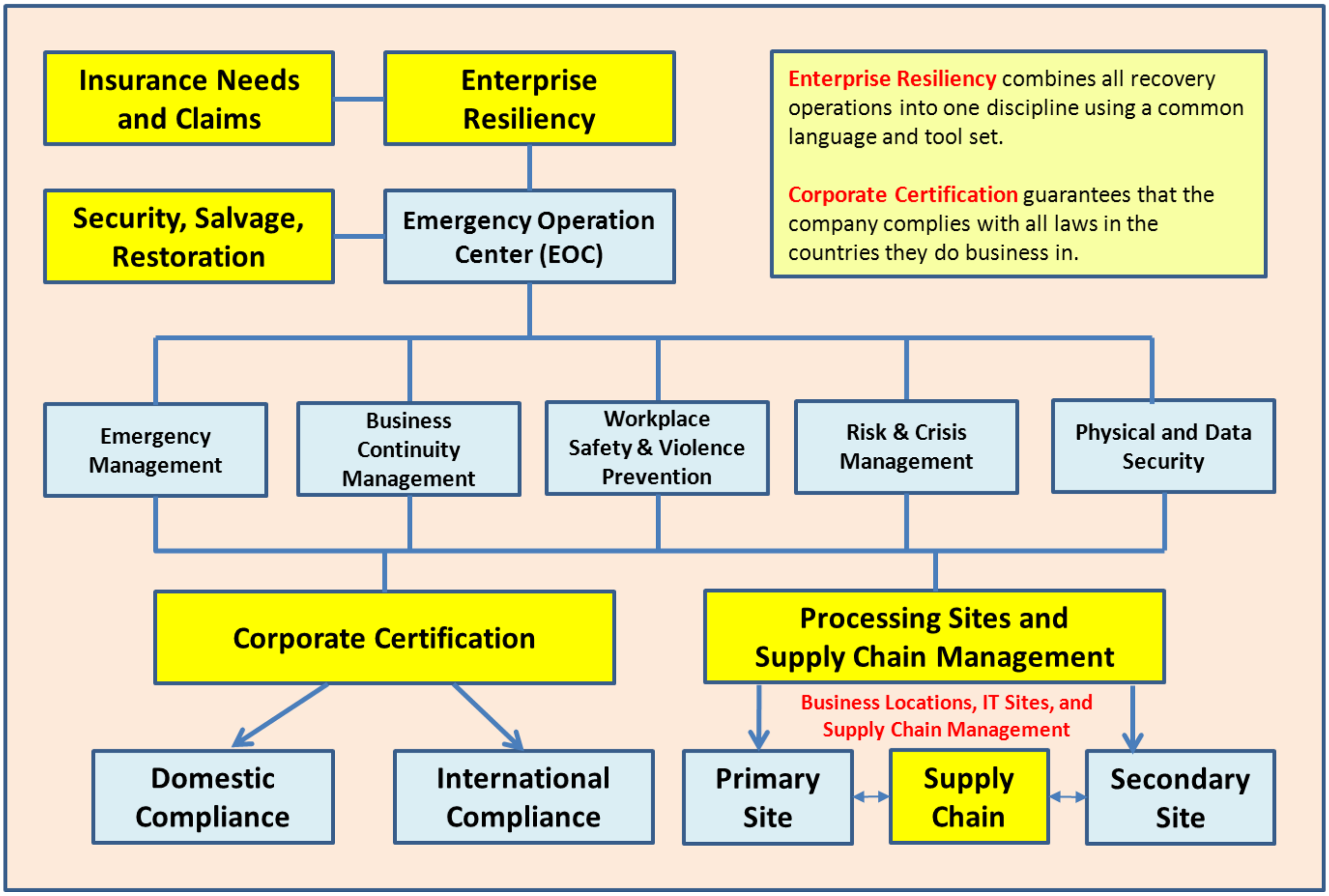
In today's business environment it is more important than ever to be able to; recover your business within Recovery Time Objectives (RTO) described in a client's Service Level Agreement (SLA), adhere to compliance laws, and meet the critical needs of your business and its clients. Additionally, protecting client information and adhering to security / regulatory requirements of the countries you do business in has become crucial.

A company can be sanctioned for failing to meet recovery and security objectives, but it could also suffer a loss of reputation that would harm them in the public's eyes and result in a loss of trust and business, sometimes so great that the company would never recover if a disaster event interrupts production processing.

To better protect an organization and adhere to compliance and recovery requirements, organizations are turning to **Enterprise Resilience** to combine all recovery operations and personnel within a single entity that speaks the same language and uses the same tool set, while **Corporate Certification** assures that the company adheres to the laws and regulations of all countries they do business in. Combining these two objectives will best protect the company and assure compliance. This document will help you achieve these goals.

An explanation of the components that make up Enterprise Resiliency and Corporate Certification is provided below.

Enterprise Resiliency and Corporate Certification



Insurance Needs and Claims
Enterprise Resiliency
Security, Salvage, Restoration
Emergency Operation Center (EOC)
Emergency Management
Business Continuity Management
Workplace Safety & Violence Prevention
Risk & Crisis Management
Physical and Data Security
Corporate Certification
Processing Sites and Supply Chain Management
Business Locations, IT Sites, and Supply Chain Management
Domestic Compliance
International Compliance
Primary Site
Supply Chain
Secondary Site

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

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

Emergency Operation Center (EOC) is the heart of recovery operations and is responsible for coordinating recovery operations and assisting executive management in continuing business operations from the primary or secondary site (either Information Technology or Business Unit Location). The EOC speaks with the Help Desk to determine that a problem has occurred that requires the activation of an emergency response plan. The response plan can be conducted by First Responders (Police, Fire, Government, Utility Supplier, Homeland Security, OEM, EMT, etc.), Business Recovery professionals (Business Unit recovery), Disaster Recovery professionals (Information Technology services and locations), or the activation of a Crisis Management Plan (Risk Managers, Auditing, Medical, etc.). Also, any workplace violence act (like and active shooter or disgruntled employee) must be addressed through the EOC. Because of the many recovery disciplines and their differing languages, it is important that EOC personnel know the language spoken by the disciplines and the procedures they normally follow. Additionally, EOC personnel must be aware of any compliance issues that may occur because responding to compliance violations can result in criminal, civil, and reputational loss and a proper response must be formulated and delivered as soon as possible to limit exposure and protect the company reputation. Because of these demands, Enterprise Resiliency and Corporate Certification were created.

Components included in **Enterprise Resiliency** are: Emergency Management; Business Recovery; Disaster Recovery; Risk & Crisis Management; and Physical and Data Security to produce a safe work space. Achieving this goal requires the use of a common language and set of tools for recovery management so that the recovery teams can better communicate, are more efficient, and can easily share knowledge and information.

Corporate Certification ensures compliance with domestic and international laws where the company does business. Implementation, testing, and periodic audits of compliance must be conducted with the resolution of any detected gaps and exceptions performed in a timely manner.

Insurance covering management and an interruption to business must be obtained so that outages can be resolved without interrupting the profit or any new line of business. It is important to have a public advocate assist you in reviewing your insurance needs and obtaining the appropriate level of insurance best suited to protecting your business. Public advocates will also assist you in time of disaster by formulating recovery strategies, hiring companies to provide recovery services, and submitting claims for work that had to be performed to resolve the disaster event.

Site Security, Salvage, and Restoration, must be achieved when a disaster event results in First Responders being called (i.e., Fire, Flood, Workplace Violence, etc.) and the loss of access to the site for a prolonged period of time due to police action, or damage due to resolution of a disaster event.

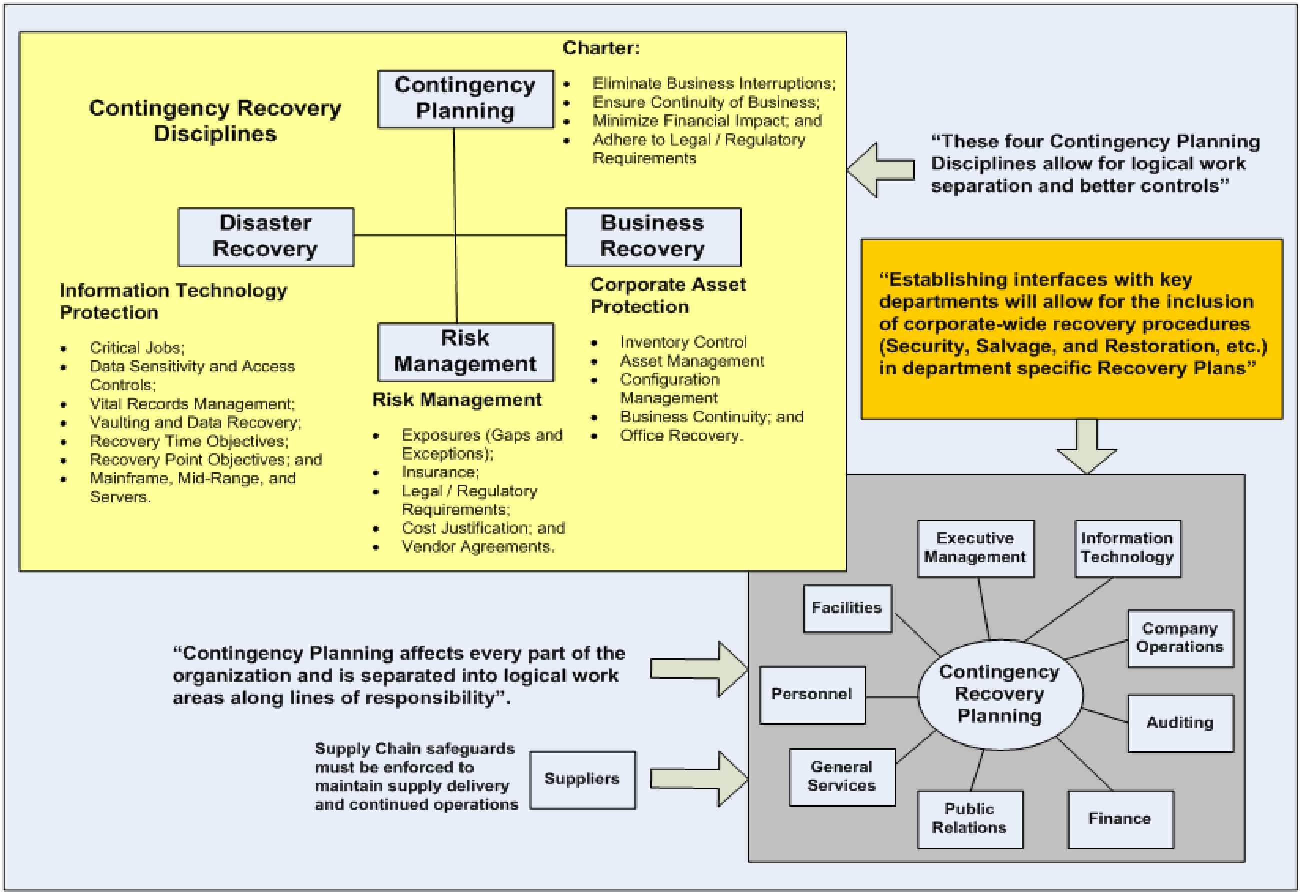
Primary and Secondary site application migration in support of recovery operations and the relocation of business locations to an alternate site are imperatives that must be included in Disaster and Business Recovery Plans. **Business Recovery** locations must have sufficient personnel, seats, equipment, and supplies to support business, while IT Recovery sites must have sufficient processing capacity and performance to support business operations. **Network Communications** must also be addressed to support primary and secondary sites.

Supply Chain Management must be assured in time of disaster, so it is imperative that providers adhere to national and international guidelines (ISO 27301) and laws regarding suppliers (ISO 24762) both domestically (SSAE 16, NIST 800-34) and internationally (SSAE 3402).

The disciplines included in Enterprise Resiliency and Corporate Certification are shown above, but how you get to that structure requires many people combining their knowledge of the business, its products and services, its clients, and the procedures needed to more efficiently support and maintain clients going forward.

Achieving Enterprise Resiliency and Corporate Certification requires the combined knowledge of the corporation and its participants (i.e., vendors, business associates, etc.), along with a strong knowledge of the laws and regulations that must be adhered to by the company in order to achieve compliance. An overview of Business Continuity requirements is shown in the following illustration.

How to integrate Business Continuity Management within the organization



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"

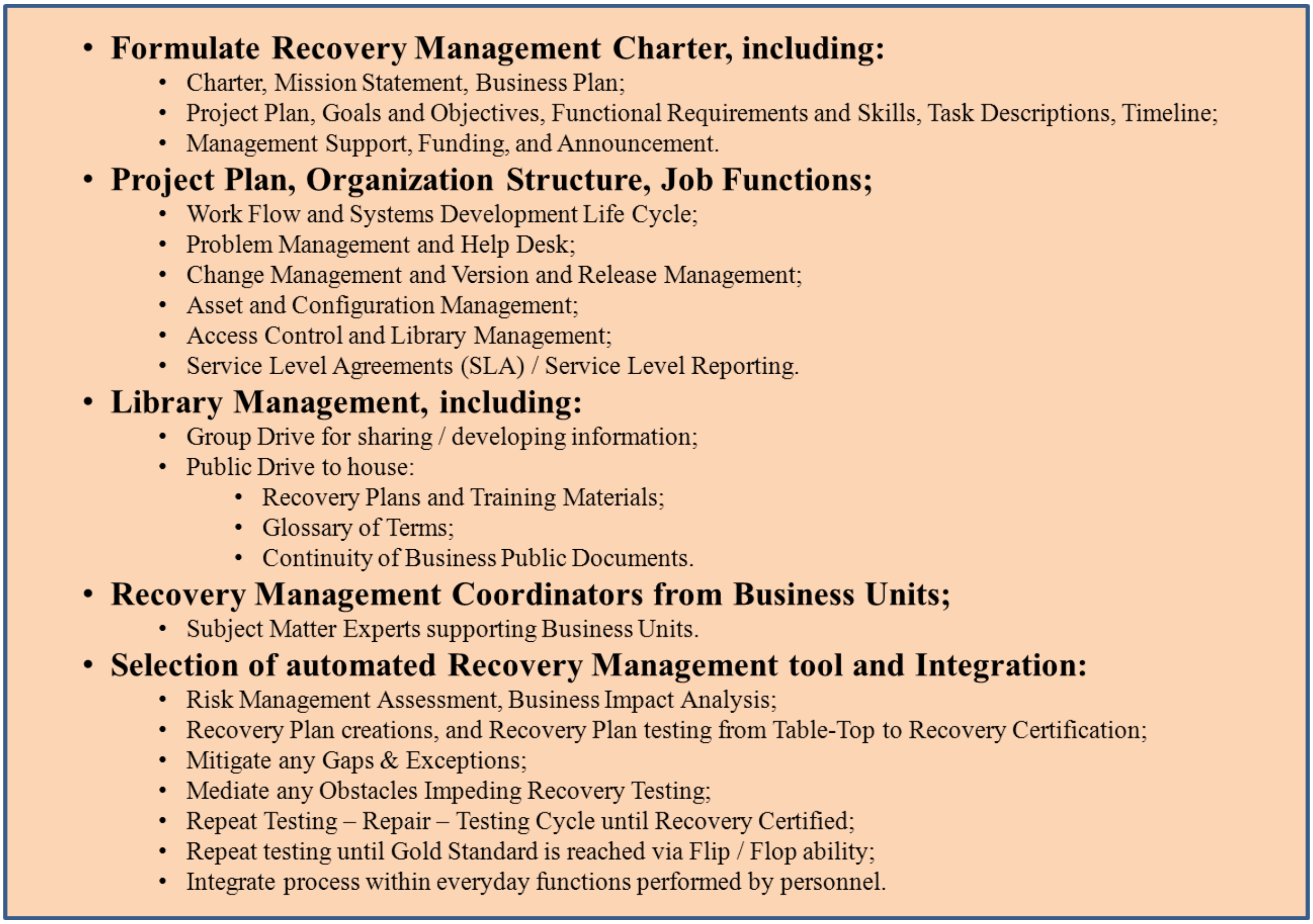
"Contingency Planning affects every part of the organization and is separated into logical work areas along lines of responsibility".

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

The picture shown above illustrates the many disciplines needed to contribute to achieving an environment that integrates Enterprise Resiliency and Corporate Certification within every day functions performed by personnel and included in their job descriptions and supportive documentation. The development process starts with a Charter and then goes on to discussions with the many business areas, including suppliers and vendors, who must understand corporate goals and how their participation can help achieve the objectives described in the Charter document.

From the combined knowledge of staff and participating people, the company will formulate a direction leading to compliance and improved recovery operations. That decision would be described within a Business Plan submitted to management in both written and presentation format. Its goal is to receive management approval, a budget to implement and maintain Enterprise Resiliency and Corporate Certification going forward, and the strong support of management to encourage participation in creating and maintaining these disciplines throughout the organization. The Business Plan will contain sections describing the Charter and Mission Statement, all goals and objectives, and a Project Plan leading to implementation of the process. These sections are described below.

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 everyday functions performed by personnel.

The above illustration demonstrates the direction to take in order to achieve the goals of Recovery Management and Enterprise Resiliency. Recovery Management is concerned with the restoration of business operations as shown in the Charter statement in the previous diagram, whereas Enterprise Resiliency combines the various recovery disciplines into a cohesive organization all speaking the same language and using the same tools.

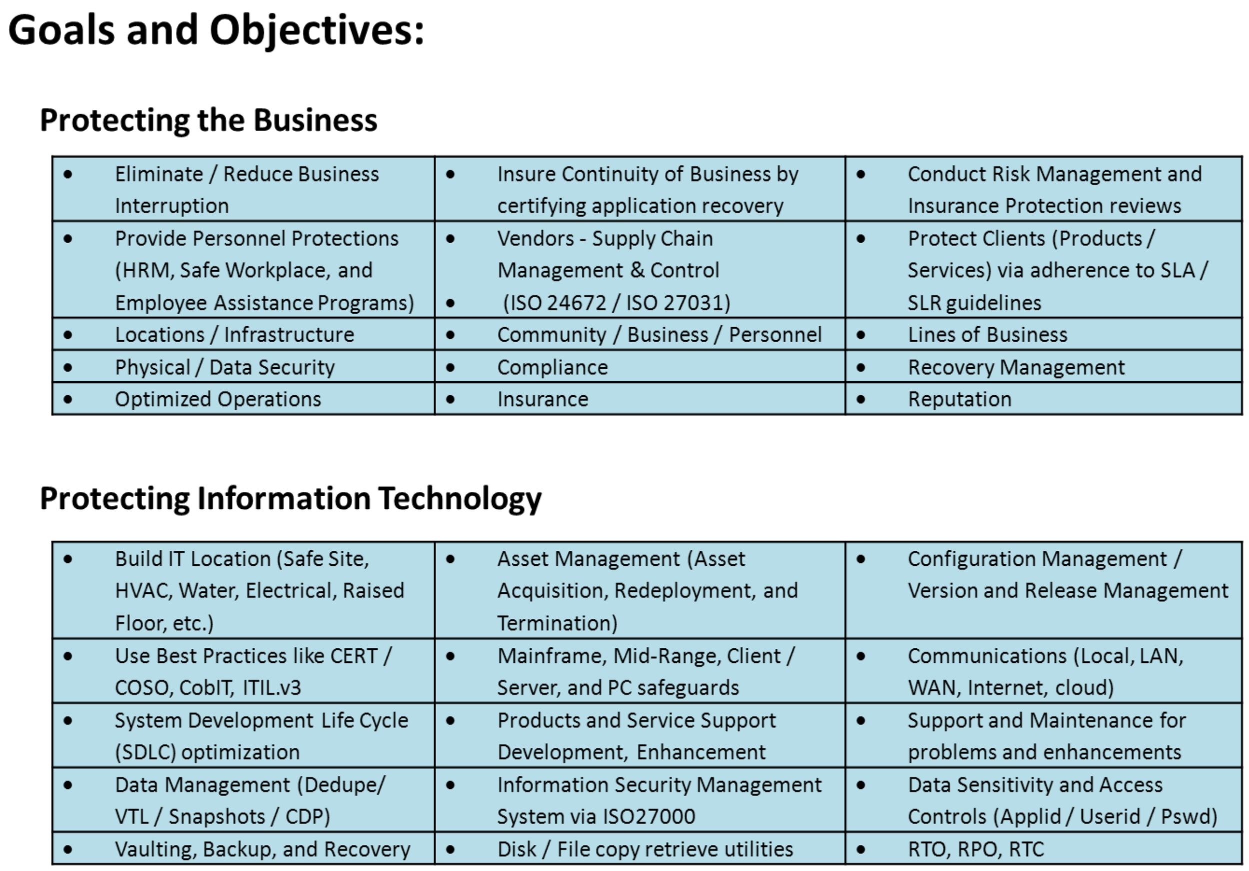
Enterprise Resiliency turns the present “Tower of Babel” of recovery management into a unit following the same cultural and using the same language. It helps a company best optimize the use of the recovery experts presently on staff and in the community (i.e., Government, Industry Organizations, etc.). Through implementation, documentation, training, and integration an optimized environment will be maintained.

Charter and Mission Statement

The Business Plan establishes a direction leading to the implementation of Enterprise Resiliency and Corporate Certification" that would improve efficiency and protection for clients and business operations (both domestically and internationally). It addresses:

- **Enterprise Resiliency** to combine recovery operations using a common set of tools and speaking a common language that fosters improved detection and recovery from disaster events and incidents;
- **Corporate Certification** to comply with regulatory requirements within the countries that the company does business;
- Adherence to **recovery times** demanded within a Service Level Agreement (**SLA**) and the Recovery Time Objectives (**RTO**) of applications and operations;
- Utilization of **data synchronization** in accordance to SLA / RTO requirements by utilizing the best Information Technology methods associated with Library Management, Data Sensitivity, Access Control, and Vital Records Management.
- Utilizing industry "**Best Practices**" to build and implement Enterprise Resiliency and Corporate Certification;
- Achieve "**Zero Downtime**" objectives through "**Certified Recovery**" for High Availability (HA) applications and achieving a "**Gold Standard Certification**" for Continuously Available (CA) applications. Failover / Failback capabilities allow applications to move from a primary site to a secondary site within SLA / RTO guidelines (usually from 2 – 72 hours), while Flip / Flop goals allow CA application to process in either the primary or secondary site at any time and have the capability to immediately flip operations between sites. Flip / Flop requires data to be in sync at both the primary and secondary sites, while Failover / Failback requires incremental synchronization of data between the primary and secondary site in accordance to SLA / RTO requirements.
- Incorporation of **problem / incident** recognition, circumvention, reporting, routing & escalation, resolution / recovery, tracking, reporting, post-mortem, and correction of any procedures that would improve operations and reduce outages.
- Incorporation of **recovery plans** for a full-range of problems that could impact production operations.
- Definition of updates / changes to personnel **functional responsibilities** and **job descriptions**.
- Fully **document** all standards and procedures and provide awareness and **training** sessions to staff and other participants.
- **Integrate** all new procedures and standards within the everyday functions performed by the staff and participants.
- Incorporate **support and maintenance** procedures going forward.
- Periodically **exercise recovery plans** to insure their accuracy, documenting the event and making any changes needed to improve recovery operations.

Objectives and Goals needed to protect the business and achieve compliance



Goals and Objectives:

Protecting the Business

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

Protecting Information Technology

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

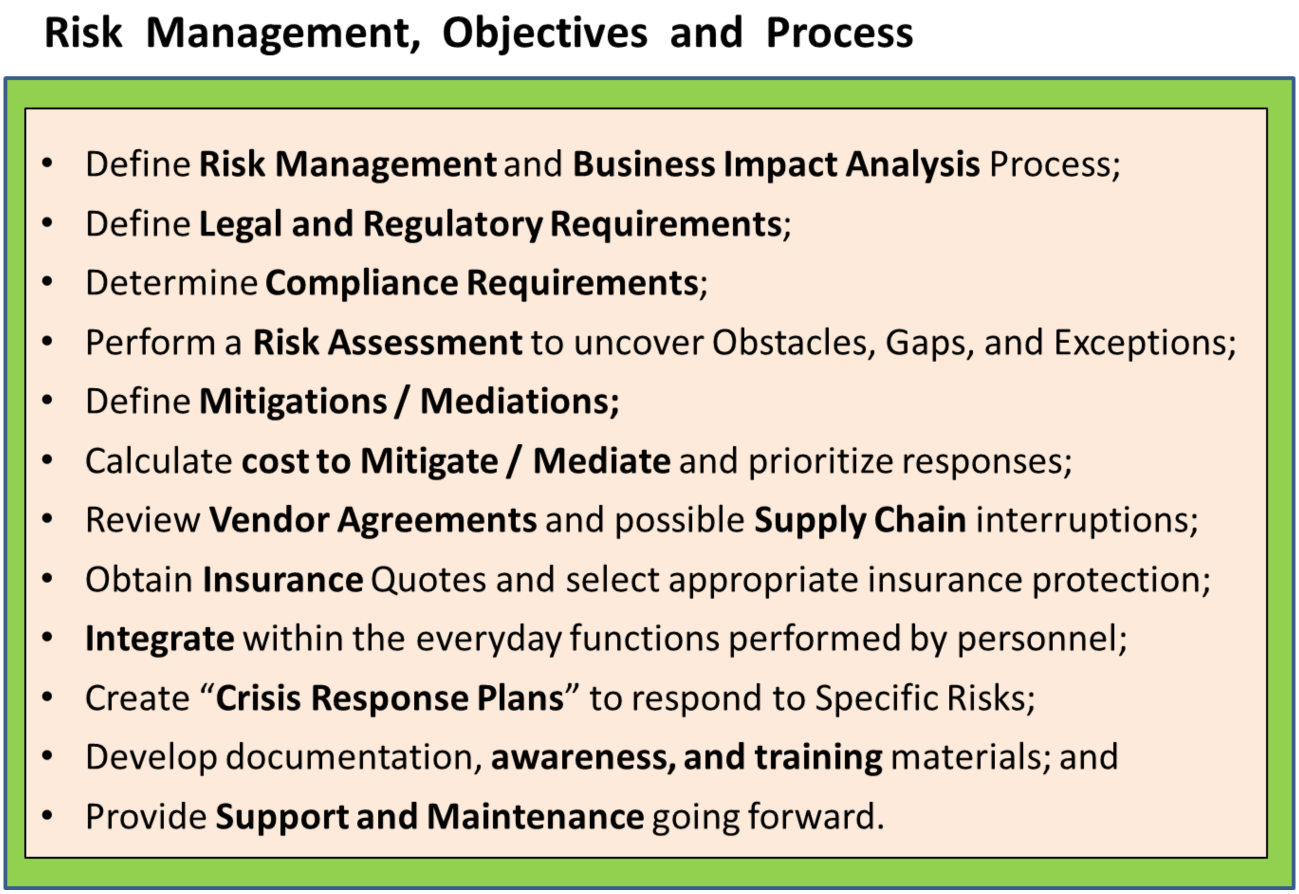
The Goals and Objectives included in the Business Plan are designed to develop and implement disciplines that would lead to better protecting the business through the use of Information Technology and Workflow process improvements.

The guidelines formulated through this process will require input from all recovery management disciplines so that the best results can be achieved through their combined knowledge and experience. **Emergency Management** personnel would help define methods for protecting the Workplace, **Disaster Recovery** personnel would help define methods for protecting Information Technology, and **Business Continuity** personnel would help establish methods for protecting, evacuating, and recovering business locations.

Risk Management would benefit through these new disciplines by being better able to identify audit requirements and the development of Crisis Management Plans to respond to risks and exposures. Risk Management will also obtain Insurance, negotiate Vendor contracts, and communicate with management.

Workplace Safety would be achieved through **Physical Security** guidelines (OSHA, DHS, OEM, NYPA 1600, etc.) and company information safeguards would be achieved through **Data Security** (ISO 27000). All clients would be better served and protected through improved data management, access controls, and vital records management related to backup and recovery operations.

Establishing the Risk Management Environment



Risk Management, Objectives and Process

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

Risk Management must be performed to define your compliance requirements and to detect any gaps and exposures you may have that interferes with achieving compliance. Also, any obstacles that may impede your ability to achieve compliance, or recovery, must be identified too. Refer to **COSO** and **CERT** guidelines for performing Risk Management to adhere to "Best Practices".

Once identified impediments and obstacles are rated as to their relative cost and likelihood of occurrence and reported to management, where a decision is made to either repair the problem or seek insurance to protect against the occurrence.

When compliance is required, the gaps and exceptions must be mitigated. If an obstacle impedes production or recovery operations then it must be repaired as well. Gaps and Exceptions are related to compliance regulation adherence, while Obstacles are mostly related to equipment, capacity, or performance restrictions. Obstacles occur mostly when production growth or new technologies are not factored into recovery operations at the secondary site. It is therefore imperative that change management include capacity and performance profiles and the use of new technologies so that appropriate precautions can be made to support recovery operations.

Similarly, whenever new laws and regulations are enacted, then existing Risk Management techniques must be adjusted accordingly. Finally, all documentation must be compatible with new and changed applications via Version and Release Management, awareness, and training to designated personnel.

Establishing the Recovery Management Process

At first, establishing the Enterprise Resiliency and Corporate Certification environment requires the formulation of a **Recovery Management Plan** used to outline how to protect Business Locations, Information Technology, and assist Risk Management in protecting the enterprise from intrusion, data loss, or corruption.

The Recovery Management process includes people who need to have their **functional responsibilities** and job descriptions modified / updated to meet their new responsibilities. Documentation used by affected people must be upgraded to reflect their new responsibilities and procedures used to achieve new standards, which is accompanied by awareness and training sessions.

Finally the new Enterprise Resiliency and Corporate Certification process is **integrated** into the everyday operations performed by the staff, including support and maintenance procedures going forward. This process includes:

- Formulate Recovery Management **Business Plan**;
- Create a **Project Plan** to achieve Recovery Management Goals;
- Define Recovery Management **organization structure** and **job functions**;
- Implement a **Recovery Management Library Management System** to contain recovery documents, training materials, and recovery plans;
- Develop a **common** Recovery Management Glossary of Terms to create a Common **Language** used by recovery personnel, thereby making it easier to understand threats and responses;
- Select / create an automated Recovery Management **Tool Set** that will be used by all recovery management personnel, so that problem relationships and trends can be best understood and corrective actions be pro-actively achieved;
- Identify Recovery Management **Stakeholders and Participants** from all areas of the company;
- Formulate **Recovery Teams** and a Chain of Command for identifying events and reporting them to the appropriate person;
- Establish **Command Center Procedures** for all types of problems and have them interface with the Help Desk and Emergency Operations Center when critical issues arise;
- Have the **Help Desk** respond to problems and escalate disaster events to a point where they select a recovery plan and contact the Contingency Command Center for them to validate the event and initiate recovery procedures;
- Have the **Contingency Command Center** coordinate recovery activities with responders and the Emergency Operations Center;
- Initiate **Security, Salvage, and Restoration** procedures to insure rapid recovery of the failing site. It would be wise to establish this relationship early on so this company can assist in the planning and implementation process;
- Have the **Emergency Operations Center** formulate emergency teams to man the EOC and have them monitor recovery actions, while EOC management coordinates with Executive Management on progress and/or set-backs;
- Have **Executive Management** coordinate communications to clients and the outside world regarding the response to emergency events and the progress being made to restore business operations;
- Process production at the **Secondary Site** during the disaster event; and,
- **Return to the failing site** after the disaster event has been resolved and the primary site has been made ready to receive returning personal.

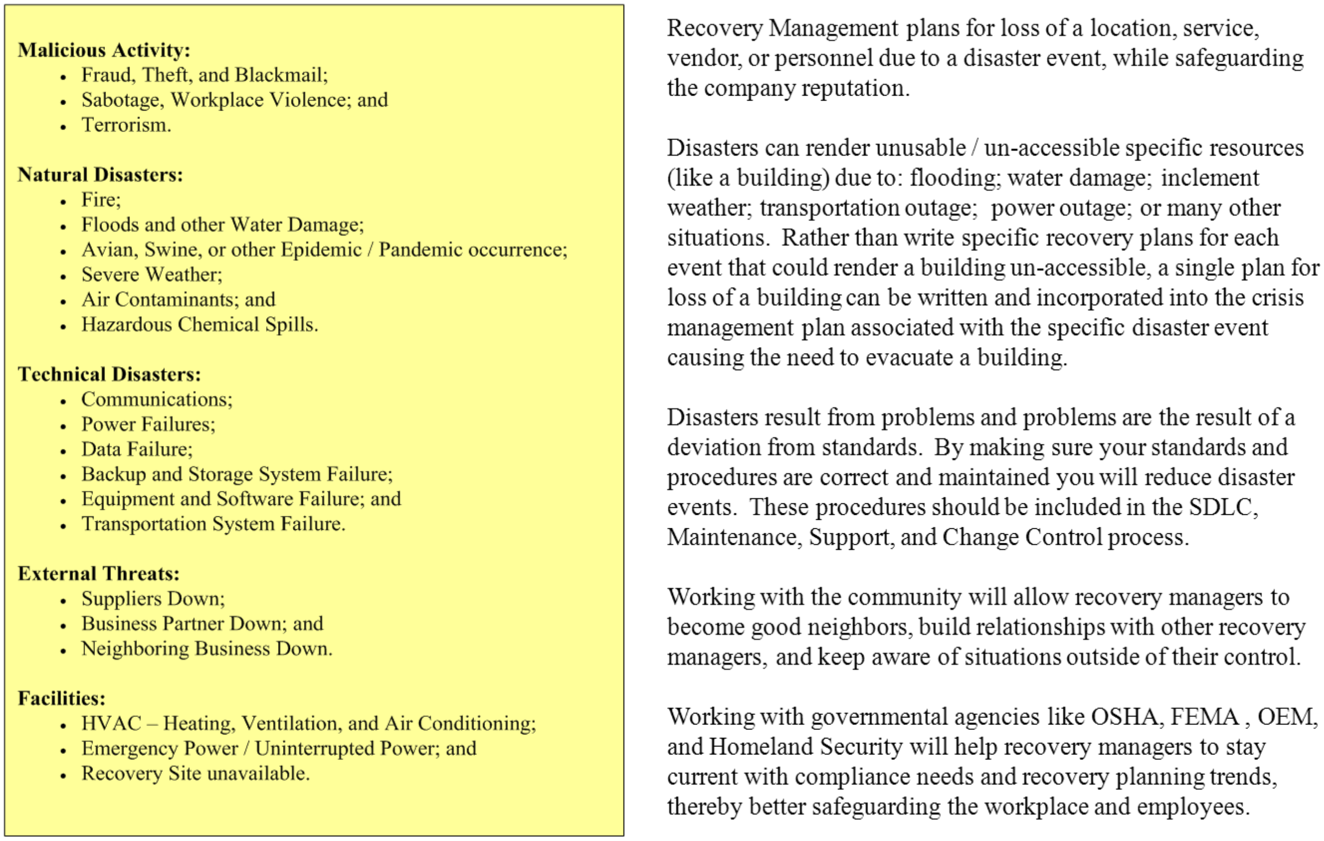
Pathway to achieving Enterprise Resiliency and Corporate Certification

In order to achieve Enterprise Resiliency and Corporate Certification it is necessary to perform the following tasks, including:

- Identify the **Enterprise Resiliency** goals and objectives that management wants achieved;
- Define Domestic and International **Compliance** requirements;
- Review all existing **Security and Recovery** operations;
- Perform a **Risk Assessment** to define existing gaps, exceptions, and obstacles that would interfere with recovery operations associated with Zero Downtime, High Availability, and Continuous Availability as defined by management and contained in Service Level Agreements (SLA);
- Define Lines of Business and their recovery requirements by performing a **Business Impact Analysis** (BIA);
- Review **SLA and RTO** recovery time objectives that must be adhered to and establish Data Management Standards associated with Data Sensitivity, Access Controls, and Vital Records Management;
- Review all **mandated** industry and application recovery time requirements;
- Examine **present capability** to recovery operations within required time limits;
- **Evaluate Command Center** operations and how they respond to encountered problems / incidents to insure that they identify and respond to emergency events appropriately;
- Ensure that the **Help Desk** is provided with a Recovery Plan Library that they can utilize to identify emergency events and follow procedures used to initiate recovery operations;
- Connect Help Desk Operations with the **Contingency Command Center** to initiate recovery operations;
- Determine how best **to integrate** recovery and security operations within the everyday functions performed by the staff and participants;
- Select **automated Recovery Management Tool** to create, test, and implement Recovery Plans;
- Define standards and **documentation** requirements and produce materials;
- Create an **Awareness and Training** program for staff and participants;
- **Implement Security** (Physical and Data) procedures and test their effectiveness;
- Develop **Recovery Plans** and test their ability to achieve recovery guidelines;
- Create an Enterprise Resiliency and Corporate Certification "**Proof of Concept**" process and obtain management approval to go forward;
- **Implement and Roll-Out** Enterprise Resiliency and Corporate Certification;
- Create / update all job **functional responsibilities and job descriptions,** as needed;
- Publish updated **Standards and Procedures** and other necessary supportive documentation materials;
- Initiate **Training and Awareness** programs for existing and new staff and participants;
- Establish **Support and Maintenance** procedures going forward; and,
- **Continuously test** and upgrade recovery and security operations, as needed.

Following this process will help establish the Enterprise Resiliency and Corporate Certification and maintain it going forward, thereby insuring your company's ability to respond to disaster and security events both domestically and internationally. It will eliminate / reduce disaster events, safeguard the company reputation, improve workflow and operations, lead to better retention and attraction of staff and clients, and thereby improving business profitability and the company's reputation.

Potential threats and their impact on the business



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, while safeguarding the company reputation.

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, Support, 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 OSHA, FEMA , OEM, and Homeland Security will help recovery managers to stay current with compliance needs and recovery planning trends, thereby better safeguarding the workplace and employees.

The goal of Recovery Planning within a company is to be aware of the potential events that could lead to a disaster, ranging from Malicious Activities, Natural Events and Disasters, Technical Disasters, External Threats, and Facility Failures.

The range of potential disaster events has resulted in a number of different recovery disciplines from First Responders and Emergency Management (Fire, Police, EMT, Government, Utilities, etc.) through Risk / Crisis Management (specific events like Pandemics or Hazardous Materials, etc.), Audit Gaps / Exceptions / Obstacles impeding production or recover operations (usually related to Information Technology or Disaster Recovery), and Business Recover responsible for business location operations and recoveries.

The range of Potential Threats must be factored into the planning and testing process associated with Recovery Management and Enterprise Resiliency to best safeguard the business through normal production and recovery operations.

Adhering to Compliance Laws and Regulations

Some of the Laws and Regulations that must be adhered to include:

1. **Gramm Leach Bliley (GLB)** – Safeguard Act (was Bank Holding Act);
2. **Basel III** – for banks and financial institutions;
3. **Dodd-Frank** – Wall Street Reform and Consumer Protection Act;
4. **HIPAA** – Healthcare regulations including HITECH, ePHI, Final Ombudsman Rule, and Patient Protection and Affordable Care Act (Obama Care);
5. **Sarbanes – Oxley Act (SOX)** – on financial assessment and reporting by authorized signing office;
6. **EPA Superfund** – governing land fill, pollutants, and asset disposal;
7. **Supply Chain Management** – to safeguard supply delivery to both primary and secondary sites including ISO 24762 (SSAE 16 for domestic suppliers and SSAE 3402 for international suppliers) and ISO 27301;
8. **Patriots Act** – Includes Know your Customer, and Money Laundering investigations to detect terrorist and illegal activities;
9. **Workplace Safety and Violence Prevention** – includes OSHA, DHS, OEM, and Governmental Regulations designed to insure the protection of people within the working environment;
10. **Office of the Comptroller of the Currency** (OCC), including Foreign Corrupt Practices Act, OCC-177 requiring a Recovery Plan, OCC-187 identifying Financial Records, OCC-229 governing Access Controls, and OCC-226 covering end user computing compliance.

Periodic audits of the business must be performed to insure compliance and to generate a "**Letter of Attestation**" by executive management and the CEO stating successful compliance. If Gaps, Exceptions, and Obstacles are found that interfere with compliance, then they must be identified and plans to mitigate / mediate them documented and submitted to auditors and regulators.

Gaps, Exceptions, and Obstacles reported to auditors and regulators must be review to determine the best response to correct the problem. They must be assigned to a resolver who is identified and a due date must accompany the responsibility. A follow-on audit will examine past problems to insure that they have been resolved, if not a further audit exception will be triggered which could be worse than the initial problem. Sanctions and fines are usually associated with Gaps and Exceptions that have not been repaired as promised. These penalties can have a high price tag through; criminal, civil, monetary fines, and restrictions placed on the business. The damage to a corporation's reputation through these penalties and restriction could be uncorrectable and result in a loss of revenue that may cause clients to stay away and the business to close.

It is therefore crucial to maintain adherence to laws and regulations in the countries that your company does business. It is just as critical to be able to recover your business if a disaster event occurs because clients will leave if you cannot meet the service delivery goals outlines in the Service Level Agreement. In some cases, non-conformance to SLA requirements will trigger costly fines to cover the client's loss of business and damage to the client's reputation. These costs can be extreme in some cases.

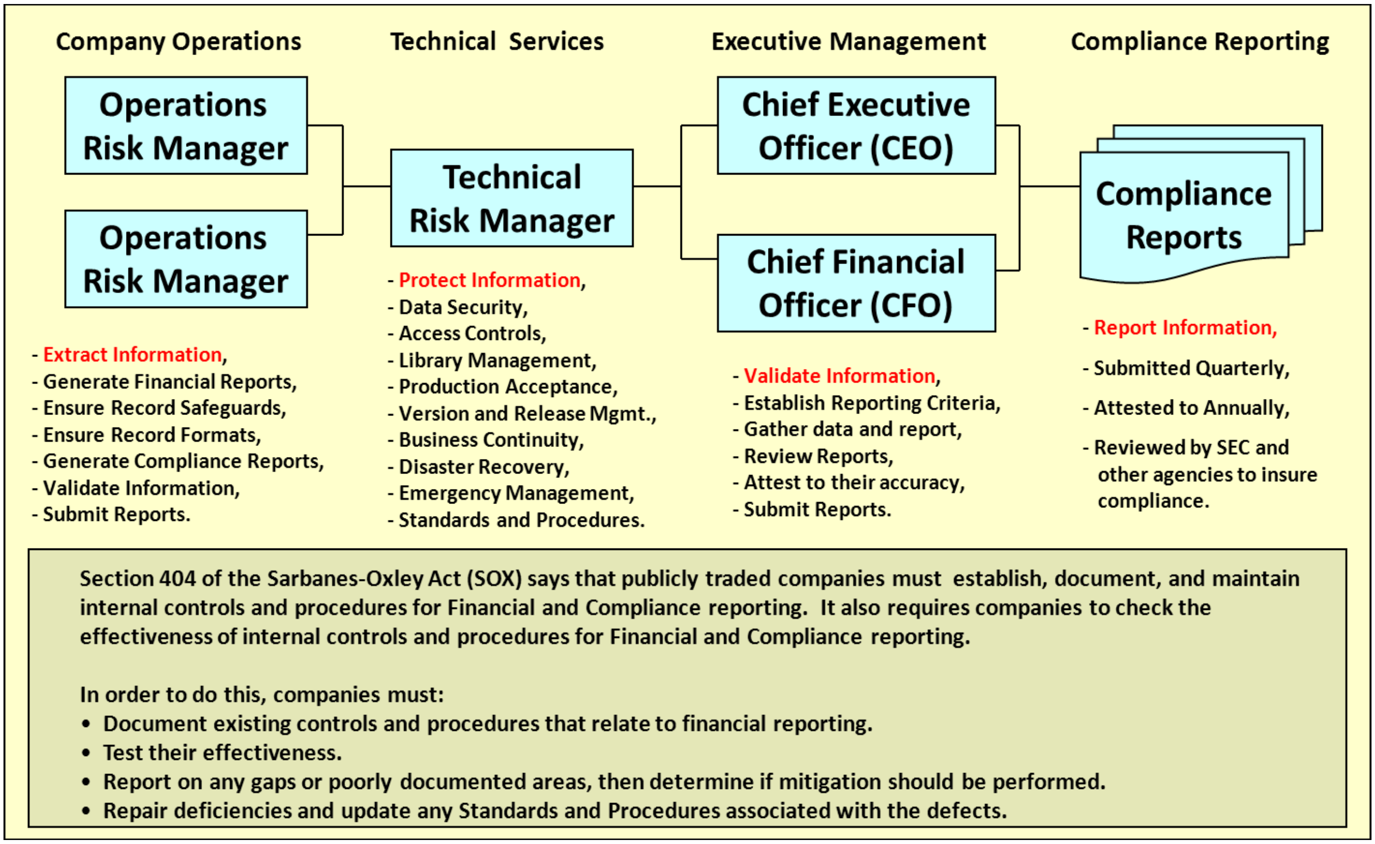
Strategies for eliminating Audit Exceptions, Gaps, and Obstacles

- **Review** Business and Industry Compliance Requirements, both domestically and internationally;
- **Ensure** Data Sensitivity, IT Security, and Vital Records Management;
- **Eliminate** Data Corruption, Certify High Availability (HA) applications, Continuous Availability (CA) applications in order to achieve the Zero Downtime goal;
- **Upgrade** the Systems Development Life Cycle (SDLC) to insure compliance is maintained;
- **Utilize** automated tools whenever practical to improve efficiency and workflow;
- **Eliminate** Single Point of Failure throughout the IT Environment;
- **Create** Asset Management / Configuration Management / Inventory Management procedures;
- **Develop** Problem / Incident reporting and Crisis Management;
- **Achieve** Enterprise Resiliency;
- **Implement** Corporate Certification;
- **Fully Document** the environment, procedures, and supportive materials;
- **Integrate** within the everyday functions performed by personnel through job descriptions;
- **Provide** awareness and Training to staff and outside participants;
- **Conduct** periodic testing and repeated audits to insure compliance is maintained; and,
- **Perform** Post Mortems to isolate problems and make corrections as needed.

The next two illustrations will further explain how to verify compliance to regulatory requirements and recovery time frames.

Compliance Reporting Technique

Compliance reporting is achieved by gathering information from Business Units by their Operations Risk Managers, who then pass the information to the corporate Compliance Technical Risk Manager who validates the information and formulates a report to management where the Signing Officer reviews the report and signs a "Letter of Attestation" statement that is submitted to the regulatory organization.



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

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

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

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

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

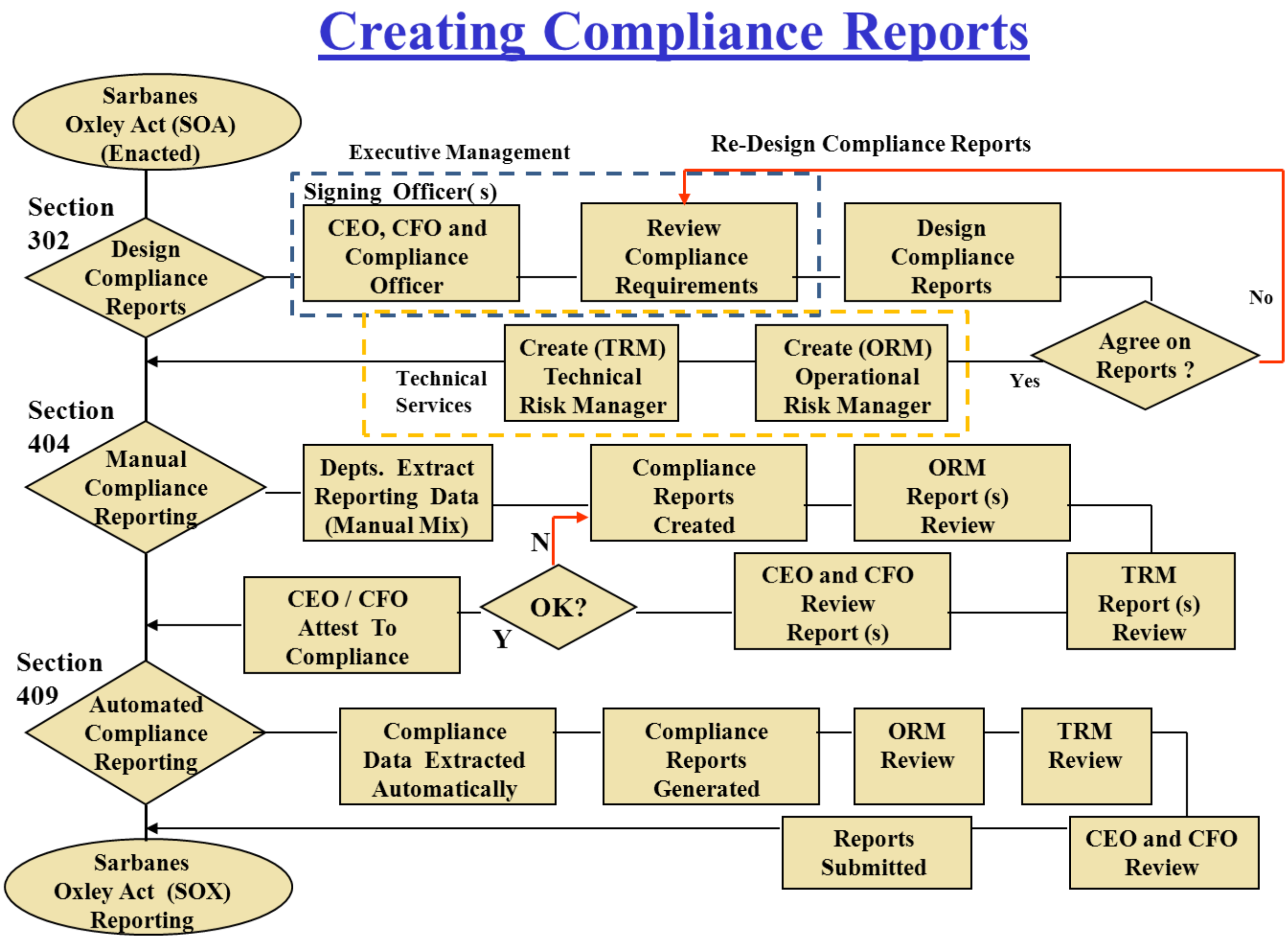
In order to do this, companies must:

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

Capturing and gathering compliance information is a corporate endeavor whose pathway is shown above. It starts with the Business Units Operations Risk Manager, who provides the Technical Risk Manager with their reports. The Technical Risk Manager validates reported information and compiles a Compliance Report to Executive Management, who reviews the information and generates a "***Letter of Attestation"*** for delivery to regulators along with any required Compliance Reports. This activity is performed on a periodic basis.

The method shown above is use to support and validate many types of compliance and recovery operations with only slight alterations related to each type of operation being reviewed.

Creating Compliance Reports and a Letter of Attestation

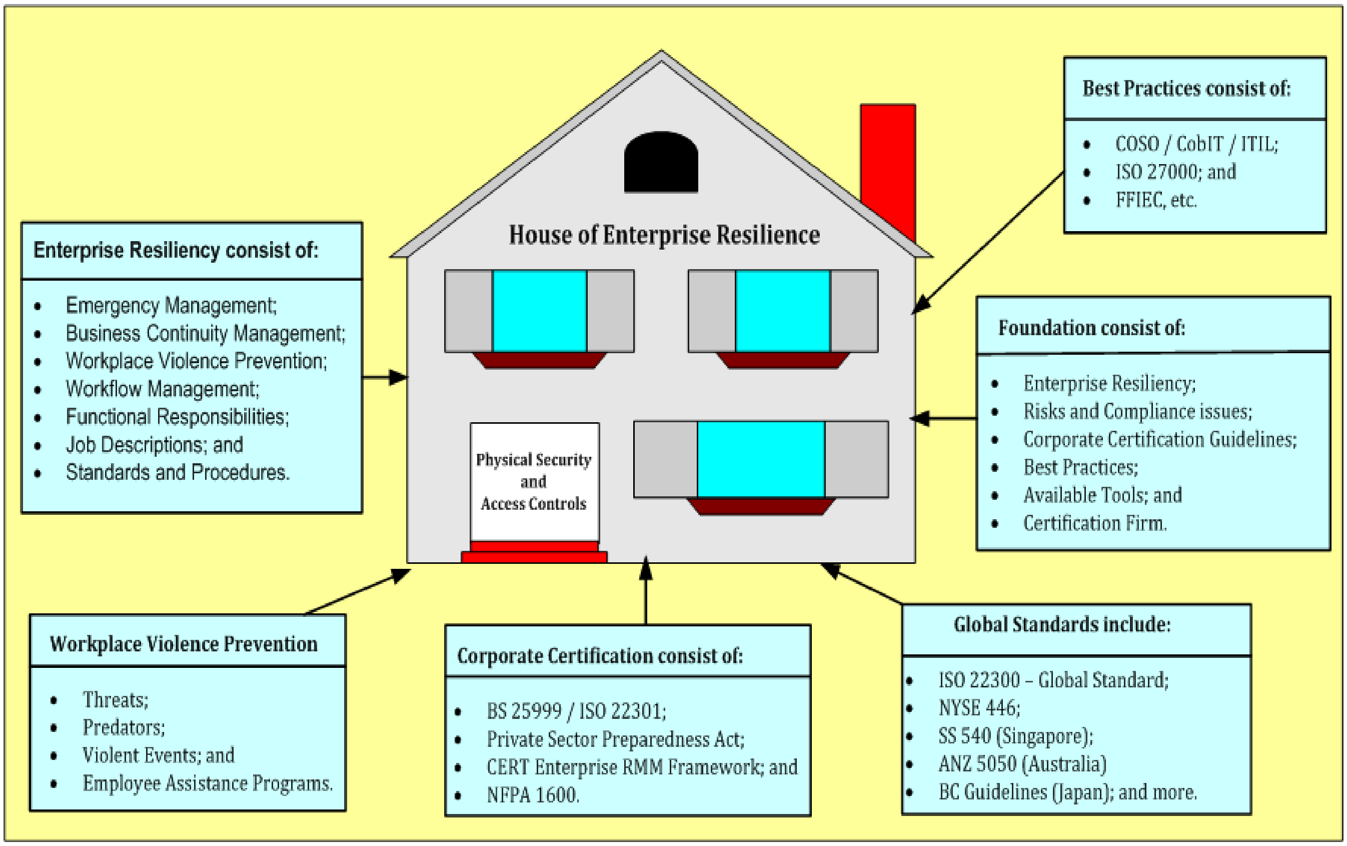

Creating Compliance Reports
Sarbanes Oxley Act (SOA) (Enacted)
Section 302
Design Compliance Reports
Executive Management
Signing Officer(s)
CEO, CFO and Compliance Officer
Review Compliance Requirements
Re-Design Compliance Reports
Design Compliance Reports
No
Agree on Reports ?
Yes
Technical Services
Create (TRM) Technical Risk Manager
Create (ORM) Operational Risk Manager
Section 404
Manual Compliance Reporting
Depts. Extract Reporting Data (Manual Mix)
Compliance Reports Created
ORM Report (s) Review
N
OK?
Y
CEO / CFO Attest To Compliance
CEO and CFO Review Report (s)
TRM Report (s) Review
Section 409
Automated Compliance Reporting
Compliance Data Extracted Automatically
Compliance Reports Generated
ORM Review
TRM Review
Reports Submitted
CEO and CFO Review
Sarbanes Oxley Act (SOX) Reporting

The above illustration is how Compliance Reporting is performed within a business organization with the Sarbanes Oxley (SOX) act being used as an example. The Sox Act was created after the financial crisis to ensure that financial organizations maintain current accounting methods that can be reviewed on a periodic basis by regulators. There are three phases to the SOX Act from originating reporting and content (section302) to gathering financial information into a concise report that is safeguarded and accurate (section 404) to where an automated financial system is implemented that constantly monitors and reports on the financial status of the company (section 409).

Information is gathered and reported on as shown in the last two illustrations, then reviewed and approved. When approved, a “Letter of Attestation” is submitted by management to the regulators.

This methodology is used to report on most compliance issues and is also used to validate recovery operations where a “Letter of Attestation: is generated to certify recovery for HA and CA applications in accordance with compliance and recovery time frames.

Enterprise Resiliency and Corporate Certification must be built on 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.

The Enterprise Resiliency and Corporate Certification process must be built on a solid structure. Like a house needs a solid foundation to build its structure on, Enterprise Resiliency and Corporate Certification must utilize industry Best Practices in order to successfully achieve its goals, while insuring management that their direction has been validated by appropriate experts and proven industry operational improvements.

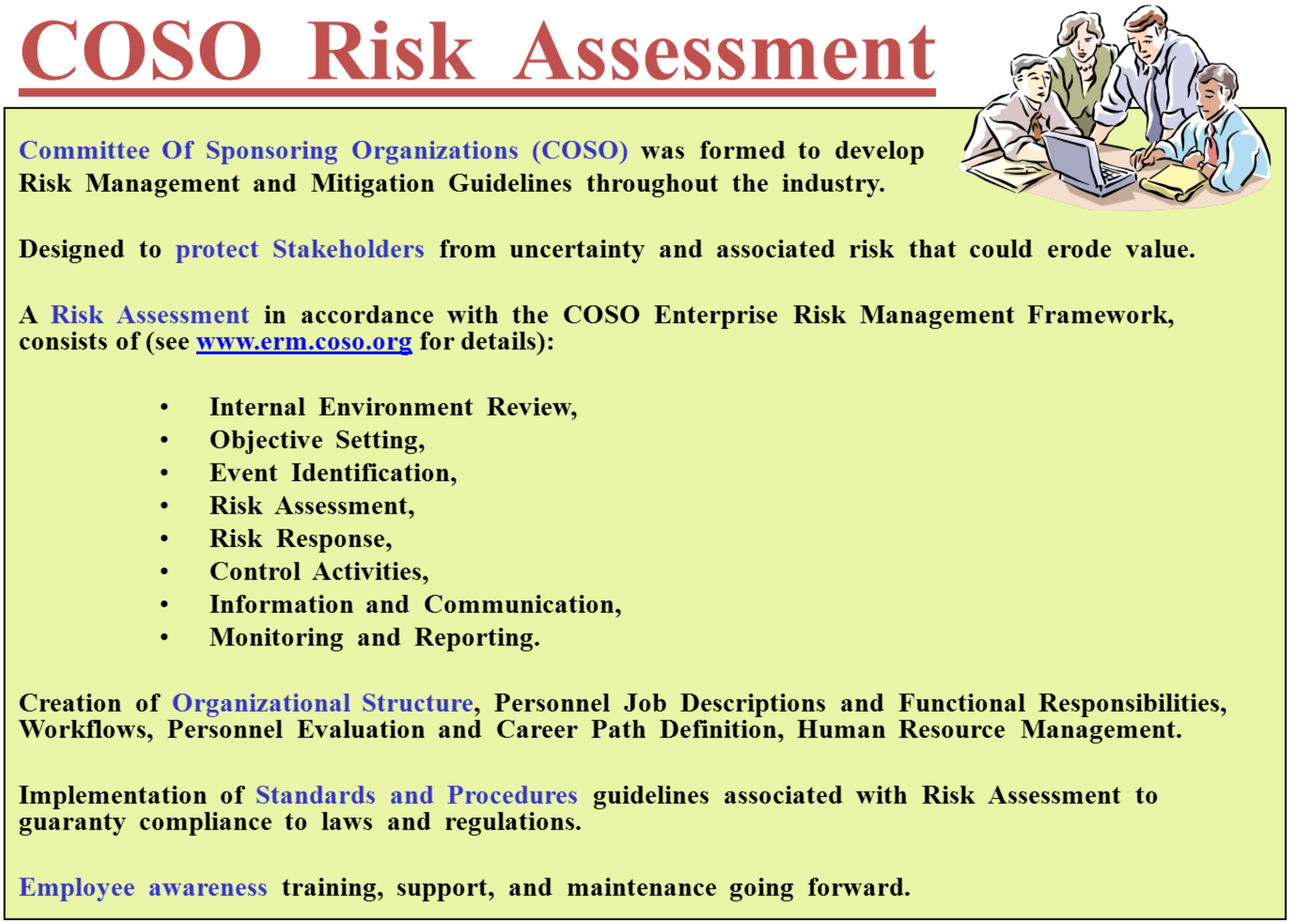
The picture above shows that the house and its structure is built on the Best Practices of **COSO / CERT** Risk Management guidelines, **CobIT** Business Integration guidelines, ITIL Workflow Management, ISO 2700 Information Security Management System guidelines, and the latest Recovery Management guidelines (industry and goal dependent) used to achieve Zero Downtime (Recovery Certification and Global Recovery Certification Standards) and the disaster and recovery objectives used to protect business locations and Information Technology services.

Like all houses, access is governed by Physical and Data Security guidelines, while interactions of people within the house are governed by domestic and international access control guidelines.

The immediate goal of achieving Enterprise Resiliency and Corporate Certification is to protect the company and its reputation from: threats; predators; violent events; and unauthorized access to physical environments or sensitive information. Building this "***Dome of Protection***" over the company will keep business operations safe from interruptions caused by outside disturbances, while improving the efficiency of the staff and supporting participants (i.e., sub-contractors and business associates).

The long term goal of Enterprise Resiliency and Corporate Certification is to better prepare the company for the way business will be conducted in the future. New laws and technologies will be easier to integrate, the efficiency of the staff and operations workflow will improve, a greater degree of physical and data secured achieved, and the reputation of the corporation will be held in the highest esteem – thereby helping to support and generate business.

COSO Risk Assessment Guidelines



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.

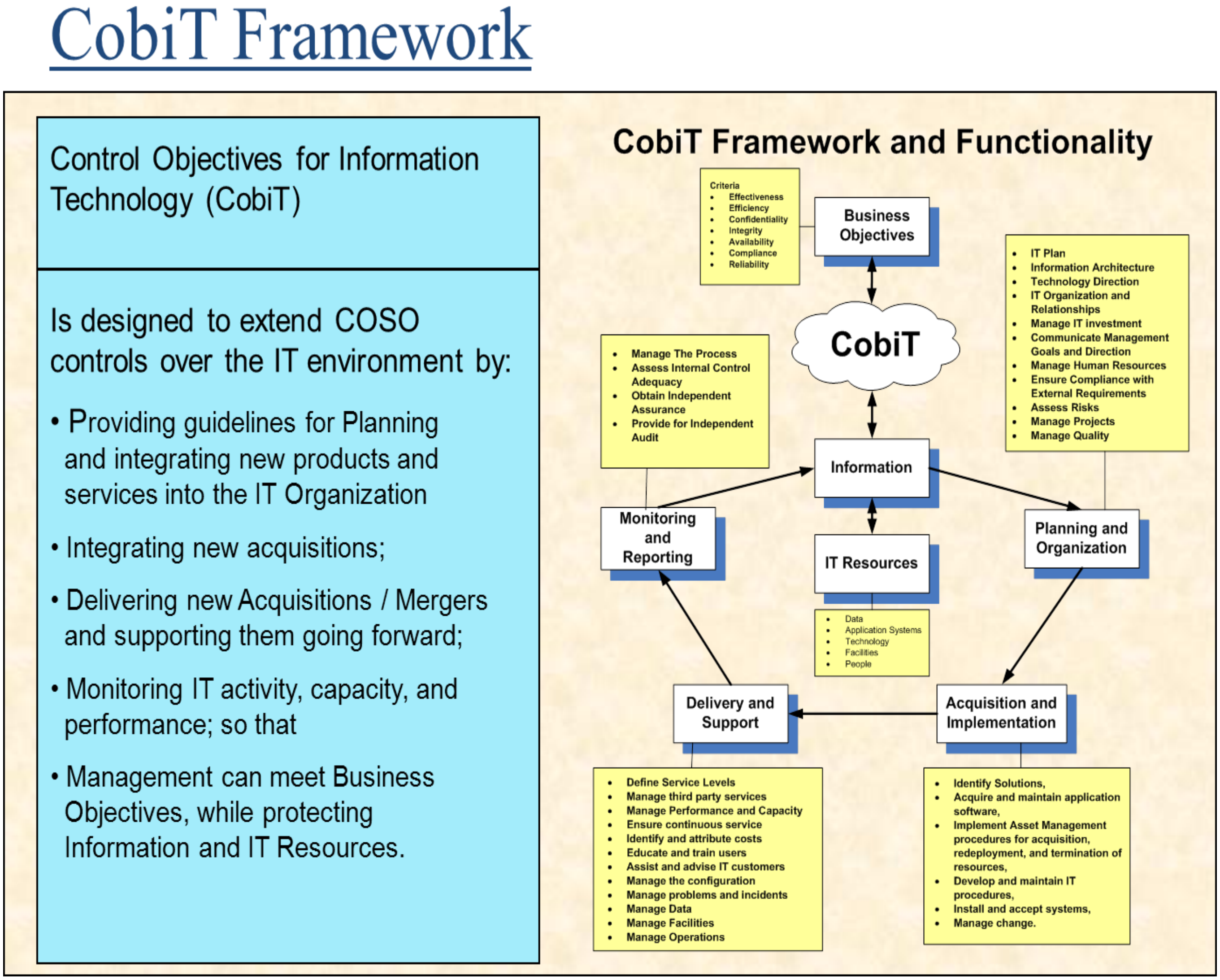
Implementation of Standards and Procedures guidelines associated with Risk Assessment to guaranty compliance to laws and regulations.

Employee awareness training, support, and maintenance going forward.

Starting with a Risk Assessment of your company will assist in defining the requirements associated with Enterprise Resiliency and Corporate Certification. The above illustration above shows the Risk Management Guidelines developed by COS and are considered industry “Best Practices”. CERT also has Risk Management Guidelines that are considered industry “Best Practices” and are very similar to COSO.

CobIT Framework review

After performing a COSO and/or CERT related Risk Analysis of the environment, you will next have to determine how best to implement business priorities in the Information Technology environment. CobIT was developed by industry experts to assist in determining how to migrate products and services to production and is considered industry "Best Practices". A review of CobIT is provided in the illustration below.



CobiT Framework

Control Objectives for Information Technology (CobiT)

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

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

CobiT Framework and Functionality

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

Business Objectives

CobiT

Information

IT Resources

- Data
- Application Systems
- Technology
- Facilities
- People

Monitoring and Reporting

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

Planning and Organization

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

Delivery and Support

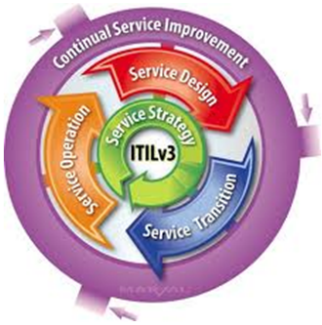
- Define Service Levels
- Manage third party services
- Manage Performance and Capacity
- Ensure continuous service
- Identify and attribute costs
- Educate and train users
- Assist and advise IT customers
- Manage the configuration
- Manage problems and incidents
- Manage Data
- Manage Facilities
-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

Acquisition and Implementation

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

CobIT helps company's migrate business products and services to the Information Technology environment. It includes: Planning and Organization; Acquisition and Implementation; Delivery and Support; Maintenance, and finally Monitoring and Reporting. All of these topics are included in this paper.

Information Technology Infrastructure Library (ITIL) structure.



Information
Technology
Infrastructure
Library (**ITIL**)

ITIL Five Phase approach to IT Service Support

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

ITIL Available Modules

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

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

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

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

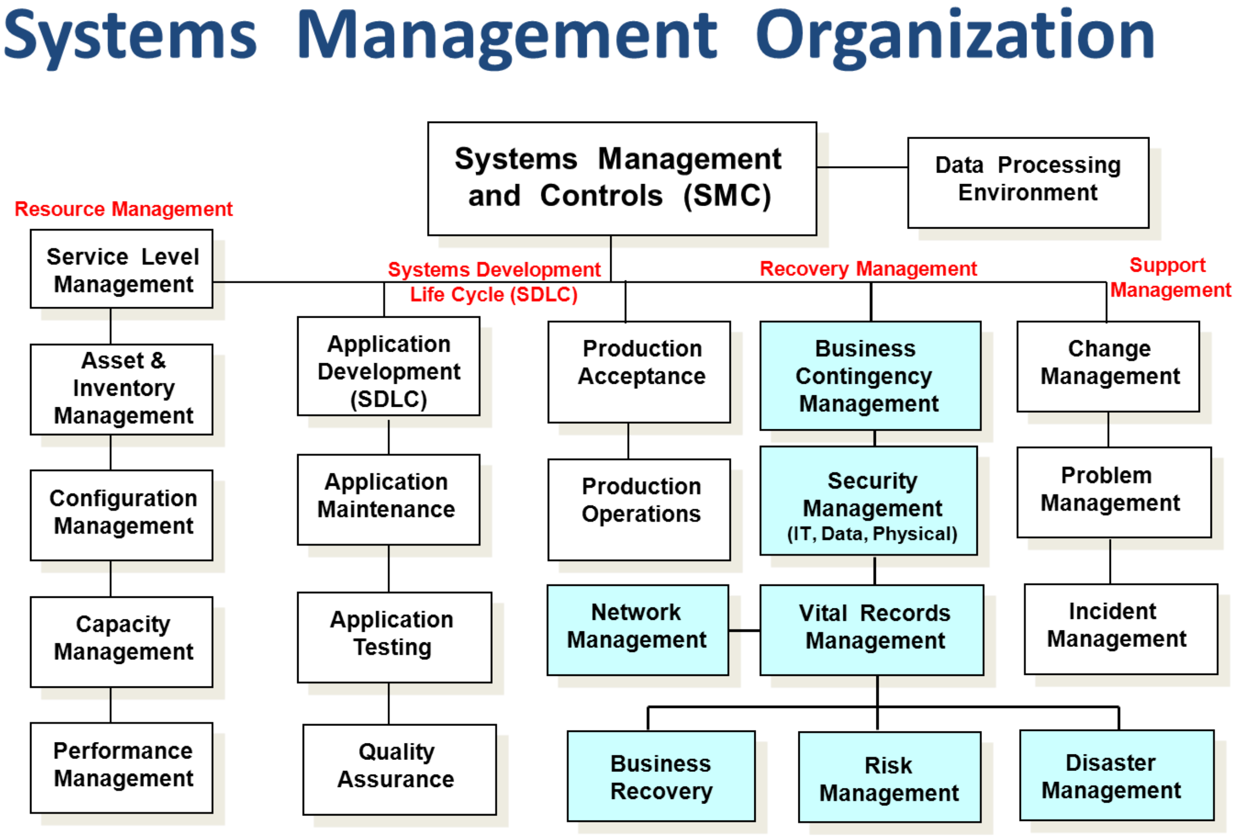
ITIL provides Forms Management and Control functions and is used to maintain libraries and support service delivery and maintenance. Information contained in ITIL Libraries can be used to satisfy a wide range of functional responsibilities from documentation, to performance, to auditing, and compliance. It is am excellent tool and highly recommended.

Combining the Risk Assessment of COSO with the implementation techniques of CobIT will help you successfully implement business products and services within the production environment. After that is accomplished, you will need to monitor and respond to problems, while supporting workflow and personnel needs via ITIL.

The three disciplines of COSO, CobIT, and ITIL are considered industry “Best Practices” and will lead to a safeguarded and efficient business environment, with happy personnel and a positive reputation.

The Systems Management Organizational Structure (SMC)

- **Resource Management** (Asset, Inventory, Configuration Management);
- **Capacity and Performance Management** to monitor present environment and respond to growth needs or the introduction of new technology;
- **Systems Development Life Cycle** (Development, Maintenance, Testing, QA, Production Acceptance, Production Operations);
- **Recovery Operations** (Information Technology / Data / Physical Security, Vital Records Management, On-Site and Off-Site Vaulting, Back-Up and Recovery Operations, and the relocation of operations to a secondary site for both IT functions and Business locations);
- **Data Management** for real-time and incremental data synchronization between primary and secondary sites;
- **Network Management** to ensure that required bandwidth is available to support production and recovery operations;
- **Support and Maintenance** (for problem repair and Enhancement Implementation);
- **Change Management** and **Version and Release Management**; and,
- **Documentation, Supportive Literature, Awareness, and Training.**

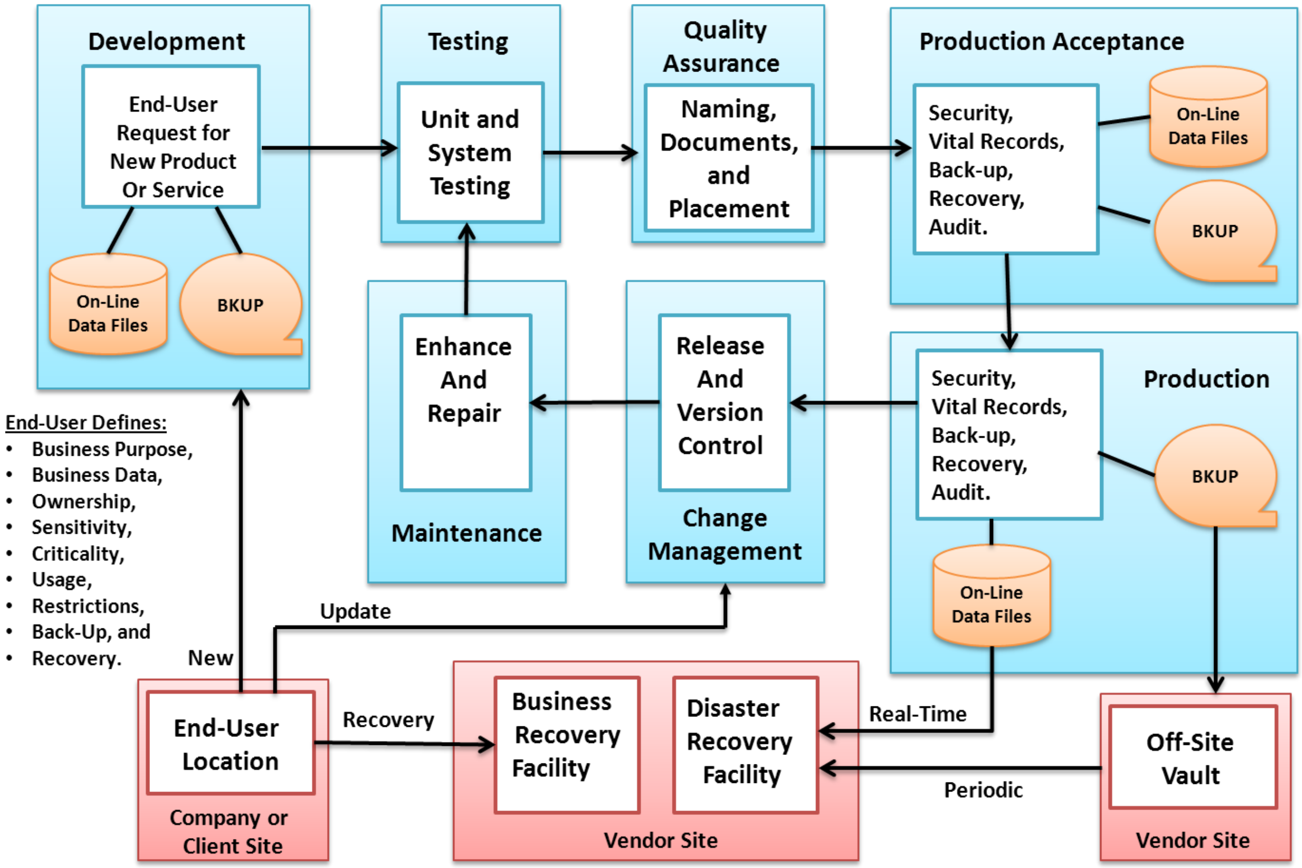


All of these functions are performed to maintain the production and recovery environments in an efficient and safeguarded manner, thereby supporting and protecting business operations and the company reputation.

The Systems Development Life Cycle (SDLC)

How products and services are produced and maintained is through a Systems Development Life Cycle (SDLC) which is shown and explained below.

Systems Development Life Cycle (SDLC), Components and flow



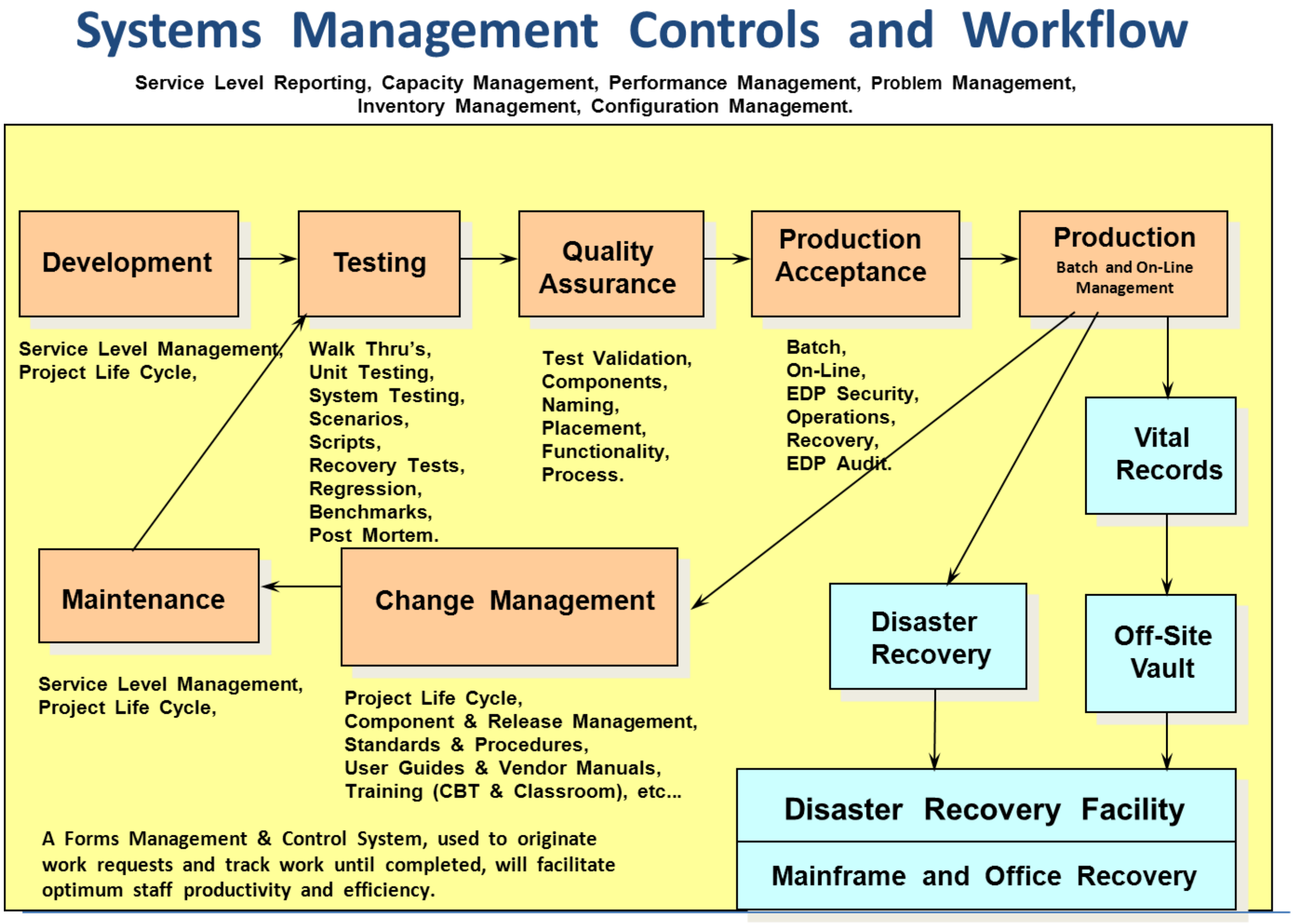
Organizations utilize a Systems Development Life Cycle (SDLC) to implement new products and services, while providing; production acceptance, production operations, and support / maintenance to correct problems and implement enhancements.

Initially, the end user makes a development request that is approved and scheduled for creation. The development group produces test data that is used to verify proper operations for both normal and error processing. When testing is successful, the Quality Assurance Group reviews the documentation and procedures associated with the new product or service to insure they provide production operations with the information they need to set-up, process, backup, and recover production. The Quality Assurance Group also ensures Version and Release Management to guaranty that all of the documentation is pertinent to the release to eliminate confusions caused by out-of-date documentation and procedures which could lead to problems.

The Production Acceptance Group is responsible for performing all set-up tasks associated with a service, including Library Management, Access Controls, Vital Records Management, and anything needed to perform production operations. The Production operations process is responsible for processing services, performing security, vital records management, backup / recovery, and audit compliance. The production operations group will also coordinate recovery operations by exercising Disaster Recovery plans for Information Technology Disaster and Business Recover Plans for business locations suffering a disaster event.

A fully implemented Enterprise Information Technology Operation will include many sites with varying types of equipment that support a diverse set of production services.

Systems Management and Controls



Systems Management Controls and Workflow

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

Development

Service Level Management, Project Life Cycle,

Testing

Walk Thru's, Unit Testing, System Testing, Scenarios, Scripts, Recovery Tests, Regression, Benchmarks, Post Mortem.

Quality Assurance

Test Validation, Components, Naming, Placement, Functionality, Process.

Production Acceptance

Batch, On-Line, EDP Security, Operations, Recovery, EDP Audit.

Production
Batch and On-Line Management

Vital Records

Off-Site Vault

Disaster Recovery

Disaster Recovery Facility

Mainframe and Office Recovery

Maintenance

Service Level Management, Project Life Cycle,

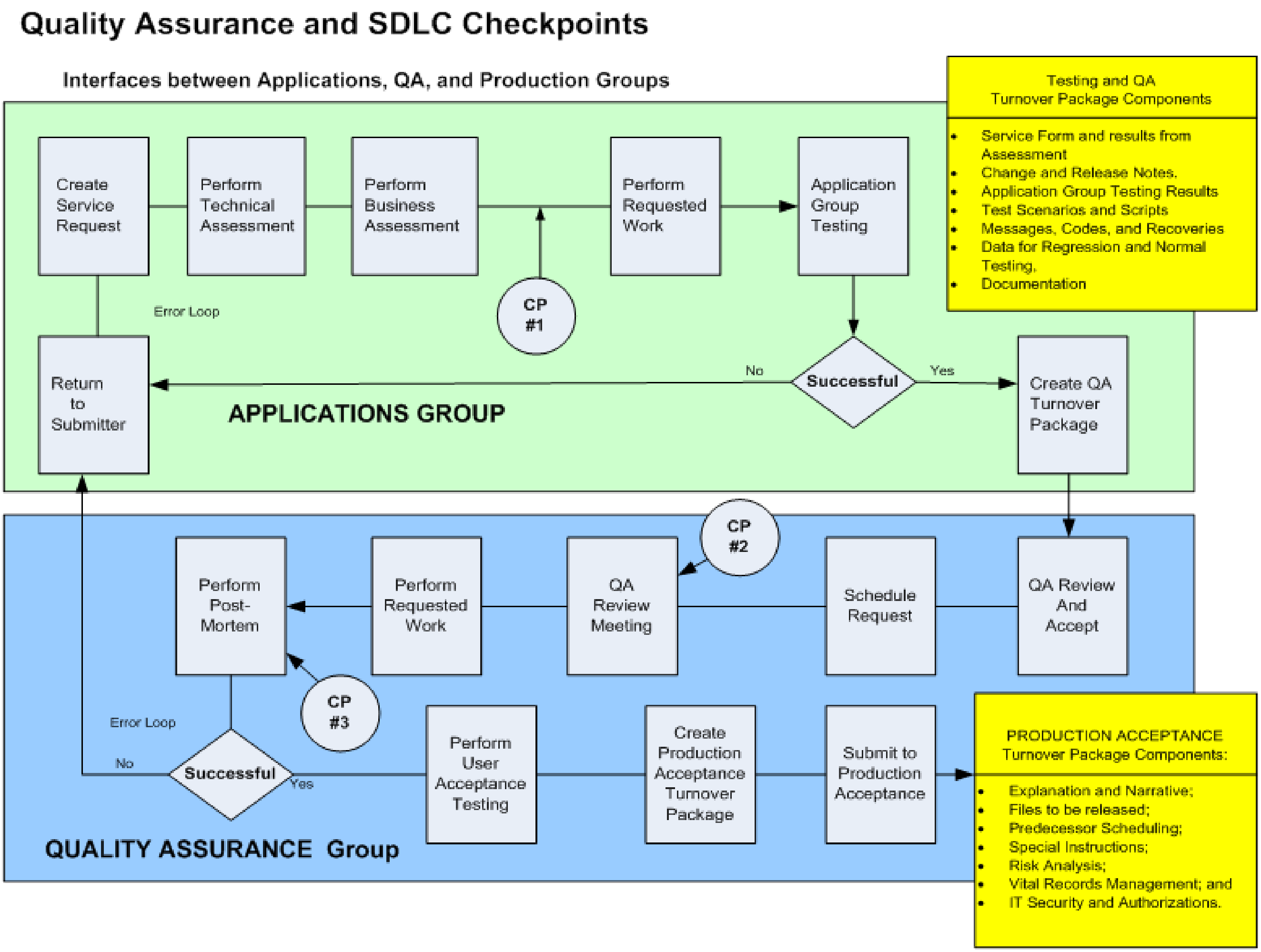
Change Management

Project Life Cycle, Component & Release Management, Standards & Procedures, User Guides & Vendor Manuals, Training (CBT & Classroom), etc…

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

The tasks performed to support the SDLC are shown above.

Migrating Applications to the Production Environment


Quality Assurance and SDLC Checkpoints
Interfaces between Applications, QA, and Production Groups
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
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
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
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.
QUALITY ASSURANCE Group

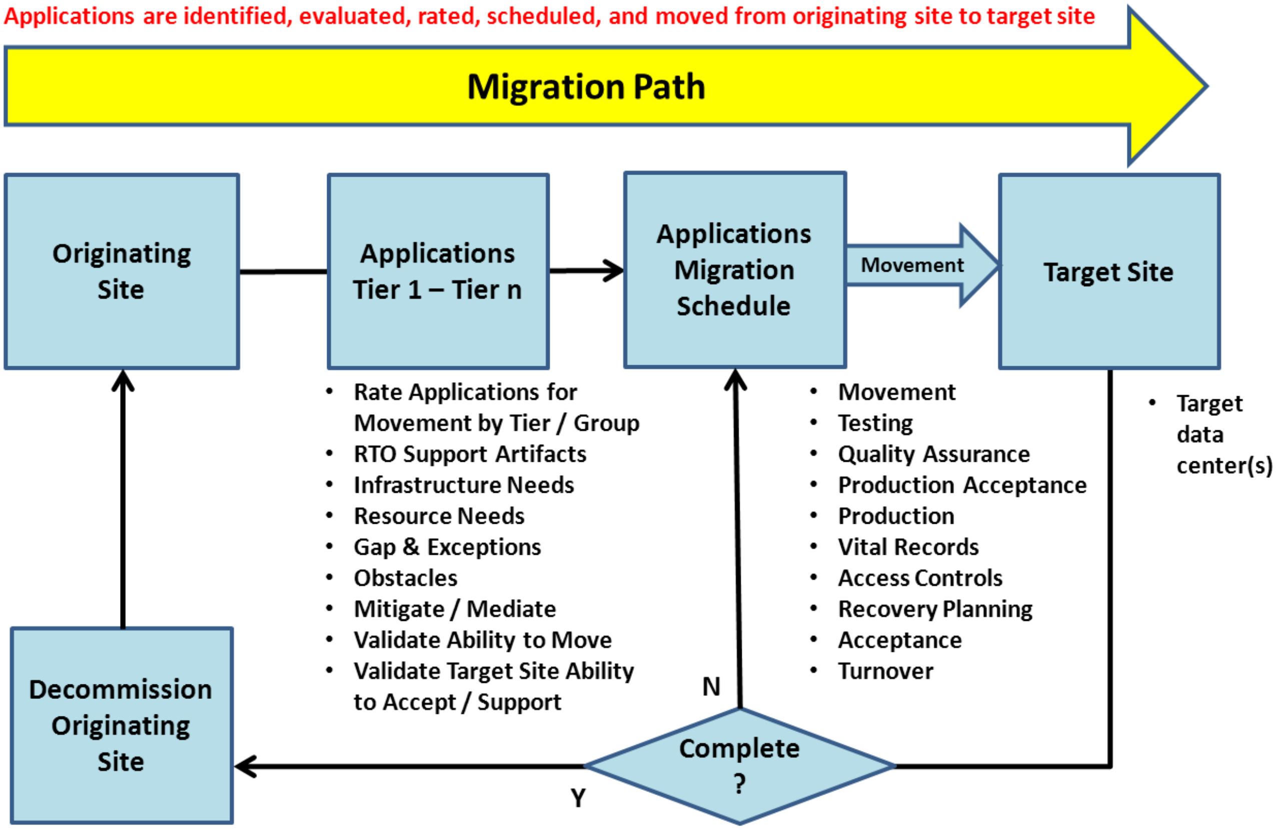
The steps associated with migrating applications to the production environment are shown in this illustration. Forms, Documentation, Actions, Results, and Checkpoints are embedded within the process, so that reviews can be conducted, corrective actions formulated, and go / no-go decisions can be made.

Information requirements can be accumulated via a Relational Database System (RDBS) used for forms completion and movement. This information can be accessed through structured query language instructions (SQL) that pick information from various forms and generate specific reports for management and technical analysis.

Migrating Applications between sites

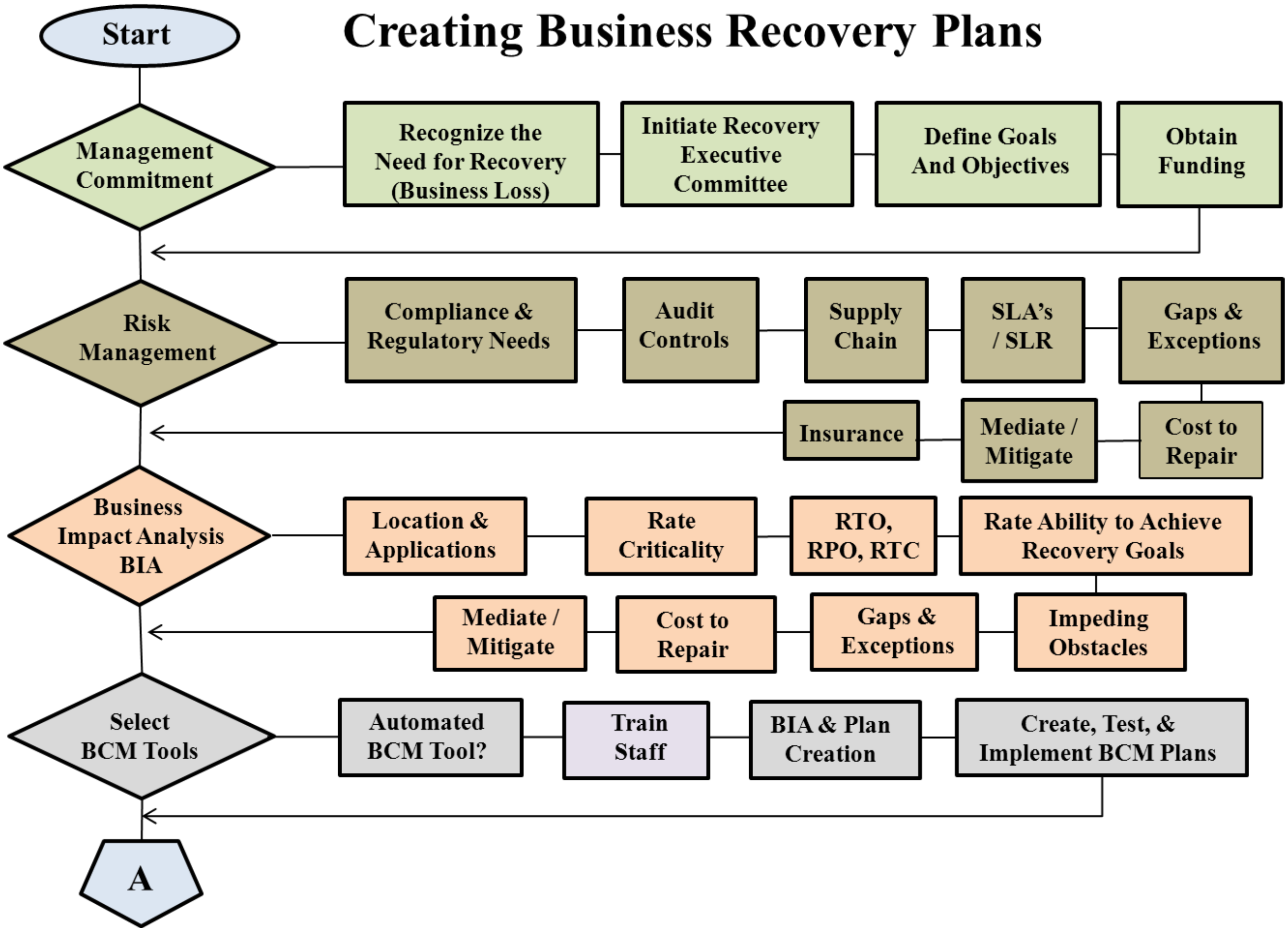
Application Migration can occur when:

- New Products and Services are introduced;
- When Maintenance is performed to correct problems or introduce enhancements;
- When changing an applications location from one site to another (new, maintained, migration, recovery, consolidating sites, reducing sites, eliminating sites);
- Application Migration can be controlled via High Availability (2 – 72 hour recovery) or Continuous Availability (immediate recovery) requirements;
- HA applications follow a Failover / Failback philosophy where recovery is accomplished with recovery time objectives; and,
- CA applications follow a Flip / Flop philosophy where recovery is immediate and the application can process in either the primary or secondary site for prolonged periods of time.



In all cases, proper documentation is required to support operations in primary and secondary locations so that the staff knows what actions to perform and what is the expected outcome of operations.

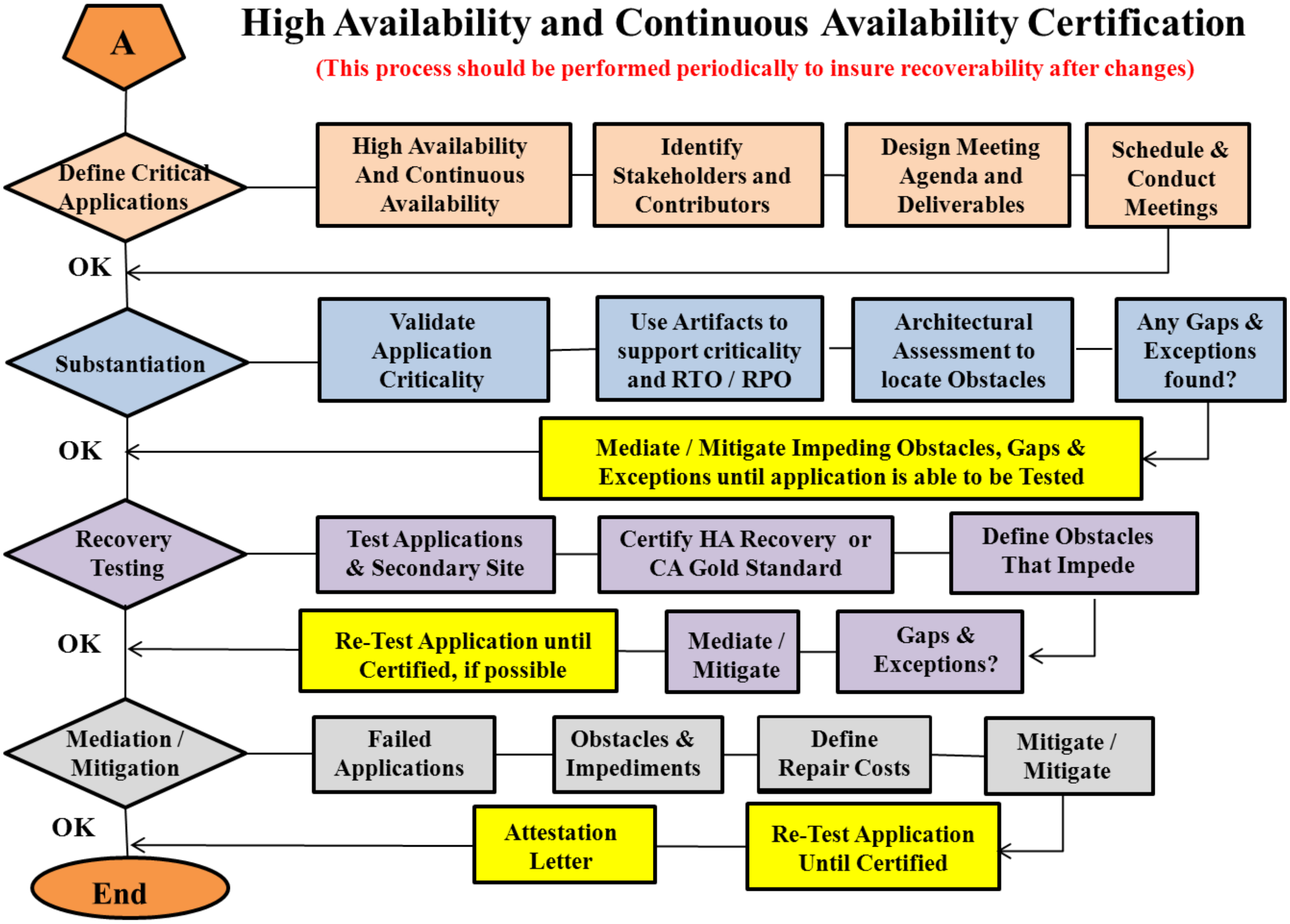
Creating Recovery Plans (Flowchart)



The process of creating recovery plans is illustrated in the above flowchart. It includes:

1. Obtaining Management Commitment, funding, and strong support where management recognizes the importance to recovery planning to the continuation of business operations and in support of the company reputation.
2. Conducting a Risk Management Analysis to uncover Gaps, Exceptions, and Obstacles that impede the company's ability to support production and recovery operations. It includes Audit Controls, Supply Chain Management, SLA / SLR / PKI / and Client Contract performance and recovery time frames. At the end of a Risk Analysis, a report and presentation is provided to management documenting the risk and the cost to control/repair the risk. Management will then choose between repairing the risk or obtaining insurance to cover the risk.
3. A Business Impact Analysis is performed to identify location vulnerabilities and recovery actions.
4. Finally an automated Recovery tool is selected and recovery plans developed, implemented, and integrated within the everyday functions performed by personnel, with periodic testing to insure accuracy.

Certifying Recovery Plans (Flowchart)


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

Testing of Recovery Plans is conducted in following phases, which are:

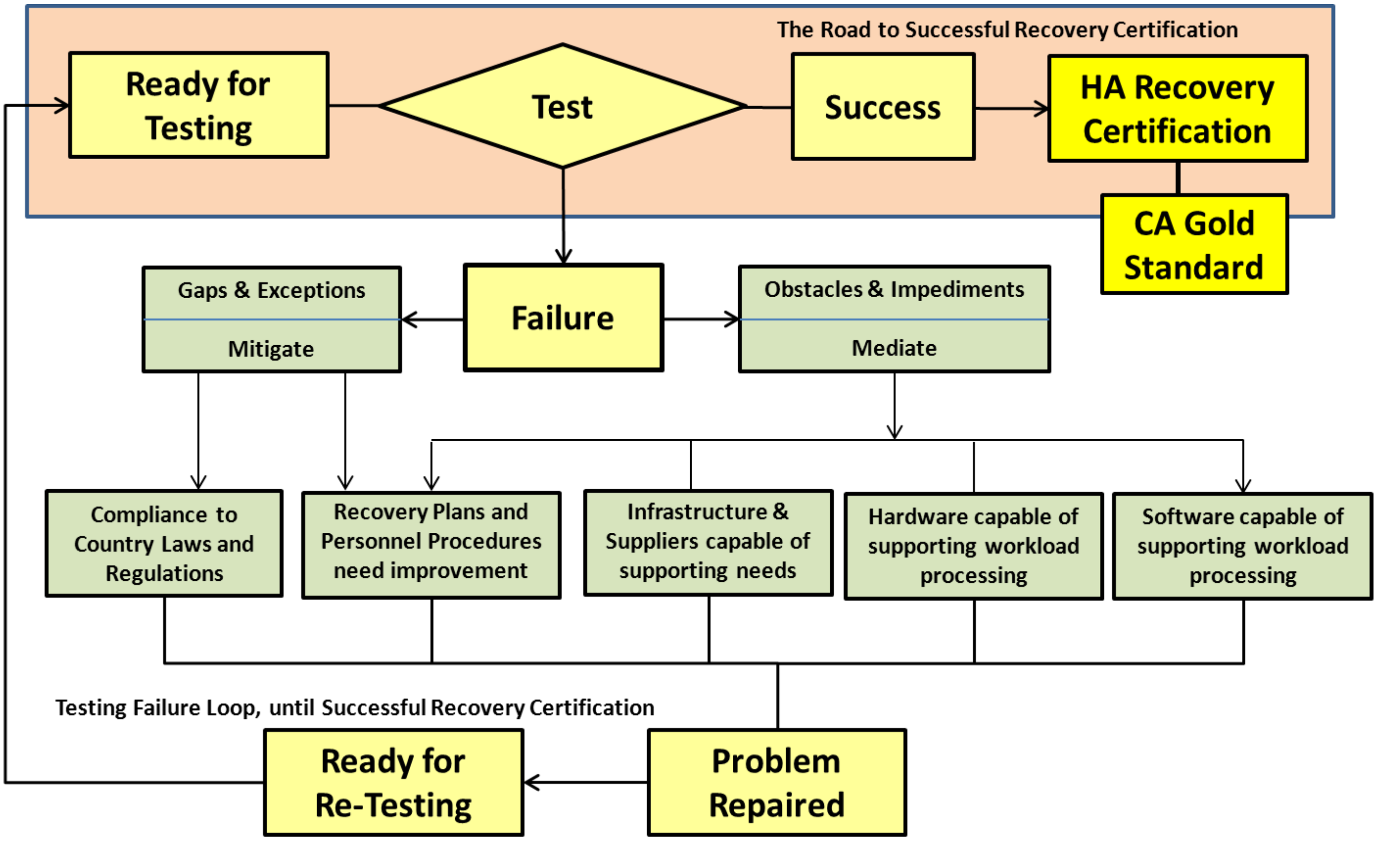
1. Identify and rate applications based on recovery criteria (Tier-1 through Tier-n, where Tier-1 is most critical and requires Continuous Availability (CA) and Gold Recovery Certification via immediate Flip / Flop recovery operations in either the primary or secondary site for prolonged times and without notice; Tier-2 are High Availability (HA) applications requiring failover / failback recovery certification for recovery within 2 – 72 hours; and all other applications falling below that recovery range).
2. Supportive information and artifacts are used to justify recovery time requirements and the criticality of applications.
3. Facility capacity / performance / asset verification is conducted to insure that the application can process at the target site. This is necessary to respond to growth and the introduction of new technologies.
4. Testing is finally conducted in a scheduled manner with a ramp up from Tier-1 through Tier-n. Any uncovered Gaps, Exceptions, or Obstacles are detected and repaired. After repairing problems, the application is re-tested until certification is achieved.

Testing migrated applications to certify recovery status (Flowchart)

Applications being migrated between the primary and recovery site must be certified to insure that they comply with recovery time objectives. The flowchart shown below illustrates how High Availability (HA) Recovery Certification (2-72 hour recovery guidelines) and Continuous Availability (CA) (immediate recovery) Gold Standard Recovery Certification is achieved.

Applications are maintained in Tiers (1-n) in accordance with their recovery requirements. Recovery testing is usually performed from Tier-1 through Tier-n.

An illustration of application recovery testing is shown below.


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

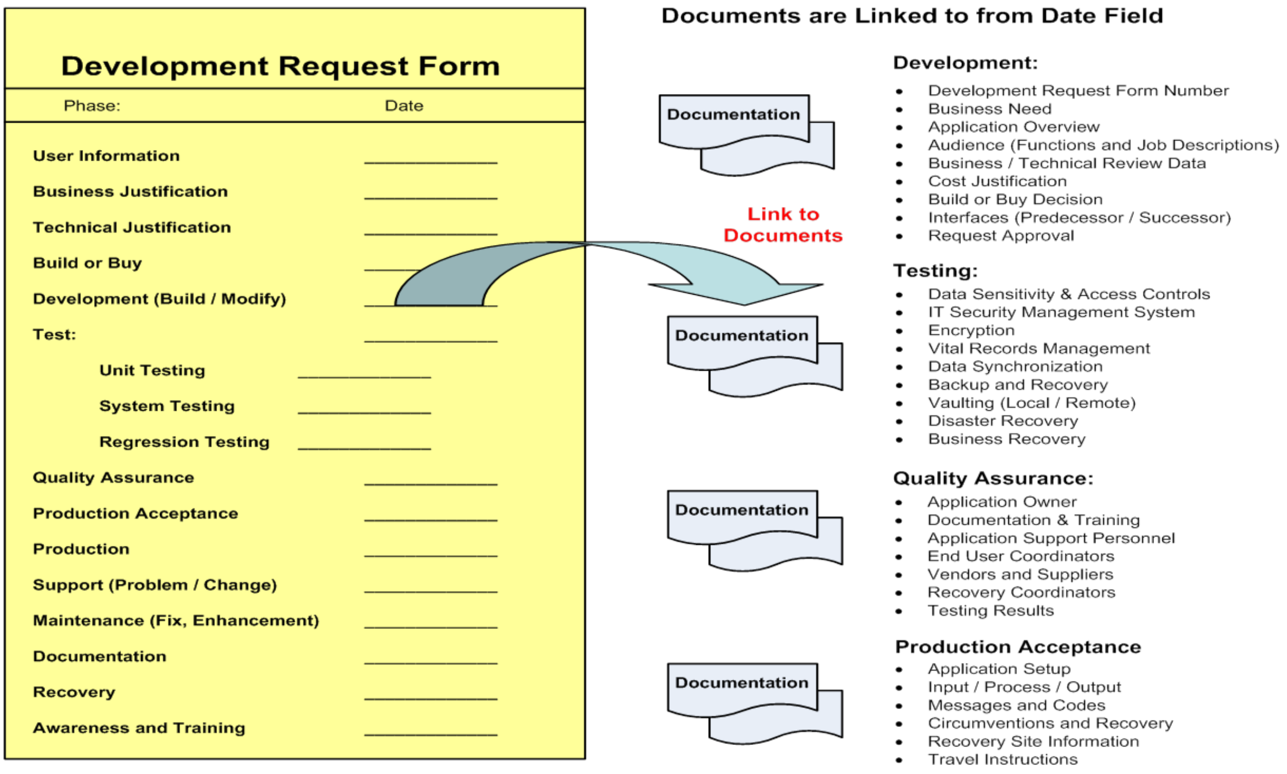
Steps include:

1. Validate Application Recovery Guidelines via artifacts like BIA, PKI, SLA, or Service Contract.
2. Review applications resources and capacity are present to support recovery operations and identify any obstacles that might impede recovery testing.
3. Test application ate recovery site.
4. Report any encountered problems to management.
5. Mitigate Gaps and Exceptions and Mediate Obstacles impeding recovery operations.
6. Continue testing process until successful.

Job Documentation process

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

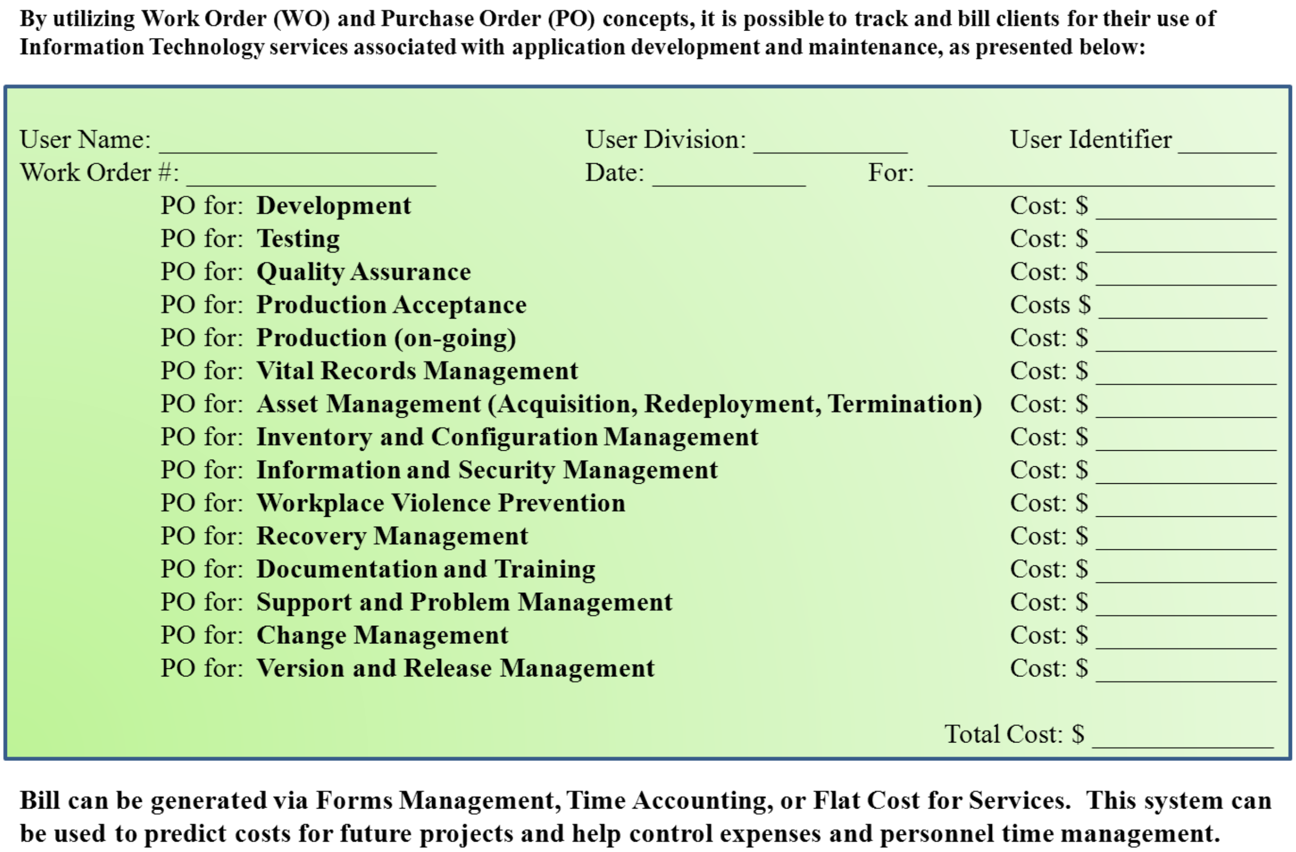
Forms Management and Control has been the single greatest loss of productivity for many years so it is essential to properly document the phases and actions associated with development, testing, quality assurance, production acceptance, production, support, maintenance, and recovery operations so that time frames can be established and reviews conducted to constantly make improvements.

Using a relational database system to support forms management and control will allow for the accumulation of information from various forms to generate management and performance reports, as needed.

Information Technology Infrastructure Library (ITIL) is used to support forms management and control operations in many of today's information technology environments. The new version is an excellent tool and can be used to supply information to most people associated with IT and Business operations.

Refer to ITIL section earlier provided to obtain a fuller understanding of forms management and control used to support production and recovery operations.

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 application development and maintenance, as 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: $ _____________

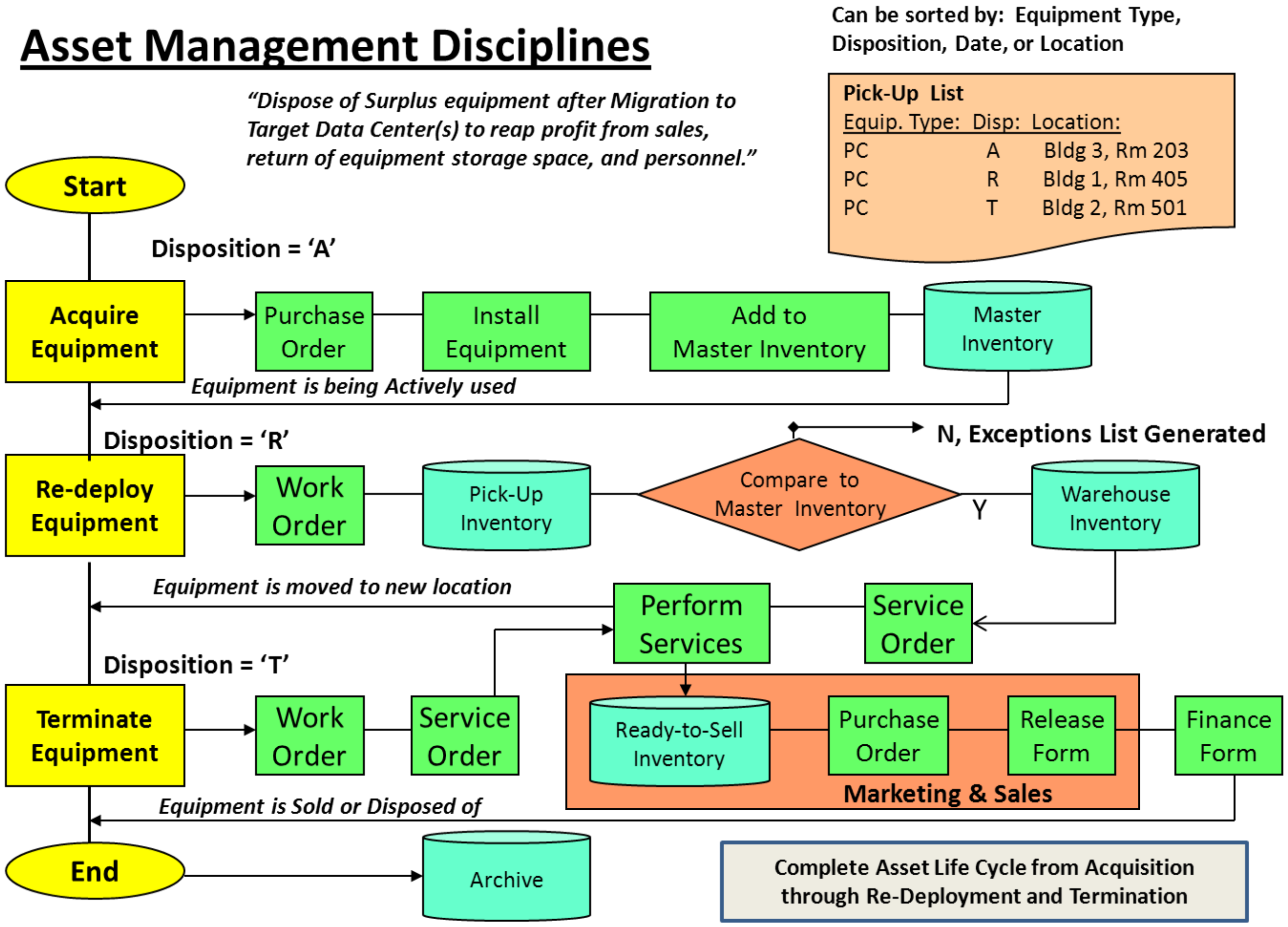
Total Cost: $ _____________

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.

The tasks performed to implement, support, and maintain products and services can be treated like a Work Order / Purchase Order System with accounting performed as demonstrated above. Tasks, Time, Resources, and Assets are included in the accounting system and charges are based on the results accounted for in the system

The accounting system can be used to judge the cost of future projects by reviewing similar past projects and calculating costs appropriately, with adjustments to asset and resource costs and the amount of time needed to complete a task. Costs can go down through reduced equipment costs and the use of automated tools that reduce labor costs.

Asset Management (Asset Acquisition, Redeployment, and Termination)


Asset Management Disciplines
"Dispose of Surplus equipment after Migration to Target Data Center(s) to reap profit from sales, return of equipment storage space, and personnel."
Can be sorted by: Equipment Type, Disposition, Date, or Location
Pick-Up List
Equip. Type: Disp: Location:
PC A Bldg 3, Rm 203
PC R Bldg 1, Rm 405
PC T Bldg 2, Rm 501
Start
Disposition = 'A'
Acquire Equipment
Purchase Order
Install Equipment
Add to Master Inventory
Master Inventory
Equipment is being Actively used
Disposition = 'R'
N, Exceptions List Generated
Re-deploy Equipment
Work Order
Pick-Up Inventory
Compare to Master Inventory
Y
Warehouse Inventory
Equipment is moved to new location
Perform Services
Service Order
Disposition = 'T'
Terminate Equipment
Work Order
Service Order
Ready-to-Sell Inventory
Purchase Order
Release Form
Finance Form
Marketing & Sales
Equipment is Sold or Disposed of
End
Archive
Complete Asset Life Cycle from Acquisition through Re-Deployment and Termination

Asset are purchased to support new products and services, or to incorporate new technologies. Their status and ownership are logged into the Asset Management System and an asset profile created (what it is, what features does the asset contain, who is responsible for it, where is it located, is the asset owned / leased/ or rented, etc.).

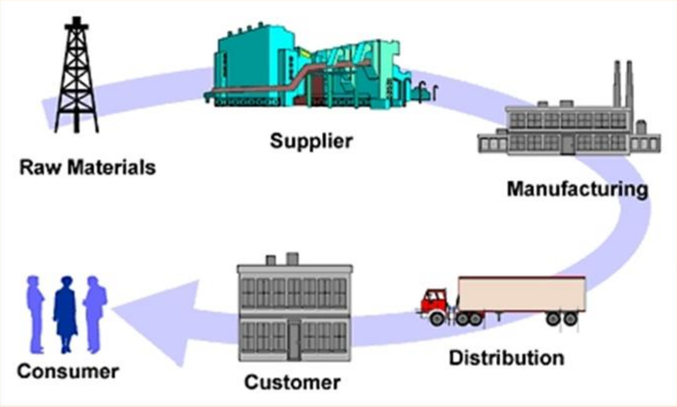
When the asset is updated due to repairs or enhancements, the asset status is updated to reflect the change. Should an asset be redeployed, because the user left the firm or the product is moving to a new location, then data must be erased from the private drive and updates made to the asset profile. When assets are terminated, sensitive data must be erased and the asset must be disposed of within EPA guidelines, or stiff penalties will be levied by the EPA and Superfund.

The process for achieving Asset Management is shown above.

Supply Chain Management

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

International visibility through satellites and cloud technology
DEMAND
Global Air
Customers
Home Delivery
Retail Store
Global DC
Raw Material Supplier
Component Supplier
Retail Store
Ocean
Component Supplier
Raw Material Supplier
Global DC
SUPPLY



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

Since supplies and assets are critical to production and recovery operations, it is important to know where your supplies come from and to insure that you are aware of any Single-Points-Of-Failure or weaknesses in your supply chain. The above illustration shows how in today's business environment, raw materials are located, and supplies are manufactured all over the world.

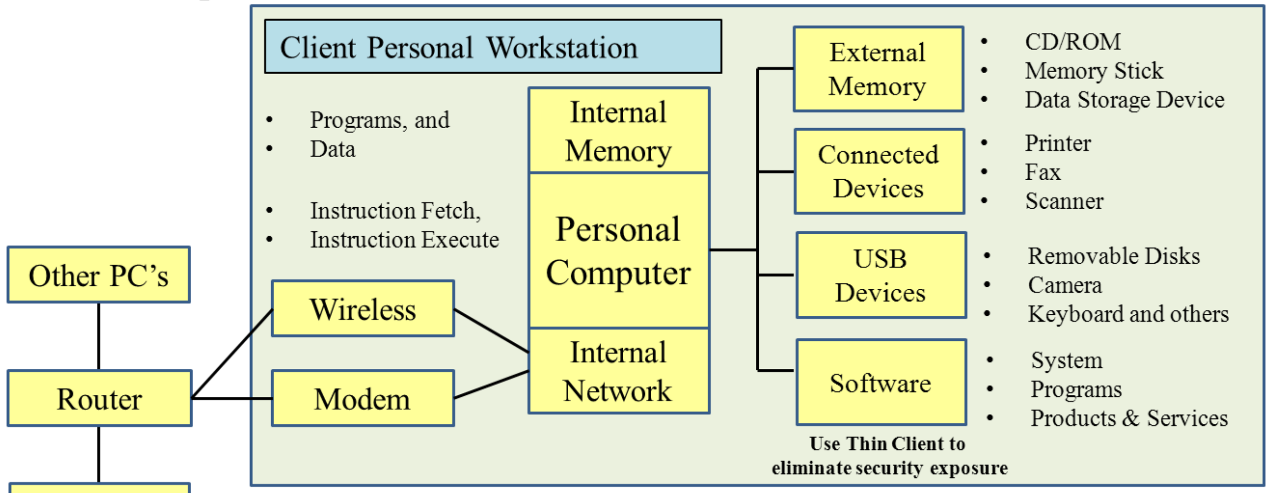
Suppliers accumulate supplies and transport them to their clients via an established schedule, or in respond to demand. Should the Supplier, Manufacturer, or Distributor have a failure and cannot make deliveries as required, then they can contribute to your experiencing a disaster – not because of a disaster event, but because of a lack of supplies.

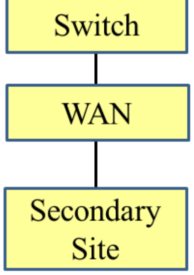
For the reasons mentioned above, it is important that you pay attention to supply chain management so that you can quickly become aware of any failures and take appropriate actions to protect your business operations and continue to provide products and services to your clients.

Supply chain problems can result in growth opportunities when your company responds to a supply chain failure more rapidly than you competition or you could lock up supplies that may not be replenished for a long period of time. It is sometimes a double-headed coin and you can either win big or lose big. Better to prepare.

Personnel Computer Environment

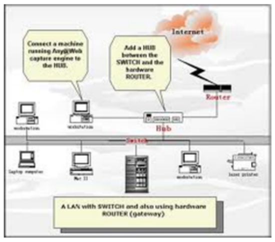
Personnel Computer environment





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 connected through the "Cloud", which is a physical site owned by an outside supplier (public) or the enterprise (private).


Internet
Connect a machine running Any@Web capture engine to the HUB.
Add a HUB between the SWITCH and the hardware ROUTER.
Router
Hub
Switch
A LAN with SWITCH and also using hardware ROUTER (gateway)

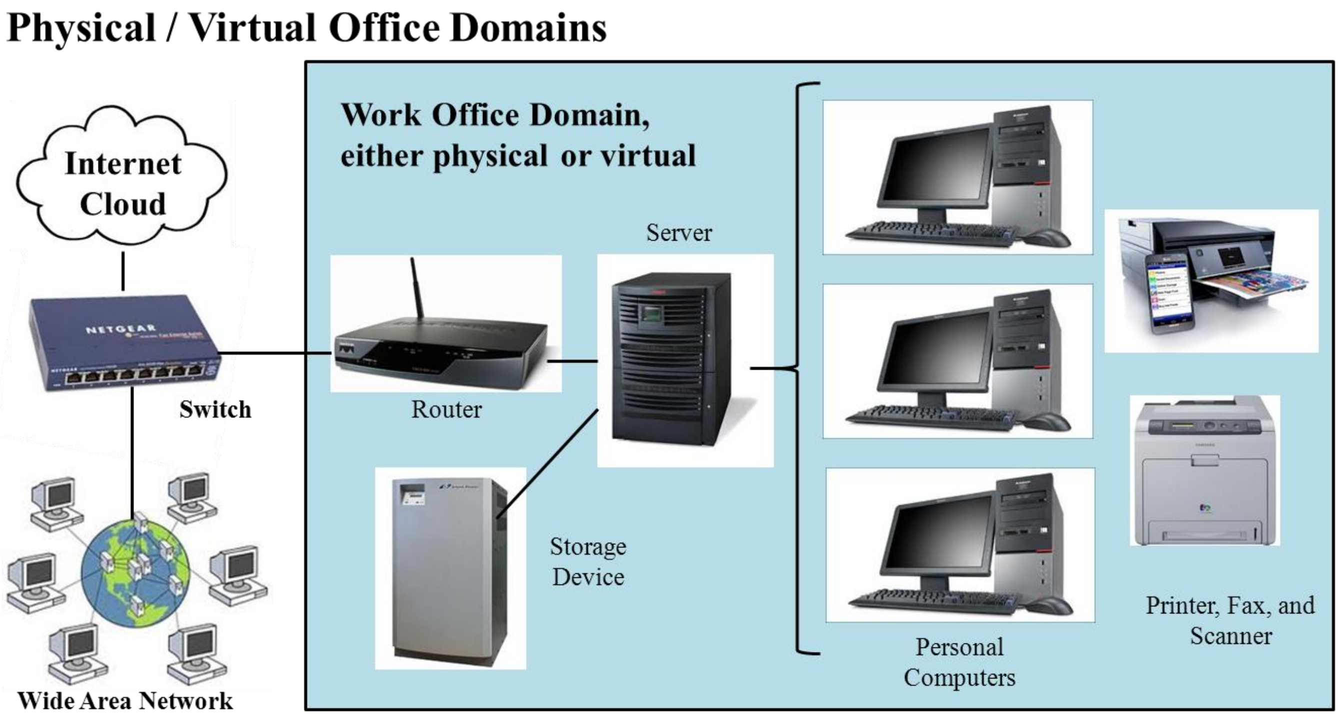
Programs can be stored in the server or accessed through the server, which will result in reduced costs and greater security by limiting access to authorized personnel only. This will also reduce costs for data and equipment.

Personnel Computers have grown over the years from a simple Disk Based Operating System (DOS – Disk Operating System) where programs and data had to be loaded into memory via floppy disk drives using a basis 80-80 processing system (computer card based) to a VMware based system using Virtual Memory Partitions and high speed devices connected over a Broadband Network utilizing land lines and satellite based networks.

As time went by, the devices connected to personnel computer posed a security threat when date files were downloaded to removable devices (i.e., flash drives, etc.). This information could then transfer data between systems, or even be used to introduce viruses into secured systems.

It became evident that something had to be done to close the exposure that personnel computer systems had on the security of a business and its information. One path was to incorporate Encryption throughout the network so that outside personnel could not view and use the data. Another was to eliminate the use of transportable media and store all data on the company devices, most recently on Cloud Hosted Systems (like Google Chrome where your information is stored on the Google Site and recovery is performed by Google if a problem arises). These methods provided a much higher degree of security and helped companies more rapidly recovery data and restore operations when disaster events occur.

Thin Client personnel computer environment


Physical / Virtual Office Domains
Internet Cloud
Switch
Wide Area Network
Work Office Domain, either physical or virtual
Server
Router
Storage Device
Personal Computers
Printer, Fax, and Scanner

The use of Thin Client personnel computers eliminates removable media drives from the PC environment. A single access point is used to connect the PC, Its Screen(s), video / audio device, and telephone.

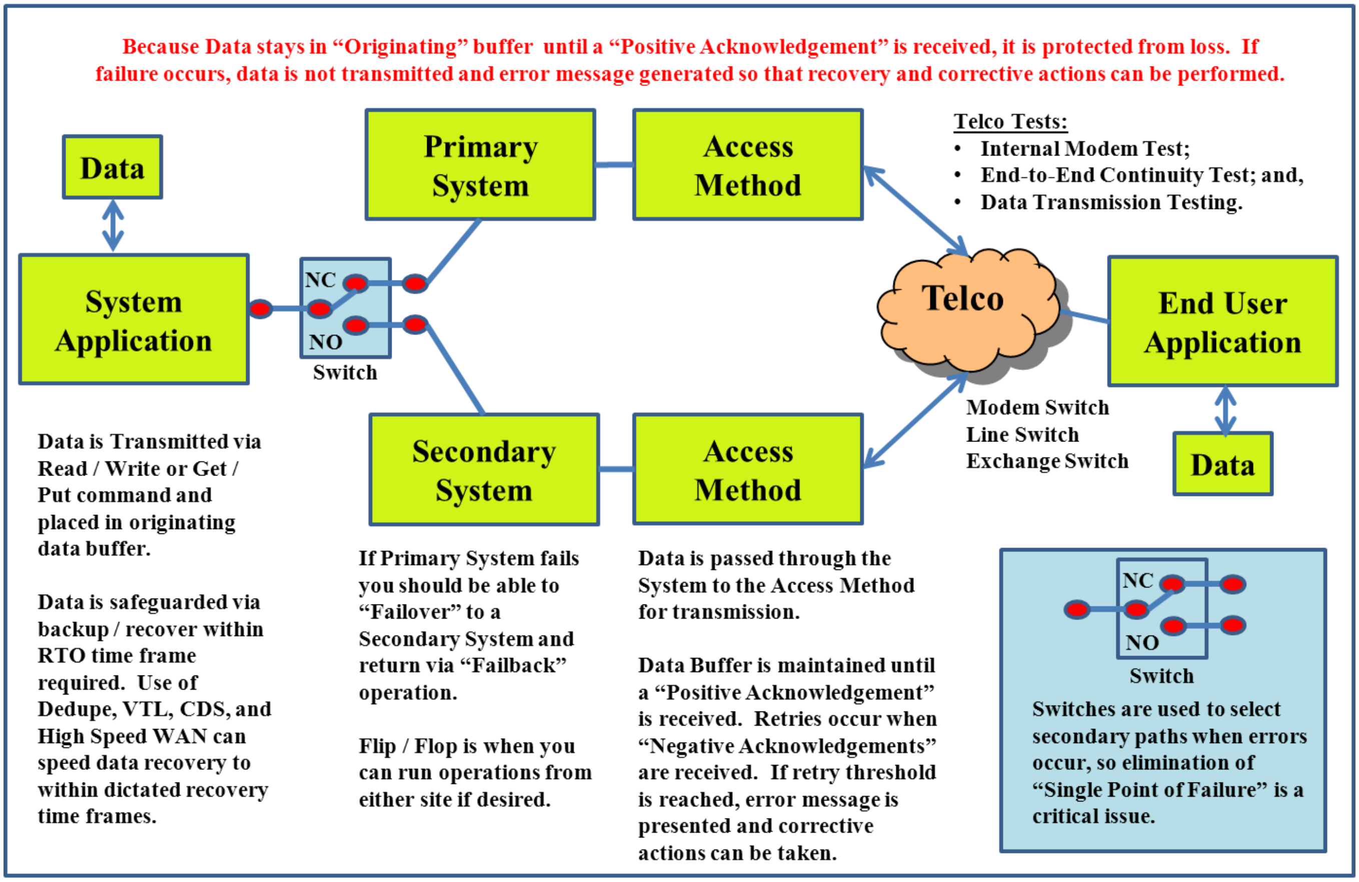
Utilizing this approach eliminates the possibility of personnel downloading data onto transportable media that can be taken off-site and used to expose company secrets or sensitive information. Also, taking personal data away from a protected company environment may result in Identity Theft and large lawsuits against the company.

The Thin Client environment protect company assets, provides rapid data and system recovery, and can support access to current information from any authorized location (home, work, recovery location) by authorized personnel. Utilizing this advantage, the personnel at a failing site can go off-site to a recovery location (or from even home) and re-log onto the system again. These people will be able to resume uninterrupted operations using the current data and programs they were previously attached to, thereby speeding recovery and decreasing business outages.

Utilizing the Internet or company Wide Area Network (WAN) will allow business operations to resume from any global location connected to the company system via Cloud Hosted computing services. This supports the ability of support centers from all over the globe to pick-up uninterrupted customer services with a minimum of processing performance degradation.

Data Transmission between programs and devices

Store and Forward concept for data transmission / reception



Because Data stays in "Originating" buffer until a "Positive Acknowledgement" is received, it is protected from loss. If failure occurs, data is not transmitted and error message generated so that recovery and corrective actions can be performed.

Telco Tests:

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

Data is Transmitted via Read / Write or Get / Put command and placed in originating data buffer.

Data is safeguarded via backup / recover within RTO time frame required. Use of Dedupe, VTL, CDS, and High Speed WAN can speed data recovery to within dictated recovery time frames.

If Primary System fails you should be able to "Failover" to a Secondary System and return via "Failback" operation.

Flip / Flop is when you can run operations from either site if desired.

Data is passed through the System to the Access Method for transmission.

Data Buffer is maintained until a "Positive Acknowledgement" is received. Retries occur when "Negative Acknowledgements" are received. If retry threshold is reached, error message is presented and corrective actions can be taken.

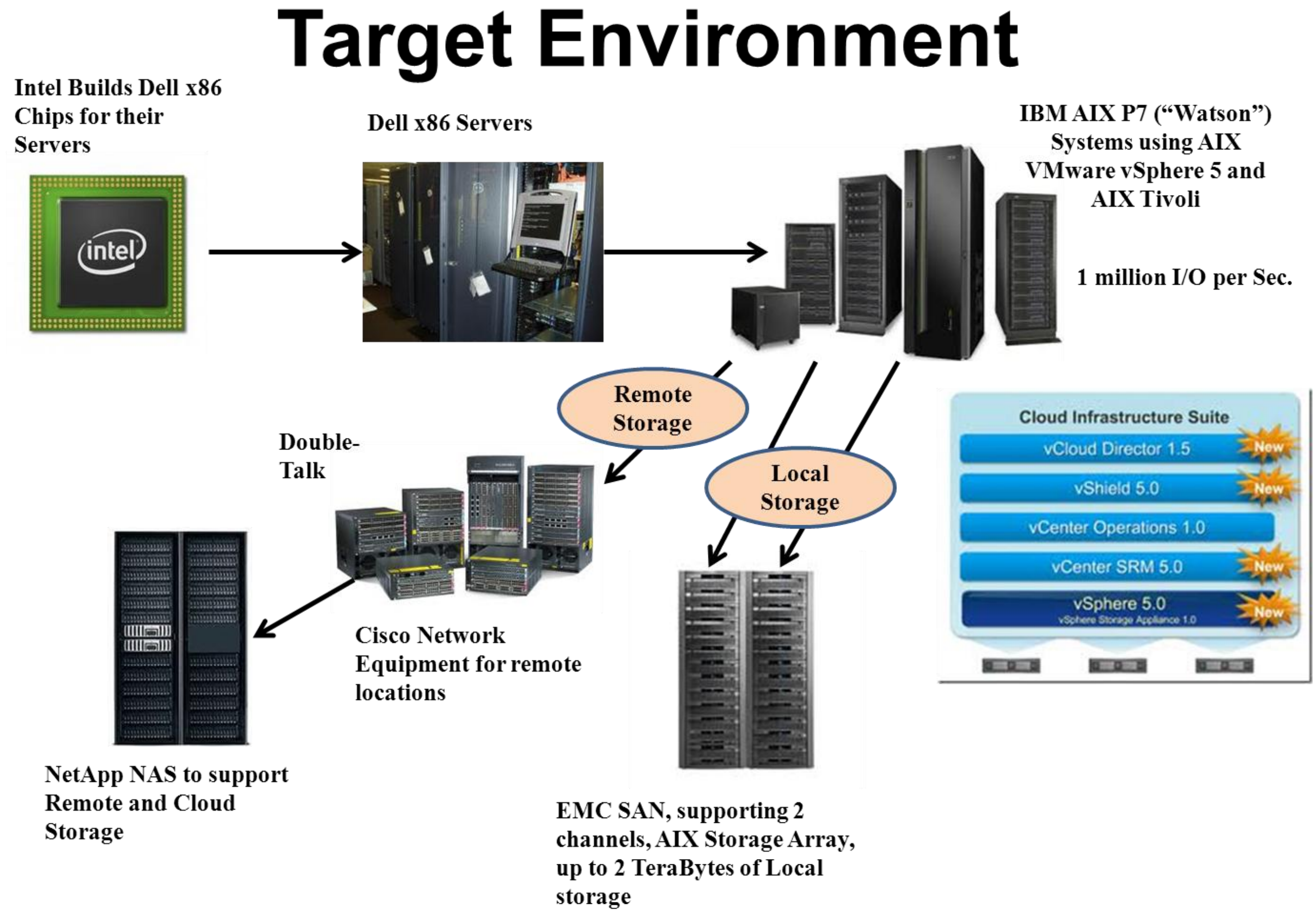
Switches are used to select secondary paths when errors occur, so elimination of "Single Point of Failure" is a critical issue.

The "Store and Forward" method used to transfer data between programs and devices is shown above and used to ensure the safe arrival of transmitted information.

A positive acknowledgement (ACK) indicates the successful receipt of information and will result in the next data item being transmitted until the end of the message is reached. A negative receipt (NAK) indicates that the data was not received successfully and will trigger an error report and retransmission request until an error threshold is reached (40 Read Retries and/or 15 Write Retries) and a permanent problem reported.

If the computer hangs during transmission, the operator can hit the "Stop Key" on the computer console and check to see which device is hung-up in the middle of a transmission (usually dropped Ready State). The operator can then write down the error sense information related to the transmission, reset the device to the Ready State, depress the "Check Reset Button: and then the Start button on the console. Normally, the computer will pick-up processing of the transmission without any loss of data, thereby saving the need to restart the computer or program and saving a lot of time.

Sample IT Systems Target Environment


Target Environment
Intel Builds Dell x86 Chips for their Servers
intel
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
Cloud Infrastructure Suite
vCloud Director 1.5
vShield 5.0
vCenter Operations 1.0
vCenter SRM 5.0
vSphere 5.0
vSphere Storage Appliance 1.0
New
New
New
New
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

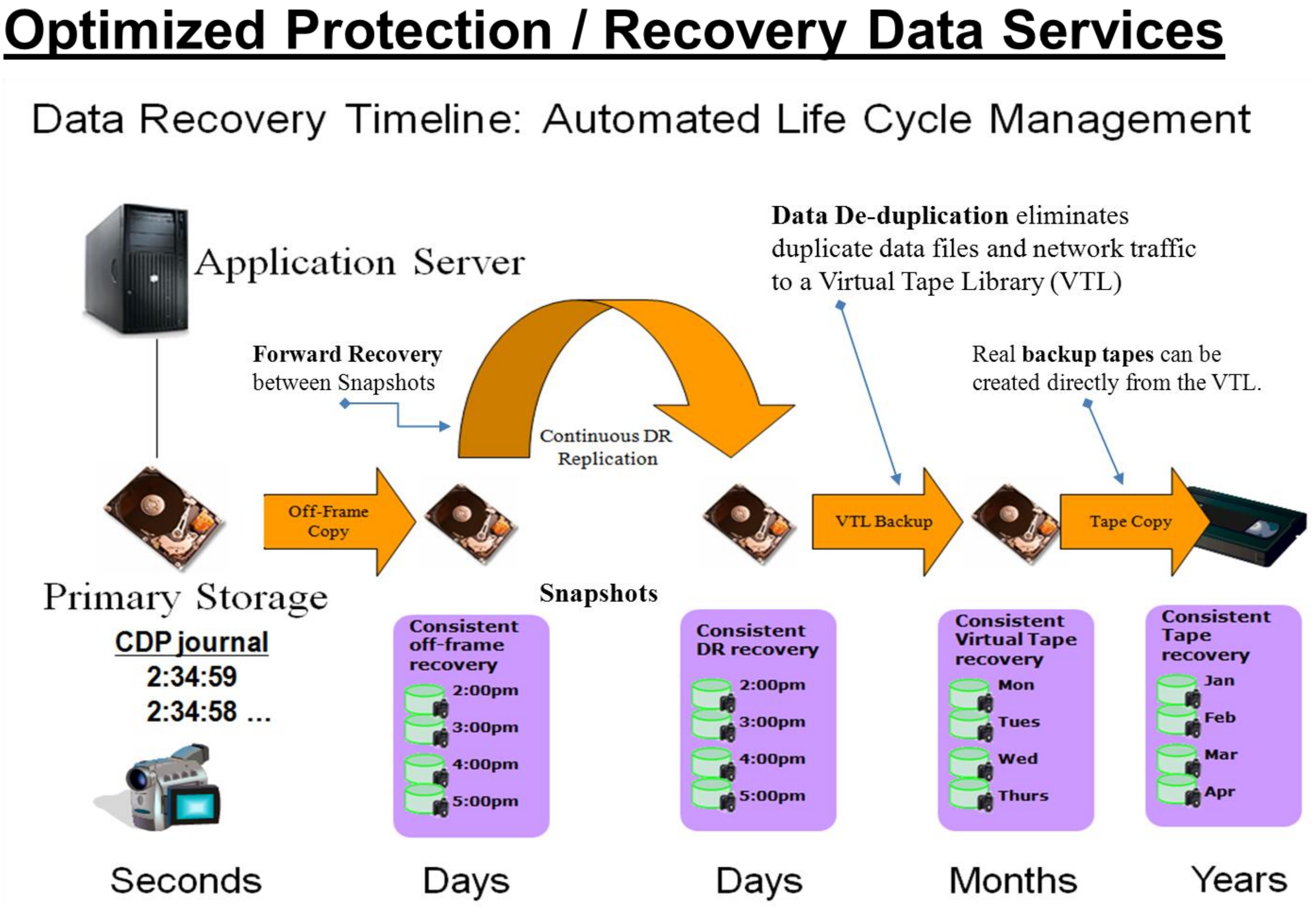
Today's most advanced Information Technology Organizations utilize systems like the one shown above, where a Power Saving computer (i.e., IBM "Watson" P7 computer like the one used on Jeopardy) connects locally and remotely connected servers supporting personnel computers used to support business operations.

By incorporating the vSphere 5.0 environment the client can host multiple virtual server environments within a single physical server, or server cabinet. The vSphers 5.0 system product directs traffic to the appropriate VMware system, vShield is used to provide security protections, vCenter Operations manages the operating environment and vCenter SRM provides performance guidelines over processing programs.

Locally attached storage (i.e., EMC SAN) and remotely attached storage (NetApp NAS Storage) connected via network control devices (Cisco Modems, Routers, Switches, etc.). Utilizing this type of configuration will allow a company to scale up its Information Technology operations with minimal interruption, thereby reducing interruptions to production business operations.

Virtual Machines can support production, maintenance, testing, and recovery environments which will optimize performance and allow for a higher level of quality assurance.

Optimizing Data Storage and Recovery

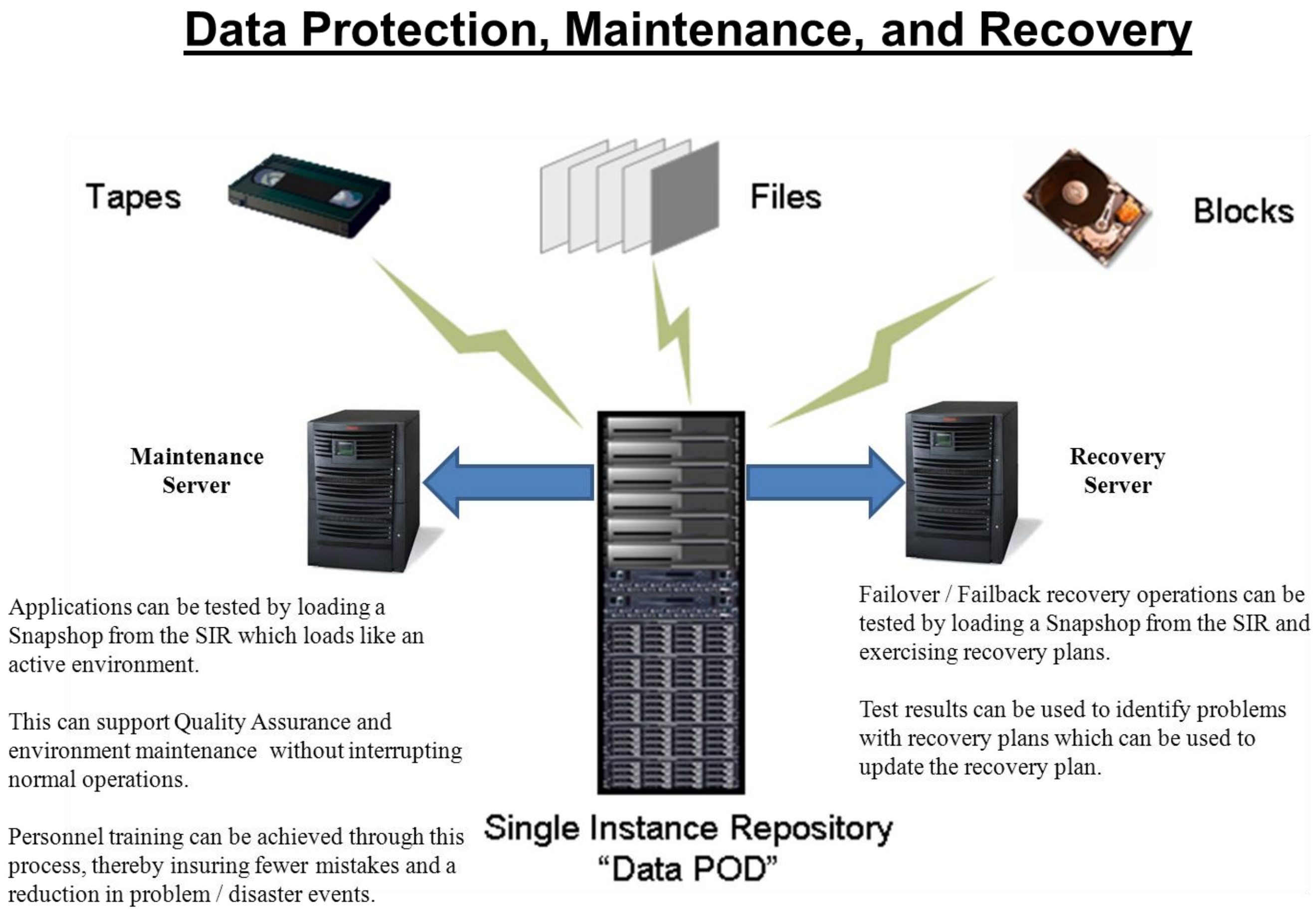

Optimized Protection / Recovery Data Services
Data Recovery Timeline: Automated Life Cycle Management
Application Server
Data De-duplication eliminates duplicate data files and network traffic to a Virtual Tape Library (VTL)
Forward Recovery between Snapshots
Continuous DR Replication
Real backup tapes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

As systems become more important to the business, protecting and restoring data becomes crucial. Today's technology is shown in the above illustrations and includes:

- Data De-Duplication (DeDupe) and Virtual Tape Libraries (VTL) are used to more quickly perform back-up and restore operations. DeDupe only copies data files one time and marks duplicate files in a directory used to restore data files when necessary, thereby reducing transmission times and data. The VTL stores data in various types of media, from tape cartridge to high speed memory systems depending upon the time needed to recover data.
- Snapshots and Continuous Data Protection is when a system snapshot is periodically taken (like every hour or every 15 minutes depending upon recovery time expectations). Continuous Data Protection (CDP) performs a forward recovery of data from when the last snapshot was taken to when the interruption occurred and a recovery performed. After CDP performance, the data at the recovery site is in synch with the data at the time of interruption and normal processing can resume.

Snapshots and CDP can be used to support rapid recovery for Continuously Available (CA) applications or incremental recovery for High Availability (HA) applications. The use of these techniques will depend upon the recovery time requirements associated with applications and business operations.

Recovering Data and Restoring Operating Environments



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.

The use of a “Single Instance Repository (SIR)” will allow a company to go back in time to perform a recovery operation. This may prove essential when a virus is detected, because the only way to completely eliminate a virus is to go back in time just prior to the virus being introduced.

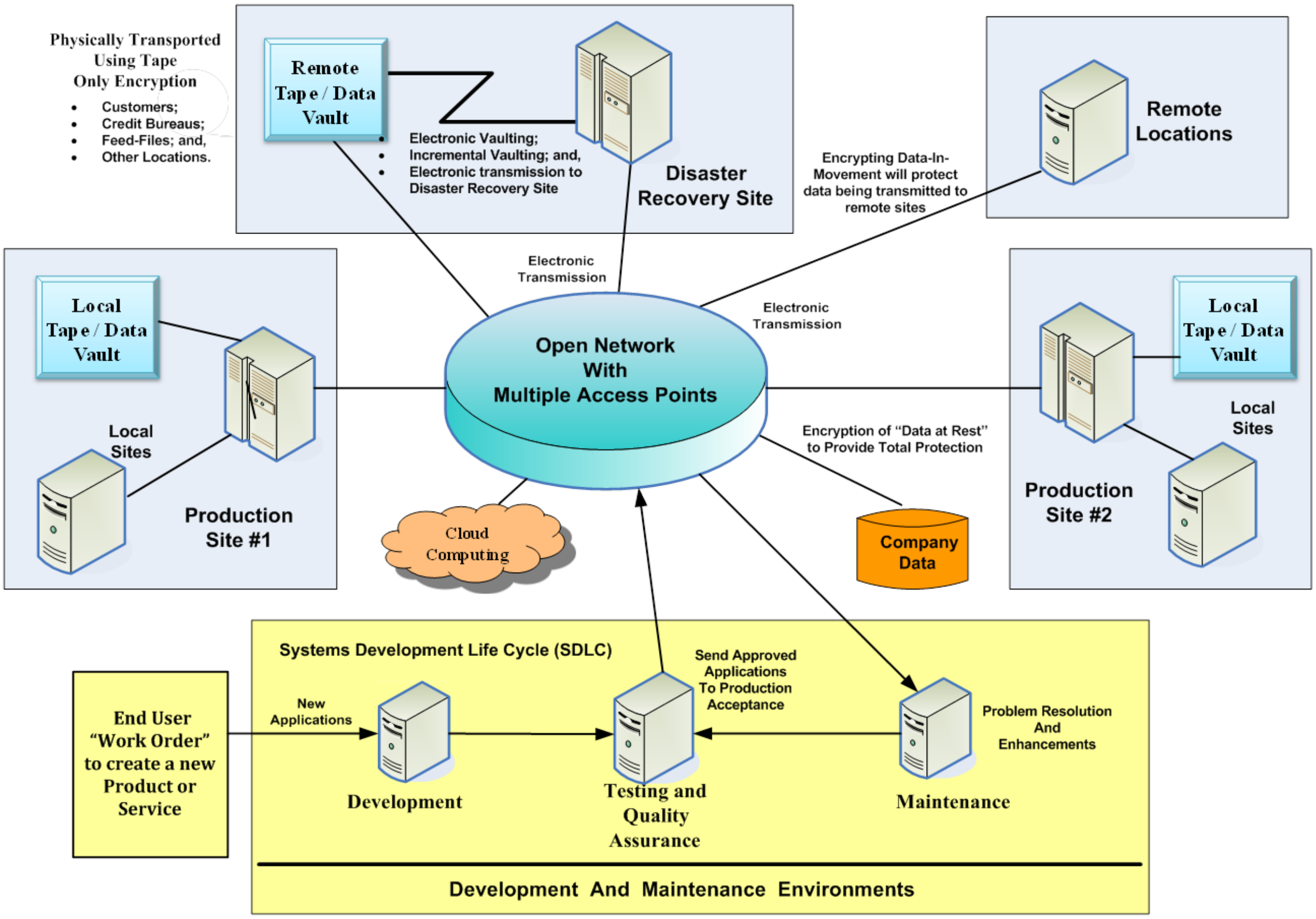
Beyond protection purposes, SIR Snapshots can be used to test maintenance and recovery operations by restoring the production environment to a test or recovery environment and running operations in a controlled manner from the site. This will allow a company to better ensure successful operations after problem repairs, enhancements, or to test recovery procedures and train recovery personnel.

The use of a SIR concept will allow companies to become more efficient without taking a chance on damaging the production environment. An additional benefit is a better trained and confident staff whose morale is high because they know what to do in time of failure and do not have the fear presently associated with recovery operations. A trained and relaxed staff will be a happy staff with high morale and high retention rates. Of course this will have a positive impact on the company reputation and make it easier to recruit quality personnel and improve the client base.

The Enterprise Information Technology Environment

An example of a fully implemented Enterprise Information Technology environment is shown to illustrate how the SDLC, Support, and Maintenance operations interacts with production operations in support of normal and recovery procedures. Users / Clients make requests for new products and services which are created via the SDLC. Problem Repairs and Enhancements are created through the SDLC from the production copy and the Version and Release number is updated appropriately. An Open Network with multiple access points (could be Wide Area Network - WAN) connects development and maintenance to receiving sites and associated vaults to safeguard data. Real-Time and Incremental data synchronization is provided between the production and recovery site, in support of application criticality and recovery time demands. Cloud computing is shown as a Private / Public / Hybrid cloud hosting site to support production and recovery operations.

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
Remote Locations
Encrypting Data-In-Movement will protect data being transmitted to remote sites
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
Cloud Computing
Company Data
Systems Development Life Cycle (SDLC)
End User "Work Order" to create a new Product or Service
New Applications
Development
Send Approved Applications To Production Acceptance
Testing and Quality Assurance
Problem Resolution And Enhancements
Maintenance
Development And Maintenance Environments

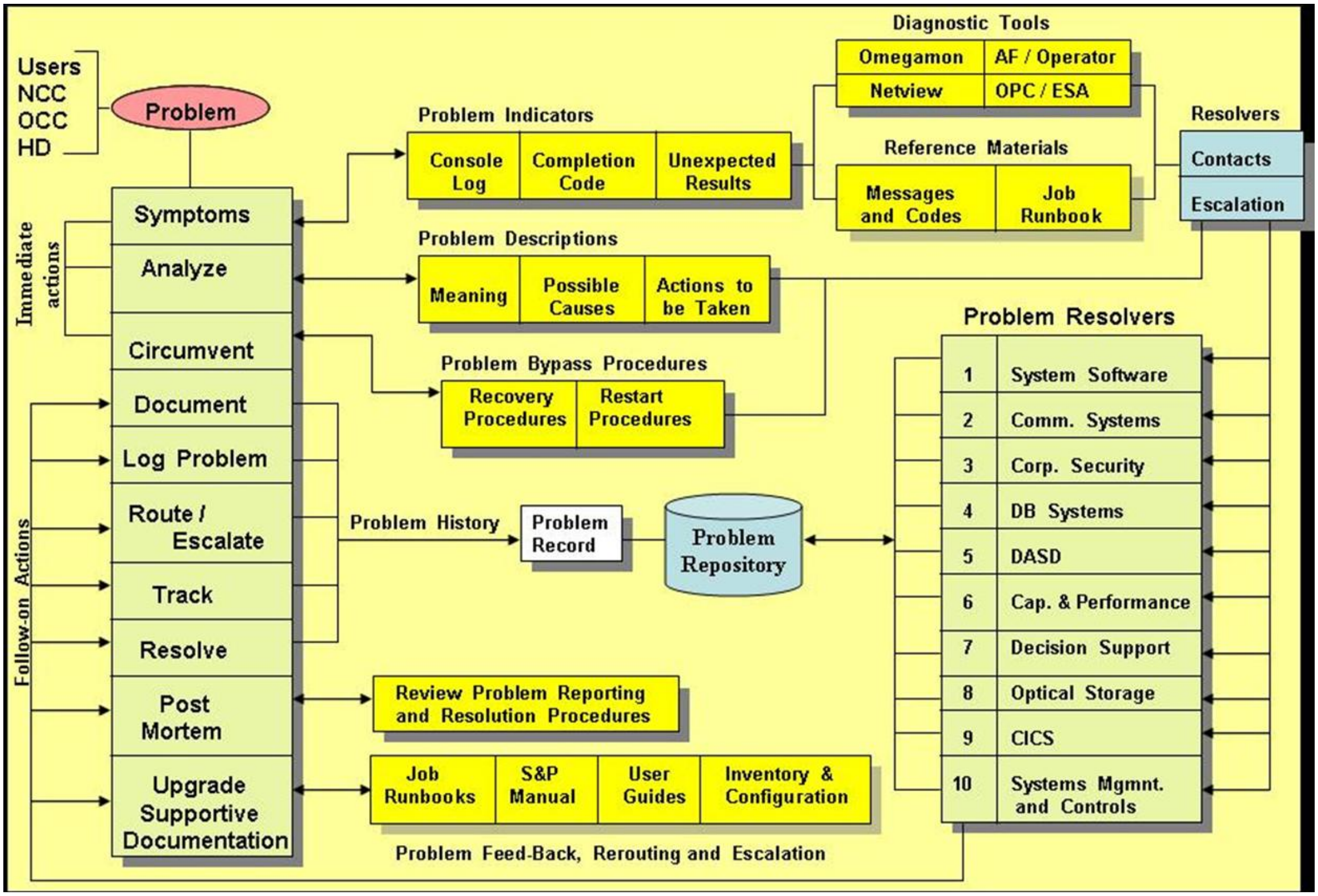
New development requests, enhancements, and problem resolutions are presented to the Development and Maintenance departments and follow the Systems Development Life Cycle (SDLC) described earlier. An enterprise must be able to recover production operations to a secondary site in accordance to SLA / RTO requirements and be able to return to the production site when a disaster event is over. This environment is shown above.

To support this responsibility, Recovery Plans are developed, tested, and implements. There are many types of recovery plans that must be developed, each with sections that must comply with company standards.

The recovery plans are designed to recognize, declare, and respond to disaster events and major incidents that interrupt production operations. Incidents are occurrences that are outside of the normal planning process, like personnel injury, loss of building access, or community problems, while disaster events are those occurrences that affect Information Technology or Business Locations and are events that can be easily planned for.

Support and Maintenance operations are included in the organization and they are responsible for detecting problems and incidents that interrupt business operations and initiating repair / recovery procedures. They are shown in the next two illustrations.

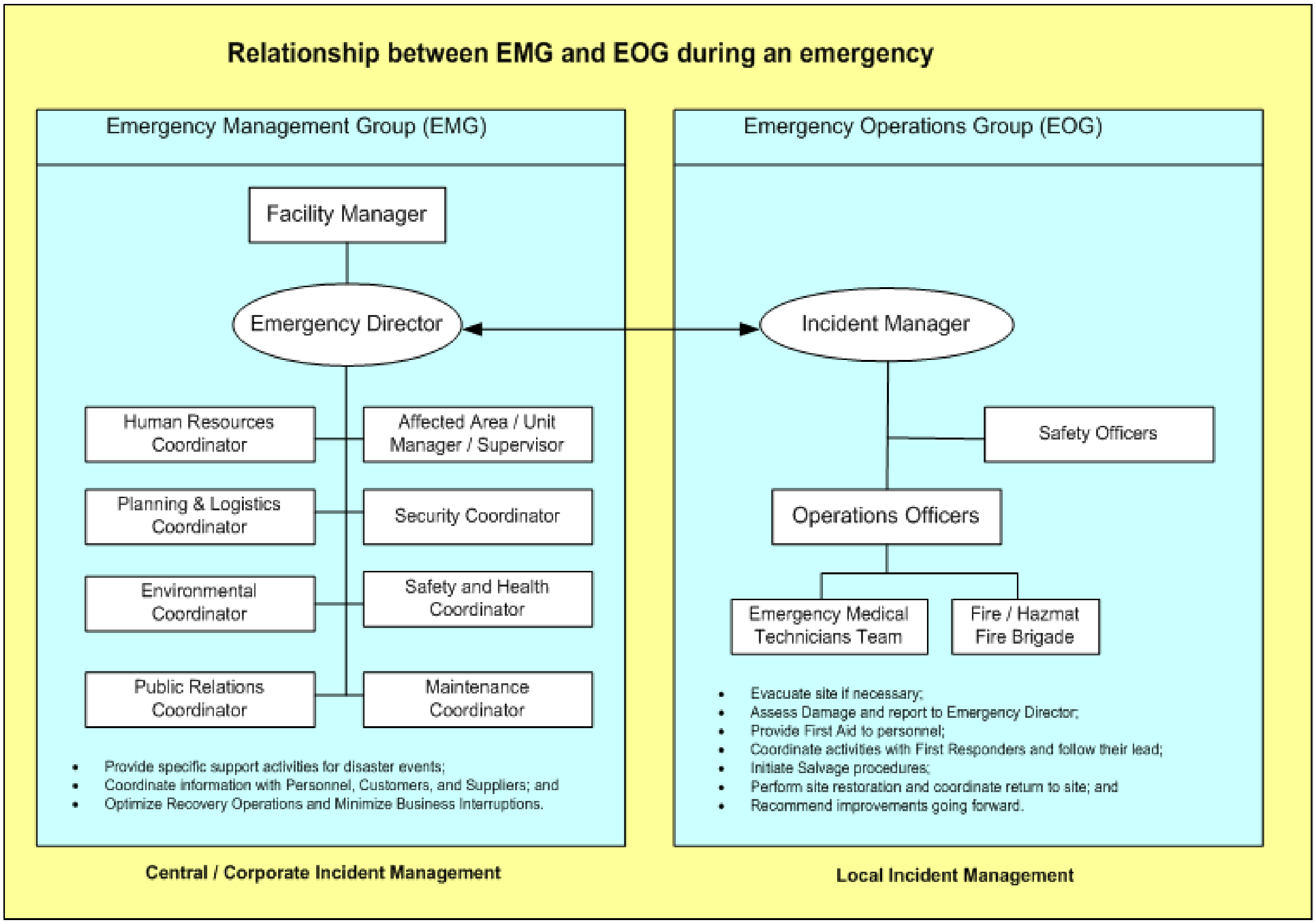
Problem Recognition and Circumvention Techniques



How problems are recognized, circumvented and reported is shown above. Some problems are repeats or easy to repair (Level 1). These problems are repaired by Help Desk personnel. Other problems may require that the Subject Matter Expert become involved in resolving the problem (Level 2), while even harder problems will require the vendor to repair the problem (Level 3). On rare occasions the problem results in a disaster event

(Level D) and the initiation of a recovery plan. These problems are routed to the Contingeny Coordinator associated with the problem type and they enact a Contingency Command Center / Emergency Operations Center environment to react to the disaster event.

Incident Management Organizational Structure



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

Incidents are similar to problems, but are usually related to unplanned for natural or other events not normally included in recovery planning. Incidents usually include medical emergencies, bio hazards, transportation failure and issues, weather caused emergencies like downed lines or trees, flash floods, etc.

First Responders and Emergency Managers will usually take direct control over incidents. Remote Incident Command Centers are responsible for supplying incident response though a limited staff, while Corporate Incident Command Centers are fully staff and provide additional support to remote locations.

Incident Command Centers (ICC) are similar to Contingency Command Centers (CCC) in that they are responsible for contacting personnel responsible for responding to specific types of incidents. They are both coordinated through the Emergency Operations Center (EOC).

Workplace Violence Prevention Act

June 7, 2008 – 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 (card key, recorders, guards, etc.).

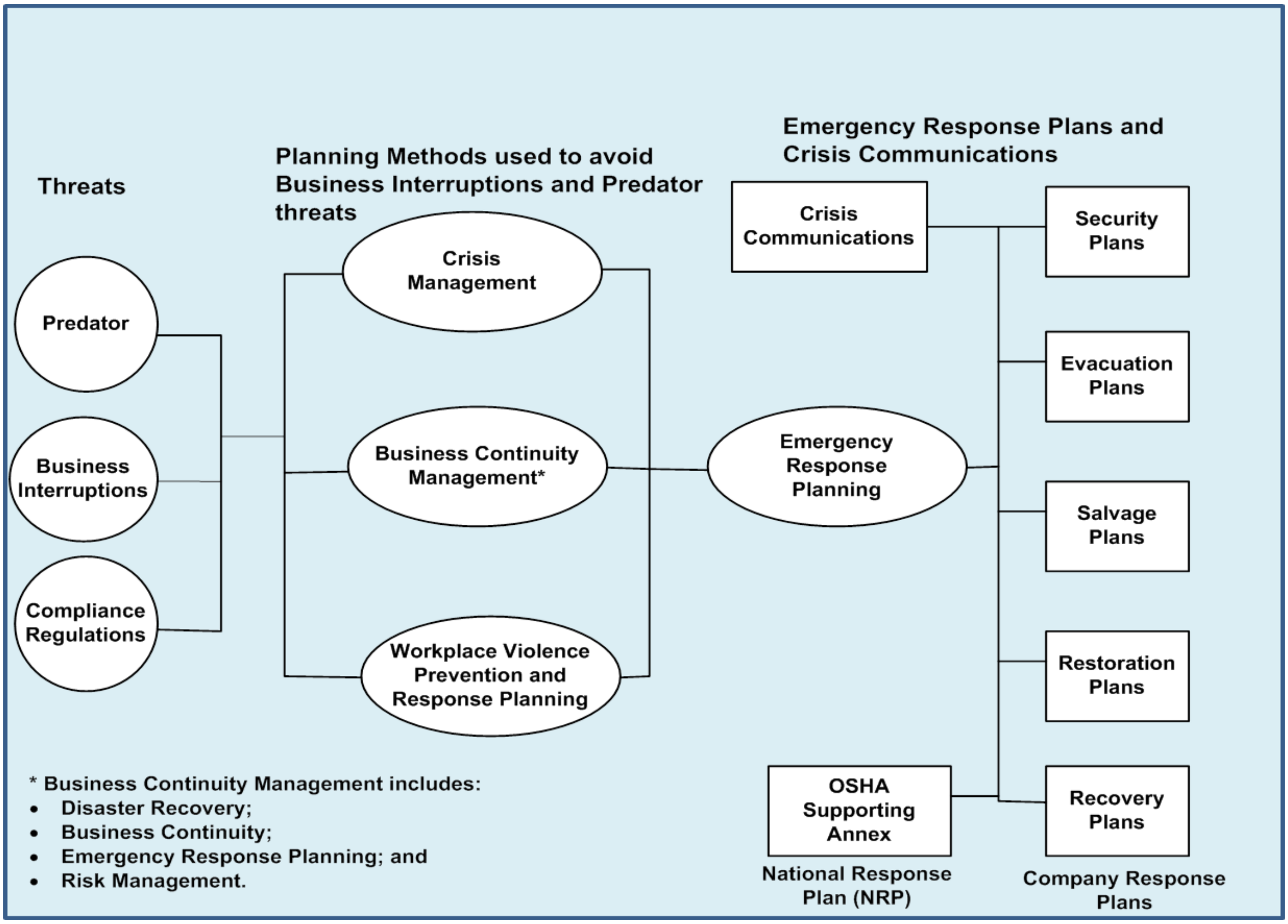
Why Workplace Violence occurs and most likely reasons for offence:

- Number one cause is the loss of a job perceived loss of job.
- Presently being addressed REACTIVELY, but should be addressed PROACTIVELY.
- 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 is $78K, while the average award to a Workplace Violence act is $2.1 million – with 2.1 million incidents a year, 5,000 events a day, and 17 homicides a week.
- Survey found that business dropped 15% for 250 days after an event. Onsite security costs $25K with all preventive costs being under $250 per year (i.e., Guards, Access Cards with restrictions to specific areas, CCTV, Monitoring of CCTV, Evidence Collection and Dissemination, etc.)
- Offender Profile consist of:
  - Loner (age 26 – 40) who was made fun of, teased, and abused by workmates.
  - Culture change has promoted Gun Usage.
  - Their identity is made up of their job, so if you fire them they are losing their identity / lifecycle and will respond violently.
  - Instead of Workplace Violence, perpetrator may use computer virus, arson, or other methods to damage / sabotage / ruin the business.
  - Hiring tests can be used to identify potential Workplace Violence perpetrators.
  - Does not take criticism well and does not like people in authority.

- 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.

By following the rules laid out in the Workplace Violence Prevention Act, your company will develop an environment similar to the one shown in the next illustration.

Workplace Safety and Violence Prevention

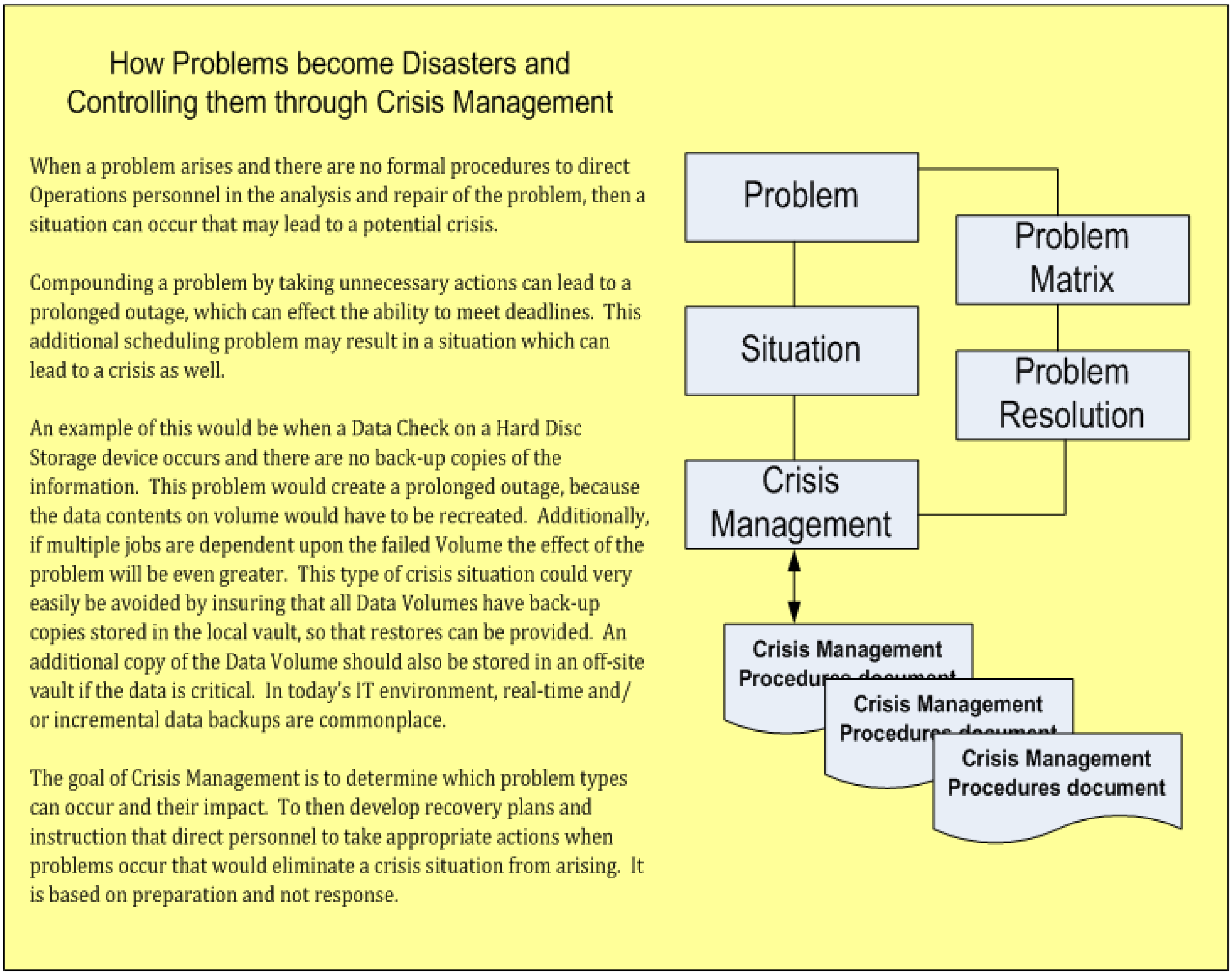

Threats
Planning Methods used to avoid Business Interruptions and Predator threats
Emergency Response Plans and Crisis Communications
Predator
Business Interruptions
Compliance Regulations
Crisis Management
Business Continuity Management*
Workplace Violence Prevention and Response Planning
Crisis Communications
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.

Threats are detected, classified, related to recover activities, and responded to so that people are protected and company operations can continue with minimal interruption.

Crisis Management and responding to 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.

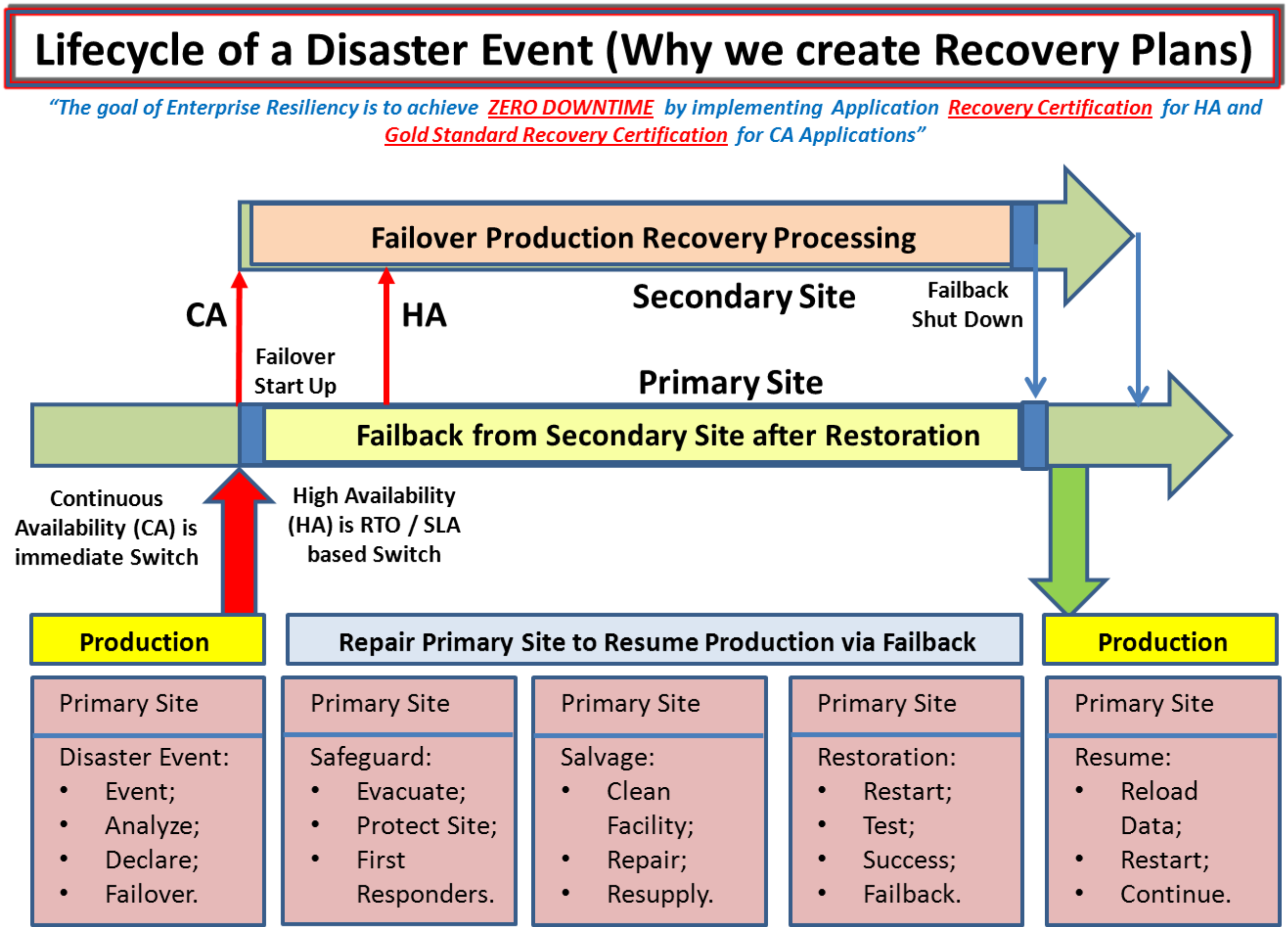
The goal of Crisis Management is to determine which problem types can occur and their impact. To then develop recovery plans and instruction that direct personnel to take appropriate actions when problems occur that would eliminate a crisis situation from arising. It is based on preparation and not response.

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

Problems sometimes grow into crisis situations when response plans are not created and followed as illustrated above. It is therefore imperative that Risk Management uncovers potential problems and Crisis Management plans created to respond to these potential problems.

Properly responding to crisis events will eliminate many problems from occurring and help sustain uninterrupted production operations.

The Disaster Life Cycle



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

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

Failover Production Recovery Processing

Secondary Site

Failback Shut Down

CA

HA

Failover Start Up

Primary Site

Failback from Secondary Site after Restoration

Continuous Availability (CA) is immediate Switch

High Availability (HA) is RTO / SLA based Switch

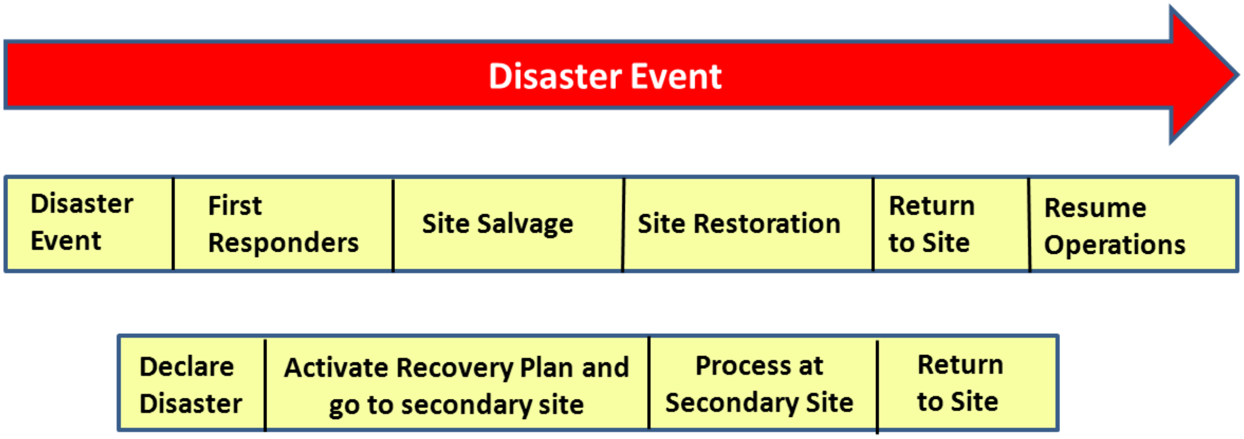
Production	Repair Primary Site to Resume Production via Failback			Production
Primary Site	Primary Site	Primary Site	Primary Site	Primary Site
Disaster Event: • Event; • Analyze; • Declare; • Failover.	Safeguard: • Evacuate; • Protect Site; • First Responders.	Salvage: • Clean Facility; • Repair; • Resupply.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

Disasters have a Life Cycle that is shown below. When a disaster event occurs, it must be recognized and acted upon appropriately. This initial action is included in a recovery plans initial problem analysis section. Once recognized, the problem is reported to management and the Help Desk. Management will determine if a disaster plan should be initiated and they will notify the recovery plan coordinator that actions must be taken. At that point, recovery actions are communicated between the Contingency Command Center (CCC), Emergency Operations Center (EOC), Executive Management, and Help Desk personnel. The events associated with a disaster event include:

- Primary Site operations are interrupted by a disaster event.
- Recovery Plan is activated and Contingency Command Center / EOC activation occurs.
- Help Desk is kept informed of recovery operations so they can communicate to personnel.
- Recovery Operations are initiated at Secondary Site.
- Security, Salvage, and Restoration activities are performed at Primary Site.
- Business Operations are continued at Secondary Site, with appropriate escalations as time passes.
- Business Operations is restored at Primary Site after the disaster event and the primary site is ready to continue business as normal.

Security, Salvage, and Restoration procedures

Responding to Disaster Events



Disaster Event

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

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

Site Security, Salvage, and Restoration is initiated when a disaster event occurs and is responsible for protecting, salvaging, and repairing the primary site in preparation for the production staff returning to the primary site to resume normal production operations. Their function begins when the First Responders declare the site clear for repair and reoccupation.

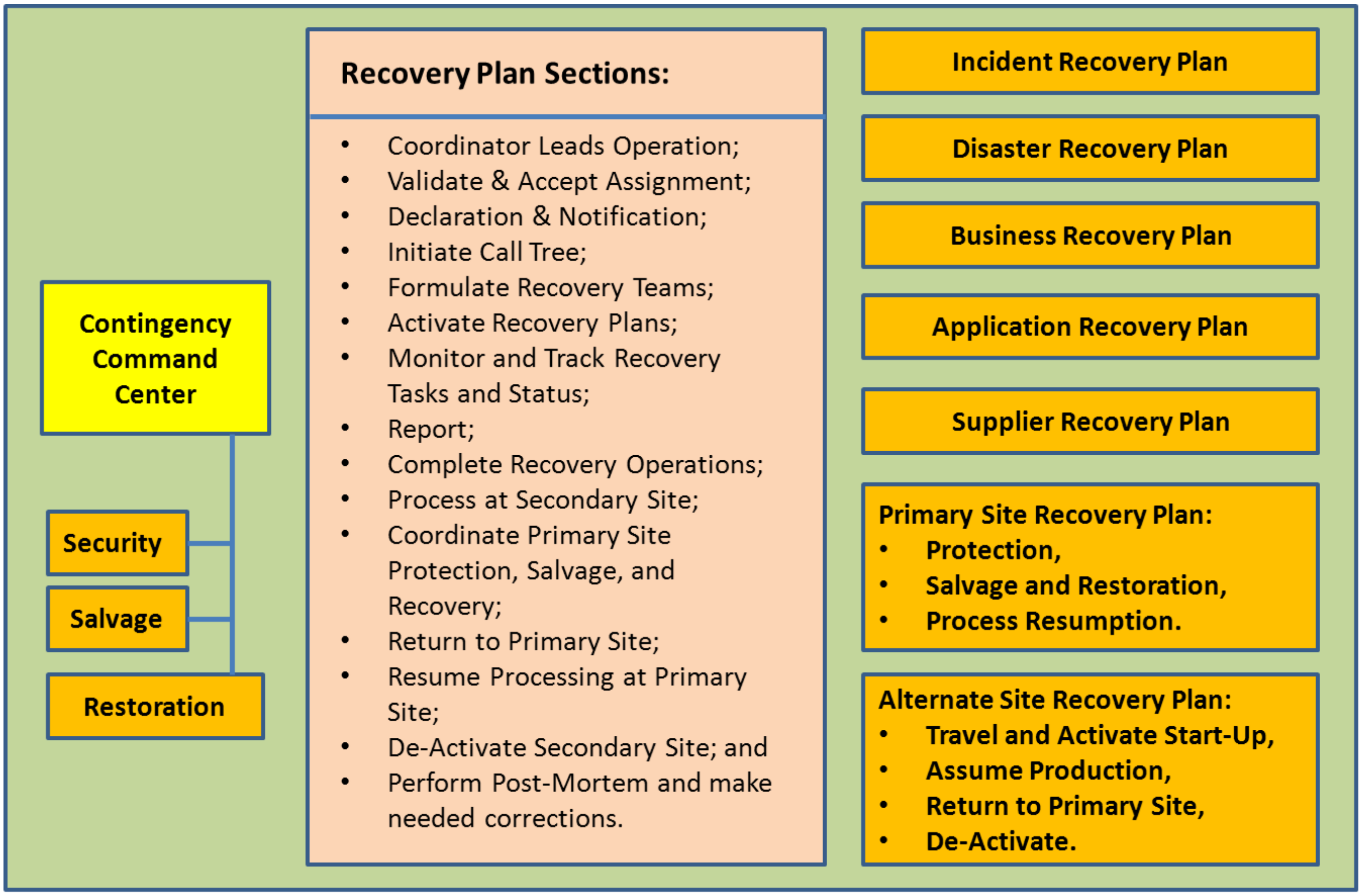
Site security is initiated immediately after a disaster is declared so that personnel are safely evacuated and building safety is provided. Security also insures equipment, supplies, or other critical business information is not taken from the premises, because espionage can take many faces or opportunist can seize the disaster event to illegally acquire business valuables. Company security coordinates activities with the local police department.

First Responders (consisting of the police, fire department, and emergency medical technicians) will perform their tasks immediately upon arrival on the scene. In some cases the building or affected area will be cordoned off which would interfere with normal business operations. You can usually be assured that the crime scene, or affected area, will be off-limits for multiple hours so the initiation of recovery plans should occur immediately when first responders are called to a business location.

Salvage and Restoration for sites is accomplished by companies like **ServePro** who are contracted to clean the affected area, salvaging any equipment or other business documents that may have been damaged, and then performing restoration activities needed to allow for the return of personnel after a disaster event.

By **combining Enterprise Resiliency with Salvage and Restoration** organizations, it may be possible to quicken recovery operations by having a partner who can better protect, salvage, and repair a location suffering from a disaster event because they helped develop the recovery plan and have participated in recovery plan testing. Utilizing companies like ServePro in a partnership type of arrangement will enhance recovery planning and operations because they have a unique perspective on how a disaster can affect a company's operations and how long it normally takes to recovery a primary site after a disaster event.

Types of Recovery Plans and their Sections



Contingency Command Center

Security

Salvage

Restoration

Recovery Plan Sections:

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

Incident Recovery Plan

Disaster Recovery Plan

Business Recovery Plan

Application Recovery Plan

Supplier Recovery Plan

Primary Site Recovery Plan:

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

Alternate Site Recovery Plan:

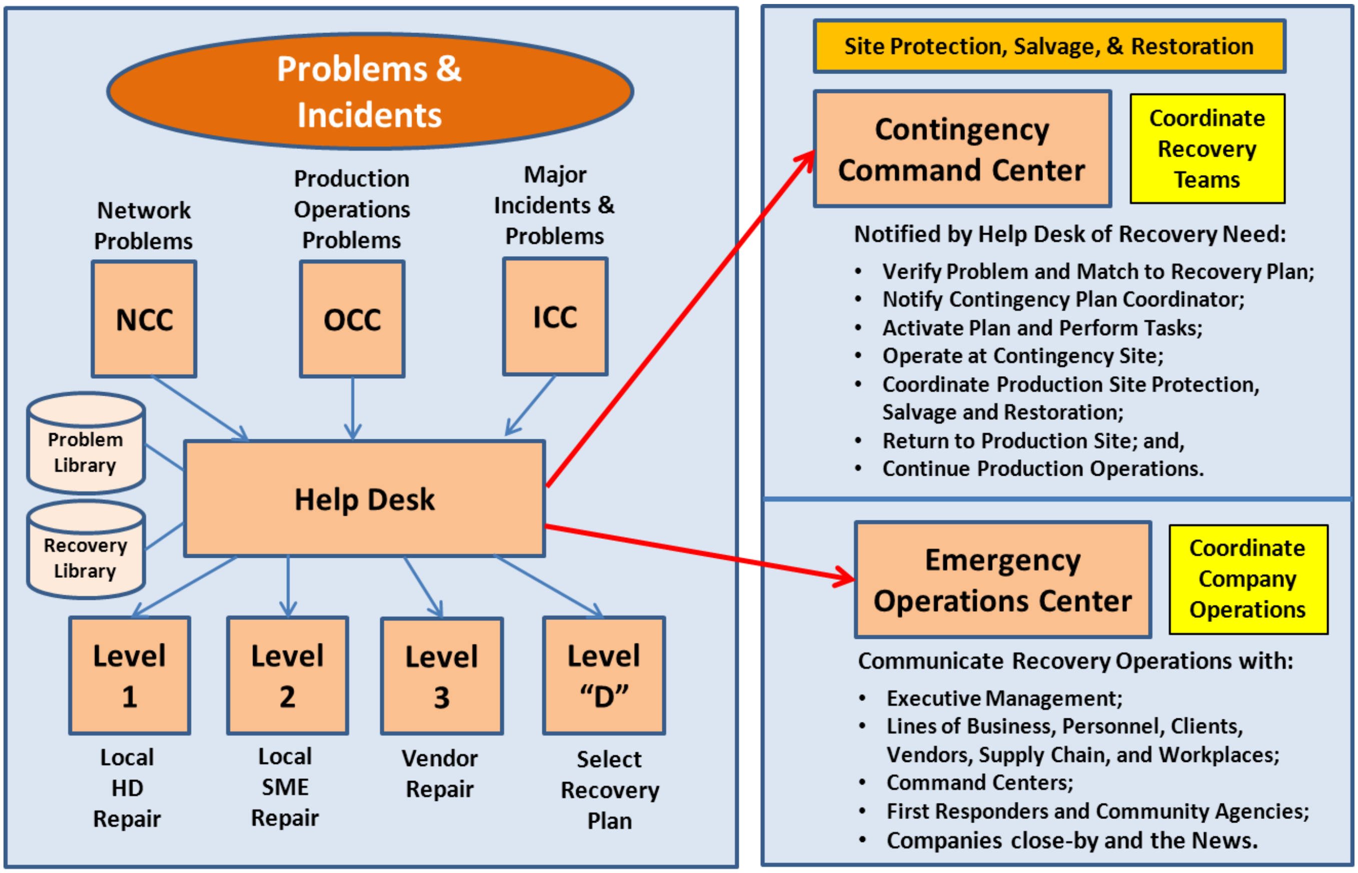
- Travel and Activate Start-Up,
- Assume Production,
- Return to Primary Site,
- De-Activate.

Once recovery plans are created, they must be identified, declared, and acted upon which requires interactions between end-users, command centers, and management.

Problems are detected by command centers (NCC for Network Problems, OCC for Operations Problems, ICC for Incidents) and reported to the Help Desk. The Help Desk records the problem and initiates problem resolution efforts. Level I problem resolutions are those that can be accomplished by the Help Desk directly (like password changes or repeat problems where resolutions have already been identified), Level II problem recovery is performed by the Subject Matter Expert associated with the failure, Level III problem resolution is accomplished by the Vendor, and Level "D" problem resolutions are provided when the Help Desk relates the problem to a recovery plan and notifies the Contingency Command Center (CCC) of the disaster event.

The Contingency Command Center (CCC) will validate the disaster event and notify the Contingency Coordinator associated with that recovery plan. The Contingency Coordinator will initiate the recovery plan by calling recovery team members and starting recovery operations. The CCC will coordinate recovery operations with the Emergency Operations Center (EOC) which is established when a disaster is declared. The EOC will coordinate business operations and communicate disaster event status with Executive Management. Executive Management is responsible for communication recovery status to the clients and outside world.

Activating and Coordinating Disaster Recovery Plans


Problems & Incidents
Network Problems
Production Operations Problems
Major Incidents & Problems
NCC
OCC
ICC
Problem Library
Recovery Library
Help Desk
Level 1
Level 2
Level 3
Level "D"
Local HD Repair
Local SME Repair
Vendor Repair
Select Recovery Plan
Site Protection, Salvage, & Restoration
Contingency Command Center
Coordinate Recovery Teams
Notified by Help Desk of Recovery Need:
Verify Problem and Match to Recovery Plan;
Notify Contingency Plan Coordinator;
Activate Plan and Perform Tasks;
Operate at Contingency Site;
Coordinate Production Site Protection, Salvage and Restoration;
Return to Production Site; and,
Continue Production Operations.
Emergency Operations Center
Coordinate Company Operations
Communicate Recovery Operations with:
Executive Management;
Lines of Business, Personnel, Clients, Vendors, Supply Chain, and Workplaces;
Command Centers;
First Responders and Community Agencies;
Companies close-by and the News.

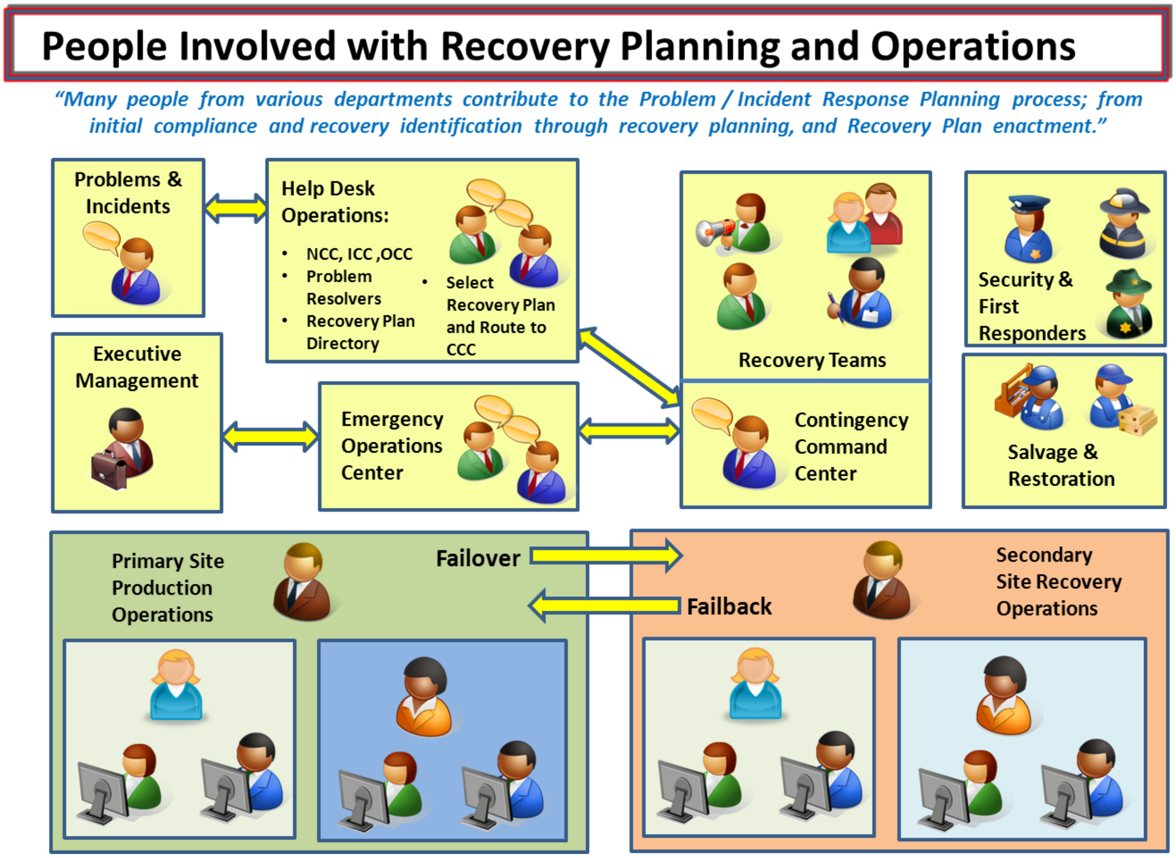
Disaster Recovery Plans can be initiated by the Help Desk when normal recovery actions cannot resolve the encountered problem or incident. The Help Desk would record the problem and the results of problem circumvention procedures, then they would first try to repair the problem themselves (Level I), or escalate the problem to the Subject Matter Expert (SME) responsible for the failing component (Level II). If the SME cannot resolve the problem, it is escalated to the failing components Vendor (Level III). If all repair attempts fail, the Help Desk will escalate the problem to Level "D" and declare a disaster event has occurred. The Help Desk then refers to its library of Recovery Plans and picks the plan that best responds to the disaster event. The Help Desk then contacts the Contingency Command Center who validates the recovery plan is appropriate to the encountered disaster event and then they contact the Contingency Coordinator related to the plan.

The Contingency Coordinator would activate the recovery plan and perform all tasks contained in the plan from notification through relocation to the secondary site and the resumption of production processing at the secondary site. Once the primary site has been repaired and is ready to receive personnel and resume normal production, the Contingency Coordinator will manage the return to the primary site and the resumption of normal production processing.

The Emergency Operation Center (EOC) coordinates business operations to minimize the impact of the disaster and communicates with Executive Management on the status of the disaster event, while Executive Management is responsible for communicating with clients and the outside world on when normal business operations will be resumes and the extent of the damage suffered during the disaster event.

An illustration of the many people involved with recovery operations is provided below, while Physical Recovery Operations and Logical Recovery Operations illustrations are provided on later pages to demonstrate the “End Goal” associated with achieving Enterprise Resiliency and Corporate Certification.

Many people are affected by the disaster and incident management process



People Involved with Recovery Planning and Operations

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

Problems & Incidents

Help Desk Operations:

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

Recovery Teams

Security & First Responders

Executive Management

Emergency Operations Center

Contingency Command Center

Salvage & Restoration

Primary Site Production Operations

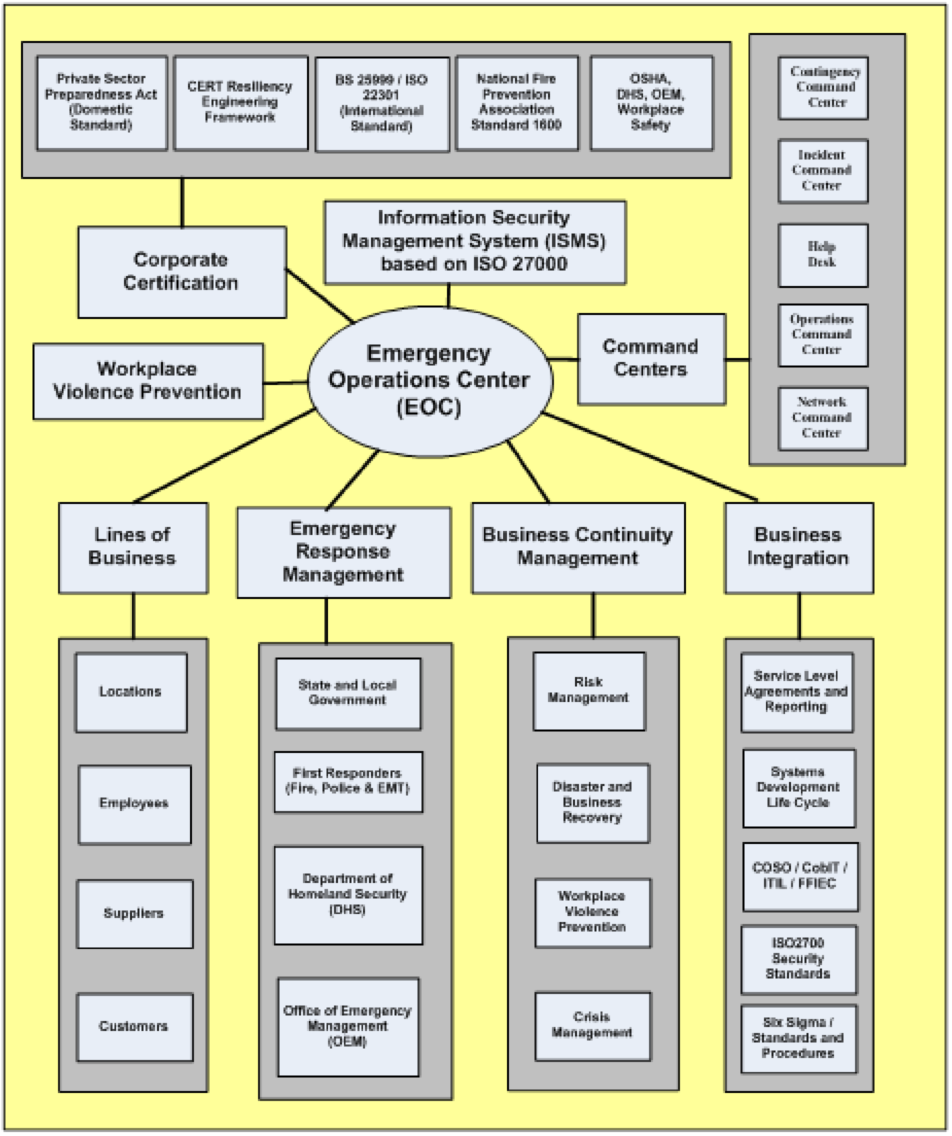
Failover

Failback

Secondary Site Recovery Operations

The above illustration demonstrates the many people involved in recovery operations and support the logistic, documentation, and training problems associated with recovery management

Fully Integrated Recovery Operations and Disciplines (Physical End Goal)

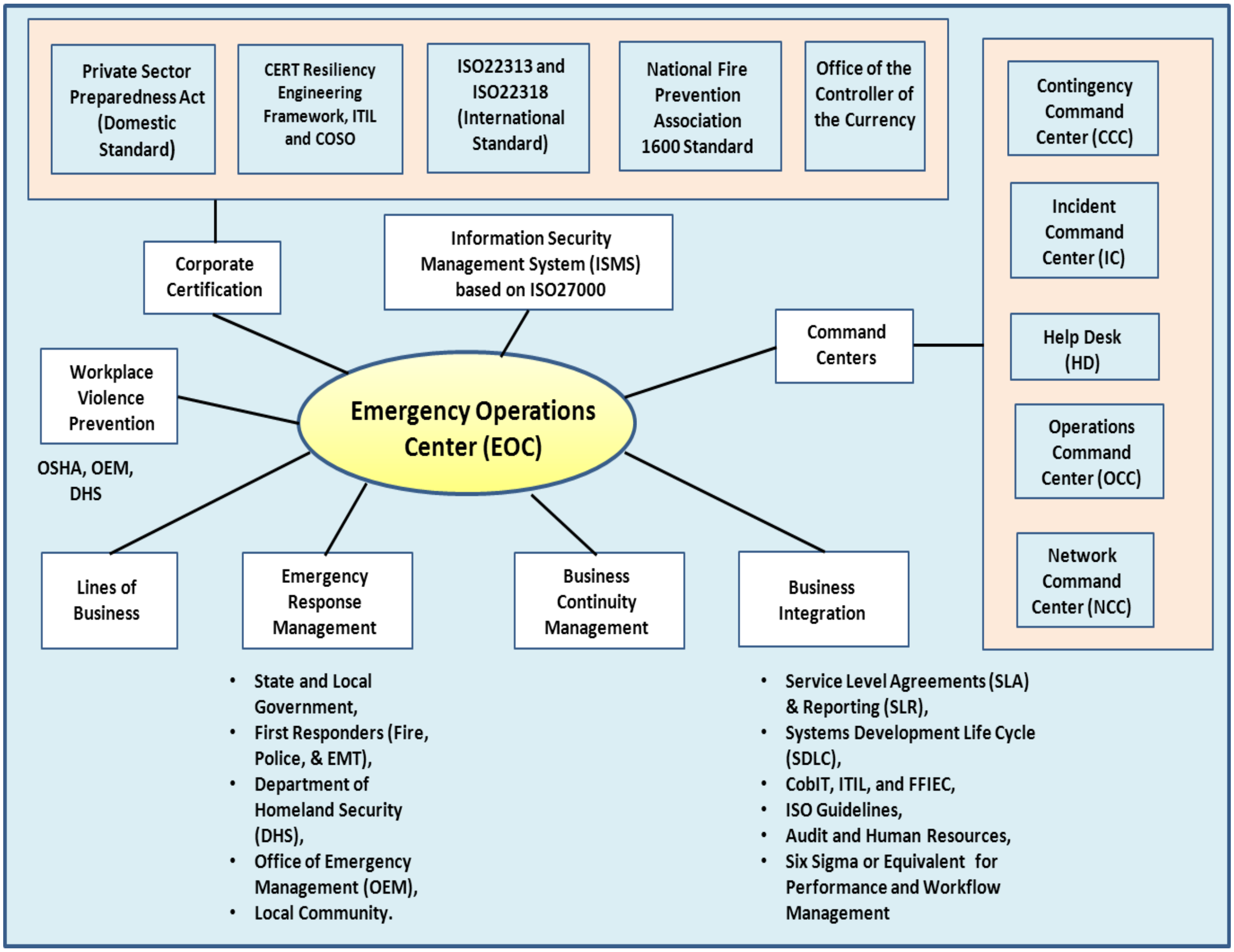

Private Sector Preparedness Act (Domestic Standard)
CERT Resiliency Engineering Framework
BS 25999 / ISO 22301 (International Standard)
National Fire Prevention Association Standard 1600
OSHA, DHS, OEM, Workplace Safety
Contingency Command Center
Incident Command Center
Help Desk
Operations Command Center
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

The EOC is activated when a disaster event occurs. It communicates with the Help Desk, Contingency Command Center, Business Units, and Executive Management in order to coordinate recovery operations and maintain business requirements associated with Corporate Certification and Enterprise Resiliency.

The EOC coordinates activities with the Lines of Business, the Emergency Response Teams, the Business Continuity Management Teams, and for insuring that Business Integration requirements like SLA/RTO, SDLC, Risk Management, Security, and Workflow are maintained.

Corporate Certification is maintained from the EOC by insuring that compliance requirements are adhered to domestically and internationally, as needed, and the EOC insures that a Safe Workplace in maintained and that Workplace Violence Prevention guidelines and protections are supported at all times

Fully Integrated Resiliency Operations and Disciplines (Logical End Goal)


Private Sector Preparedness Act (Domestic Standard)
CERT Resiliency Engineering Framework, ITIL and COSO
ISO22313 and ISO22318 (International Standard)
National Fire Prevention Association 1600 Standard
Office of the Controller of the Currency
Contingency Command Center (CCC)
Incident Command Center (IC)
Help Desk (HD)
Operations Command Center (OCC)
Network Command Center (NCC)
Corporate Certification
Information Security Management System (ISMS) based on ISO27000
Command Centers
Workplace Violence Prevention
OSHA, OEM, DHS
Emergency Operations Center (EOC)
Lines of Business
Emergency Response Management
Business Continuity Management
Business Integration
• State and Local Government,
• First Responders (Fire, Police, & EMT),
• Department of Homeland Security (DHS),
• Office of Emergency Management (OEM),
• Local Community.
• Service Level Agreements (SLA) & Reporting (SLR),
• Systems Development Life Cycle (SDLC),
• CobIT, ITIL, and FFIEC,
• ISO Guidelines,
• Audit and Human Resources,
• Six Sigma or Equivalent for Performance and Workflow Management

This illustration is used to show the logical components that comprise Enterprise Resiliency and Corporate Certification, including regulatory requirements, command centers, response management, and the business units. It shows the optimum method for coordinating emergency responses and is generally utilized by government and business organizations all over the world.

By achieving this goal you will insure that the corporation is receiving optimum protection against business interruptions that would negatively affect the company reputation. Through this process, the company's reputation will be enhanced should a disaster event occur because the company response will be shown as effective and well thought out. This can actually result in better retention of existing clients and the possible addition of new clients who want to have their services provided by a company who prepares to respond to normal and disaster events.

Achieving Enterprise Resiliency and Corporate Certification will allow a company to optimize production operations and enhance its reputation world-wide. It is the direction that all companies will eventually have to achieve in order to stay competitive, so why wait when you can be considered as an industry leader instead of a laggard. Reaping the many benefits of Enterprise Resiliency and Corporate Certification will improve efficiency and the bottom line. *"What's not to lose…."*

If you would like help to achieve Enterprise Resiliency and Corporate Certification I would be delighted to assist you in your endeavor. Simply contact me to schedule a meeting or phone discussion.

About the Article and the Author

Achieving Enterprise Resiliency and Corporate Certification

This article is designed to explain how **Enterprise Resiliency** can assist a corporation maximize their recovery operation by combining the various recovery disciplines and utilizing a common recovery language and tool set, thereby encouraging better communications and recovery techniques. **Corporate Certification** is responsible for insuring that a company complies with the regulatory requirements of the countries that they do business in. **Zero Downtime** objectives and staff awareness and will be improved through the presentations contents. Clear examples are show to help achieve optimized operation using industry Best Practices.

Thomas Bronack Bio.

Tom is a Certified Business Recovery Professional (CBRP) from DRII with a strong Compliance and Recovery Management background. He has over 30 years of technical, managerial, sales, and consulting experience implementing safeguarded environments that comply with business/regulatory requirements. He is adept in planning and improving the efficiency of data processing systems/services by optimizing information technology productivity through automated tools, quality improvements, procedures, documentation, and training. Tom has presented materials and conducted workshops at IFSA, ISACA, ISSA, ACP and CPE User Groups and is presently on the Board of Directors of the NYC Metro Chapter of the Association of Contingency Planners and serves as the Director of Vendor Relations. He can be reached via the contact information listed below.

Thomas Bronack
Phone: (718) 591-5553
Cell: (917) 673-6992
Email: bronackt@dcag.com
Web Site: www.dcag.com