Achieving

Enterprise Resilience

and

Corporate Certification

by

Combining Recovery Operations through a

Common Recovery Language and Recovery Tools,

while adhering to

Domestic and International Certification Standards

Created by:

Thomas Bronack, CBCP
Phone: (917) 673-6992
Email: bronackt@dcag.com
Web Site: www.dcag.com

Creation Date: January 1, 2006
Release Date: July 11, 2013

Table of Contents:

Table of Figures:

The purpose of this document

Management is responsible for providing uninterrupted operations even if a disaster event occurs and their inability to achieve that goal could result in the company suffering penalties from criminal, civil, and regulatory violations. But the worse effect of all is reputational loss which may never be recovered. The aim of this paper is to assist management in identifying problem areas that may affect their ability to provide uninterrupted business operations and achieve the goals of recovery and compliance all within a single approach based on industry best practices. That approach is "Enterprise Resiliency and Corporate Certification" which is meant to address the many operational, recovery, and compliance concerns of management. The approach will optimize Workflow, and integrate Recovery and Compliance within the everyday functions performed by the staff, thereby producing an optimized and safeguarded environment that is always compliance and protected. It addresses the following areas to achieve the goals of Enterprise Resiliency and Corporate Certification:

1. Identify the need to provide continued business operations and adhere to regulatory requirements.
2. Define the types of risks and their financial, criminal, civil, regulatory, and reputational affect.
3. Determine how to best define operational requirements via contracts (SLA, PKI, Service Contract)/
4. Create a Service Level Reporting (SLR) mechanism and provide management with a means to monitor the operational status of the business and respond to any areas that require attention to overcome weaknesses.
5. Assist in the design and implementation of a Systems Development Life Cycle (SDLC) and a Systems Management and Control organization to support the SDLC.
6. Build a Resource Management structure to perform Asset Management, Inventory Management, and Configuration Management throughout the life of an asset.
7. Help management understand how to best implement Recovery Management.
8. Illustrate why Corporate Compliance must be achieved in the countries where business is conducted.
9. Introduce Enterprise Resiliency to combine all recovery disciplines under one organization using a common toolset and speaking a common language that improves efficiency and the knowledge base of all recovery personnel.
10. Create a Corporate Certification organization to guaranty adherence to the laws and regulations that must be adhered to in the countries that the company does business in.
11. Develop an Organizational Structure that will perform all functions associated with Resource Management, SDLC, Recovery Management, Support, and Maintenance.
12. Formulate Functional Responsibilities and Job Descriptions for personnel.
13. Produce Documentation covering Standards and Procedures, User Manuals, Product / Service product manuals, and any other documentation needed to define and support the business.
14. Develop Orientation (new Hires, New Technologies, New Procedures, etc.), Awareness, and Training Programs and provide them to personnel. Assist personnel define and achieve their career path goals whenever possible through training and internal promotion.
15. Develop, test, implement, support, and maintain Recovery Plans.
16. Develop and implement Information Technology and Compliance Audits. Conduct periodic testing to insure compliance in the countries where you do business.
17. Integrate functions associated with business operations, audit, and recovery within the everyday functions performed by personnel and have documentation requirements validated during the Quality Assurance process.

18. Develop methods for identifying Gaps, Exceptions, and Obstacles that impede operations and compliance.
19. Implement compliance reporting, mitigation of gaps an exceptions, and mediation of obstacles when failures are identified.
20. Continue to monitor and improve operations going forward.

Introduction

When an emergency occurs, most companies will activate the Emergency Operations Center (EOC) where First Responders take control and direct recovery operations. Unfortunately, First Responders are usually from the Emergency Management discipline and may not be familiar with Business Continuity Management or Workplace Violence Prevention. Valuable time and decision making abilities can be lost due to the different languages and tools used by the various recovery disciplines, thereby exposing the business to confusion, extended outages, and loss of reputation.

The goal of this document is to provide a method to develop a common recovery language and toolset that can be used by all recovery disciplines, resulting in better communications, faster recovery times, and a safeguarded reputation. Domestic and International Corporate Certification guidelines are reviewed to help establish a foundation upon which the company can implement recovery operations, while Best Practices are reviewed to help direct the creation of recovery operations in adherence to industry accepted practices. By following these guidelines, your company will be prepared to incorporate new and updated recovery techniques as they are introduced and accepted by the industry. You will also be confident that you are developing recovery operations that have a wide acceptance by industry.

This paper is designed to illustrate the complexity of today's corporate recovery operations, now referred to as **"Enterprise Resiliency"**, and the many components that have to be considered when developing and integrating this most critical business function. Because of this complexity, it is essential that your direction and the techniques used to achieve Enterprise Resiliency establish a solid foundation supporting the development of Recovery Operations that provides a common language and toolset for the integration of:

- Emergency Management;
- Business Continuity; and
- Workplace Violence Prevention.

Many companies have responded to this issue by developing a set of standards and procedures that will help them implement Enterprise Resiliency in accordance with industry Best Practices. As a result of this path, a company can achieve Corporate Certification in its implementation and integration of Enterprise Resiliency disciplines. This document will describe Corporate Certification guidelines; Emergency Management functions and responsibilities; Workplace Violence Prevention functions and responsibilities, and how to integrate these disciplines within the Systems Development Life Cycle (SDLC) so that new developments and maintenance to Enterprise Resiliency are kept current and able to best support continuous business operations.

If your company is new to recovery management, or interested in incorporating Enterprise Resiliency, then this document will provide:

- An understanding of existing recovery disciplines;
- Corporate Certification and Best Practices guidelines;
- A Business Plan and a Project Plan to help implement Enterprise Resiliency and Corporate Certification;
- Integrating Recovery Operations with the Systems Development Life Cycle; and
- Providing personnel with Job Descriptions and Standards and Procedures.

Executive Management is responsible for continued business operations

Today, most companies are **dependent upon Information Technology** to present, sell, implement, support, and maintain products and service for their clients and prospects. Should a company's business be interrupted because of a loss of Information Technology Services, it would suffer a revenue loss proportional to the duration of the outage and the clients affected (e.g., outage cost = duration X number of clients x revenue potential for example 60 minute outage affecting 125 customers at an average loss per customer of $5 is 60 * 125 * 5 - $35,500) This would be considered a small outage when compared to the cost of an outage for a large company or financial institution. It is the responsibility of Risk Management to identify risk exposures and calculate their impact on the business. They would then present their finding to Executive Management who decides if it is cost justified to repair the problem or purchase insurance to protect against the occurrence.

Should an outage occur, whose potential had previously been reported, then the company and Executive Management would be liable for damages and the company reputation could suffer unrecoverable damage. If recovery plans are in place to respond to disaster events, then the company and its clients are less exposed to outages, failure to comply, and even more damaging – a loss of reputation. You can recover from an outage, calm clients over time, but repairing a company's reputation has been shown very hard indeed. Because of all these potential problems and their impact on the business and management, it is imperative that an approach be developed that would produce a "Safeguarded and Efficient Business Environment" that is capable of responding to and recovering from disaster event while complying with the laws and regulations of the countries they do business in. The purpose of this document is to show you an approach that will help you achieve that goal.

How to protect your business environment

How do you protect an environment that is so diverse and constantly changing? How do you keep your staff informed of and trained on products, procedures, and changing objectives? What guarantees can you provide that a quality product or service is delivered? Is operations and support informed of potential error conditions and successful output checks for products and services? Are they provided with "Messages & Codes" to instruct them on the successful completion or encountered problem? Has the Messages & Codes been tested? Do you have Standards and Procedures documenting how tasks are to be performed and to what standard? We can go on, but you get my drift. It is necessary to identify all of the Stakeholders and Participants for every process performed and then make sure that "**Best Practices**" are followed to insure a quality product and service is provided to clients.

A **well trained staff** usually has high morale and will be easier to retain, so providing training and awareness will create a path that will result in a win-win for the company and its personnel. Also happy personnel will reflect the character of a company, making it easier to retain current clients while attracting new business. Now it is a win-win-win – every salesman's mantra.

To **protect against outages** and to insure the delivery of quality products you must first define your business and its clients (including any contract obligations). Then you can accumulate statistics regarding capacity and performance to see how well you have supported your clients and uncover any weaknesses. Next a Risk Analysis (RA) and Business Impact Analysis (BIA) should be performed to identify exposures, gaps, and obstacles that impede your creation of an optimized and compliant environment.

With this in mind, your next step should be to **define your business goals** (Strategic, Tactical, and Operational) and create a Business Plan that can be presented to the Board of Directors, Clients, and Prospects to identify the path you have chosen to achieve an optimized and compliant environment that is capable of recovery from disaster events and maintaining business operational services in accordance to contractual agreements and industry best practices. From this document, a **Systems Development Life Cycle** (SDLC) should be created to identify how products and services are developed, tested, quality assured, production accepted, production processed, supported, maintained, and changed in accordance to **Version and Release Management** concepts. Following this direction will insure that supportive documentation is synchronized with any changes so that personnel will have a high degree of confidence that the instructions and guidelines provided are current and accurate..

An **Organizational Structure** should be developed to separate functional responsibilities in accordance with workflow and controls, like Resource Management, SDLC, Recovery Management, Customer Support, and Maintenance. All personnel should have their **Functional Responsibilities** defined in their **Job Description**, while procedure and guideline **documents** are provided in synchronization with the products and services. Personnel should be provided with **orientation** (upon hire and when new technologies, services, or procedures are creared0, **awareness, and training** as deemed necessary and in accordance with regulatory requirements. This of course will enhance employee knowledge and morale and help retain and recruit people and clients.

All **laws and regulations** that the company must adhere to in the countries that you do business must be identified and their compliance requirements defined. If possible, integrating compliance into the everyday functions performed by personnel will insure continued compliance and the maintenance of recovery operations, thereby reducing outages and protecting the bottom and reputation of the business.

Service Level Agreements (SLA), Performance Key Indicators (PKI), or contractual performance guarantees must be identified and a **Service Level Reporting** (SLR) system developed to identify any deviation to contracted service delivery.

The creation of **Command Centers** where subject matter experts can be utilized to define and repair encountered problems should be developed and implemented. Command Centers consist of:

- **Emergency Operations Center** (EOC) responsible for overall business operations during an emergency situation. They coordinate Command Center Operations, Communicate with Executive Management on status, and make recommendations to return business to normal as quickly as possible.

- **Help Desk** (HD) responsible for accepting problem reports from customers and coordinating their repair via a leveled approach consisting of – Level I is repaired by the Help Desk and is usually a repeated problem that has been previously repaired or a simple repair like a password update; Level II is when the problem is escalated to the Subject Matter Expert (SME) responsible for the failing components; Level II is when the problem is escalated to the Product Vendor for repair; and Level 'D' is when a Disaster Recovery Plan must be initiated to respond to the problem. At this point the Help Desk will transfer the problem to the Plan Manager who will initiate the Contingency Command Center and activate the recovery team.
- **Contingency Command Center** (CCC) is responsible for activating and coordinating Disaster Plan actions and for providing the EOC with status information on the active Disaster Recovery Plan(s).
- **Network Control Center** (NCC) is responsible for monitoring network operations, identifying problems, and taking resolution actions. The NCC will coordinate with the Help Desk and CCC and EOC as necessary.
- **Operations Control Center** (OCC) is responsible for monitoring business processing and the status or jobs, services, and products utilizing information technology resources. They will respond to processing operator requests (WTOR – Write to Operator with Request command), perform supportive services like tape mounts etc., identify error and respond to them, and coordinate with the Help Desk, CCC, and EOC as necessary.
- **Incident Command Center (ICC)** is responsible for responding to incident (which are not the same as a problem which can be previously defined and planned for, incidents reflect natural disasters not directly the responsibility of the firm, or personnel problems like a Heart Attack). The ICC has local branches at business locations that have minimal staff backed up by volunteer's and local First Responders. A corporate ICC is fully staffed and will coordinate responses with local branches.

After achieving these goals, your company may be interested in exploring how "**Enterprise Resiliency**" can combine all recovery disciplines into one organization using the same tools and speaking the same language, which will improve the recovery knowledge base and reduce the outage potential. You may also be interested in incorporating "**Corporate Certification**" guidelines into the charter to guaranty compliance to the laws and regulations of the countries where you do business. The best method for achieving these goals is to use "**Best Practices**" like COSO, CobIT, and ITIL to implement the disciplines.

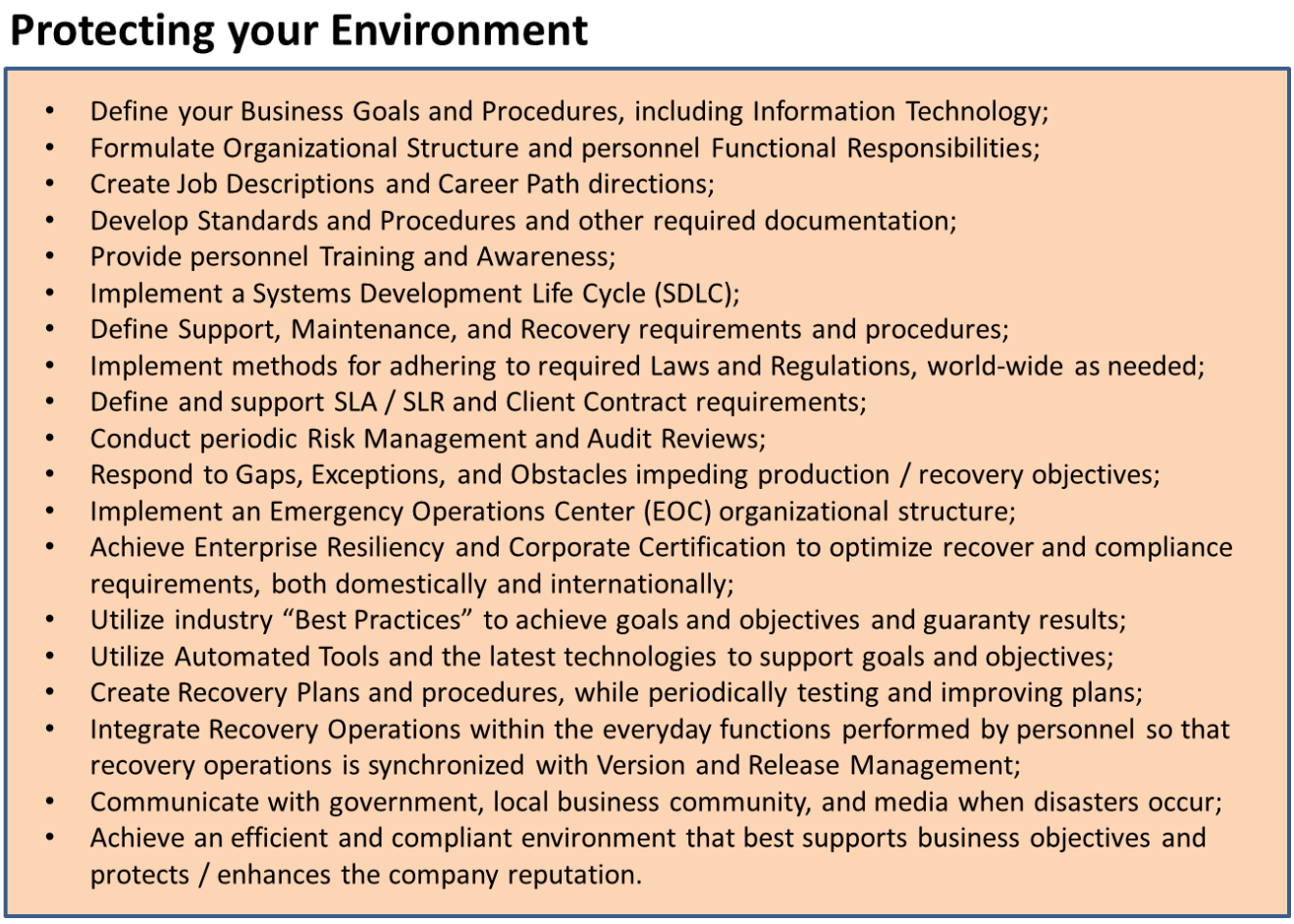
At this point, you should develop **Recovery Plans** (business locations and services / products, applications, and information technology facilities) that adhere to compliance requirements and safeguard the business. These plans should be tested periodically and **integrated into the everyday functions** performed by personnel so that recovery and compliance is always maintained in a current and efficient manner.

An overview of these tasks is shown below.

A review of the material included in this document is provided below. This information will lead to the implementation of procedures to optimize the Systems Development Life Cycle associated with implementing, supporting, and maintaining products and services. Additionally, recovery management and compliance adherence will be integrated within the everyday functions performed by the staff, thereby guarantying that your company is always in compliance and capable of recovering from a wide range of disaster events.

Protecting your Environment

Figure 1: Protecting your Environment



Following the process illustrated above and explained earlier will assist you achieve an optimized and efficient production business environment that is always in compliance and capable of recovering from a wide range of disaster events. It will contain a well thought-out Systems Development Life Cycle (SDLC) that adheres to industry Best Practices, a strong Systems Management and Control (SMC) process that insures quality operation, support, and maintenance, Version and Release Management to guaranty documentation matches products and procedures, a well trained staff, and a high level of morale that is reflected in the company's reputation for quality and compassion.

Why Recovery Management should be accomplished by experts

Figure 2: Recovery Management is Hard and Demanding

Abstract – Recovery Management is hard and demanding on management

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

It is hard enough for management to pay attention to their everyday functional responsibilities, but adding the additional responsibility for recovery management of recovery and compliance may be overwhelming and result in management looking like the poor guy shown above.

With all of the laws and regulations that have to be adhered to, and the many types of recovery plans that require specific viewpoints on protecting resources, it is best to approach recovery planning by utilizing a Subject Matter Expert (SME) who specializes in implementing recovery operations for companies similar to yours. Having this person work with your staff to transfer knowledge will improve the skill level of your personnel and may eventually result in your being able to support recovery operations internally.

Using SME's for Compliance is also a necessity, and sometime a must because of checks and balances included within some of the laws like Sarbanes Oxley (SOX) where the consulting firm is responsible for Attestation of the CIO's compliance and recovery ability.

What can be achieved through Recovery Management

The illustration shown below provides an overview of how Recovery Management can protect the company and help provide continued operation in accordance to client contract requirements and industry guidelines.

Figure 3: Recovery Management Objectives overview

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

These goals can be achieved in a systematic approach that has been performed by many companies over time and are taught by major training organizations like Disaster Recovery Institute International (DRII) when people seek to become Certified Business Continuity Professionals (CBCP).

The goal of Recovery Management is to certify that applications (Services and Products) can recover within a contracted recovery period, or that business locations and their personnel can be relocated to a secondary site should a disaster event block access to the primary location. Recovery Certification is classified as High Availability (recover from 2 – 72 hours) or Continuous Availability which requires an immediate recover without any perceived interruption to the end user. HA (High Availability) applications are recovery certified when they can Failover to a secondary site and Failback to the primary site after a disaster event, while CA (Continuous Availability) applications must be able to Flip / Flop between their primary and secondary sites and to be able to process their workloads at either site for prolonged periods of time. CA recovery certification is considered the "Gold Standard" of Recovery Certification, because it is the end goal of all recovery operations.

What can be received through Enterprise Resiliency and Corporate Certification

The illustration shown below describes some of the advantages received through implementing Enterprise Resiliency and Corporate Certification, but the most important points are:

1. Both normal production operations and recovery operations are maintained through the SDLC.
2. Production and Recovery objectives are integrated within the Version and Release Management function, so you can be assured that current documentation is valid.
3. Audit functions are integrated in the process and reporting is constantly achieved.
4. An added level of protection for production and recovery operations is achieved through the same process, so additional steps are not needed, thereby assuring both production and recovery procedures are completed and validated.

Figure 4: The objective of this document

All regulatory requirements will be identified for every country that the company does business in and audits periodically performed to insure adherence to compliance requirements.

Gaps and Exceptions will be mitigated, while obstacles impeding operations or recovery are mediated. Periodic testing to certify recovery will be constantly performed. Post Mortems will be conducted to incorporate enhancements and repair problems, thereby achieving excellence through this evolutionary approach.

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.

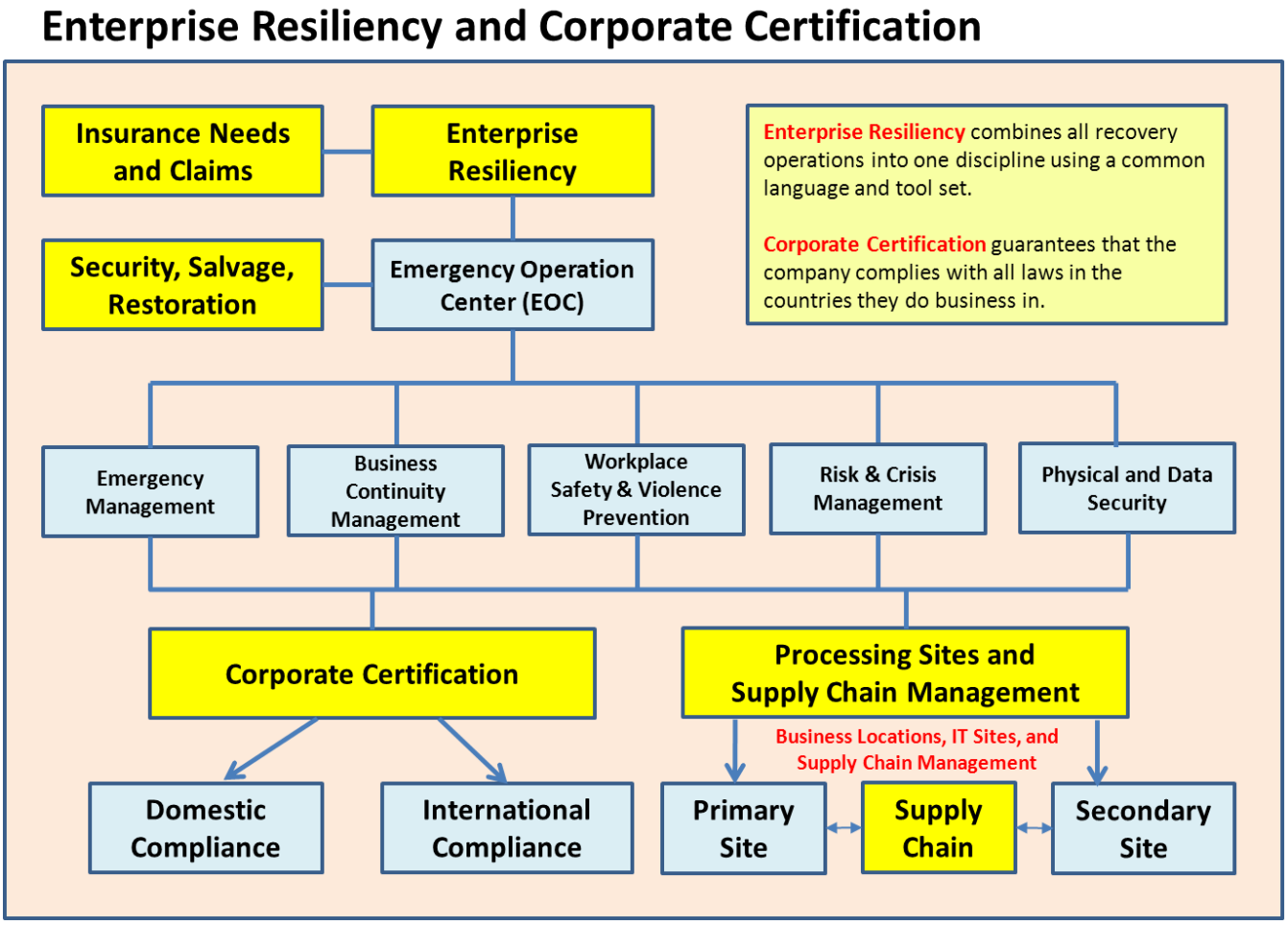
To better protect an organization and adhere to compliance and recovery requirements, organizations are turning to **Enterprise Resilience** to combine all recovery operations and personnel within a single entity that speaks the same language and uses the same tool set, while **Corporate Certification** 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, along with an illustration of the components, including:

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.

Figure 5: What is Enterprise Resiliency and Corporate Certification



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.

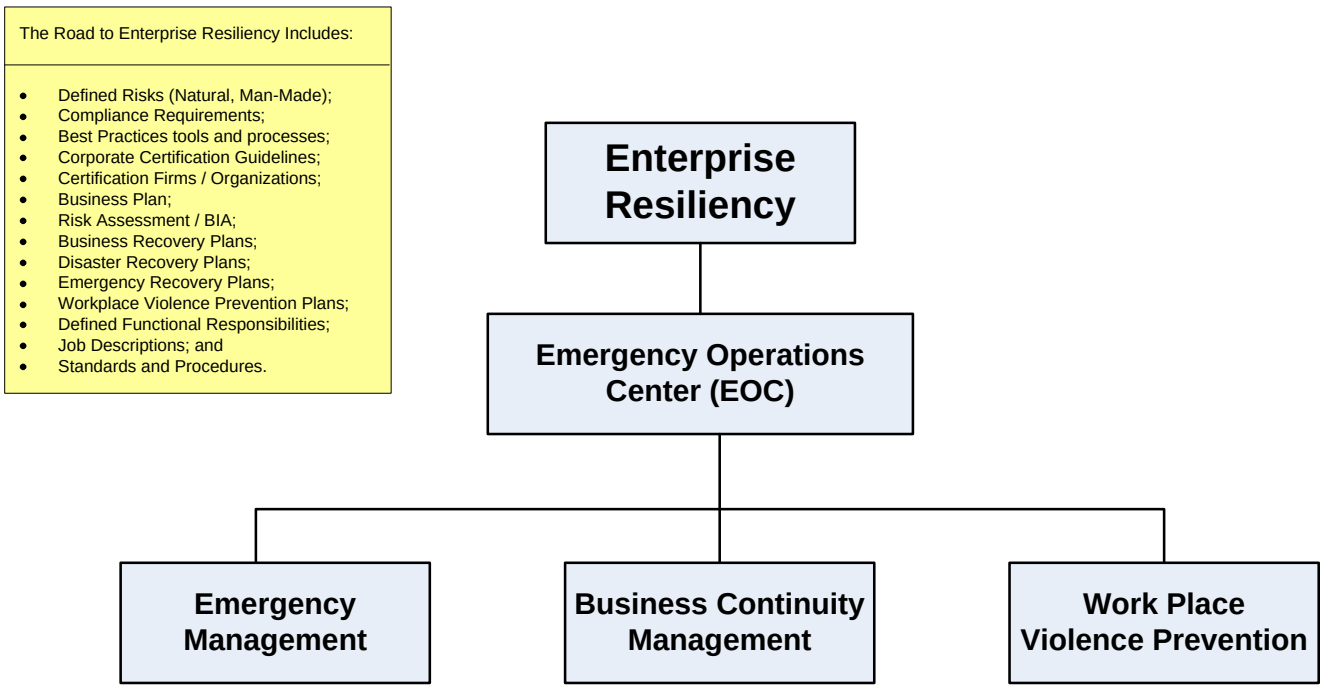
Achieving Enterprise Resiliency and Corporate Certification requires the combined knowledge of the corporation and its participants (i.e., vendors, business associates, etc.), along with a strong knowledge of the laws and regulations that must be adhered to by the company in order to achieve compliance.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

Corporate Certification

Based on international and domestic standards developed by leading corporations and standards committees, achieving Corporate Certification insures clients that companies have implemented Resiliency procedures and processes that meet, or exceed, the most recognized and stringent of standards for Recovery Operations. Enterprise Resiliency is based on the disciplines of Emergency Management Preparedness, Business Continuity Management and Workplace Violence Prevention.

Enterprise Resiliency

Figure 6 - The Enterprise Resiliency Environment



When emergencies occur, the Emergency Operations Center (EOC) is activated and manned by First Responders, Emergency Management personnel, Business Continuity Management (Business Recovery, Disaster Recovery, Crisis Management, and Risk Management) personnel, and Workplace Violence Prevention personnel. Other people work at the EOC in supportive and administrative positions as well. In order to be efficient and to optimize recovery operations, it is essential that all EOC personnel communication and use a common set of tools for analysis, communications, and reporting purposes.

Why implement Enterprise Resiliency and Corporate Certification

Figure 7 - Why implement Enterprise Resiliency and Corporate Certification

Why implement Enterprise Resiliency and Corporate Certification?

The Problem

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

The Solution:

Develop Enterprise Resiliency Operation, including:

- **Emergency Management;**
- **Business Continuity Management; and**
- **Workplace Violence**

Gain Corporate Certification by adhering to industry guidelines, including:

- **BS 25999 (international);**
- **Private Sector Preparedness Act (domestic);**
- **National Fire Prevention Association 1600; and**
- **Certify Recovery Personnel via DRII or BCI training / testing.**

Use Best Practices to achieve goals, including:

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

Integrating Enterprise Resiliency throughout the Corporation, including;

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

The purpose of implementing Enterprise Resiliency is to create a single Recovery Operation consisting of Emergency Management, Business Continuity Management, and Workplace Violence Prevention that utilizes a common language and a common set of recovery tools. Through this effort it will be possible to respond to emergency events in a more accurate manner because less confusion will be experienced due to lack of understanding of terminology and procedures.

Normally it is the First Responders who will be in charge of a disaster event. Although First Responders are extremely knowledgeable in their field, they often do not fully understand Business Recovery, Disaster Recovery, or other disciplines outside of their sphere. By developing a common Recovery Operations language and toolset, this communications problem will be eliminated and a better line of communications will be established throughout the Recovery Operations arena. This will support quicker Recovery Operations and eliminate problems due to a lack of understanding of the various disciplines associated with recovering from disaster events.

The Problem addressed through Enterprise Resiliency is therefore how to optimize recovery operations by:

- Coordinating Recovery Operations for all disciplines;
- Better safeguarding personnel, clients, suppliers, and business operations;
- Improving response to problems and disaster events;
- Developing a common Recovery Language and Toolset throughout the corporation;
- Adhering to compliance requirements;
- Insuring clients and suppliers that recovery operations are sufficient;
- Complying with domestic and international recovery guidelines; and
- Gaining Corporate Certification for Recovery Operations.

The Solution provided through Enterprise Resiliency and Corporate Certification is:

- Develop Enterprise Resiliency Operations;
- Use Best Practices to achieve goals,
- Gain Corporate Certification by adhering to industry guidelines, and
- Integrate Enterprise Resiliency throughout the corporation.

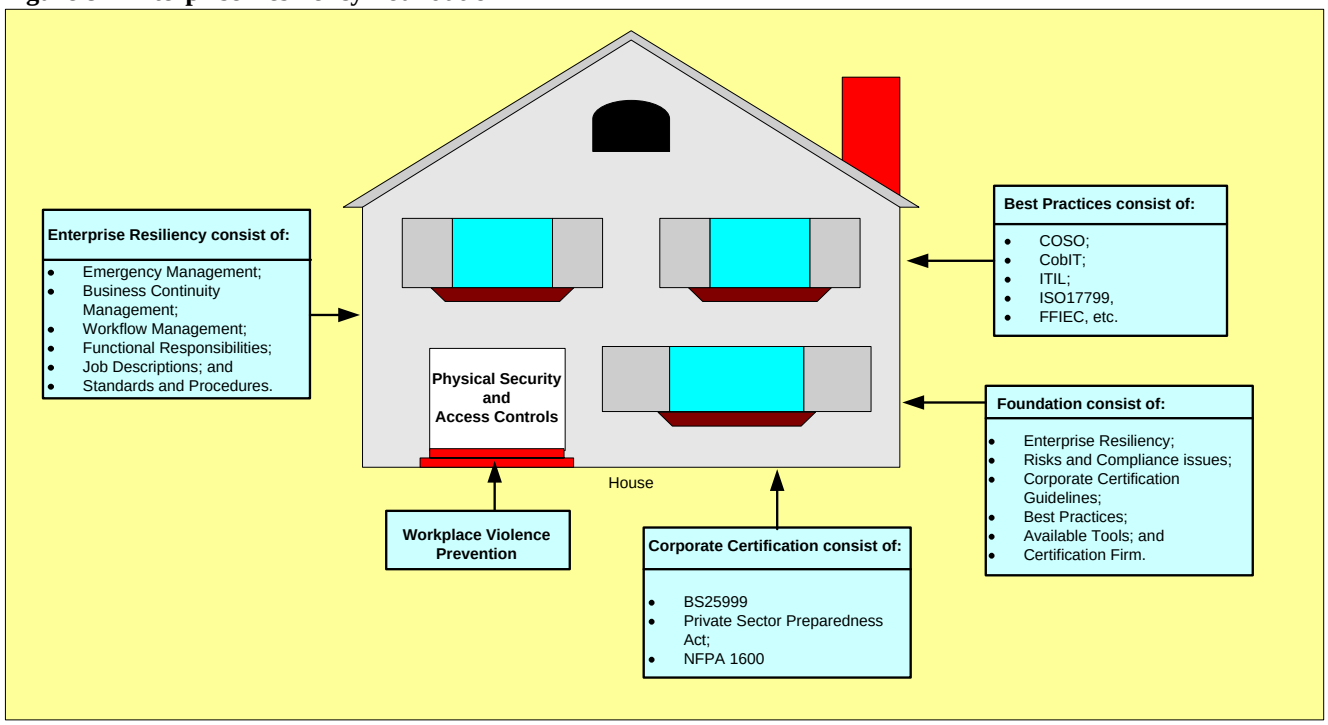
The direction described in this document will help guide you to achieve Enterprise Resiliency by:

- First understanding your problem (Risk Assessment, Compliance requirements, etc.);
- Reviewing existing recovery operations;
- Evaluating Command Centers and their interaction with the Emergency Operations Center;
- Defining Company Lines of Business;
- Documenting Integration Requirements;
- Reviewing common recovery languages and available tools;
- Creating a Enterprise Resiliency Business Plan;
- Developing a Project Plan to Implement Enterprise Resiliency;
- Define Functional Responsibilities and Job Descriptions for personnel;
- Create training and awareness programs describing Enterprise Resiliency and its purpose;
- Help personnel gain certification in their recovery discipline; and
- Integrating Enterprise Resiliency within the Standards and Procedures manual.

When management plans to integrate the many disciplines associated with Enterprise Resiliency they must first start with a solid foundation and then build all of the functional areas used to protect employees, clients, suppliers, and business operations on top of that foundation.

Enterprise Resiliency Requires a Solid Foundation to build on

Figure 8 - Enterprise Resiliency Foundation



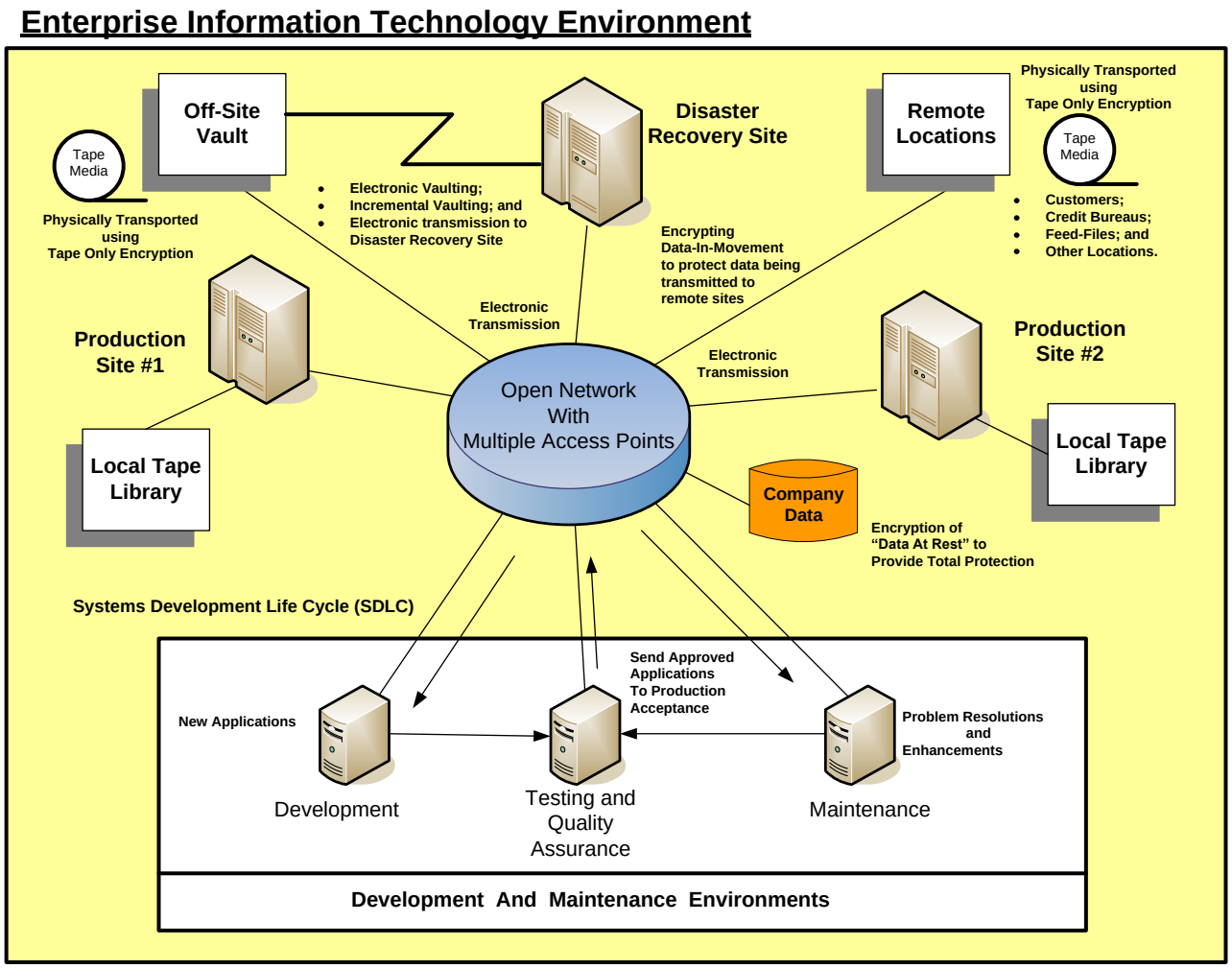
Implementing Enterprise Resiliency is like building a house. If you do not have a solid foundation the house will not survive for long. Likewise when implementing Enterprise Resiliency and gaining a Corporate Certification, you must start with knowing your needs (Risk Assessment) and how to achieve your goals (Business Plan, Best Practices, etc.). The above picture may help visualize how to construct an Enterprise Resiliency environment and obtain a Corporate Certification.

To identify foundation requirements, it is first necessary to identify the Risks and Compliance issues that a company must respond to. Then tools and processes used to achieve Best Practices can be selected and Corporate Certification Guidelines researched to best define the direction that the corporation should take to achieve Enterprise Resiliency. A Certification Firm / Organization must be selected so that Certification can be achieved, because an outside firm must be used to approve certification.

Once these components are put in place, the corporation can develop a Business Plan that will define the steps that need to be performed in order to achieve Enterprise Resiliency and Corporate Certification. These steps include a Risk Assessment and a BIA, the development of Business Recovery Plans, Disaster Recovery Plans, and Emergency Management Preparedness Plans. After building and testing these plans, the corporation can define the functional responsibilities that must be performed and create Job Descriptions for personnel. Finally Standards and Procedures can be created and used to guide personnel in the performance of their assigned functional responsibilities.

Enterprise Resilience and the IT Environment

Figure 9 - Overview of IT Environment



Applications are created in the Development environment and forwarded to the Testing and Quality Assurance Environments before being forwarded to the Production Acceptance environment for preparation to being accepted into the Production Environment. This sequence insures that applications function appropriately and meet Service Level Agreement (SLA) performance guidelines. It is referred to as the Systems Development Life Cycle (SDLC). When changes are made to applications in response to enhancements or problem resolutions, the application(s) is copied from the production environment to the Maintenance Environment (where its Version Level is upped by one). After maintenance is performed the application is forwarded to the Testing, Quality Assurance, and Production Acceptance environments in preparation for replacement in the Production Environment.

Included in this process are checks for compliance and the identification of Vital Records which must be backed up and stored in Local and Remote Vaults to support Recovery Operations. Some Vital Records are static (like programs and some types of data files), while other Vital Records are dynamic (like data bases and customer data files). Static files can be copied to backup files when being accepted into the Production Environment and made available for restoration when needed (disaster

events, equipment failures, damage to existing data files, etc.) from either Local or Remote Vaults. Normally, Local Vaults contain copies of data that can be directly restored to replace a damaged file, while Remote Vaults must transport data to the restore location before copying files to the target location.

Restoration of files must meet Compliance and Service Level Agreements (SLA) and have a time requirement associated with them called a Recovery Time Objective (RTO), which dictates the required time between data failure and recovery times dictated by the SLA or Compliance requirements. To achieve RTO requirements, Recovery Point Objectives (RPO) are defined that dictates when backups must be taken so that the restoration of required files can be accomplished within RTO guidelines. This can be explained through the following example. If the RTO is 4 hours and the existing RPO takes 5 hours to recover data, then you must improve the RPO by using faster equipment to restore data or changing the RPO to less than 4 hours. This issue is being addressed by the industry through improved storage management techniques and equipment, along with Failover techniques like VMWare.

Backup and Recovery times have been enhanced through improved vaulting techniques like Electronic Vaulting (also referred to as Shadow Data) and Incremental Backup (periodic backup based on timer pops or data record counter pops). Data is being more widely protected via Encryption that has little or no overhead because encryption is now being accomplished in the hardware. Encryption protects both active files and those files being transmitted or trucked to recovery vaults. Also data can be Electronically Transmitted to recovery sites through high speed communications, rather than through physically trucking files to the recovery facility. Finally, Virtual Tape is now being widely used in which tape cartridges are replaced by hard drives that can collect and restore data more quickly and can eliminate the need for tape cartridge devices altogether.

As can be seen, the Information Technology environment is complex and has its own language due to the hardware, software, products, and its unique functional responsibilities. Recovery of the IT environment is called Disaster Recovery, while recovery of client locations is called Business Recovery, and protection of personnel at work locations is called Workplace Violence Prevention. Finally, Emergency Management is responsible for natural disasters, hazardous materials, and terrorist attacks. Emergency Management personnel are sometimes referred to as First Responders and normally manage the Emergency Operations Center (EOC) which is responsible for collecting information and responding to emergency events.

All of these disciplines have their own set of responsibilities and functions. Enterprise Resiliency must address all of these disciplines and therefore must include methods for understanding and utilizing the disciplines to respond to disaster events in the most efficient manner possible. To achieve optimized Recovery Operations it is therefore necessary to create a common language and set of tools that all recovery disciplines use to accomplish their functional responsibilities. This would be analogous with using English as a common language instead of having Spanish, French, and Chinese used by separate disciplines.

This paper will try to explain these diverse recovery disciplines and can help provide personnel with a means of understanding and utilizing all recovery disciplines to best respond to emergency situations.

The Goal of Combining Recovery Operations:

Figure 10 - Defining the problem

- **Desire to most rapidly and efficiently respond to encountered disaster events, or other emergencies by melding Emergency Management, Business Continuity, and Workplace Violence Prevention:**
- **Best approach to protecting Employees, Customers, Suppliers, and Business Operations:**
- **Ensuring the Reputation and Integrity of the Organization;**
- **Combining many Lines of Business into a cohesive recovery structure with a common set of objectives, templates, tools, and a common language;**
- **Ensuring that your recovery environment meets and exceeds industry Best Practices;**
- **Utilization of Automated Tools;**
- **Integration of Best Practices like COSO, CobIT, ITIL, Six Sigma, ISO 17799, and FFIEC to optimize personnel performance, Standards and Procedures;**
- **Certify the business recovery environment and its components;**
- **Staffing, Training and Certifying Recovery Personnel;**
- **Integration with the Corporation, Customers, and Suppliers;**
- **Interfacing with First Responders, Government, and the Community;**
- **Working with Industry Leaders to continuously enhance recovery operations and mitigate gaps and exceptions to current practices;**
- **Achieve Compliance through Risk Management and Audit adherence;**
- **Testing and Quality Assurance; and**
- **Support and Maintenance going forward.**

Reviewing the goal and its implications

Today's Enterprise Resiliency practitioners are faced with a different world than even a few years ago because of mergers, acquisitions, world-wide operations, and a changing emphasis from Business Recovery to Emergency Management utilizing First Responders, External Agencies, and Internal Recovery Teams. Compiling these disciplines into a cohesive recovery operation that: safeguards personnel and company operations; adheres to compliance requirements; and integrates with standards and procedures is management's responsibility.

Additionally, the world economy, growing terrorist threats, global climate changes, natural disasters, reduced personnel levels, heightened workplace violence incidents, and new technologies has compounded the effort needed to integrate new and old disciplines within an organization.

Technologies used to perform Load Balancing and Automated Recovery have been integrated within Information Technology for operating systems, applications, and data storage. Storage systems incorporate redundancy and encryption to reduce data loss and unauthorized access with little or no overhead, as was the case in the past.

Disaster Recovery products and services have greatly reduced the chance of a Information Technology Disaster by protecting computers, their system software, applications, and hardware - all with improved efficiency and fewer personnel. Business Continuity Management and its disciplines are now being addressed through automated tools as well (i.e., LDRPS, Archer, etc.). But as these products are used by an even larger audience of end users and business managers, additional awareness and training issues must be addressed. Emergency Management Preparedness now has become the leader of the pack because First Responders, External Agencies, and Internal Recovery Operations must all be coordinated. Add compliance requirements and you can easily see how Enterprise Resiliency has become an important issue to address.

Beyond the ability to respond more quickly to disaster events, the Resiliency Practitioner must be able to utilize many different tools and practices that use technology and terminology that may not be familiar to the Resiliency Practitioner. This problem hinders the ability to design a cohesive approach to Enterprise Resiliency because a centralized group has not been provided with the authority to include all parties in the conception, design, development, roll-out, implementation, support, and maintenance of an all-inclusive Enterprise Resiliency Organization.

Integrating Best Practices within the Enterprise Resiliency environment would further improve recovery operations by insuring that personnel are aware of and trained on best practices, like: COSO. COBIT, Six Sigma, Business Continuity Management, Emergency Management, Workplace Violence, ITIL, and company based Standards and Procedures.

Finally, obtaining Corporate Certification of Enterprise Resiliency best practices will provide a solid foundation on which to build the Enterprise Resiliency program. The three approaches for achieving this goal are: the Private Sector Preparedness Act, NFPA 1600, and the international standard of BS25999. Working with a certifying organization will provide proof to outside interests that your organization is indeed adhering to the best Corporate Enterprise Resiliency practices known to protect your employees, customers, suppliers, and business operations.

Enterprise Resiliency and Recovery Disciplines

An example of the many disciplines, products, and techniques associated with Recovery Operations is provided below.

Figure 11 - Enterprise Resiliency and Recovery Disciplines

- **Emergency Management Preparedness:**
  - First Responders;
  - Emergency Operations Center (EOC);
  - Department of Homeland Security (DHS); and
  - Office of Emergency Management (OEM).
- **Business Recovery Management:**
  - Business Recovery;
  - Disaster Recovery;
  - Risk Management; and
  - Crisis Management.
- **Workplace Violence Prevention:**
  - Security (Physical and Data) and Guards;
  - Access Controls and Card Key Systems;
  - Video Recording Systems;
  - Response Plans and Crisis Management; and
  - Employee Assistance Programs.
- **Supportive Agencies:**
  - Disaster Recovery Institute International (DRII);
  - Business Continuity Institute (BCI);
  - Contingency Planning Exchange; and
  - Association of Contingency Planners.
- **Supportive Tools:**
  - Living Disaster Recovery Planning System (LDRPS);
  - Six Sigma;
  - Information Technology Infrastructure Library (ITIL);
  - Company Standards and Procedures; and
  - Training and Awareness services.
- **Corporate Business Resiliency Certification:**
  - Private Sector Preparedness Act (PL 110-53 Title IX Section 524);
  - National Fire Prevention Association Standard 1600; and
  - International Standard (IS 25999 /ISO 22301.

Emergency Management

What Is an Emergency?

An emergency is any unplanned event that can cause deaths or significant injuries to employees, customers or the public; or that can shut down your business, disrupt operations, cause physical or environmental damage, or threaten the facility's financial standing or public image.

Obviously, numerous events can be "emergencies," including:

• Fire	• Hazardous materials incident	• Flood or flash flood
• Hurricane	• Tornado	• Winter storm
• Earthquake	• Communications failure	• Radiological accident
• Civil disturbance	• Loss of key supplier or customer	• Explosion

The term "disaster" has been left out here because it lends itself to a preconceived notion of a large-scale event, usually a "natural disaster." In fact, each event must be addressed within the context of the impact it has on the company and the community. What might constitute a nuisance to a large industrial facility could be a "disaster" to a small business.

Emergency management is the process of preparing for, mitigating, responding to and recovering from an emergency. Emergency management is a dynamic process. Planning, though critical, is not the only component. Training, conducting drills, testing equipment and coordinating activities with the community are other important functions.

Making the "Case" for Emergency Management

To be successful, emergency management requires upper management support. The chief executive sets the tone by authorizing planning to take place and directing senior management to get involved. When presenting the "case" for emergency management, avoid dwelling on the negative effects of an emergency (e.g., deaths, fines, criminal prosecution) and emphasize the positive aspects of preparedness. For example:

- It helps companies fulfill their moral responsibility to protect employees, the community and the environment.
- It facilitates compliance with regulatory requirements of Federal, State and Local agencies.
- It enhances a company's ability to recover from financial losses, regulatory fines, loss of market share, damage to equipment, products, or business interruptions.
- It reduces exposure to civil or criminal liability in the event of an incident.
- It enhances a company's image and credibility with employees, customers, suppliers and the community.
- It may reduce your insurance premiums.

Emergency Management Preparedness Environment and Tools

The Emergency Manager will be the First Responder in the event of a disaster event. He/she will head the Emergency Operations Center and coordinate all communications between management, command centers, government agencies, and internal Lines of Business.

The Emergency Manager will have to communicate with all recovery personnel to obtain a definition of the disaster event and initiate recovery plans that address:

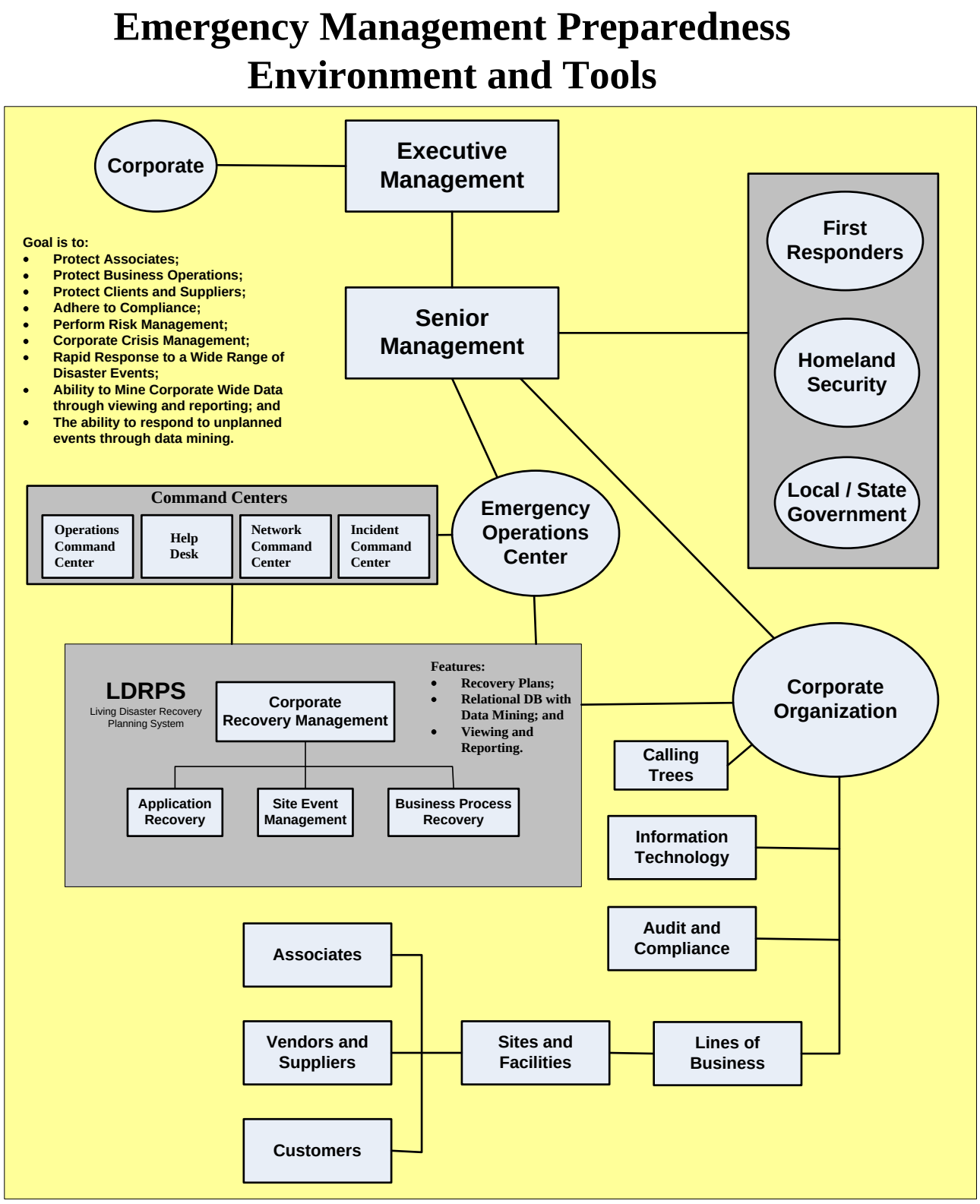
- Business Recovery (loss of a Business Unit or Office);
- Disaster Recovery (loss of a Data Center or Information Technology operation);
- Workplace Violence event (disgruntled employee, shooting, or terrorist type of event);
- Crisis Management and Communications;
- Risk Management and Compliance;
- Evacuation;
- Recovery Plan initiation;
- Event Monitoring and Reporting.

It is therefore important that the Emergency Manager know the recovery techniques, languages, and tools used by all recovery disciplines. But this is a difficult responsibility to expect anyone to be in command of because of the vastness of recovery techniques and tools. It is therefore necessary to develop a common language and toolset that encompasses all of the recovery disciplines.

The following figure illustrates the complexity of the recovery environment.

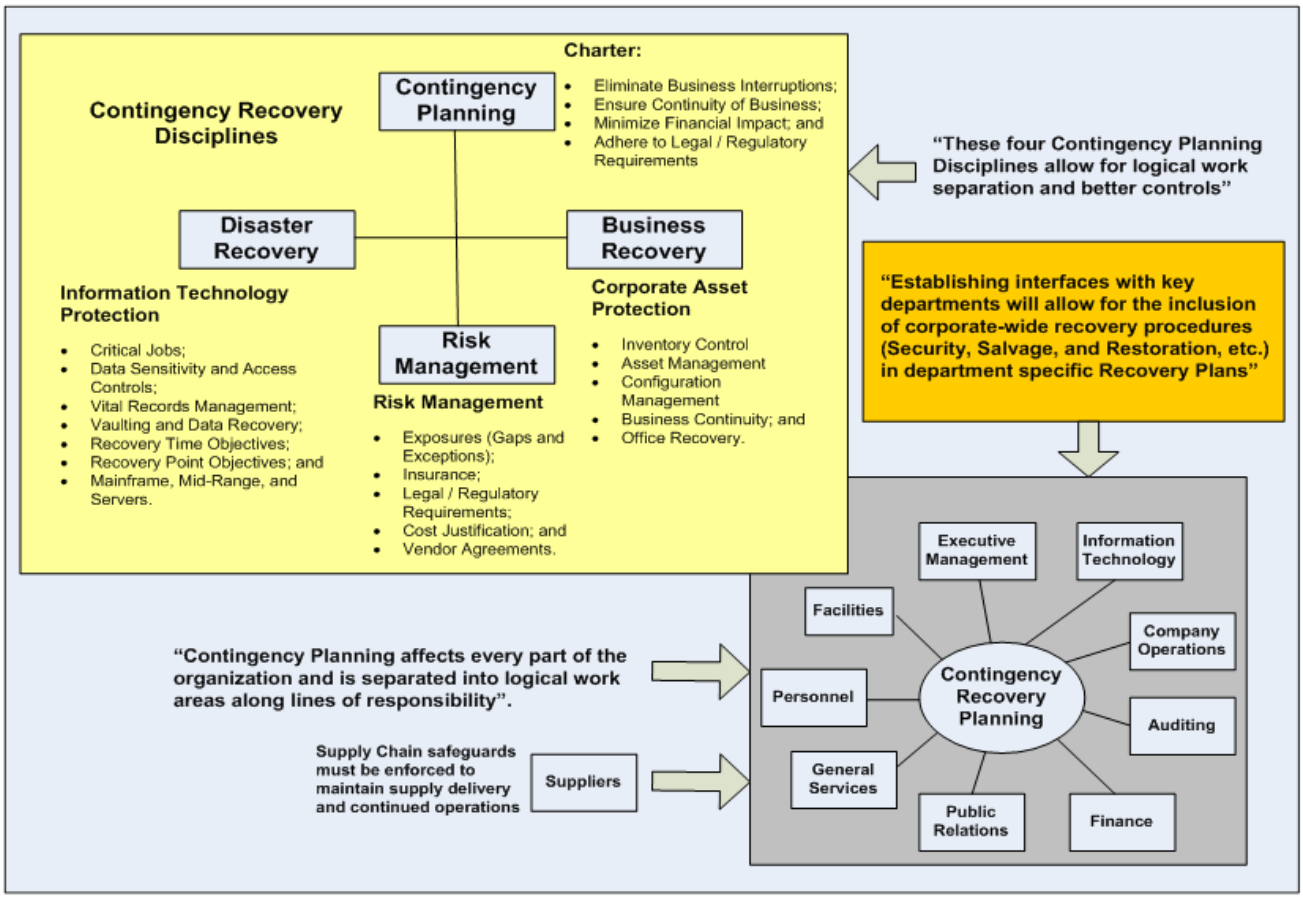
Emergency Management EOC environment concept

Figure 12 - Emergency Management Preparedness Environment and Tools



How to integrate Business Continuity Management within the organization

Figure 13: Overview of Business Continuity Management

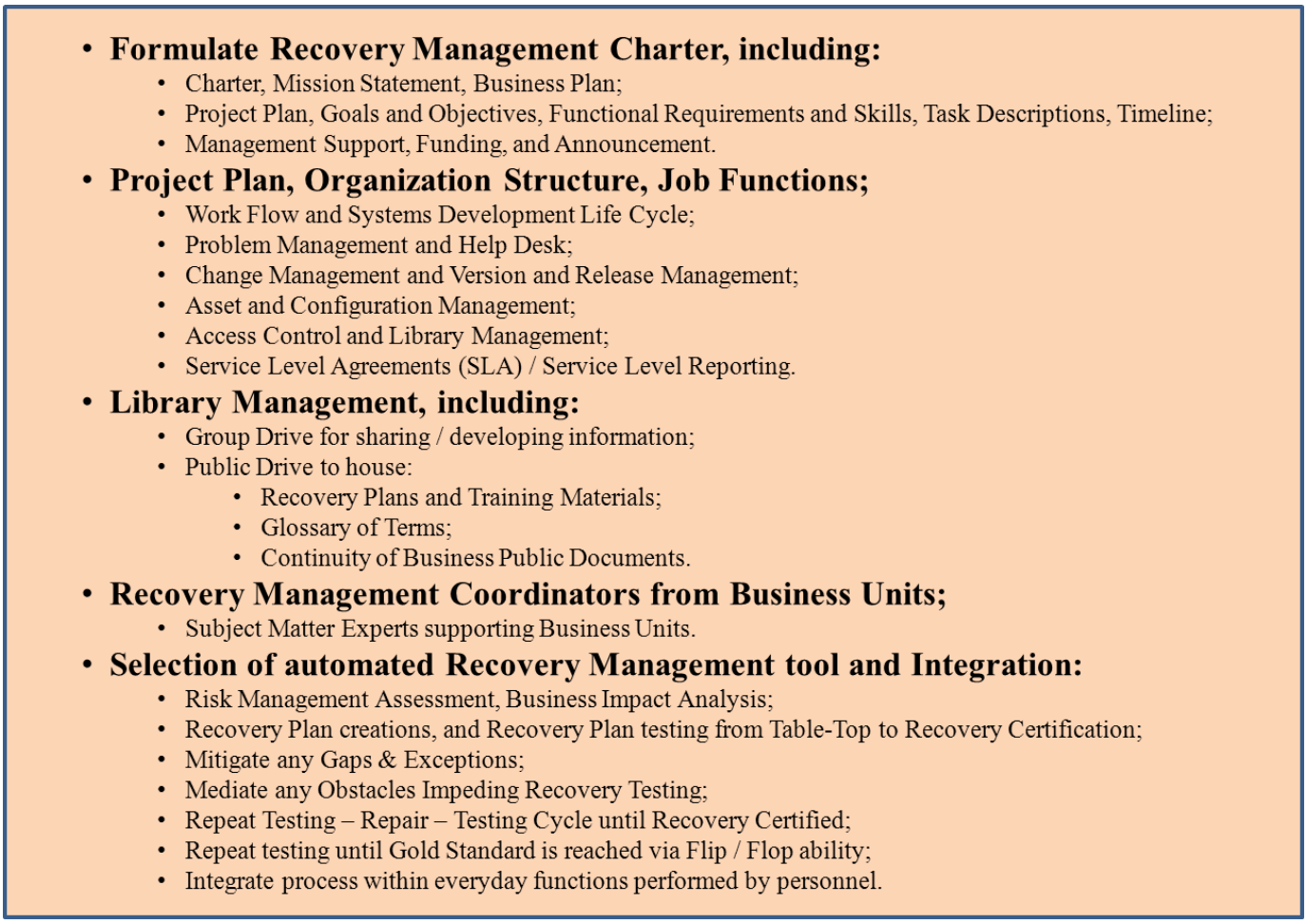


The picture shown above illustrates the many disciplines needed to contribute to achieving an environment that integrates Enterprise Resiliency and Corporate Certification within every day functions performed by personnel and included in their job descriptions and supportive documentation. The development 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

Figure 14: Steps to achieving Recovery Management and Enterprise Resiliency



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.

Building a Business Plan

It is important to take the time to develop a Business Plan for the implementation, support, and maintenance of Enterprise Resiliency and Corporate Certification because it will be integrated within the everyday functions performed by personnel . Once implemented it will be difficult to remove.

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.

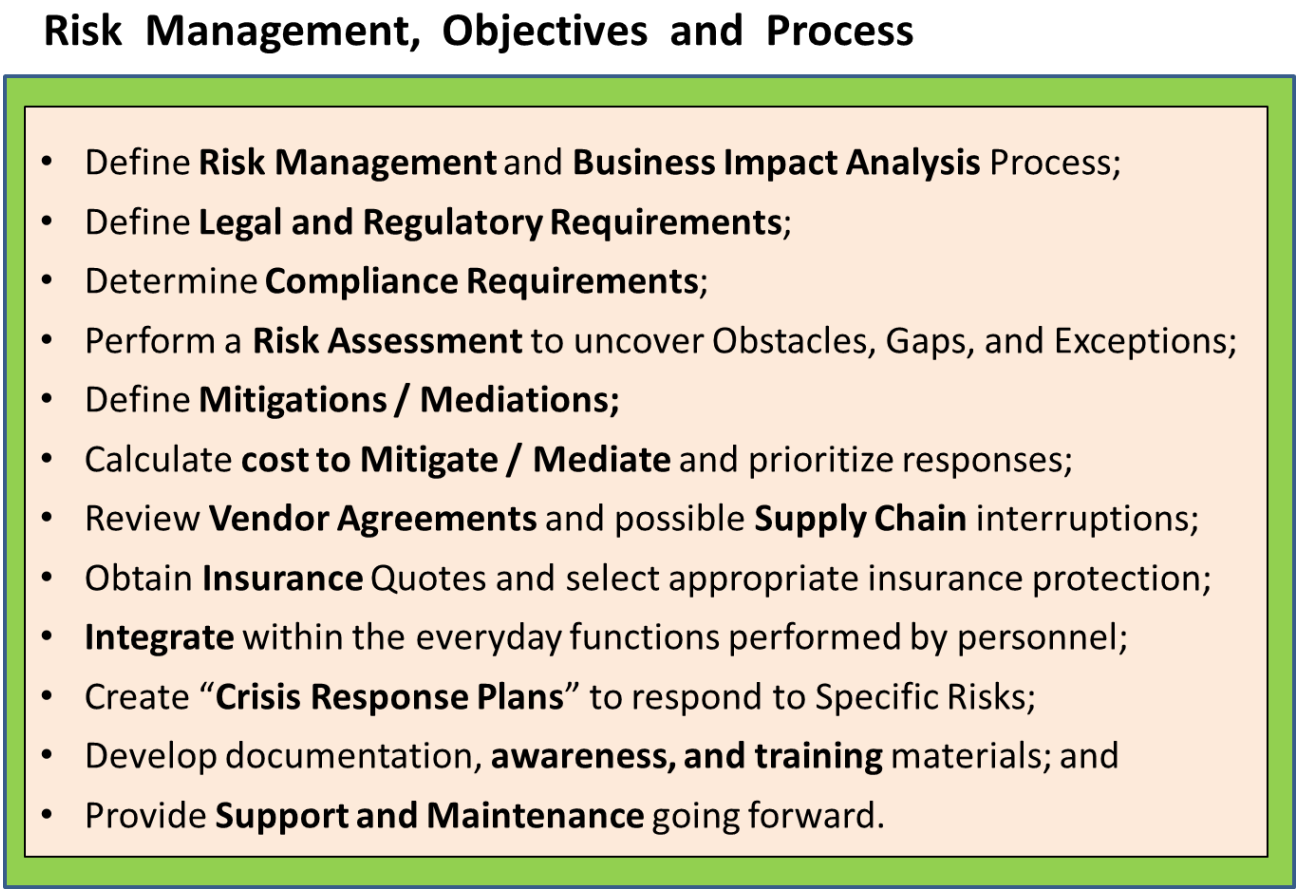
The guidelines formulated through this process will require input from all recovery management disciplines so that the best results can be achieved through their combined knowledge and experience. **Emergency Management** personnel would help define methods for protecting the Workplace, **Disaster Recovery**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

Figure 15: Risk Management Goals and Objectives



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.

How to get started implementing Enterprise Resiliency

Figure 16 - How to get started implementing Enterprise Resiliency

How to get started

Review existing Recovery Operations, including:

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

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

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

Define Company Lines of Business (LOB), including;

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

Document Integration Requirements, including:

- Service Level Agreements (SLA) and Service Level Reporting (SLR);
- Systems Development Life Cycle (SDLC) and Workflow Management;
- Best Practices tools and procedures; and
- Define Functional Responsibilities, Job Descriptions, and Standards and Procedures.

Create Business Plan, including:

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

This process is further explained in the following pages.

Reviewing Existing Recovery Operations

All of the existing Recovery disciplines should be reviewed to determine their weaknesses and strengths as well as detailing the tools used and the language associated with the discipline. An organization chart should be developed for each discipline and individuals assigned to the functions identified. Functions performed by these individuals and the tools they use should be documented. If standards and procedures exist, along with documentation and training for the people assigned to these functions, they should be identified and reported on. Once all of the research has been completed, an analysis of the information should be performed to identify weaknesses that could be corrected by a common language and tool set. Existing recovery disciplines to be examined are listed below.

Emergency Management Preparedness – is concerned with natural disasters, terrorism, malicious activity, external threats, and infrastructure facilities.

Business Continuity Management – is responsible for disaster recovery (Information Technology equipment, products and services), business recovery (loss of business office or location), crisis management (incident management and communications), and risk management (legal / regulatory requirements, compliance, gaps and exceptions, controls, insurance, vendor agreements, and cost justifications).

Workplace Violence Prevention – is responsible for insuring that personnel are protected within the workplace. It deals with physical security perimeters around the overall facility and internal locations that may require restricted access to authorized personnel only. Guards, key cards, access controls are all included in this discipline along with employee assistance programs to provide assistance to personnel who may be going through a personal crisis. This function is usually managed by the Human Resource department.

Enterprise Security Operations (both physical and data security) – is responsible for protecting assets including Information Technology, computerized data, physical data, physical locations, and all access controls.

Evaluate Command Centers and their interactions with Recovery Operations

Command Centers are functional groups within a company responsible for specific supportive activities. Command Centers allow for highly skilled personnel to concentrate their talents to address a specific range of problems in support of business operations. When researching these organizations, concentration should be placed on their area of responsibility, the tools they use, how they identify and report on problems, and areas where improvements can be made by incorporating a common language and tool set that would enhance recovery operations. Command Centers are divided into the following areas of responsibility.

Operation Control Center (OCC) – is responsible for monitoring Information Technology operations to identify the successful start and end of computers jobs, or any abnormal / problem events that may be encountered by a job. Encountered problems are reported to the Help Desk for logging and routing to repair personnel associated with the encountered event.

Network Command Center (NCC) – is responsible for monitoring communications between Information Technology resources and users attached externally or internally to these resources. Communications resources are usually defined as online systems or web based applications. When problems occur the NCC Staff attempts to identify the problem, reroute traffic around the failing components, and report the problem to the Help Desk.

Help Desk (HD) – is responsible for problem management. Help Desk personnel accept problem reports and route the problem to the person responsible for supporting the component experiencing the problem. Help Desk personnel are considered First Level Support, while Second Level Support is the party responsible for the failing component, and Third Level Support is the vendor / expert responsible for final resolution associated with the failing component.

Incident Command Center (ICC) – is responsible for the management and overall resolution of incidents that affect a facility or business operation. Problem management responsibility is usually divided into a Local Incident Command Center (LICC), a Regional Incident Command Center (RICC), and Central Incident Command center (CICC). LICC operations are limited by personnel and functions that are maintained on-site, while more problem management resources are provided regionally and centrally. Appropriate resources are brought to bear on a local problem as needed through regional and central functions. Problem escalation is dependent on the affected component and the length of the outage.

Emergency Operations Center (EOC) – Activated whenever a disaster event occurs, the EOC is responsible for identifying the problem and directing personnel and resources to resolve the problem in as an efficient a manner as is possible. Coordinating personnel, directing communications to internal and external sources, and working with First Responders from Local, State, and National organizations are primary responsibilities of the EOC. Usually commanded by the Emergency Management department, the EOC has to work with the Business Recovery and Workplace Violence Prevention departments to bring all necessary resources to play when addressing the resolution of disaster events. For these reasons, and more, it is imperative that EOC personnel speak a common language and use a common set of tools so that confusion and misinformation is kept to a minimum.

Define company Lines of Business (LOB)

Disaster events affect business operations and the Lines of Business (LOB) contained within a business. It is therefore imperative that LOB's are defined and their recovery needs identified. The EOC will be responsible for insuring that LOB's are supported during a disaster event by exercising recovery plans to safeguard personnel, clients, suppliers, business operations, community relations, and the reputation of the business. The analysis of the LOB's is usually performed within a Business Impact Analysis and Risk Assessment and includes the following areas.

Business Functions, Products, and Services – provided by a Line of Business and their relative importance to the firm are identified and rated.

Locations and Personnel – at the locations are identified and defined. Sister sites and standalone sites are classified as to their ability to recover from a disaster event.

Customers and Suppliers – Clients supported from Business Locations and a Line of Business are identified and the Suppliers used to provide resources to the site are identified and their services rated. A Recovery Time Objective (RTO) and a Recovery Point Objective (RPO) are identified during this analysis.

Applications and Business Processes – associated with a Line of Business are identified and rated as to their relative importance and sequence of operation. This information is importance when planning recovery operations.

Existing Evacuation Plans, Crisis Management Plans, and Recovery Operations – are identified and rated to determine if they meet company directives in a timely and efficient manner. Inconsistencies and areas of improvement are identified and reported to management.

Document Integration Requirements

Once developed, recovery operations must be integrated into the everyday functions performed in support of business operations and client support. This is accomplished through analysis of the following areas.

Service Level Agreements (SLA) and Service Level Reporting (SLR) – An agreement between clients and the business defining client services, their relative importance, and resources required to support client operations at the level agreed upon. Service Level Reporting is used to monitor and report on adherence to SLA's. Penalties are associated with missed SLA goals.

Systems Development Life Cycle (SDLC) – The process associated with developing new applications and their maintenance going forward. The SDLC is comprised of Development, Testing, Quality Assurance, Production Acceptance, Production, Disaster Recovery, Business Recovery, Support, Change Management, and Maintenance. This process is further explaind later in this document.

Best Practices tools and procedures – These are industry accepted guidelines and tools that will result in the implementation of products and services that meet or exceed industry standards. They consist of COSO, CobIT, ITIL, ISO 17799, and FFIEC and are explained in greater detail later on in this document.

Define Functional Responsibilities – The Functions and Responsibilities associated with integrating Recovery Operations throughout the corporation are defined during this analysis and recommendations for implementation formulated. This topic is explained in great detail later in this document.

Create Job Descriptions – Based on functional responsibilities and levels of expertise, job descriptions are developed and provided to personnel assigned to the function in question.

Develop Standards and Procedures – All Standards and Procedures are defined and included within a Standards and Procedures Manual for reference by personnel when they have to perform their assigned functional responsibilities.

Create Business Plan

To define the Enterprise Resiliency and Corporate Certification effort a Business Plan should be created and followed. Doing so will improve the quality of deliverables and reduce confusion. The sections included in a Business Plans are described below.

Mission Statement – Management definition and the level of expectation.

Goals and Objectives – What goals are expected and the objectives that must be overcome to achieve the goal.

Assumptions – What assumptions that are associated with this project.

Scope and Deliverables – The scope of the project and the deliverables that are expected.

Detailed Project Plan – Detailed project plan with phases, tasks, and resources needed to complete the project. A schedule of events associated with the project and the costs that are expected to be incurred are also included in the project plan.

Management Approval through Report and Presentation – Once developed, the project plan and business plan are documented in a report and presentation that management will review before providing their approval to move forward.

Establish Schedule of Events and Assign Personnel to Tasks – A detailed schedule of events, skills needed to complete tasks, and personnel having the talents needed to perform project plan functions are assigned. If personnel do not have required skills they should be trained or outside help sought.

Define Functional Responsibilities – The Functional Responsibilities of jobs performed by personnel are defined so that personnel with required skills can be assigned to project tasks and permanent tasks that will remain after the project is completed.

Create Job Descriptions – Job Descriptions for personnel will be created and entered into the Human Resources database.

Build Standards and Procedures – All standards and procedures will be documented and included in the S&P Manual.

Monitor, Report, Improve, and Validate results – On-going monitoring, reporting, and validation will be performed and reported to management. Improvements will be made as necessary.

Roll-Out, Train, and Implement procedures – Product Roll-Out, personnel training, and Product Implementation Procedures will be developed to support the full product implementation, support, and maintenance process going forward.

The potential Risks and Threats facing a corporation

Figure 17 - Potential Risks and Threats

Malicious Activity:

- Fraud, Theft, and Blackmail;
- Sabotage, Workplace Violence Prevention; 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.

All of these potential Threats and Risks must be addressed within Recovery Plans and procedures in order to achieve Enterprise Resiliency and Corporate Certification. They are uncovered through Risk Assessments and Business Impact Analysis (BIA) and addressed in various recovery plans conducted through the Business Recovery and Emergency Management departments, or in response to Workplace Violence Prevention requirements.

Building the Emergency Management Environment.

The following four Phase approach to implementing an Emergency Management Environment is recommended by FEMA (Federal Emergency Management Agency) and consists of:

The four step planning process

Phase 1: **4 Steps in the Planning Process** —

1. how to form a planning team;
2. how to conduct a vulnerability analysis;
3. how to develop a plan;
4. and how to implement the plan.

This process can be applied to virtually any type of business or industry.

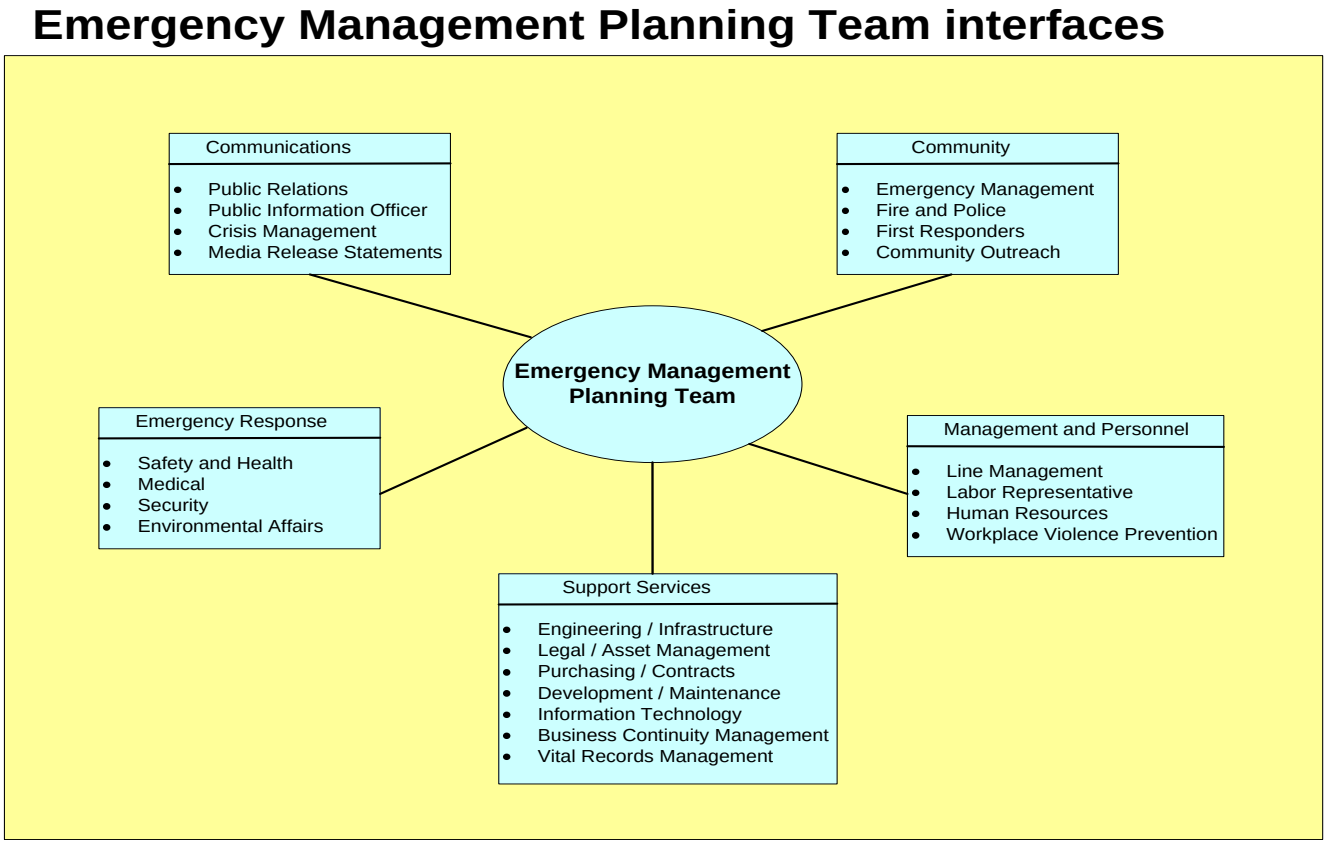
Emergency Management personnel should be formed into teams that can perform the steps listed above, including:

1. Assigning responsibilities to team members so that listed objectives can be achieved;
2. Analyzing existing hazards and the capabilities that the organization already performs to safeguard against these problem areas;
3. Developing an Emergency Response and Preparedness Plan that addresses all possible emergency events; and
4. Implement the Emergency Management Plan(s) needed to protect personnel, business operations, and the reputation of the company.

The Emergency Management Planning Team is comprised of personnel from vital areas consisting of both company and community representatives. Team members will meet to discuss Emergency Management needs and the best methods for the company to respond. Management should assign team members in writing and provide them with the authority they need to complete research and other assignments. A Mission Statement should be created and a Budget assigned to the Emergency Management Planning Team.

Emergency Management Planning Team

Figure 18 - Emergency Management Planning Team



In an emergency, all personnel should know:

1. What is my role?
2. Where should I go?

Some facilities are required to develop:

1. Emergency escape procedures and routes;
2. Procedures for employees who perform or shut down critical operations before an evacuation;
3. Procedures to account for all employees, visitors and contractors after an evacuation is completed;
4. Rescue and medical duties for assigned employees;
5. Procedures for reporting emergencies; and
6. Names of persons or departments to be contacted for information regarding the plan.

Some responsibilities that should be assigned to the planning team include:

Determine where you stand right now by:

- Reviewing Internal Plans (Business Recovery, Disaster Recovery, Emergency Recovery, etc.);
- Meet with Outside Groups to discuss concerns and formulate relationships;
- Identify Codes and Regulations;
- Identify Critical Products;
- Identify Internal Resources and Capabilities;
- Identify External Resources and Capabilities; and
- Perform an Insurance Review.

Conduct a Vulnerability Analysis, including:

- List potential Emergencies;
- Estimate Probability for each type of emergency;
- Assess the Potential Impact and costs to personnel, property, and the business;
- Assess Internal and External Resources and their ability to respond to emergencies;
- Rate the ability to respond to emergencies and the costs associated with the response;
- Compare cost of emergency to cost of response; and
- Determine best response to emergencies.

Develop the Emergency Management Plan, by following the steps and tasks below:

- **Defining Plan Components;**
  - Executive Summary and Mission Statement;
  - Emergency Management Elements;
  - Emergency Response Procedures; and
  - Support Documents.

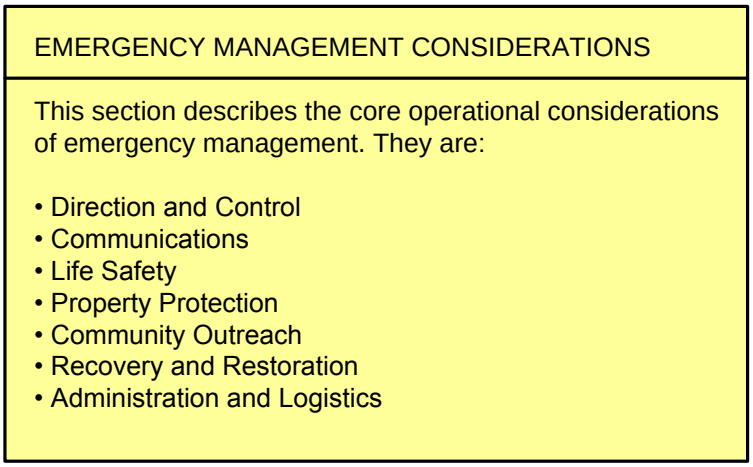
- **Define the Plan Development Process, including:**
  - Identify Challenges, Risks, Objectives, and Goals;
  - Write the Plan;
  - Establish a Training Schedule;
  - Coordinate with Outside Organizations;
  - Maintain contact with Corporate Offices;
  - Review, Conduct Training, and Revise;
  - Seek Final Approval; and
  - Distribute the Plan.

- **Implement the Plan, by:**
  - Integrate the Plan into Company Operations;
  - Conduct Training, including:
    - Orientation;
    - Table-Top Testing;
    - Walk-Thru Drills;
    - Functional Drills;
    - Evacuation Drills; and
    - Full-Scale Exercises.

- **Support and Maintain the Plan going forward, including:**
  - Implement Workflow Management Checkpoints to validate that Plans are updated when their components are changed (Personnel, Applications, Clients, Suppliers, Locations, Problem Resolutions, Enhancements, etc.);
  - Provide Support throughout the process of identifying and resolving problems;
  - Provide Change Management for enhancements and problem resolutions;
  - Define Functional Responsibilities associated with creating, supporting, and maintaining Plans;
  - Create Job Descriptions for personnel directly responsible for building, supporting, and maintaining recovery plans;
  - Create and distribute Standards and Procedures Manual for creating, supporting, and maintaining recovery plans; and
  - Provide Training and Orientation to personnel, clients, suppliers, and the community.

Emergency Management Considerations

Phase 2: Emergency Management Considerations — The process of how to build the emergency management capabilities of life safety, property protection, communications and community outreach are explained in this section.

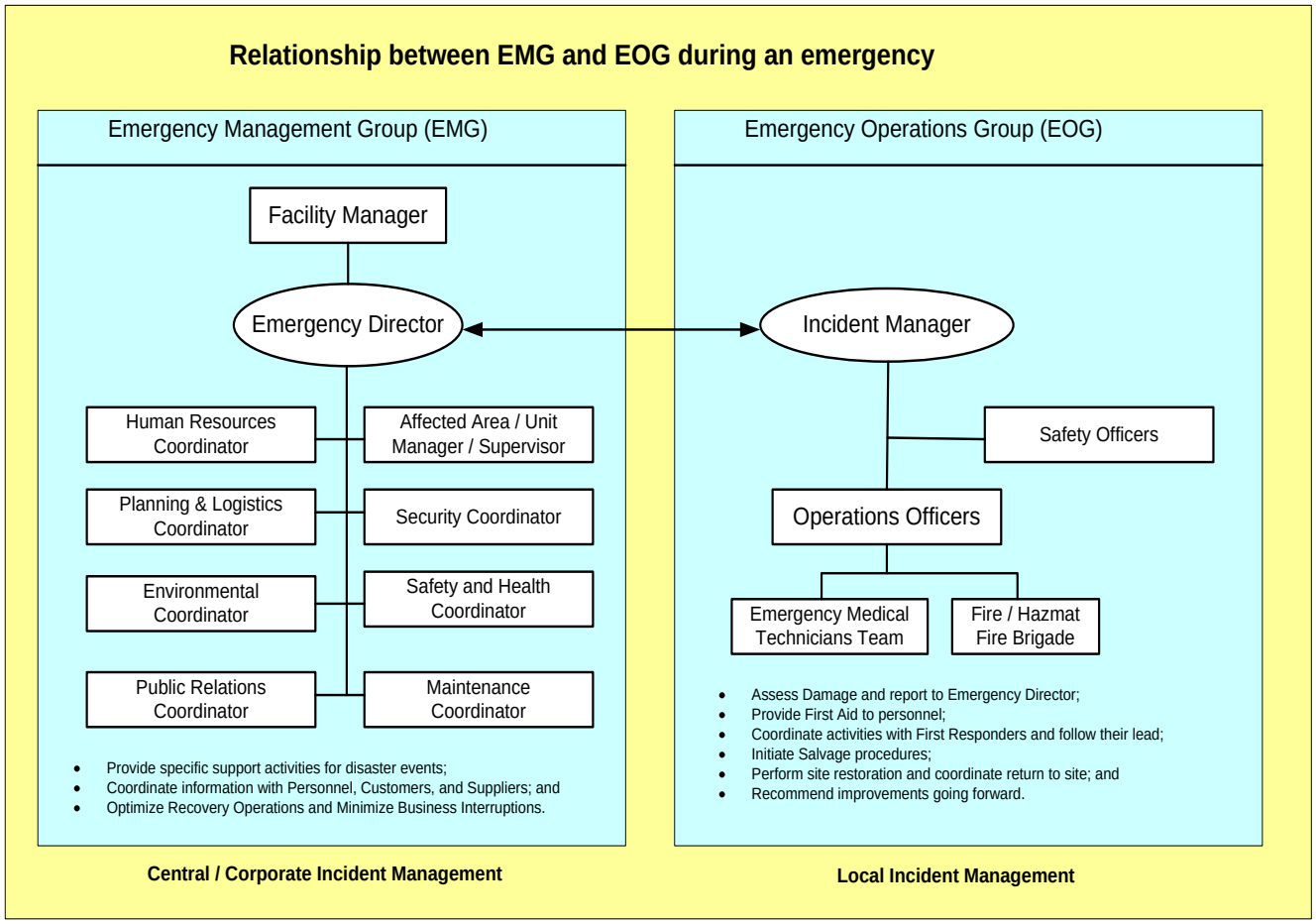


The tasks that must be completed during this phase include:

- **Direction and Control** – what actions to perform and where control over the Emergency Management process will exist (Emergency Operations Center), including:
  - Emergency Management Group and Emergency Operations Group;
  - Incident Manager and Incident Command Center;
  - Planning Considerations and Security; and
  - Coordination of Outside Response.

Incident Management Structure overview

Figure 19 - Relationship between EMG and EOC during an emergency



- **Communications** – line of command and how to document, log, submit, respond to, escalate, and resolve reported problems. Once problems have been resolved, a Post-Mortem is performed and any necessary updates to the communications and problem management process are made. Areas of responsibility associated with this task include:
  - Plan for all possible contingencies;
  - Develop Emergency Communications and Crisis Management Plans;
  - Create responses for all types of media (TV, Radio, Internet, Papers, etc.);
  - Family Communications; and
  - Notification and Warning procedures.

- **Life Safety** – the most important issue related to Emergency Management has a pre-event responsibility of insuring that life-safety equipment is in place (i.e., Fire Extinguishers, Breathing Apparatus, Fire Suppressant Systems, etc.) and a post-event responsibility to make sure personnel are provided with protection from disaster events through practiced procedures and continuous safety improvements. Areas of responsibility include:
  - Evacuation Plan with Evacuations Routes and Exits;
  - Assembly Areas and Accountability;
  - Shelter locations (outside and in-place);
  - Training and Informational Awareness;
  - Coordination with First Responders and Community Representatives; and
  - Family Preparedness.

- **Property Protection** – For all emergencies property protection considerations must be defined and formalized, including:
  - **Planning Considerations:**
    - Fighting Fires;
    - Containing Material Spills;
    - Closing or barricading doors and windows;
    - Shutting down equipment;
    - Covering or securing equipment; and
    - Moving equipment to a safe location.

  - **Protection Systems:**
    - Fire Prevention Systems;
    - Lightning Protection Systems;
    - Water level Monitoring Systems;
    - Overflow Detection Devices;
    - Automatic Shut-Off Systems;
    - Emergency Power Generation Systems; and
    - Uninterrupted Power Supply Systems.

  - **Mitigating the effects of Property Damage; including:**
    - Upgrading facilities and Flood Protection;
    - Fire Suppression Systems (Water, Hualon, etc.);
    - Use of Fire Resistant Materials;
    - Installing Storm Shutters;
    - Safeguarding work environment and securing equipment; and
    - Use of Structural Engineer to certify infrastructure.

  - **Facility Shutdown considerations and procedures, including:**
    - Define Shut-Down conditions and procedures;
    - Identify personnel who can declare a Shut-Down condition;
    - Assign personnel to Shut-Down teams;
    - Assess site Shut-Down impact on other business operations;
    - Determine the amount of time associated with a Shut-Down; and
    - Train personnel on Shut-Down procedures.

- **Records Preservation and Vital Records Management, including:**
  - Identify Financial, Compliance, and Insurance data;
  - Engineering Plans and Drawings;
  - Product Lists and Specifications;
  - Employee, Client, and Supplier data bases;
  - Formulas and Trade Secrets; and
  - Personnel Files.

- **Backup and Recovery of Vital records requires:**
  - Labeling vital records;
  - Backing up computer systems;
  - Making copies of records (encrypt where necessary);
  - Storing tapes and disks in insulated containers (Local Vaults);
  - Storing data off-site where they would not likely be damaged by an event affecting your facility (Remote Vaults);
  - Increasing security of computer facilities (Physical and Data);
  - Arranging for evacuation of records to backup facilities;
  - Backing up systems handled by service bureaus; and
  - Arranging for backup power and communications.

Community Outreach - Your facility's relationship with the community will influence your ability to protect personnel and property, while expediting your return to normal operations. You can achieve this by:

- **Maintaining a dialogue** with community leaders, first responders, government agencies, Community organizations and utilities, including:
  - Appointed and elected leaders;
  - Fire, police and emergency medical services personnel;
  - Local Emergency Planning Committee (LEPC) members;
  - Emergency Management director;
  - Public Works Department;
  - American Red Cross;
  - Hospitals;
  - Telephone company and communication suppliers;
  - Electric utility; and
  - Neighborhood groups.

- **Establish Mutual Aid Agreements** with local response agencies and businesses to avoid confusion and conflict in an emergency, including:
  - Define the type of assistance;
  - Identify the chain of command for activating the agreement;
  - Define communications procedures; and
  - Include these agencies in facility training exercises whenever possible.

- **Mutual aid agreements can address** any number of activities or resources that might be needed in an emergency. For example:
  - Providing for firefighting and HAZMAT response;
  - Providing shelter space, emergency storage, emergency supplies, medical support; and

- Businesses allowing neighbors to use their property to account for personnel after an evacuation

- **The community wants to know:**
  - What does the facility do?
  - What are the hazards?
  - What programs are in place to respond to emergencies?
  - How could a site emergency affect the community?
  - What assistance will be required from the community?

- **Media Relations** can be the most important link to the public. Try to develop and maintain positive relations with media outlets in your area. Determine their particular needs and interests. Explain your plan for protecting personnel and preventing emergencies. Determine how you would communicate important public information through the media in an emergency by:
  - Designating a trained spokesperson and an alternate spokesperson;
  - Set up a media briefing area;
  - Establish security procedures;
  - Establish procedures for ensuring that information is complete, accurate and approved for public release;
  - Determine an appropriate and useful way of communicating technical information; and
  - Prepare background information about the facility.

- **Press releases** about facility-generated emergencies should describe who is involved in the incident and what happened, including when, where, why and how. When providing information to the media during an emergency:
  - **Do's**
    - Give all media equal access to information.
    - When appropriate, conduct press briefings and interviews. Give local and national media equal time.
    - Try to observe media deadlines.
    - Escort media representatives to ensure safety.
    - Keep records of released information.
    - Provide press releases when possible.
  - **Don'ts**
    - Do not speculate about the incident.
    - Do not permit unauthorized personnel to release information.
    - Do not cover up facts or mislead the media.
    - Do not place blame for the incident.

- **Recovery and Restoration** - Business recovery and restoration, or business resumption, goes right to a facility's bottom line: keeping people employed and the business running. After a site emergency, assess the impact of the event on business neighbors and the community and take appropriate action. How you handle this issue will have long-lasting consequences on the company's ability to recover from a disaster event and continue business operations. Include:

- **Planning Considerations** - Consider making contractual arrangements with vendors for such post-emergency services as records preservation, equipment repair, earthmoving or engineering. Meet with your insurance carriers to discuss your property and business resumptions policies. Determine critical operations and make plans for bringing those systems back on-line. The process may entail:
  - Repairing or replacing equipment;
  - Relocating operations to an alternate facility;
  - Contracting operations on a temporary basis; and
  - Take photographs or videotape the facility to document company assets. Update these records regularly.

- **Continuity of Management** - You can assume that not every key person will be readily available or physically at the facility after an emergency. Ensure that recovery decisions can be made without undue delay. Consult your legal department regarding laws and corporate bylaws governing continuity of management. Establish procedures for:
  - Assuring the chain of command;
  - Maintaining lines of succession for key personnel;
  - Moving to alternate headquarters; and
  - Include these considerations in all exercise scenarios.

- **Insurance** - Most companies discover that they are not properly insured only after they have suffered a loss. Lack of appropriate insurance can be financially devastating. Discuss the following topics with your insurance advisor to determine your individual needs.
  - How will my property be valued?
  - Does my policy cover the cost of required upgrades to code?
  - How much insurance do I require to avoid becoming a co-insurer?
  - What perils or causes of loss does my policy cover?
  - What are my deductibles?
  - What does my policy require me to do in the event of a loss?
  - What types of records and documentation will my insurance company want to see?
  - Are records in a safe place where they can be obtained after an emergency?
  - To what extent am I covered for loss due to interruption of power?
  - Is coverage provided for both on- and off-premises power interruption?
  - Am I covered for lost income in the event of business interruption?
  - Do I have enough coverage?
  - For how long is coverage provided?
  - How long is my coverage for lost income if my business is closed by order of a civil authority?
  - To what extent am I covered for reduced income due to customers' not all immediately coming back once the business reopens?
  - How will my emergency management program affect my rates?

- **Employee Support** - Since employees who will rely on you for support after an emergency are your most valuable asset, consider the range of services that you could provide or arrange for, including:

- Cash advances;
- Salary continuation;
- Flexible work hours;
- Reduced work hours;
- Crisis counseling;
- Care packages; and
- Day care.

- **Resuming Operations -** Immediately after an emergency, take steps to resume operations, including:
  - Establish a recovery team, if necessary. Establish priorities for resuming operations.
  - Continue to ensure the safety of personnel on the property. Assess remaining hazards. Maintain security at the incident scene.
  - Conduct an employee briefing.
  - Keep detailed records. Consider audio recording all decisions. Take photographs of or videotape the damage.
  - Account for all damage-related costs. Establish special job order numbers and charge codes for purchases and repair work.
  - Follow notification procedures. Notify employees' families about the status of personnel on the property. Notify off duty personnel about work status. Notify insurance carriers and appropriate government agencies.
  - Protect undamaged property. Close up building openings. Remove smoke, water and debris. Protect equipment against moisture. Restore sprinkler systems. Physically secure the property. Restore power.
  - Conduct an investigation. Coordinate actions with appropriate government agencies.
  - Conduct salvage operations and segregate damaged from undamaged property. Keep damaged goods on hand until an insurance adjuster has visited the premises, but you can move material outside if it's seriously in the way and exposure to the elements won't make matters worse.
  - Take an inventory of damaged goods with the Insurance Adjuster, or the Adjuster's salver if there is any appreciable amount of goods or value. If you release goods to the salver, obtain a signed inventory stating the quantity and type of goods being removed.
  - Restore equipment and property. For major repair work, review restoration plans with the insurance adjuster and appropriate government agencies.
  - Assess the value of damaged property. Assess the impact of business interruption.
  - Maintain contact with customers and suppliers.

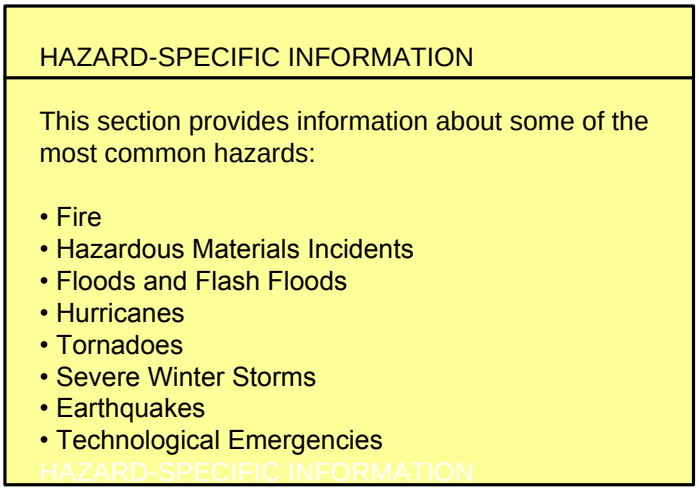
- **Administration and Logistics -** Maintain complete and accurate records at all times to ensure a more efficient emergency response and recovery. Certain records may also be required by regulation or by your insurance carriers and some may prove invaluable in the case of legal action after an incident. Administrative actions prior to an emergency include:
  - Establishing a written emergency management plan;
  - Maintaining training records;

- Maintaining all written communications;
- Documenting drills and exercises and their critiques;
- Involving community emergency response organizations in planning activities;
- Administrative actions during and after an emergency include:
  - Maintaining telephone logs;
  - Keeping a detailed record of events;
  - Maintaining a record of injuries and follow-up actions;
  - Accounting for personnel;
  - Coordinating notification of family members;
  - Issuing press releases;
  - Maintaining sampling records;
  - Managing finances;
  - Coordinating personnel services; and
  - Documenting incident investigations and recovery operations.

- **Logistics** - Before an emergency, logistics may entail:
  - Emergency funding can be critical immediately following an emergency. Consider the need for preapproved purchase requisitions and whether special funding authorities may be necessary.
  - Acquiring equipment;
  - Stockpiling supplies;
  - Designating emergency facilities;
  - Establishing training facilities;
  - Establishing mutual aid agreements;
  - Preparing a resource inventory;
  - During an emergency, logistics may entail the provision of:
    - Providing utility maps to emergency responders;
    - Providing material safety data sheets to employees;
    - Moving backup equipment in place;
    - Repairing parts;
    - Arranging for medical support, food and transportation;
    - Arranging for shelter facilities;
    - Providing for backup power; and
    - Providing for backup communications.

Hazard-Specific Information

Phase 3: **Hazard-Specific Information** — technical information about specific hazards your facility may face.



- **Fire Protection Planning** - Consider the following when developing your plan:
  - Meet with the fire department to talk about the community's fire response capabilities. Talk about your operations. Identify processes and materials that could cause or fuel a fire, or contaminate the environment in a fire.
  - Have your facility inspected for fire hazards. Ask about fire codes and regulations.
  - Ask your insurance carrier to recommend fire prevention and protection measures. Your carrier may also offer training.
  - Distribute fire safety information to employees on: how to prevent fires in the workplace, how to contain a fire, how to evacuate the facility, where to report a fire.
  - Instruct personnel to use the stairs — not elevators — in a fire. Instruct them to crawl on their hands and knees when escaping a hot or smoke-filled area.
  - Conduct evacuation drills. Post maps of evacuation routes in prominent places. Keep evacuation routes, stairways, and doorways clear of debris.
  - Assign fire wardens for each area to monitor shutdown and evacuation procedures.
  - Establish procedures for the safe handling and storage of flammable liquids and gases.
  - Establish procedures to prevent the accumulation of combustible materials.
  - Provide for the safe disposal of smoking materials.
  - Establish a preventive maintenance schedule to keep equipment operating safely.
  - Place fire extinguishers and breathing apparatus in appropriate locations.
  - Train employees in use of fire extinguishers and breathing apparatus.
  - Install smoke detectors. Check smoke detectors once a month, change batteries at least once a year.
  - Establish a system for warning personnel of a fire. Consider installing a fire alarm with automatic notification to the fire department.
  - Consider installing a sprinkler system, fire hoses and fire-resistant walls and doors.
  - Ensure that key personnel are familiar with all fire safety systems.

- Identify and mark all utility shutoffs so that electrical power, gas or water can be shut off quickly by fire wardens or responding personnel.
- Determine the level of response your facility will take if a fire occurs. Among the options are:
  - **Option 1** — Immediate evacuation of all personnel on alarm.
  - **Option 2** — Ensure that all personnel are trained in fire extinguisher use. Personnel in the immediate area of a fire attempt to control it. If they cannot, the fire alarm is sounded and all personnel evacuate.
  - **Option 3** — Ensure that only designated personnel are trained in fire extinguisher use.
  - **Option 4** — A fire team is trained to fight incipient-stage fires that can be controlled without protective equipment or breathing apparatus. Beyond this level fire, the team evacuates.
  - **Option 5** — Ensure that a fire team is trained and equipped to fight structural fires using protective equipment and breathing apparatus.

- **Hazardous Materials Incidents** - Hazardous materials are substances that are either: flammable or combustible, explosive, toxic, noxious, corrosive, an irritant or radioactive. A hazardous material spill or release can pose a risk to life, health, or property. An incident can result in the evacuation of a few people, a section of a facility or an entire neighborhood. There are a number of Federal laws that regulate hazardous materials, including: the Superfund Amendments and Reauthorization Act of 1986 (SARA), the Resource Conservation and Recovery Act of 1976 (RCRA), the Hazardous Materials Transportation Act (HMTA), the Occupational Safety and Health Act (OSHA), the Toxic Substances Control Act (TSCA) and the Clean Air Act. Title III of SARA regulates the packaging, labeling, handling, storage and transportation of hazardous materials. The law requires facilities to furnish information about the quantities and health effects of materials used at the facility, and to promptly notify local and State officials whenever a significant release of hazardous materials occurs. In addition to on-site hazards, you should be aware of the potential for an off-site incident affecting your operations. You should also be aware of hazardous materials used in facility processes and in the construction of the physical plant. Detailed definitions as well as lists of hazardous materials can be obtained from the Environmental Protection Agency (EPA) and the Occupational Safety and Health Administration (OSHA).

  - **Planning Considerations** - Consider the following when developing your plan:
    - Identify and label all hazardous materials stored, handled, produced and disposed of by your facility. Follow government regulations that apply to your facility. Obtain material safety data sheets (MSDS) for all hazardous materials at your location.
    - Ask the local fire department for assistance in developing appropriate response procedures.
    - Train employees to recognize and report hazardous material spills and releases. Train employees in proper handling and storage.
    - Establish a hazardous material response plan:
      - Establish procedures to notify management and emergency response organizations of an incident.
      - Establish procedures to warn employees of an incident.
      - Establish evacuation procedures.
      - Depending on your operations, organize and train an emergency response team to confine and control hazardous material spills in accordance with applicable regulations.

- Identify other facilities in your area that use hazardous materials. Determine whether an incident could affect your facility.
- Identify highways, railroads and waterways near your facility used for the transportation of hazardous materials. Determine how a transportation accident near your facility could affect your operations.

- **Floods and Flash Floods** - Floods are the most common and widespread of all natural disasters. Most communities in the United States can experience some degree of flooding after spring rains, heavy thunderstorms or winter snow thaws. Most floods develop slowly over a period of days. Flash floods, however, are like walls of water that develop in a matter of minutes. Flash floods can be caused by intense storms or dam failure.

  - **Planning Considerations** - Consider the following when preparing for floods:
    - Ask your local emergency management office whether your facility is located in a flood plain. Learn the history of flooding in your area. Learn the elevation of your facility in relation to steams, rivers and dams.
    - Review the community's emergency plan. Learn the community's evacuation routes. Know where to find higher ground in case of a flood.
    - Establish warning and evacuation procedures for the facility. Make plans for assisting employees who may need transportation.
    - Inspect areas in your facility subject to flooding. Identify records and equipment that can be moved to a higher location. Make plans to move records and equipment in case of flood.
    - Purchase a NOAA Weather Radio with a warning alarm tone and battery backup. Listen for flood watches and warnings, including:
      - **Flood Watch** — Flooding is possible. Stay tuned to NOAA radio. Be prepared to evacuate. Tune to local radio and television stations for additional information.
      - **Flood Warning** — Flooding is already occurring or will occur soon. Take precautions at once. Be prepared to go to higher ground. If advised, evacuate immediately.
    - Ask your insurance carrier for information about flood insurance. Regular property and casualty insurance does not cover flooding.
    - Consider the feasibility of flood proofing your facility. There are three basic types of methods.
      - **Permanent flood proofing measures** are taken before a flood occurs and require no human intervention when flood waters rise. They include:
        - Filling windows, doors or other openings with water resistant materials such as concrete blocks or bricks. This approach assumes the structure is strong enough to withstand flood waters.
        - Installing check valves to prevent water from entering where utility and sewer lines enter the facility.
        - Reinforcing walls to resist water pressure. Sealing walls to prevent or reduce seepage.
        - Building watertight walls around equipment or work areas within the facility that are particularly susceptible to flood damage.
        - Constructing floodwalls or levees outside the facility to keep flood waters away.

        - Elevating the facility on walls, columns or compacted fill. This approach is most applicable to new construction, though many types of buildings can be elevated.
    - **Contingent flood proofing measures** are also taken before a flood but require some additional action when flooding occurs. These measures include:
        - Installing watertight barriers called flood shields to prevent the passage of water through doors, windows, ventilation shafts or other openings;
        - Installing permanent watertight doors; and
        - Constructing movable floodwalls.
        - Installing permanent pumps to remove flood waters
    - **Emergency flood proofing measures** are generally less expensive than those listed above, though they require substantial advance warning and do not satisfy the minimum requirements for watertight flood proofing as set forth by the National Flood Insurance Program (NFIP). They include:
        - Building walls with sandbags;
        - Constructing a double row of walls with boards and posts to create a "crib," then filling the crib with soil; and
        - Constructing a single wall by stacking small beams or planks on top of each other.
- **Consider the need for backup systems:**
    - Portable pumps to remove flood water;
    - Alternate power sources such as generators or gasoline-powered pumps; and
    - Battery-powered emergency lighting.
- **Participate in community flood control projects.**

- **Hurricanes** - Hurricanes are severe tropical storms with sustained winds of 74 miles per hour or greater. Hurricane winds can reach 160 miles per hour and extend inland for hundreds of miles. Hurricanes bring torrential rains and a storm surge of ocean water that crashes into land as the storm approaches. Hurricanes also spawn tornadoes. Hurricane advisories are issued by the National Weather Service as soon as a hurricane appears to be a threat. The hurricane season lasts from June through November.

    - **Planning Considerations** - The following are considerations when preparing for hurricanes:
        - Ask your local emergency management office about community evacuation plans.
        - Establish facility shutdown procedures. Establish warning and evacuation procedures. Make plans for assisting employees who may need transportation.
        - Make plans for communicating with employees' families before and after a hurricane.
        - Purchase a NOAA Weather Radio with a warning alarm tone and battery backup. Listen for hurricane watches and warnings.
            - **Hurricane Watch** — A hurricane is possible within 24 to 36 hours. Stay tuned for additional advisories. Tune to local radio and television stations for additional information. An evacuation may be necessary.
            - **Hurricane Warning** — A hurricane will hit land within 24 hours. Take precautions at once. If advised, evacuate immediately.
        - Survey your facility. Make plans to protect outside equipment and structures.
        - Make plans to protect windows. Permanent storm shutters offer the best protection. Covering windows with 5/8" marine plywood is a second option.

- Consider the need for backup systems:
  - Portable pumps to remove flood water;
  - Alternate power sources such as generators or gasoline-powered pumps; and
  - Battery-powered emergency lighting.
- Prepare to move records, computers and other items within your facility or to another location.

- **Tornadoes** - Tornadoes are incredibly violent local storms that extend to the ground with whirling winds that can reach 300 mph. Spawned from powerful thunderstorms, tornadoes can uproot trees and buildings and turn harmless objects into deadly missiles in a matter of seconds. Damage paths can be in excess of one mile wide and 50 miles long. Tornadoes can occur in any state but occur more frequently in the Midwest, Southeast and Southwest. They occur with little or no warning.

  - **Planning Considerations** - The following are considerations when planning for tornadoes:
    - Ask your local emergency management office about the community's tornado warning system.
    - Purchase a NOAA Weather Radio with a warning alarm tone and battery backup. Listen for tornado watches and warnings.
      - **Tornado Watch** — Tornadoes are likely. Be ready to take shelter. Stay tuned to radio and television stations for additional information.
      - **Tornado Warning** — Tornadoes have has been sighted in the area or is indicated by radar. Take shelter immediately.
    - Establish procedures to inform personnel when tornado warnings are posted. Consider the need for spotters to be responsible for looking out for approaching storms.
    - Work with a structural engineer or architect to designate shelter areas in your facility. Ask your local emergency management office or National Weather Service office for guidance.
    - Consider the amount of space you will need. Adults require about six square feet of space; nursing home and hospital patients require more.
    - The best protection in a tornado is usually an underground area. If an underground area is not available, consider:
      - Small interior rooms on the lowest floor and without windows
      - Hallways on the lowest floor away from doors and windows
      - Rooms constructed with reinforced concrete, brick or block with no windows and a heavy concrete floor or roof system overhead
      - Protected areas away from doors and windows
      - **Note:** Auditoriums, cafeterias and gymnasiums that are covered with a flat, wide-span roof are not considered safe.
    - Make plans for evacuating personnel away from lightweight modular offices or mobile home-size buildings. These structures offer no protection from tornadoes.
    - Conduct tornado drills.
    - Once in the shelter, personnel should protect their heads with their arms and crouch down.

- **Severe Winter Storms** - Severe winter storms bring heavy snow, ice, strong winds and freezing rain. Winter storms can prevent employees and customers from reaching the facility, leading to a temporary shutdown until roads are cleared. Heavy snow and ice can also cause structural damage and power outages.

  - **Planning Considerations** - Following are considerations for preparing for winter storms:
    - Listen to NOAA Weather Radio and local radio and television stations for weather information:
      - **Winter Storm Watch** — Severe winter weather is possible.
      - **Winter Storm Warning** — Severe winter weather is expected.
      - **Blizzard Warning** — Severe winter weather with sustained winds of at least 35 mph is expected.
      - **Traveler's Advisory** — Severe winter conditions may make driving difficult or dangerous.
    - Establish procedures for facility shutdown and early release of employees.
    - Store food, water, blankets, battery-powered radios with extra batteries and other emergency supplies for employees who become stranded at the facility.
    - Provide a backup power source for critical operations.
    - Arrange for snow and ice removal from parking lots, walkways, loading docks, etc.

- **Earthquakes** - Earthquakes occur most frequently west of the Rocky Mountains, although historically the most violent earthquakes have occurred in the central United States. Earthquakes occur suddenly and without warning. Earthquakes can seriously damage buildings and their contents; disrupt gas, electric and telephone services; and trigger landslides, avalanches, flash floods, fires and huge ocean waves called tsunamis. Aftershocks can occur for weeks following an earthquake. In many buildings, the greatest danger to people in an earthquake is when equipment and non-structural elements such as ceilings, partitions, windows and lighting fixtures shake loose.

  - **Planning Considerations** - Following are guidelines for preparing for earthquakes:
    - Assess your facility's vulnerability to earthquakes. Ask local government agencies for seismic information for your area.
    - Have your facility inspected by a structural engineer. Develop and prioritize strengthening measures. These may include:
      - Adding steel bracing to frames
      - Adding sheer walls to frames
      - Strengthening columns and building foundations
      - Replacing unreinforced brick filler walls
    - Follow safety codes when constructing a facility or making major renovations.
    - Inspect non-structural systems such as air conditioning, communications and pollution control systems. Assess the potential for damage. Prioritize measures to prevent damages.
    - Inspect your facility for any item that could fall, spill, break or move during an earthquake. Take steps to reduce these hazards:
      - Move large and heavy objects to lower shelves or the floor. Hang heavy items away from where people work.
      - Secure shelves, filing cabinets, tall furniture, desktop equipment, computers, printers, copiers and light fixtures.

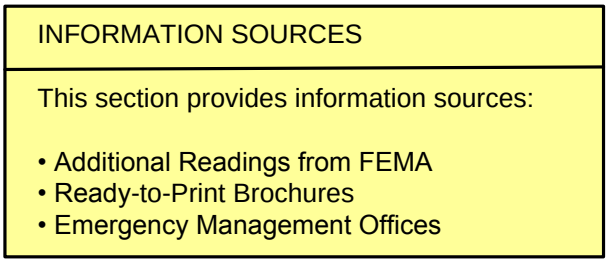
    - Secure fixed equipment and heavy machinery to the floor. Larger equipment can be placed on casters and attached to tethers which attach to the wall.
    - Add bracing to suspended ceilings, if necessary.
    - Install safety glass where appropriate.
    - Secure large utility and process piping.
  - Keep copies of design drawings of the facility to be used in assessing the facility's safety after an earthquake.
  - Review processes for handling and storing hazardous materials. Have incompatible chemicals stored separately.
  - Ask your insurance carrier about earthquake insurance and mitigation techniques.
  - Establish procedures to determine whether an evacuation is necessary after an earthquake.
  - Designate areas in the facility away from exterior walls and windows where occupants should gather after an earthquake if an evacuation is not necessary.
  - Conduct earthquake drills. Provide personnel with the following safety information:
    - In an earthquake, if indoors, stay there. Take cover under a sturdy piece of furniture or counter, or brace yourself against an inside wall. Protect your head and neck.
    - If outdoors, move into the open, away from buildings, street lights and utility wires.
    - After an earthquake, stay away from windows, skylights and items that could fall. Do not use the elevators.
    - Use stairways to leave the building if it is determined that a building evacuation is necessary.

- **Technology Emergencies** - Technological emergencies include any interruption or loss of a utility service, power source, life support system, information system or equipment needed to keep the business in operation.

  - **Planning Considerations** - The following are suggestions for planning for technological emergencies:
    - Identify all critical operations, including:
      - Utilities including electric power, gas, water, hydraulics, compressed air, municipal and internal sewer systems, wastewater treatment services
      - Security and alarm systems, elevators, lighting, life support systems, heating, ventilation and air conditioning systems, electrical distribution system.
      - Manufacturing equipment, pollution control equipment
      - Communication systems, both data and voice computer networks
      - Transportation systems including air, highway, railroad and waterway
    - Determine the impact of a service disruption.
    - Ensure that key safety and maintenance personnel are thoroughly familiar with all building systems.
    - Establish procedures for restoring systems.
    - Determine need for backup systems.
    - Establish preventive maintenance schedules for all systems and equipment.

Information Sources

Phase 4: Information Sources — where to turn for additional information.



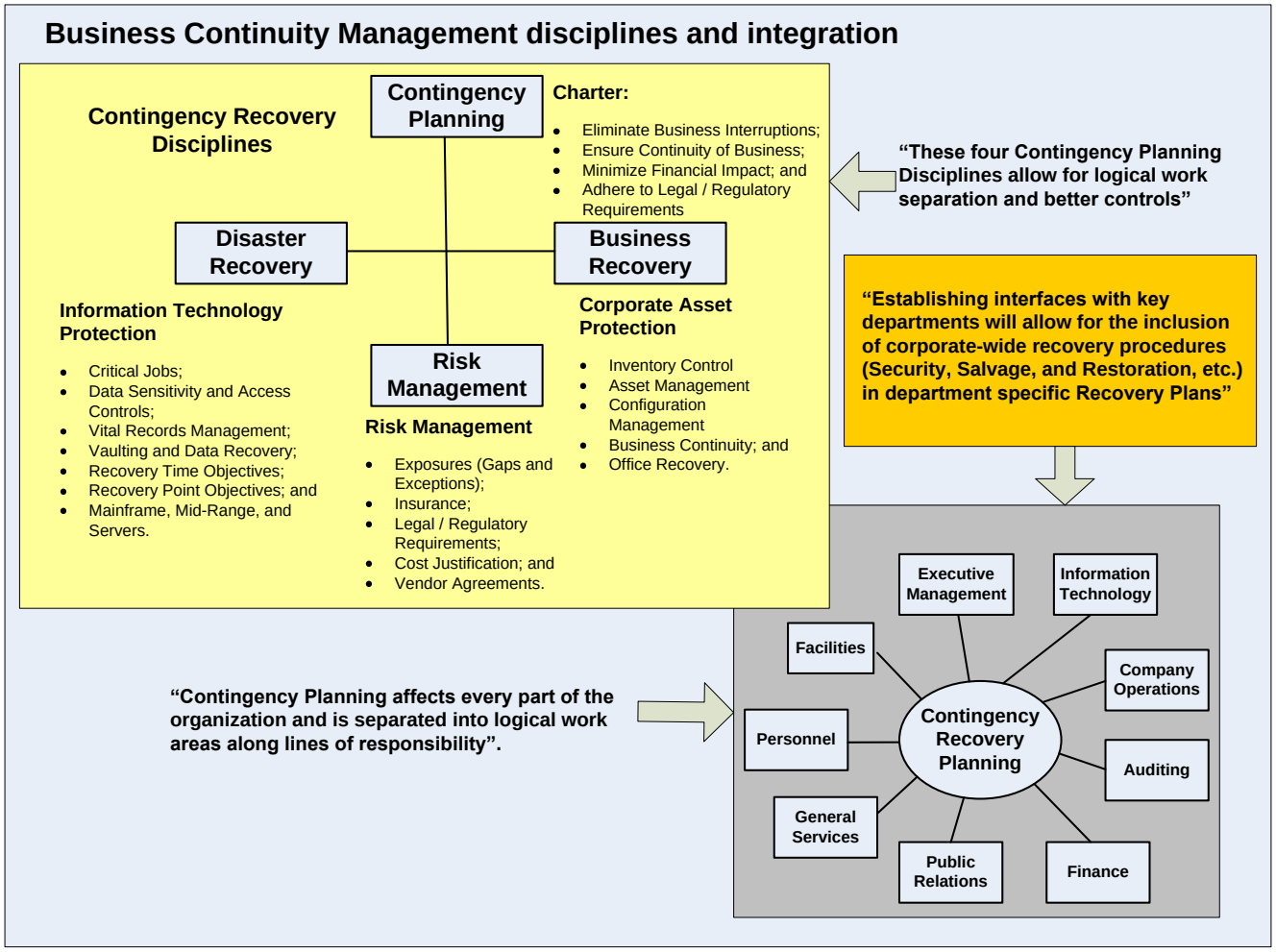
Additional information related to Emergency Management Preparedness Planning can be found through the sources listed above, or by simply performing an internet search. Additionally, industry User Groups and Certification Organizations can provide information related to Emergency Management Preparedness.

Business Continuity Management

Business Continuity Management (BCM) is responsible for: Eliminating Business Interruptions; Ensuring Continuity of Business; Minimizing the Financial Impact of a Business Interruption; Adhering to Legal / Regulatory requirements; and Protecting the Integrity and Reputation of the Business.

Business Continuity Management Disciplines

Figure 20 - Contingency Management Disciplines



Business Continuity Management is comprised of three unique disciplines including:

- **Business Continuity Planning** – to protect business locations, products, and services.
- **Disaster Recovery Planning** - to protect Information Technology resources, services, and operations.

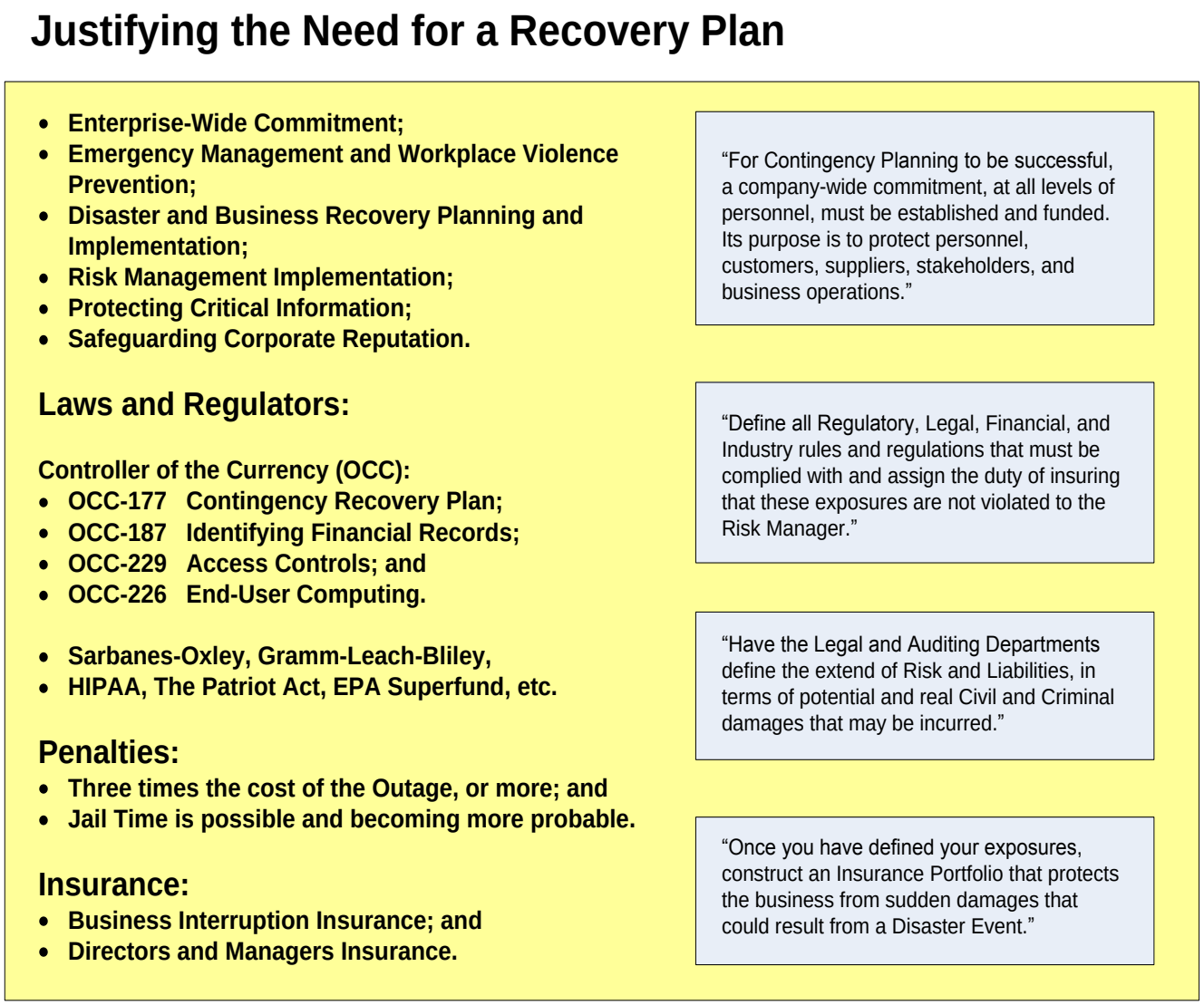
- **Risk Management** – to mitigate identified Gaps and Exposures to compliance and regulatory requirements, legal and insurance needs, vendor and supplier agreements, and insurance offerings that can be purchased to lessen the impact of an encountered disaster event.

- **Crisis Management** – to provide instructions for evacuating locations and assembly sites with procedures for ensuring personnel are accounted for. To provide media releases and a central point for corporate communications to the outside world.

Contingency Recovery Planning will require the cooperation and inclusion of personnel from many departments to plan and implement recovery planning throughout the corporation.

Laws and Regulations associated with Recovery Planning

Figure 21 - Why you need a Recovery Plan

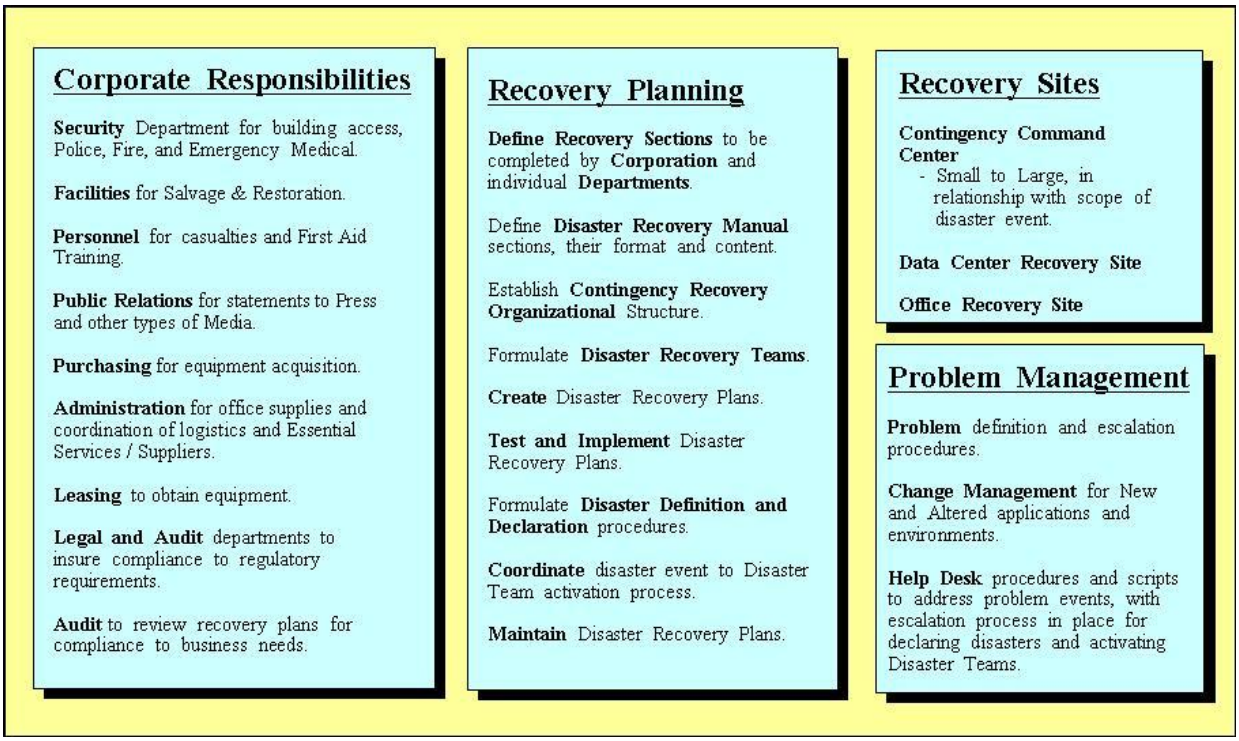


Besides Compliance Laws and Regulations, there is a need to implement Business Continuity Management disciplines to protect personnel, customers, suppliers and business operations. Business Recovery Management has to respond to the needs of the company and historic occurrences that led to the creation of these requirements.

Starting with a Korean incident when Boeing was accused of fraud by paying Korean representatives to obtain contracts for plane sales and the government asking for financial records that Boeing said they lost in an Information Technology accident, these laws were created to prevent the loss of financial and compliance data going forward. The Office of the Controller of the Currency (OCC) was the first regulating agency that required adherence to their compliance issues, the laws were later expanded by other agencies to further protect information from loss or destruction.

BCM Corporate and Departmental Responsibilities

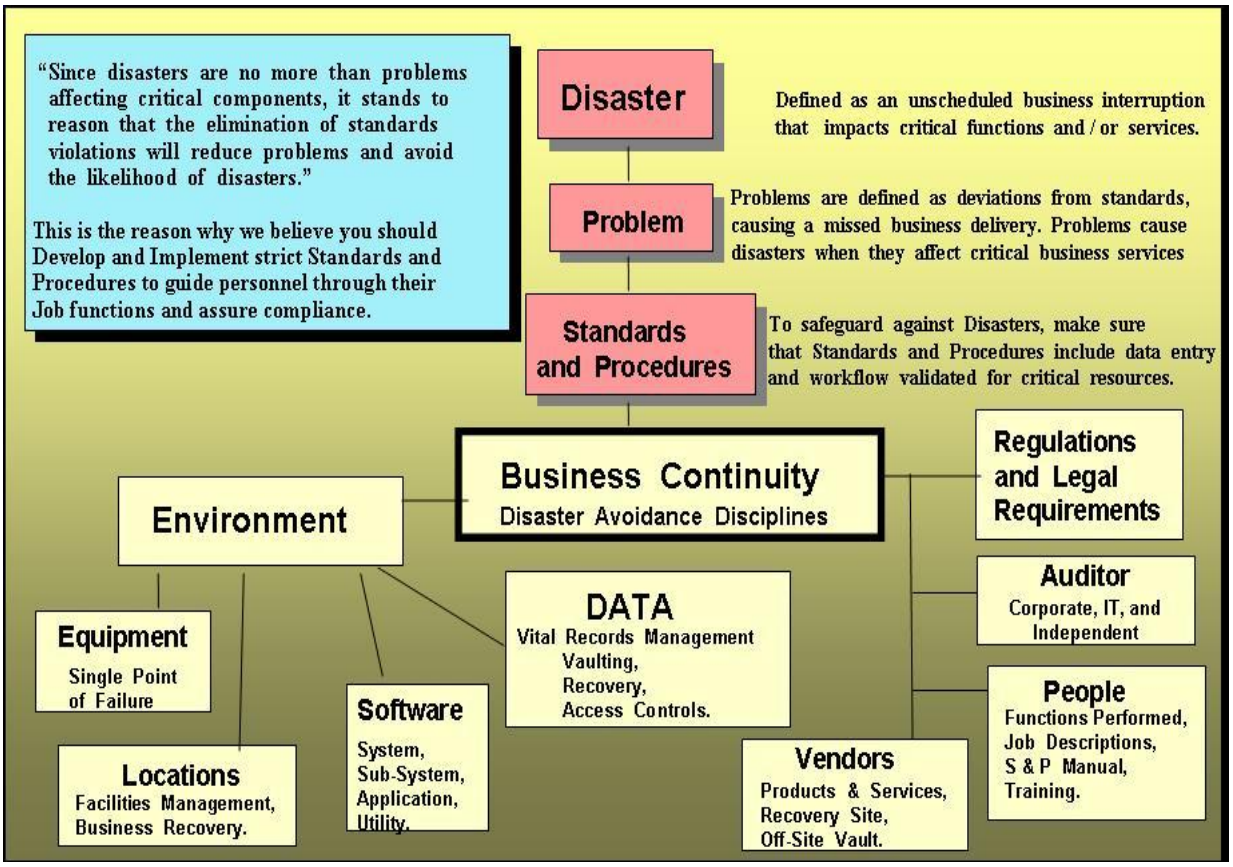
Figure 22 - BCM Corporate and Departmental Responsibilities



Corporate and Departmental responsibilities associated with Business Continuity Management planning include the areas shown above. Integrating these functions will require enhancing the Work Flow, Functional Responsibilities, Job Descriptions, and Standards and Procedures adhered to throughout the company.

Disasters and How they Occur

Figure 23 - How disaster occur, and how to avoid them



A disaster is a problem that interrupts business operations, while a problem is a deviation from standards and procedures. So, to eliminate or reduce disasters, adherence to standards and procedures must be assured.

Disaster avoidance disciplines will help reduce the likelihood of a disaster event arising from a problem incident, they include:

- Adherence to Legal and Regulatory requirements through periodic audits and the mitigation of Gaps and Exceptions uncovered during an audit.
- Have solid job descriptions for people to follow based on their functional responsibilities and ensure that a Standards and Procedures Manual is created and maintained.
- Include vendors in recovery planning to ensure continuation of supplies and services.
- Follow Vital Records Management procedures to safeguard data via backup, vaulting, and restoration of data from local and remote vaults.
- Safeguard software through vaulting and Vital Records Management.
- Develop recovery plans for all locations to ensure the safety of personnel and continuation of the business.
- Eliminate Single Point of Failure instances for critical systems.

Business Continuity Management

Figure 24 - Overview of Business Continuity Management

Business Continuity Management overview and disciplines

Business Continuity Management

Business Continuity Management disciplines are comprised of:

- Disaster Recovery to cover Information Technology;
- Business Continuity to address how to restore business operations;
- Emergency Response Planning to respond to natural disasters and environmental concerns;
- Crisis Management to protect against and coordinate actions if disaster events occur; and
- Risk Management to address compliance, vendor relationships, insurance, and business requirements.

Ten step process to develop and implement Business Continuity Management practices, include:

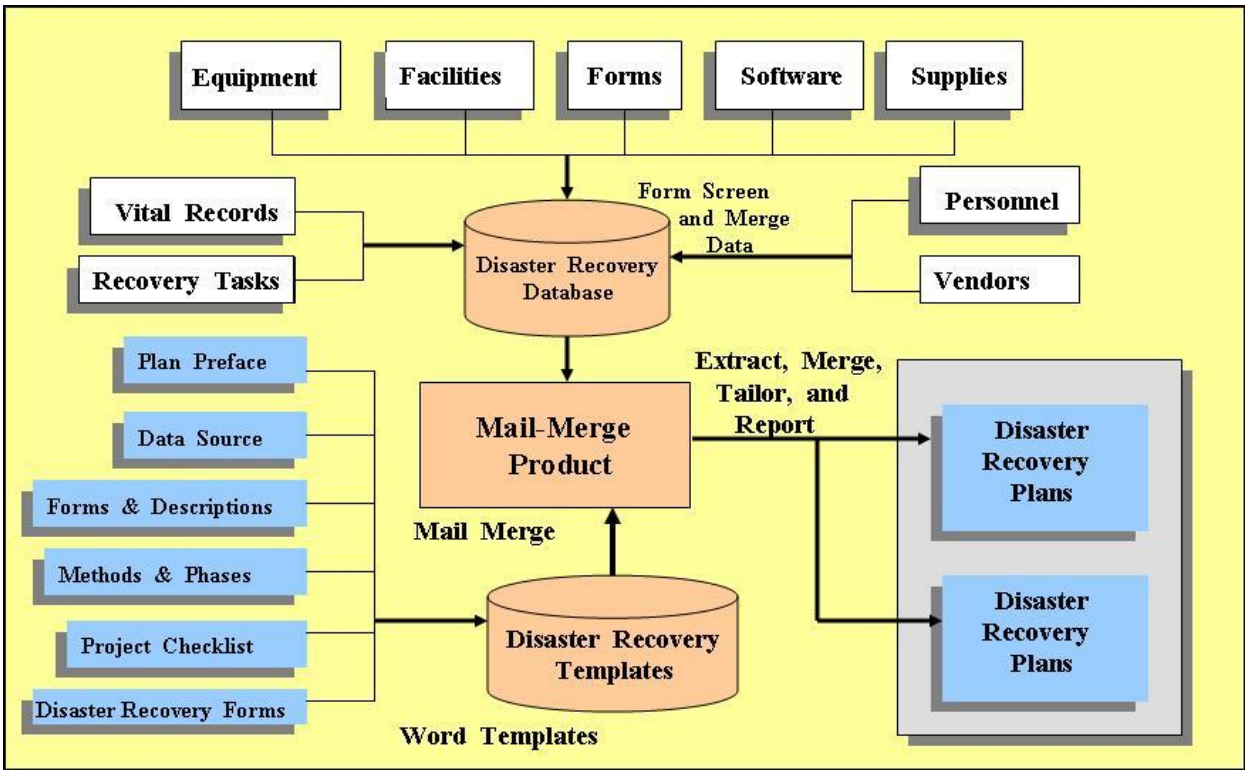
- Project Initiation and Management;
- Risk Evaluation and Control;
- Business Impact Analysis;
- Developing Business Continuity Management Strategies;
- Emergency Response and Operations;
- Developing and Implementing Business Continuity Plans;
- Awareness and Training Programs;
- Exercising and Maintaining Business Continuity Plans;
- Crisis Management and Communications; and
- Coordinating with External Agencies and the general community surrounding company locations.

Desired Results:

- Business Continuity Management disciplines implemented and integrated within everyday functions performed by staff;
- Workplace Violence Prevention Response Plan created and integrated with Standards and Procedures;
- Crisis Management Plan;
- Emergency Response Plans to address environmental and natural disasters;
- OSHA Supportive Annex created and National Response Plans provided to national agencies;
- Personnel Evacuation Plans and External Notification of Vendors and Customers of a crisis event;
- Better communications with businesses surrounding your facility;
- Better coordination with First Responders and the Police Department;
- All disciplines integrated within everyday functions performed by personnel;
- Standards and Procedures Guidelines are documented and available to authorized personnel; and
- Awareness and Training programs provided to personnel with current and accurate procedures to follow in the event of a disaster event.

Components of a Business Continuity Recovery Plan

Figure 25 - Recovery Plan data sources and output generation



By combining information obtained from the Risk Assessment and the BIA, Business Recovery Forms can be completed and recovery plans produced through normal mail-merge operations. Today's Business Recovery tools use an integrated front end to obtain the information needed to complete recovery plans. This information is merged with forms kept in a relational data base to produce recovery plans. These new tools are more efficient and are equipped with help and data entry validation to guaranty the data and plan creation meets company standards.

The Disaster Recovery Data Base can be a simple flat file or a relational data base, depending on the techniques agreed upon by your corporation. Flat files are mail-merged with forms and used to produce recovery plans. These reports are fixed and cannot be changed without recoding the report. It is difficult to mix and match data fields contained within flat files, while data base fields can be grouped via queries that make producing ad-hoc report much easier. Relational Data Bases are the recommended choice for recovery systems because of their flexibility and ability to produce ad-hoc reports in response to emergency events.

Information Technology Disaster Recovery Plans and Business Recovery Plans for Business Units and Sites can be developed and implement in the same manner through automated tools. The components contained within a Recovery Plan (white boxes above) are merged with recovery forms (blue boxes) to create a Recovery Plan. Both Disaster Recovery and Business Recovery Plans are stored on-line via automated tools and their creation or viewing can be easily performed via newly introduced automated recovery tools.

The DRII Ten-Step Disaster Recovery / Business Continuity Process

The following ten-step process for implementing recovery plans was developed by the Disaster Recovery Institute International (DRII) and is taught in its Business Continuity Certified Professional (CBCP) classes. This process is a proven method to achieve recovery operations that will protect personnel, clients, suppliers, and business operations.

1. Project Initiation and Management

a. Establish the need for a Business Continuity Plan (BCP), including:
b. Obtaining management support and guidelines,
c. Distributing BCP initiation memo outlining scope and requesting resources,
d. Creating Business Continuity Organization,
e. Managing the project to completion within agreed upon time and budget limits.

2 Risk Evaluation and Control

a. Determine the events and environmental surroundings that can adversely affect the organization and its facilities with a disruption or disaster event and calculate the damage such events can cause (Risk Identification).
b. Establish the controls needed to prevent or minimize the effects of potential loss (Problem Management and Control).
c. Provide cost-benefit analysis to justify investment in controls to mitigate risks (Risk Management).

3 Business Impact Analysis (BIA)

a. Identify the impacts resulting from disruptions and disaster scenarios that can affect the organization and techniques that can be used to quantify and qualify such impacts.
b. Establish critical functions, their recovery priorities, and inter-dependencies so that Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) can be set.

4 Developing Business Continuity Strategies

a. Determine and guide the selection of alternative business recovery operating strategies for recovery of business and information technologies within the recovery time objective, while maintaining the organization's critical functions.
b. Deliver solutions.

5 Emergency Response and Operations

a. Develop and implement procedures for responding to and stabilizing the situation following an incident or event.
b. Establish and manage an Emergency Operations Center (EOC) to be used as a command center during the emergency.
c. Demonstration of practical experience in handling an Emergency.

6 Design and Implementing Business Continuity Plans

a. Design, develop, and implement the Business Continuity Plan that provides recovery within the recovery time objective.

7 Awareness and Training Programs

a. Prepare a program to create corporate awareness and enhance the skills required to develop, implement, maintain, and execute the Business Continuity Plan.

8 Maintaining and Exercising Business Continuity Plans

a. Pre-plan and coordinate plan exercises, evaluate and document plan exercise results, and make improvements to plans as necessary.
b. Develop processes to maintain the currency of continuity capabilities and the plan document in accordance with the organization's strategic direction.
c. Verify that the Plan will prove effective by comparison with a suitable standard, and report results in a clear and concise manner.

9 Public Relations and Crisis Communication

a. Develop, coordinate, evaluate, and exercise plans to handle the media during crisis situations.
b. Develop, coordinate, evaluate, and exercise plans to communicate with key customers, critical suppliers, owners/stockholders, and corporate management during crisis.
c. Ensure all stakeholders are kept informed on an as-needed and continuing basis.
d. Provide trauma counseling for employees and their families.

10 Coordination with Public Authorities

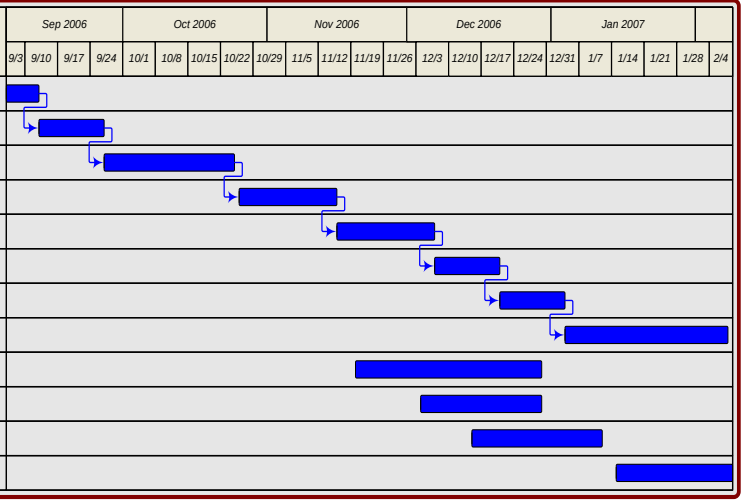
a. Establish applicable procedures and policies for coordinating response, continuity, and restoration activities with local authorities while ensuring compliance with applicable statutes or regulations.
b. Demonstration of practical experience in dealing with Local Authorities

DRII Ten-Step Process Project Plan

Figure 26 - Business Continuity Management Project Plan overview

Business Continuity Planning Project Gantt Chart

ID	Task Name	Start	Finish	Duration
1	Project Initiation and Management	9/6/2006	9/12/2006	1w
2	Risk Evaluation and Control	9/13/2006	9/26/2006	2w
3	Business Impact Analysis	9/27/2006	10/24/2006	4w
4	Develop Business Continuity Strategies	10/26/2006	11/15/2006	3w
5	Emergency Response and Operations	11/16/2006	12/6/2006	3w
6	Crisis Communications	12/7/2006	12/20/2006	2w
7	Coordination with External Agencies	12/21/2006	1/3/2007	2w
8	Developing and Implementing Business Continuity Plans	1/4/2007	2/7/2007	5w
9	Awareness and Training Programs	11/20/2006	12/29/2006	6w
10	Integration with SDLC (Development)	12/4/2006	12/29/2006	4w
11	Integration with ITIL (Maintenance)	12/15/2006	1/11/2007	4w
12	Ongoing Support & Maintenance	1/15/2007	2/16/2007	5w

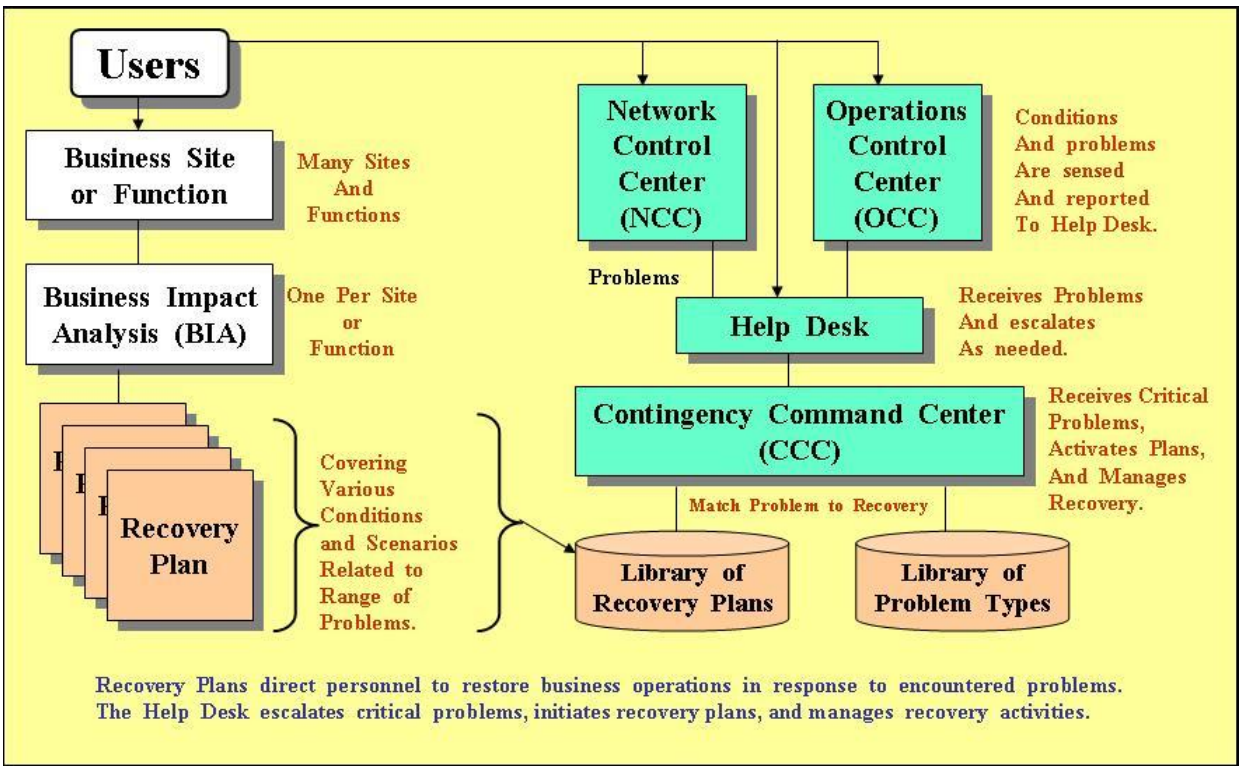


1. **Project Initiation** – establishes need for a Business Continuity Plan (BCP) and gains management support. Defines process for creating BCP and solicits personnel to contribute to BCP development and implementation.
2. **Risk Evaluation and Control** – defines what a Risk Assessment is and how to apply it to the organization. A Risk Assessment is then performed to define major areas of concern (Compliance, Vital Records, etc.).
3. **Business Impact Analysis** – used to categorize each business location as to their importance and determines the resources needed to support the business function (personnel, supplies, fixed assets, IT, RTO, RPO, etc.).
4. **Develop Business Continuity Strategies** – Determine which strategies to apply to various recovery conditions and events that are best suited to the company and its personnel.
5. **Emergency Response Operations** – define Emergency Management structure and operation, including: identification of problem, first responders, escalation, and notification procedures. During this phase you will define emergency evacuation and personnel safety, plan activation procedures, Emergency Operations Center activation, and Command Center activation.
6. **Crisis Communications** – designed to assist in the development of communicating the status of the crisis to various media (TV, Radio, Papers, employees, stock holders, etc.).

7. **Coordinating with External Agencies** – how to apply communications techniques, investigate partnering, and review Incident Command System procedures. Compliance issues will also be addressed in detail during this phase so that all BCP personnel will understand terminology, priorities of first responders, and how to interface with emergency agencies.
8. **Developing and Implementing Business Continuity Plans** – Plan Activation and Plan Development guidelines will be established so that management knows how to activate Recovery Plans, the Emergency Management structure, and procedures for managing a crisis and implementing action plans to recover from a disaster event.
9. **Awareness and Training Programs** - must be designed and provided to BCP personnel and all personnel associated with recovering from a disaster event. Hands on training will be provided to Recovery Team Members so that they know how to use the tools at their disposal and to respond to the specific disaster event.
10. **Integration with System Development Life Cycle (SDLC)** – Once established, it is imperative to maintain BCP standards over new applications or other business services that will need a recovery plan or are already part of a critical business function. This process is designed to maintain BCP standards over any new entity entering the critical business environment, or changes made to existing critical components..
11. **Integration with Information Technology Information Library (ITIL)** - or Change Management so that enhancements or problem resolutions to existing applications or critical business locations are added to Recovery Plans.
12. **Ongoing Support and Maintenance** – is designed to maintain Business Continuity and Disaster Recovery Plans in a constant state of readiness, as well as providing training and refresher courses to personnel.

Business Continuity and BIA Relationship

Figure 27 - Overview of Business Continuity Planning and BIA's



A Business Impact Analysis is used to define business units or functions, their relative importance to the business, and what is needed to protect them from a disaster event. The above illustration shows how Business Sites or Functions are evaluated through the BIA process. The BIA is used to help construct Recovery Plans that are stored in a Library. This Library of Recovery Plans can be accessed by the Help Desk which would respond to certain types of problems by pulling the Recovery Plan and initiating the calling of personnel responsible for executing the recovery plan.

Utilizing the Help Desk to initiate a Recovery Plan is a good way to integrate recovery operations because personnel are used to calling the Help Desk when a problem arises. The Help Desk staff can recognize that this particular problem is critical in nature and that a recovery plan should be activated. Once activated, recovery personnel are contacted through a calling tree of people from management to team members who are informed of the problem and directed to execute their recovery tasks as defined in the recovery plan and practiced through recovery tests.

Sections included in a BIA are

BIA Overview including – defining Products and Services provided by the Business Unit / Site, Impact Indicators of their use or loss, Enterprise Shareholders using the products or services, and Personnel used to create, support, and maintain the product or service. A Risk Rating (High, Medium, or Low) is assigned to each function or site which is used to define the overall impact should the Business Function or Site be lost due to a disaster event.

BIA Scoring – the second section of the BIA is used to assign a number value to the Risk Rating of High, Medium, or Low and total the Risk Rating of all categories to define the overall Risk Rating associated with the Business Function or Site being evaluated by the BIA.

BIA Business Scope – used to define the Business Unit within the overall Organization or the Location where the Business Unit is housed. This allows you to determine the impact of a lost Business Application used by many geographically dispersed Business Units or the loss of a Physical Site housing many Business Units. The names and contact information of personnel and address of the business site are included in this section of the BIA. Sections include:

- Organization location (Line Of Business, Division, Department, Business Unit);
- Business Unit Location(s);
- Number of Personnel at each Location;
- Product Location (could be different from BU location); and
- Contact Name and Phone Number for each application.

BIA Application Scope – includes the names of all applications used by the Business Unit, their relative importance, and Recovery Time Objectives (RTO) associated with the application. RTO Ratings include:

- Name of Server, or Mainframe, used to house the Application;
- List of all applications needed to perform a Business Function;
- Internal identification number associated with the application;
- BU Required RTO (Recovery Time Objective);
- BU Required RPO (Recovery Point Objective);
- Dependencies (predecessor and successor); and
- Work-Around Procedures in Place.

BIA Supplier Scope – used to define the Business Unit Suppliers and their relative importance to the support of the BU. Recovery responses are developed and coordinated with Suppliers to support alternate delivery and response requirements during a disaster event (such as delivering supplies to an alternate site when a disaster event occurs). Information included in this section consists of:

- Name of Server or Mainframe housing the supplier application;
- Name of Supplier Application / Product / or Service;
- Supplier company name;
- What is provided by the Supplier (Product, Application, or Service);
- Supplier Recovery Time Objective (RTO) or supplier reconnect time;
- Comments about the supplier or their product; and
- Work-Around in place or to be developed and executed during a disaster event.

Recovery Guidelines – used to define the recovery techniques available to Business Units or Locations and which one(s) they have chosen to utilize. Recovery Components are separated into groups based on their size or requirements and include:

- **Business Unit / Work Area** – site used to seat personnel should a disaster event shut down their primary location. It includes desks, computers, suppliers, and other supplies needed to support recovery operations at a remote site. Recovery Time Objectives and Options for Recovery Solutions are defined by Risk Rating within this section.

- **Computing Power Requirements** for Midrange computers, Distributed Computing / Client Server, and Mainframe computer environments are defined in this section and include: Recovery Time Objectives, Recovery Point Objectives, and Options for Recovery Solutions.

- **Supplier** recovery operations and solutions are included in this section as well.

Further instructions are divided into "Hot", "Warm", "Cold", or "Quick Ship" categories with definitions of each category provided. Additionally "Recovery Definitions" are supplied as a guideline and defined as:

- **Recovery Time Objective (RTO)** – The time associated with the recovery of a physical platform or the time that a supplier must be available after a disaster event to avoid significant impact on business operations or reputation.

- **Recovery Point Objective (RPO)** – Measures how current the restore data must be in order to resume the critical business function or avoid significant customer impact. RPO is used to define data backup and recovery schedules.

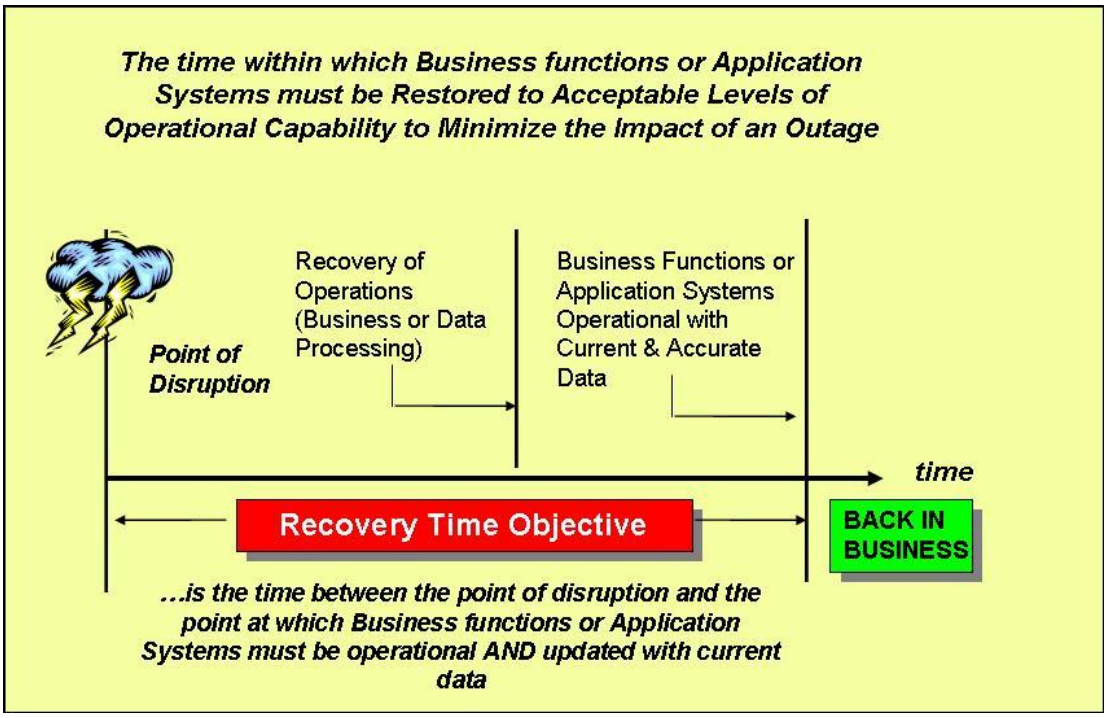
- **Recovery Time Capability (RTC)** – the demonstrated recovery time achieved through testing and actual recovery operations. If this number does not meet RPO and RTO objectives then improvements must be developed to achieve goals.

Recovery Time Objective (RTO)

The goal of Recovery Management is to ensure the safety of personnel, the locations and departments contained within the corporation, customers, suppliers, and the surrounding community – both domestically and internationally. Corporations are divided into Lines of Business that provide services to clients and internal departments. These LOB's can be dispersed geographically or within floors in a building and are supported by personnel, applications and suppliers. Should a building or application be lost, its impact could be felt by many lines of business (referred to as a Component Failure Impact Analysis). It is therefore necessary to insure that your company has the ability to restore resources, applications, or departments located in buildings within a Recovery Time Objective (RTO) defined by a Business Impact Analysis (BIA). Based on the RTO a Recovery Point Objective (RPO) can be determined so that RTO objectives are met (i.e., if you must recover operations in 4 hours and it takes five hours to recover your data, then the RTO can not be met and a better RPO must be found).

An overview of the Recovery Point Objective process is displayed below.

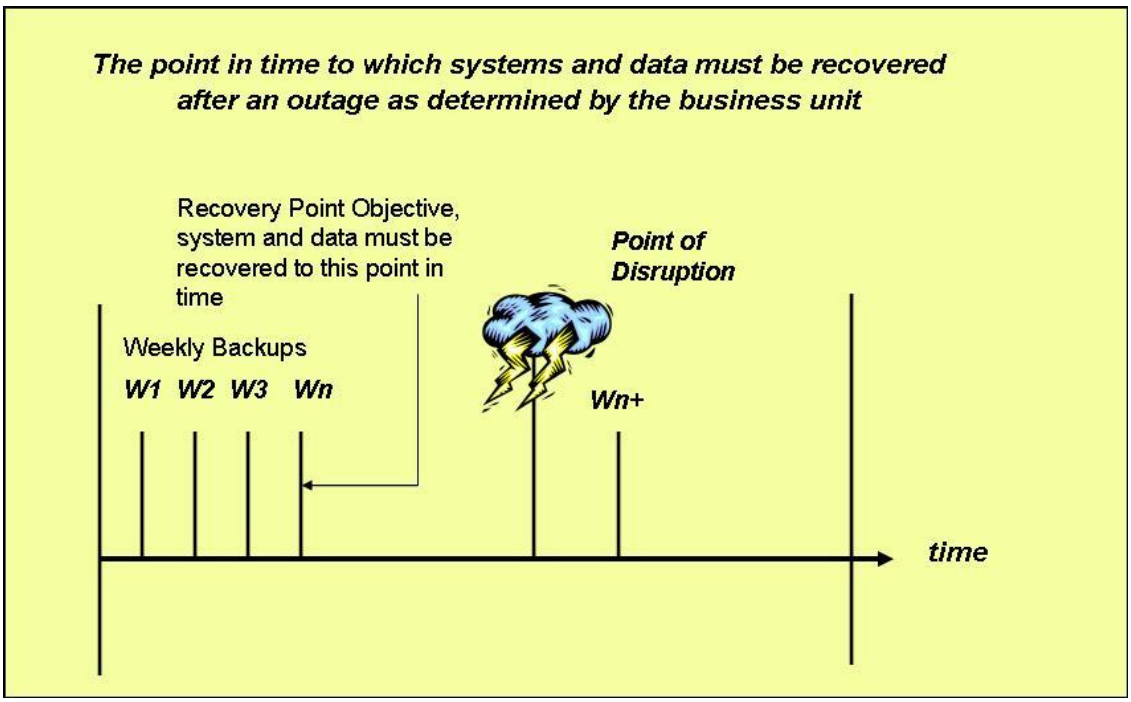
Figure 28 - Recovery Time Objective (RTO)



The RTO defines the amount of time that a recovery should be accomplished in and the Recovery Point Objective defines the steps needed to achieve the RTO. The above picture shows that all data associated with a lost operation must be loaded and ready for application use by the middle line, while applications are ready for processing at the last line. This takes into account the amount of time needed to locate and load data files and applications from vaults or other systems used to support recovery operations. If recovery times exceed RTO then improvements must be made in the process. Today's storage Management techniques support this operation in near real-time mode, thereby supporting rapid RTO goals associated with critical business functions and services.

Recovery Point Objective (RPO)

Figure 29 - Recovery Point Objective (RPO)



A Recovery Point Objective (RPO) is the point in time that data needed to support business operations must be available and loaded to system files. Applications and Information Technology (IT) services must be loaded and functional to support the RPO.

Some companies perform Backup operations on a weekly or daily basis in which all Hardware Disk Drives are copied to Cartridges and stored in Vaults (Local or Remote). In this case, the RPO is affected by the day of the week associated with a failure because the weekly backup must first be restored and then the daily backups. If the failure occurs on Thursday, you must restore the weekly cartridge and then the cartridges fro Monday – Wednesday and finally any backup data captured for Thursday (i.e., Log Tapes, Incremental Backups, etc.).

Recovery Time and Recovery Point Objectives for disaster recovery are accomplished through vaulted data files stored at remote locations. Should a file be damaged locally (i.e., Equipment Check, or Data Check), then the file can be restored from the Local Vault.

When performing a Business Impact Analysis (BIA) a Recovery Time Objective is associated with applications, business services, and vendor services. The IT Department then calculates how best to implement RPO's to support the RTO through equipment and software selections. When RTO's are short faster equipment is purchased and Storage Management is used to comply with backup and restoration requirements. Should the data be critical in nature and require access controls to protect from unauthorized access, encryption should be considered when data is backed up and restored. Also, when transporting data to off-site vaults you may want to encrypt the data to protect from loss and identity theft if the data is stolen or lost. This will protect you from the laws associated with data loss and identity theft.

Some corporations have taken the precaution to duplicate departments in multiple locations that are separated by distance and dependence on suppliers (separate telephone exchanges, electrical suppliers, communications connectivity, etc.) to eliminate any Single Point of Failure that could interrupt business operations.

Should a single location be lost, one of the other locations could pick up the load without interrupting business operations. These are called Sister Sites and when one fails the communications lines to that site are automatically switched to the Sister Site. If data bases or customer files are used, they can be passed to the Sister Site when communications is switched. This is called "Passing the Book". Employees would be able to sign-on to their business functions normally from a remote location or home after evacuating their original location. When following these procedures the failure would be transparent to end users because they would receive the same service within the same response time as before. Business recovery can be achieved by routing personnel to an alternate site that contains computer terminals and servers containing the same applications, data, and connectivity that the employees had in their normal location.

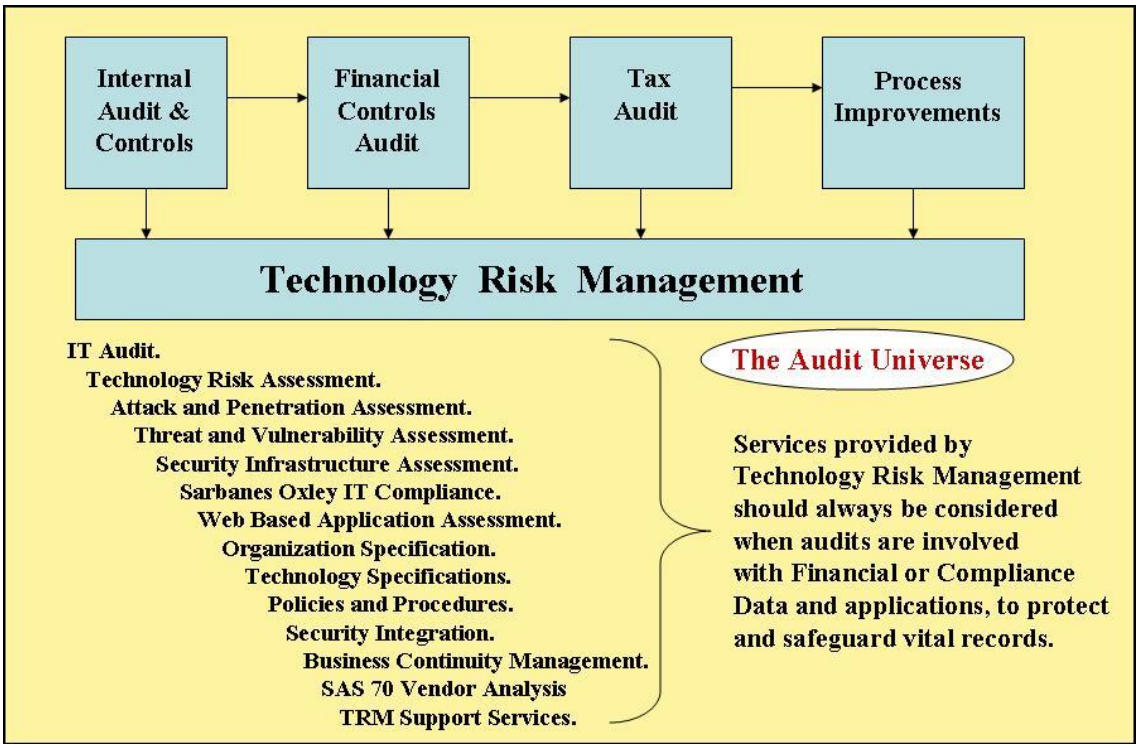
Recovering Information Technology (IT) services are a bit different, because the amount of data and equipment needed to duplicate IT services is large and RTO objectives can be difficult to achieve, but there have been many advances that are easing this burden. Failover (automatic recovery) can be achieved through VMware and Microsoft Server 2007 which support Load Balancing and Automated Recovery. Data recovery can be achieved through new Storage Systems delivered by many vendors and data protection can now be achieved through Encryption with little or no overhead. Employing these services at multiple locations can result in transparent recovery and uninterrupted business operations, but you must test, support, and maintain them to insure recovery operations.

Corporate Recovery Considerations

The BS25999 International Standard for Corporate Certification was first introduced to define the best practices associated with protecting the business environment. Recently the Private Sector Preparedness Act was introduced in the United States to tailor Corporate Certifications to the needs of American Companies. These two standards, along with NFPA 1600, can be utilized by multi-national firms to define world-wide Business Continuity and Emergency Management standards that will allow management to define the functional responsibilities and procedures assigned to personnel that will lead to a safeguarded environment that can be integrated, supported, and maintained going forward.

Risk Management

Figure 30 - Technology Risk Management disciplines and process



As Information Technology grew in importance it became necessary to develop methods for validating IT operation and effectiveness, while confirming compliance to industry and governmental regulations. Technology Risk Management was the discipline that responded to this need. Combining TRM and conventional Audit functions can be defined as the company's "**Audit Universe**" because it responds to all identified audit and compliance requirements associated with the company and its industry.

Technology Risk Management interfaces with corporate-wide regulatory requirements through:

1 - **Internal Audit and Control** procedures developed to respond to regulators;

2 - **Financial Controls Auditing** requirements used to insure that applications, services, and operations have checks-and-balances in place to validate that all financial controls are identified, in place, working appropriately, and reported on;

3 - **Tax Audits** are performed in accordance to governmental requirements and periodically reported on; and

4 - **Process Improvements** are identified and implemented to respond to improved efficiencies and enhanced operations.

Technology Risk Management disciplines

1) **IT Audit** – used to define regulatory requirements and validate that the IT environment is in compliance with them. This includes defining, implementing, and repeating audits of specific functions and services on a periodic basis.
2) **Technology Risk Assessment** – Reports on Gaps and Exceptions found during the IT Audit and defines the tasks and requirements associated with mitigating, implementing, supporting and maintaining regulatory requirements and IT efficiencies going forward.
3) **Attack and Penetration Assessment** – is responsible for reviewing the IT Security perimeter (internal and external – or physical and data) surrounding the corporation and for evaluating that an appropriate barrier to any identified weaknesses are in-place and working effectively. These responses can be as easy as locking a door or ensuring that air breathing apparatus are appropriately distributed throughout the environment, to implementing data security systems that insure that only authorized personnel are allowed access to sensitive data.
4) **Threat and Vulnerability Assessment** – this assessment defines the threats that the corporation faces and any vulnerabilities that may be included in the IT environment. As a result of this effort, management is made aware of any gaps and exposures that must be responded to.
5) **Security Infrastructure Assessment** – used to define the IT Security and access controls needed to protect sensitive data from unauthorized access. The assessment includes data sensitivity definition, defining entitlements associated with access controls, and the monitoring and reporting of security violations.
6) **IT Compliance** (Sarbanes Oxley, GLB, HIPAA, Patriot Act, etc.) – used to define the compliance requirements that the corporation must adhere to and to then perform IT Audits to ensure that compliance needs are met and that no gaps or exceptions are in existence.
7) **Web Based Application Assessment** – this function is responsible for ensuring that Web Based Applications and Services are secure and that data is protected from viruses or other security violations, both entering the IT environment or being transmitted from the IT environment (due to external or internal threat).
8) **Organization Specification** – In response to the previous TRM audits, organizational requirements can be separated into specific functional responsibilities which can be reflected by the creation of separate business functions (the IT Organizational Structure).
9) **Technology Specifications** – TRM professionals can help IT Management develop an IT Infrastructure consisting of hardware and software components that best support IT Requirements.

10) **Policies and Procedures** – once the IT Organization and IT Technology Specifications have been accepted, personnel functional responsibilities and job descriptions can be developed, then Policies (Standards) and Procedures can be developed and implemented to support personnel job requirements and corporate compliance needs.
11) **Security Integration** – Data and Physical security requirements needed to safeguard the IT and Corporate Business environment are defined, implemented, monitored, and reported on through this TRM service.
12) **Business Continuity Management and Emergency Management** – these disciplines are defined and tailored to the needs of the corporation on a world-wide basis so that any disaster event (natural or man-made) can be defined and responded to in the most efficient manner possible. This effort is made more difficult because of the many disciplines used to respond to disasters and the varying products and nomenclature used by these disciplines, tools, services, and processes.
13) **Corporate Compliance Certification**; should be defined and implemented to ensure that best practices are used to protect corporate and client products and services. How this is accomplished is the main goal of this document.
14) **TRM Support and Maintenance going forward** – must be included in the design and implementation of the TRM environment to insure that ongoing and accurate monitoring and reporting of IT compliance is always performed and provided to management and regulators.

Combining IT TRM and Auditing will ensure that Financial, Tax, Workflow Processes, and IT Operations are designed, implemented, supported, and maintained in a current and accurate manner that utilizes Best Practices to identify regulatory and business processing gaps and exceptions and recommend mitigations to meet regulatory requirements and reduce threats to personnel, business operations, or reputation.

The TRM process can be used to identify where audit controls can be integrated with work flow and personnel job functions. The Systems Development Life Cycle (SDLC) and Change Management process should be examined to insure that TRM checkpoints are included, thereby guarantying that compliance is always maintained.

Technology Risk Management and IT Security

Figure 31 - IT Security Goals and Objectives

Technology Risk Management (TRM) provides a full range of technology services, including: Data Sensitivity; IT Security; Vital Records Management; Encryption; Business Continuity Planning, and Disaster Recovery Planning.

Other disciplines perform audits on critical applications to validate compliance and identify financial data. Since Compliance Data and Applications are critical, they should have IT Security and the other TRM services applied to them.

If compliance data is lost, the company and its officers are liable for criminal and civil charges. So it is very important that management is aware of the TRM service offering and that they add TRM services to their internal operations and support organization whenever possible.

Conduct a transfer of knowledge from consulting organization to internal staff, so that continuing support and maintenance can be provided in-house. Utilize consulting organization for additional support and training going forward.

The purpose of Technology Risk Management is to identify Gaps and Exceptions to industry accepted IT practices and policies and to suggest methods to mitigate these problem areas.

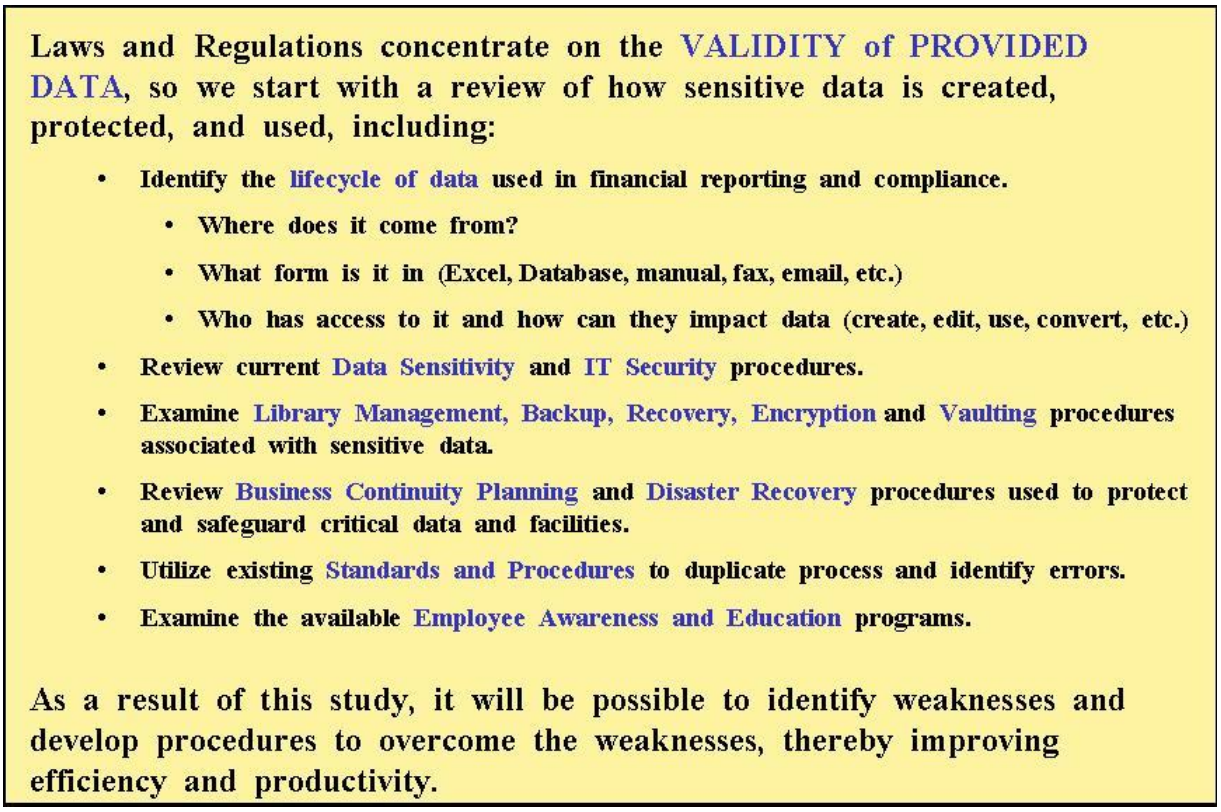
Periodic audits of the IT environment must be performed to insure on-going adherence to these guidelines. Compliance issues are also addressed by TRM along with Insurance requirements definition.

TRM functions should be integrated within the everyday functions performed by personnel, including the Systems Development Life Cycle and Change Management process so that compliance is always maintained and best practices employed and adhered to at all times.

Once standardized, TRM personnel should transfer their knowledge throughout the organization, with business units identifying Operational Risk Managers that report their findings and support TRM services with the cooperation of the corporate Technology Risk Manager.

How Technology Risk Management helps achieve Compliance

Figure 32 - How Risk Management helps reach compliance



Most compliance issues and Technology Risk Management initiatives are based on data, so it is important to perform Data Sensitivity and Vital Records Management audits to identify and safeguard sensitive data.

Once identified, the lifecycle of data is examined to see when it is created, how it is used, who has access to it and under what condition, how the data is backed up and restored, where it is vaulted and how the Library Management System interfaces with the data.

Business Continuity, Disaster Recovery, and Storage Management procedures associated with Data must be audited and reported on. Any uncovered gaps, exceptions, or weaknesses are identified and the implementation of mitigations and controls are recommended as needed.

TRM Audits are repeated on a periodic basis and results analyzed and reported on. Having a baseline to report findings against would make the audit process easier and its results better understandable. For that reason, it is recommended that TRM Audit checkpoint be utilized to make baseline comparisons more easily achievable.

As the result of an Audit, it is possible that Gaps in accounting, Exceptions from compliance standards, or Obstacles that impede production or recovery operation can be detected. When these problems are identified they are reported to management, along with their potential risk and the cost of implementing controls or problem resolutions. Management will then decide if the problem should be repaired or if insurance should be sought to protect against the problem. A method for eliminating Gaps, Exceptions, and Obstacles is shown below.

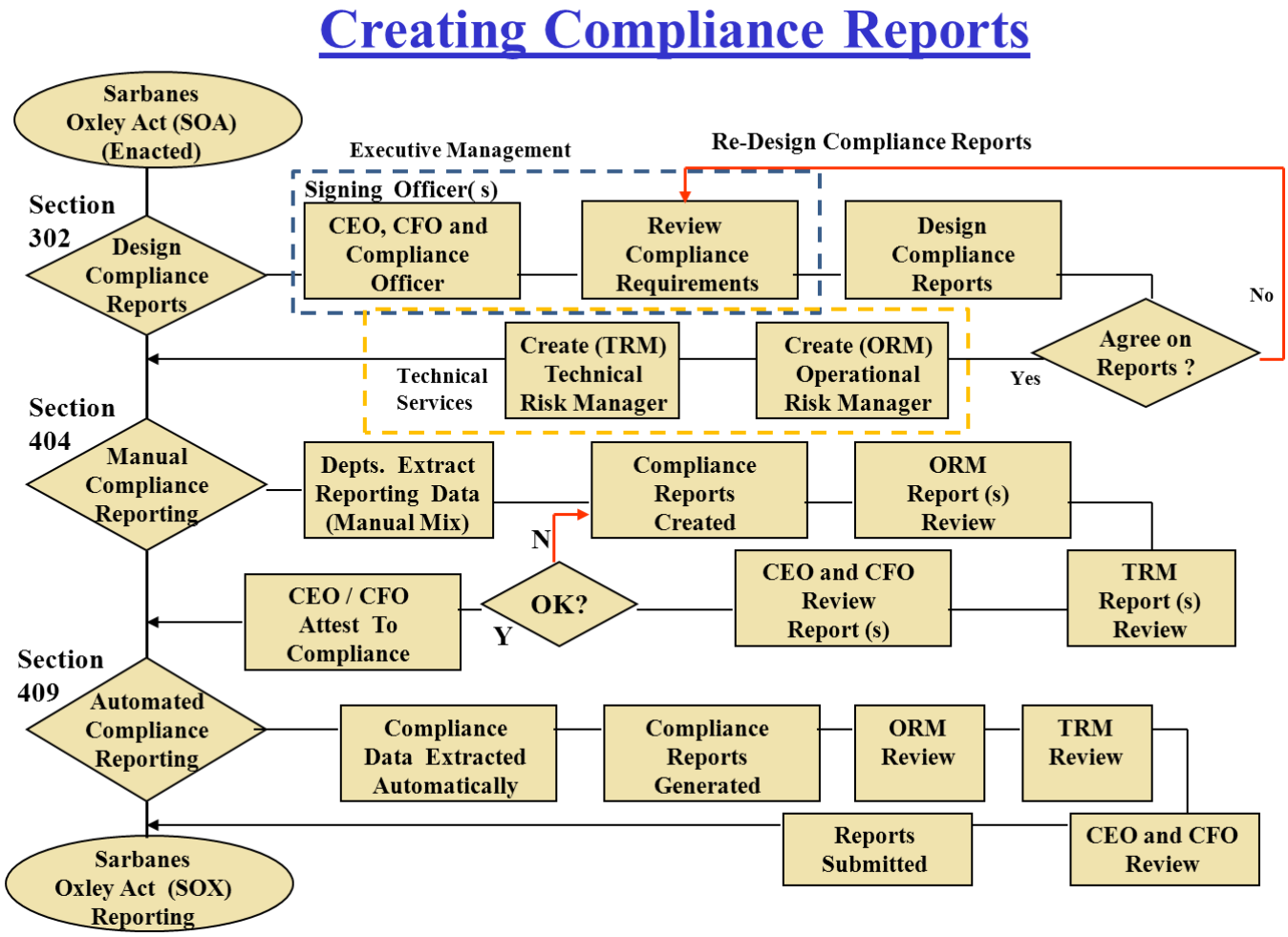
Figure 33: Strategies for eliminating Gaps, Exceptions, and Obstacles

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.

Creating Compliance Reports and a Letter of Attestation



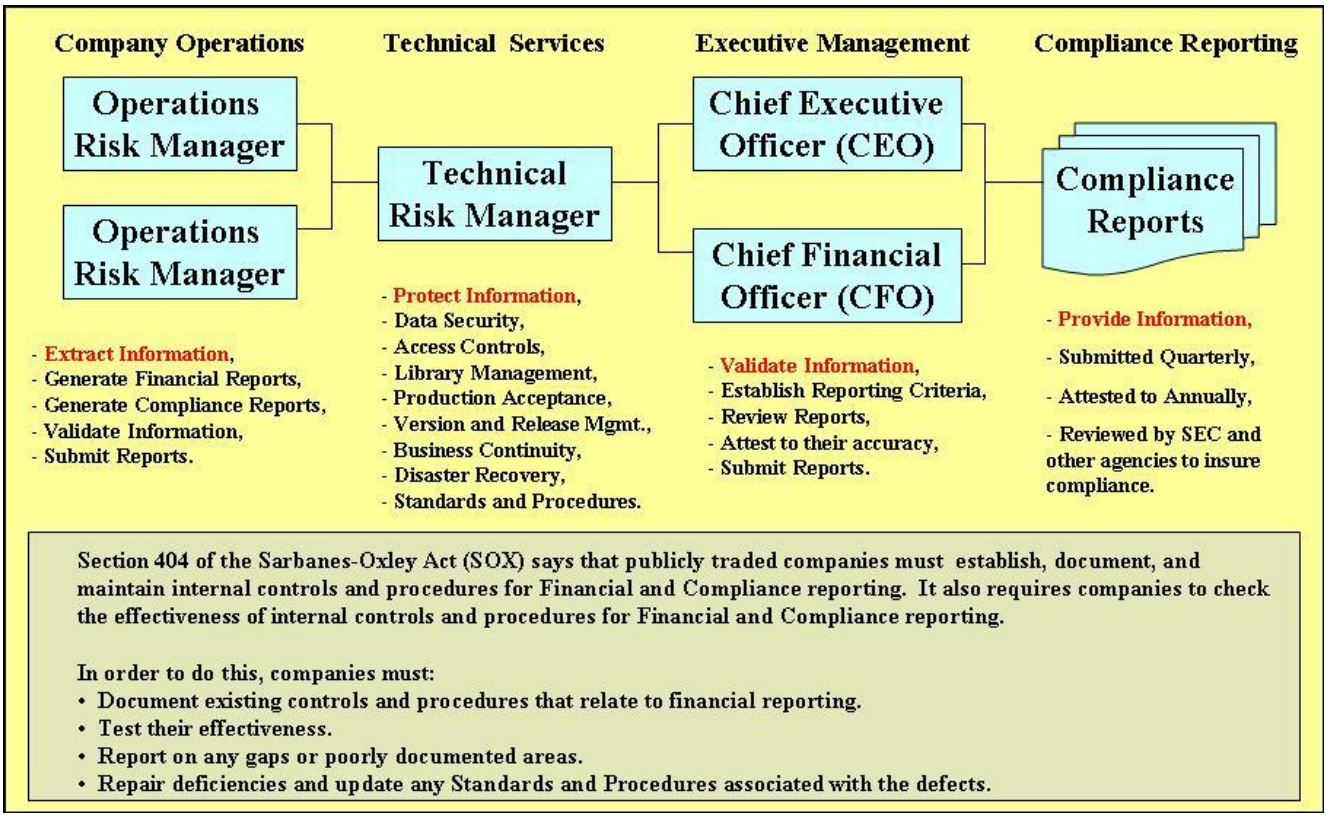
The above illustration is how Compliance Reporting is performed within a business organization with the Sarbanes Oxley (SOX) act being used as an example. The Sox Act was created after the financial crisis to ensure that financial organizations maintain current accounting methods that can be reviewed 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.

How Compliance Reporting is accomplished within an Organization

Figure 34 - Compliance Reporting Organization



To support Compliance Reporting and Recovery Operations within a corporation functional responsibilities are separated into Operational Risk Manager, Technology Risk Manager and Executive Management. Operational Risk Managers collect compliance data within their functional areas and pass the information to the Technology Risk Manager who compiles the data into management reports for approval and final reporting to compliance agencies.

This separation of responsibilities allows for better support of corporate responsibilities, improved compliance awareness, and more rapid response to compliance requirements.

Operations Risk Managers may also be responsible for completing the Business Impact Analysis (BIA) and documenting Recovery Time Objectives (RTO) for data, services, and functions. Business Recovery Plans are generated to support business operations and the Operations Risk Manager is also involved with their creation, support, and maintenance.

Workplace Violence Prevention

Workplace Violence Protection was developed to insure the safety of people and the workplace. It is primarily directed at the protection of people and the identification of potential threats, mostly related to disgruntled employees, terminated employees, and spouses who may become violent.

Services provided through Workplace Violence Prevention

Figure 35 - Workplace Violence services

Services include:

- **Management presentation on Workplace Violence Prevention and their responsibility to protect employees, customers, visitors, vendors, and neighbors;**
- **Definition of Compliance Laws and Regulations affecting the company;**
- **Workplace Violence Prevention Tabletop exercise to illustrate weaknesses and importance of a Workplace Violence Prevention Plan, Employee Assistance Programs, and Employee Handbook;**
- **Workplace Violence Prevention Risk and Vulnerability assessment to uncover exposures, gaps, and exceptions;**
- **Workplace Violence Prevention Response Plan to protect employees and minimize business interruptions (NYS Workplace Violence Prevention Law), with accompanying Employee Assistance Programs and Employee Workplace Violence Prevention Handbook;**
- **Information and Physical Security Plans to prevent unauthorized access to company locations and sensitive information;**
- **OSHA Supportive Annex and National Response Plans, as needed;**
- **Business Continuity Management services, including: Disaster Recovery, Business Continuity, Emergency Response Planning, Crisis Management, and IT Risk Management functions;**
- **Personnel Evacuation and External Notifications Plans to alert Vendors and Customers of a disaster event and instruct them on the procedures to follow during the event;**
- **Crisis Management and Communications Plans to coordinate actions with Executive Management, Personnel, First Responders, Police Department, Fire Department, Customers, Surrounding Companies within the general community, and the Media;**
- **All procedures and guidelines documented within a Standards and Procedures Manual that all authorized personnel can access;**
- **Awareness and Training programs provided to designated personnel; and**
- **On-Going Support and Maintenance going forward, as needed.**

NYS Workplace Violence Prevention Act

Figure 36 - Workplace Violence Prevention Act

NYS Workplace Violence Prevention Act

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

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

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

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

Why Workplace Violence occurs and most likely reason for offence:

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

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

Offender Profile

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

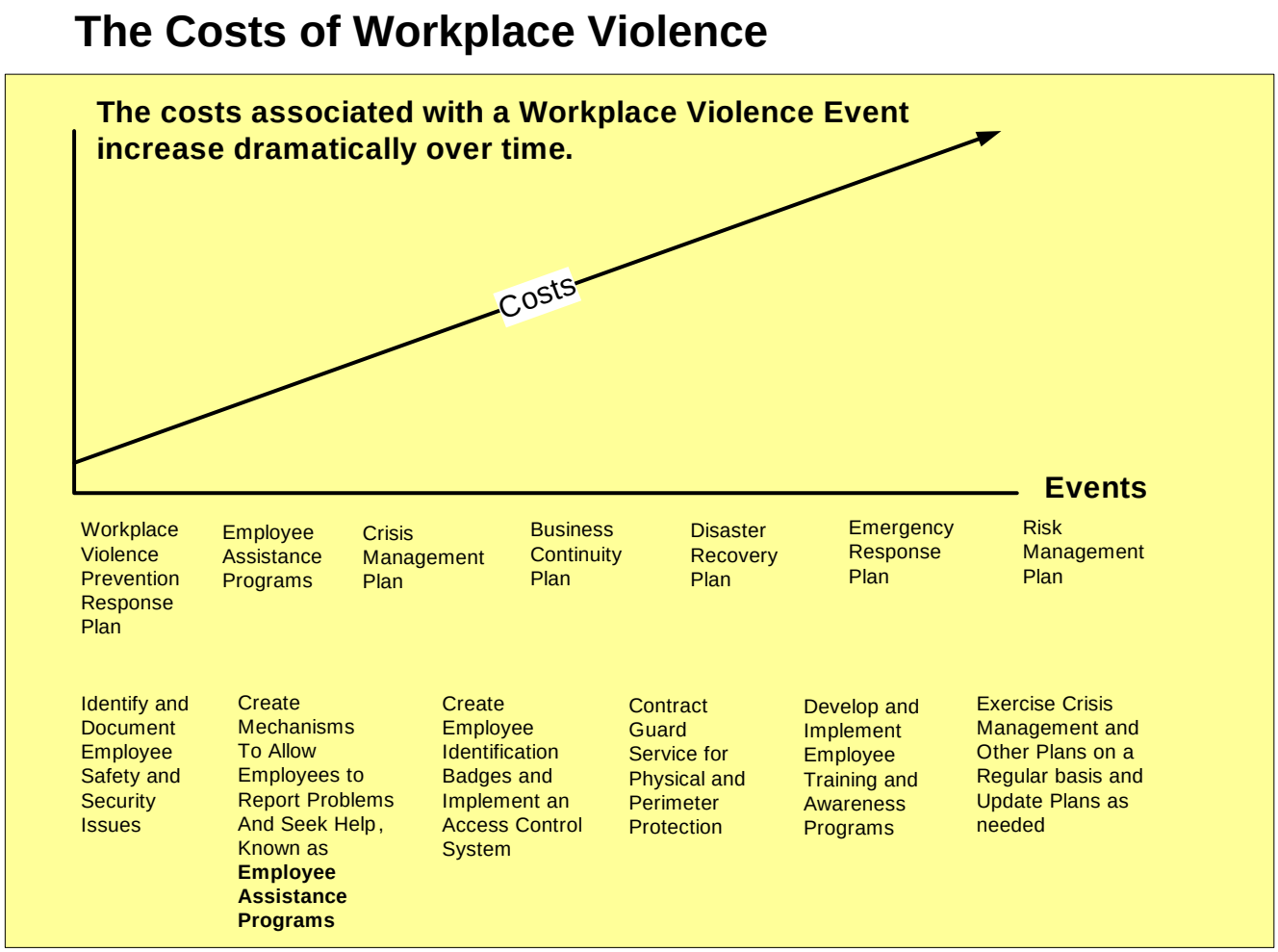
Violence Continuum

1. Indirect threats and subtle indications of discontent (body language, attitude, etc.);
2. Attention seeking activities;
3. Believes he is at last exit before toll;
    a. Adverse termination triggers Workplace Violence potential;
    b. Violent incident occurs when trauma is too great for individual;
4. Person's personality changes radically, indicating depression and giving up.
5. Withdrawal from work and society (72 hours away from violent action).

Cost associated with Workplace Violence

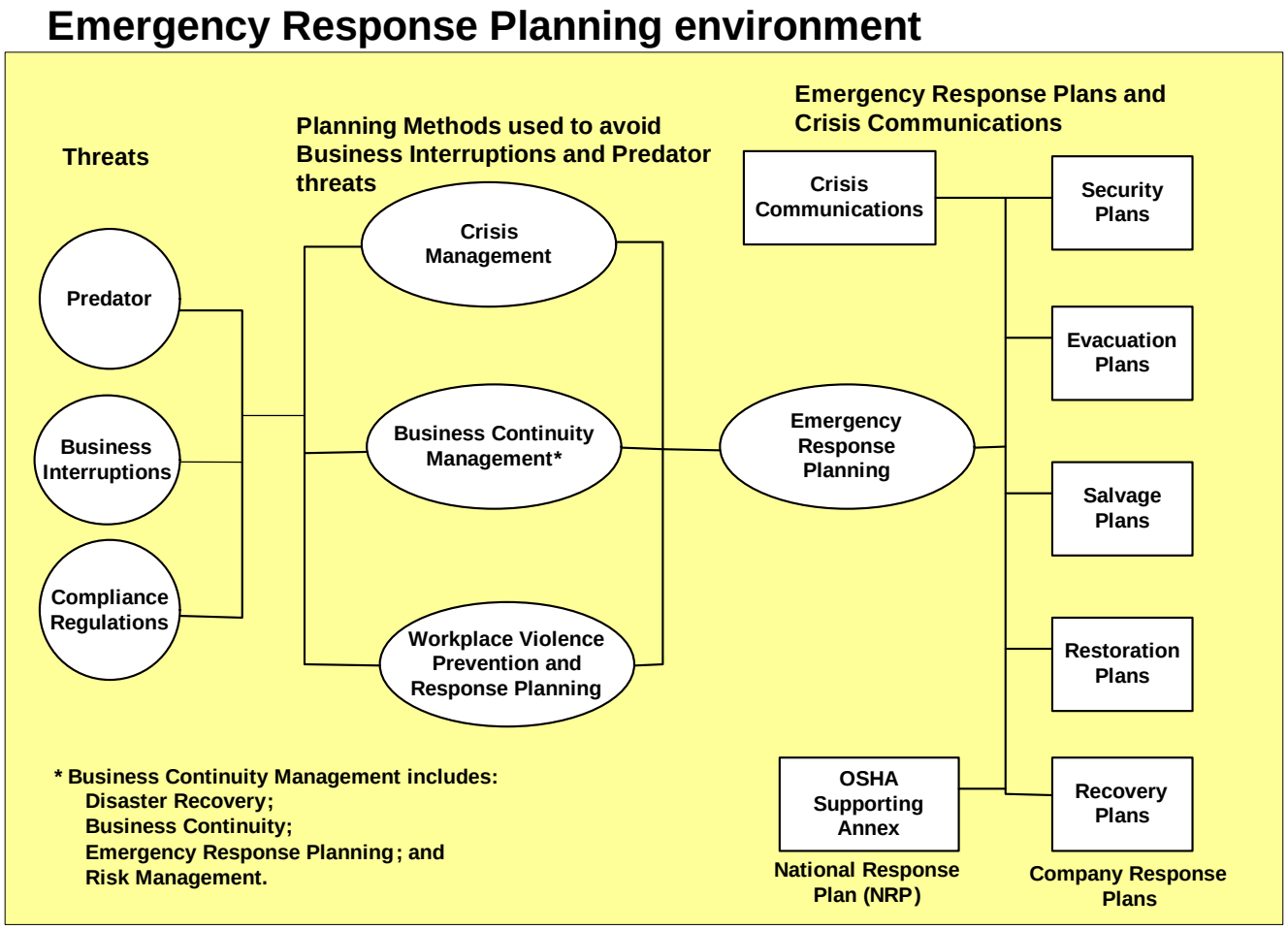
Companies can be faced with extensive costs and possible financial disaster if they do not implement a Workplace Violence Prevention program because an event can cause death or injury to personnel, damage to property and surrounding areas, and the interruption of business for the corporation and other firms located in the general vicinity of the event (Business Parks, shared building, etc.). These conditions could lead to civil and criminal charges and loss of reputation that may not be salvaged after the event. It is therefore imperative that companies address these conditions through Workplace Violence Preventions Plans and Crisis Management Plans.

Figure 37 - Costs associated with Workplace Violence



A Workplace Violence Scenario

Figure 38 - Overview of Workplace Violence scenario



The following scenario is based on actual events and is used to clearly identify how a Workplace Violence event can harm a company. It can also be used to see how easy it may be to protect the company and its employees from a Workplace Violence event.

To avoid Workplace Violence situations from causing extended damage, the above environment should be sought. It will define threats, develop methods for avoiding potential threats, and implement planned responses that adhere to regulatory requirements and provide protection for personnel, customers, suppliers, and business operations.

Scenario:

A company located in an Industrial Park on Long Island provided print supplies to firms through truck deliveries scheduled on a normal and emergency basis. The company employed 2,500 people and was a publicly traded firm. A female supervisor who was married to a male ex-supervisor, who was terminated due to poor performance and demeanor, was being threatened by her ex-husband and finally went to the police to receive a restraining order against him. After receiving the restraining

order, he called her to say he was going to get her and that a restraining order couldn't stop him. She went to work to file the restraining order with Human Resources and discuss the problem with her manager.

Before management could warn security to stop the ex-husband from entering the grounds, her ex-husband, who was known to the guards and many other people at the location, was allowed entry. He found his way to the main floor and located his ex-wife who was being escorted to the HR department by her manager. The ex-husband shot and killed her and wounded the manager. He then took a hostage and barricaded himself in the storage area that contained hazardous chemicals used in the printing process.

The company did not have a Crisis Management Plan, or an evacuation plan, so personnel were left on their own to evacuate the building and seek shelter from the gunman. Finally, the police were called and they immediately cordoned off the industrial park.

First Responders told management to recall all of their trucks so that they could check for hazardous materials. Client deliveries were missed due to this recall and many of them could not meet deadlines or satisfy customer needs, causing a ripple effect of missed deadlines and deliverables.

Finally, the police and fire department was able to resolve the issue when the gunman killed himself, but not until three people were killed and one person wounded. When the gunman shot himself he also set off a chemical reaction from the hazardous materials stored in the area he was hiding in. Since the hazardous materials were not reported to OSHA in a National Response Plan annex, the fire and police responders had to take additional precautions which prolonged the problem resolution and resulted in forced evacuations for locations surrounding the company. The incident took many hours to resolve and caused a business interruption to all of the companies in the Industrial Park, their customer and employees. Due to these interruptions, the printing firm was sued and eventually was forced to declare bankruptcy.

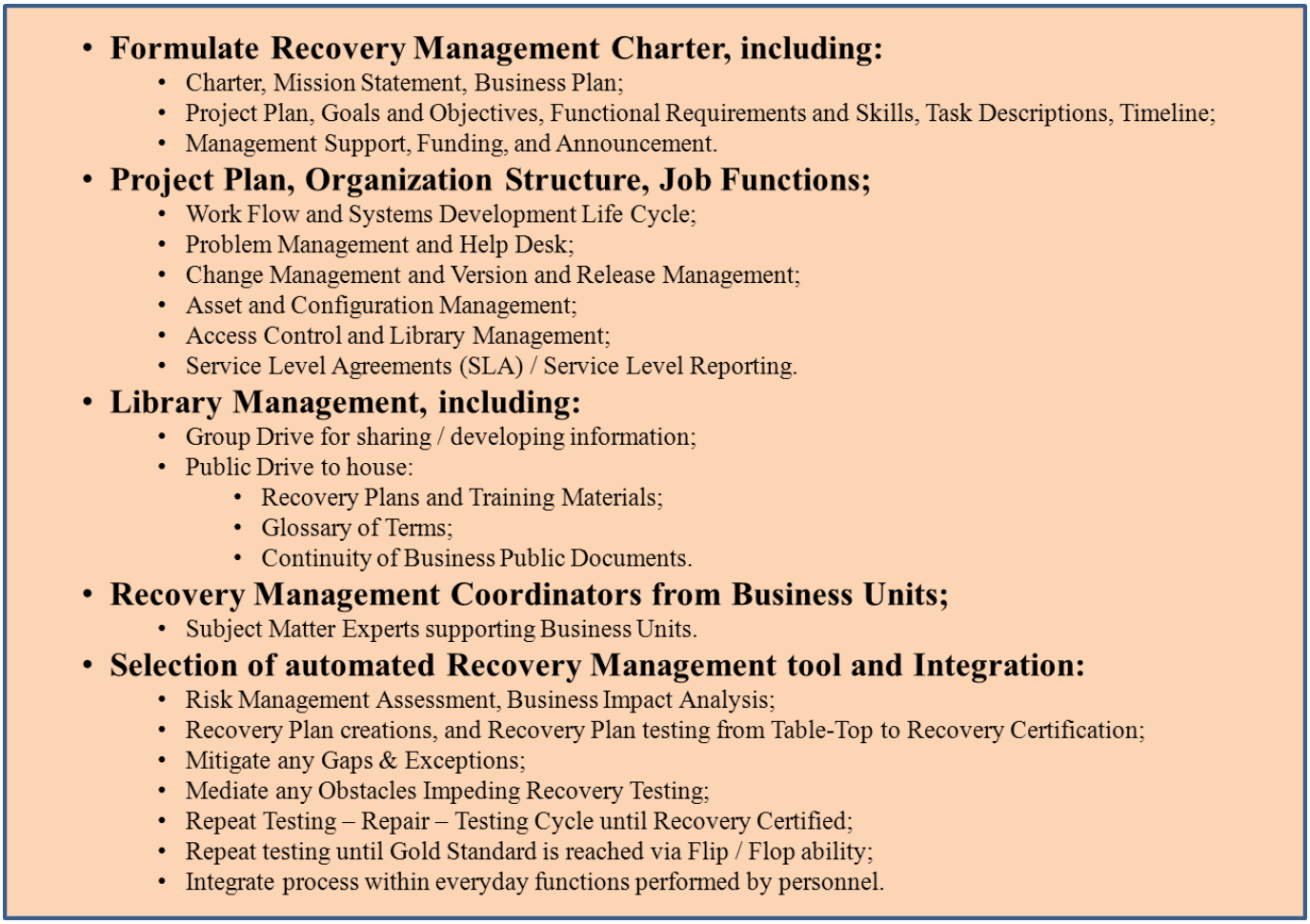
A simple solution to this type of problem would have included better physical security by the Guard, a Crisis Management and Evacuation Plan, on OSHA Supporting Annex National Response Plan for the hazardous materials, better management guidelines, and better community outreach with companies in the Industrial Park, the Fire Department, and the Police Department. A simple fix which would have cost little to nothing, but without the fix the company was dissolved - causing the loss of many jobs and forcing stock holders to pay large fines and law suites.

This sample scenario is based on a true story and can be seen over and over again in many locations, including businesses, schools, government agencies, and public locations. Since the major contributor to Workplace Violence is the loss of a job, today's economic environment makes it even more important to understanding the ramifications associated with Workplace Environment Protection. You must judge the costs of implementing Workplace Violence Prevention with the cost of not having this protection for personnel, customers, suppliers, and business operations.

It sounds like an ounce of Workplace Violence Prevention will certainly produce a pound of cure.

Steps to Recovery Management and Enterprise Resiliency

Figure 39: Steps to Recovery Management and Enterprise Resiliency



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

Figure 40: Goals and Objectives for Business Plan

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

Figure 41: Risk Management Objectives and Process

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.

Business Plan

Creating a Business Plan that outlines the direction and deliverables associated with implementing Enterprise Resilience and Corporate Certification will allow all concerned parties to have an opportunity to review the project and its deliverables. Reviewers can suggest improvements and discuss parts of the plan they do not understand, thereby providing awareness and positive input to improving the final plan. Additionally, you will solicit support for the project and the people assigned to implement Enterprise Resiliency. Examples of sections of a Business Plan may include:

Mission Statement

To implement an Enterprise Resiliency function that will combines Emergency Management, Business Continuity Management, and Workplace Violence Prevention and adheres to Domestic and International Certification Standards while utilizes industry Best Practices to protect personnel, eliminate business interruptions, and adhere to all compliance requirements. The goal of this project is to develop a common language and toolset that optimizes Recovery Operations.

Assumptions

- Management approval and support of the project and its schedule of deliverables.
- Strategic, Tactical, and Operational guidelines are defined and approved.
- Project Plan is created with personnel and required resources assigned to it.
- Review of all available Certification Standards is conducted and best standards selected to meet the specific needs of the business, while insuring that Certification Firms agree with selection.
- Continuing support and maintenance of Enterprise Resiliency will be funded going forward.

Goals and Objectives

- Performance of a Risk Assessment to define all compliance requirements.

- Review existing Recovery Operations and how they interact when emergencies arise, including:
  - Emergency Management Preparedness;
  - Business Continuity Management;
  - Workplace Violence Prevention; and
  - Enterprise Security Operations (Data and Physical).

- Review Command Centers and how they interact with Recovery Operations, including:
  - Help Desk;
  - Network Control Center (NCC);
  - Operations Control Center (OCC);
  - Incident Command Center (ICC); and
  - Emergency Operations Center (EOC).

- Review the company Lines of Business (LOB) to define:
  - Business Functions and their relative importance to the company (H, M, L);
  - Customers;
  - Applications;
  - Suppliers;
  - Employees; and
  - Locations.

- Review Business Integration requirements, including:
  - Service Level Agreements (SLA);
  - Service Level Reporting (SLR);
  - Recovery Time Objectives (RTO);
  - Recovery Point Objectives (RPO);
  - Systems Development Life Cycle (SDLC);
  - Best Practices, including:
    - COSO – Committee of Sponsoring Organizations;
    - CobIT – Control Objectives for Information Technology;
    - ITIL – Information Technology Infrastructure Library;
    - ISO 17799 – International Standard;
    - FFIEC (Federal Financial Institutions Examination Council) guidelines; and
    - Six Sigma.

- Review current Business Continuity Management practices, including:
  - Business Continuity;
  - Disaster Recovery;
  - Risk Management; and
  - Crisis Management.

- Review current Emergency Response Management practices, including:
  - State and Local Government interfaces and requirements;
  - Department of Homeland Security (DHS) guidelines and interfaces;
  - Office of Emergency Management (OEM) guidelines and interfaces; and
  - First Responders, their duties, and support requirements.

- Review of current Workplace Violence Prevention practices, including:
  - Physical Security and Perimeter Access Prevention practices;
  - Access Controls and Card Key usage;
  - Guard Posts and Security processes;
  - Video Recording and Video Storage procedures;
  - Crisis Management and Evacuation procedures;
  - Community Outreach and First Responder interactions; and
  - Awareness Training, Documentation, and Testing.

Corporate Certification Standards

Domestic and International standards established to assist corporations achieve certification have been designed to create a business recovery environment that is safeguarded and in compliance with industry and business regulations. While BS25999 has been in existence for a number of years, domestic guidelines are still being developed. Corporations should utilize these standards to govern their geographical requirements, while multi-national corporations should utilize both domestic and international standards as guidelines to achieve corporate certification. These standards are:

ISO 22301 is the new Global Standard and is scheduled to replace BS25999, but has not been implemented by many organizations as yet. You can locate more information on ISO 22301 via the internet.

BS25999 Overview

BS 25999 is the British Standards Institute (BSI) standard in the field of Business Continuity Management (BCM). This standard replaces PAS 56, a Publicly Available Specification, published in 2003 on the same subject.

BS25999 Structure

Wikipedia defines BS 25999 as a Business Continuity Management (BCM) standard consisting of two parts.

The first part, "BS 25999-1:2006 Business Continuity Management. Code of Practice", takes the form of general guidance and seeks to establish processes, principles and terminology for Business Continuity Management.

The second part, "BS 25999-2:2007 Specification for Business Continuity Management", specifies requirements for implementing, operating and improving a documented Business Continuity Management System (BCMS), describing only requirements that can be objectively and independently audited.

A useful means of understanding the difference between the two is that Part 1 is a guidance document and uses the term 'should', while Part 2 is an independently verifiable specification that uses the word 'shall'

Certification (independent verification) to this standard is available from certification bodies accredited by the United Kingdom Accreditation Service (UKAS) and is a multi stage process usually involving a number of assessment visits. The assessor will then make a recommendation that the organization receive certification or not. After initial certification a number of surveillance visits are made as per a plan to ensure that the organization is still in compliance.

BS 25999-1 code sections

1) **Scope and Applicability**. This section defines the scope of the standard, making clear that it describes generic best practices that should be tailored to the organization implementing it.
2) **Terms and Definitions**. This section describes the terminology and definitions used within the body of the standard
3) **Overview of Business Continuity Management**. A short overview is the subject of the standard. It is not meant to be a beginner's guide but describes the overall processes, its relationship with risk management and reasons for an organization to implement it along with the benefits.
4) **The Business Continuity Management Policy**. Central to the implementation of business continuity is having a clear, unambiguous and appropriately resourced policy.
5) **BCM Program Management**. Program management is at the heart of the whole BCM process and the standard defines an approach.
6) **Understanding the Organization**. In order to apply appropriate business continuity strategies and tactics the organization has to be fully understood along with, its critical activities, resources, duties, obligations, threats, risks and overall risk appetite.
7) **Determining BCM Strategies**. Once the organization is thoroughly understood the appropriate overall business continuity strategies can be defined.
8) **Developing and implementing a BCM response**. The tactical means by which business continuity is delivered. These include incident management structures, incident management, and business continuity plans.
9) **Exercising, maintenance, audit and self-assessment of the BCM culture**. Without testing the BCM response an organization cannot be certain that they will meet their requirements. Exercise, maintenance and review processes will enable the business continuity capability to continue to meet the organizations goals.
10) **Embedding BCM** into the organizations culture. Business Continuity should not exist in a vacuum but become part of the way that the organization is managed. If performing the Business Continuity process is a separate step from normal implementation and maintenance procedures, then there is a high chance that the safeguard may not be accomplished.

BS 25999-2 specifications and review

1) **Scope**. Defines the scope of the standard along with, the requirements for implementing, and operating a documented business continuity management system (BCMS)
2) **Terms and Definitions**. This section describes the terminology and definitions used within the body of the standard
3) **Planning the Business Continuity Management System (PLAN**). Part 2 of the standard is predicated on the well established ***Plan-Do-Check-Act*** model of continuous improvement. The first step is to plan the BCMS, establishing and embedding it within the organization.
4) **Implementing and Operating the BCMS (DO**). To actually implement the company recovery plan as created in Section 3. This section includes a number of topics that are found in BS25999 Part 1 although Part 1 should only be used for general guidance and information. Only what is in BS25999 Part 2 can be assessed.
5) **Monitoring and Reviewing the BCMS (CHECK).** To ensure that the BCMS is continually monitored, the Check stage covers internal audit and management reviews of the BCMS
6) **Maintaining and Improving the BCMS (ACT)** To ensure that the BCMS is both maintained and improved on an ongoing basis this section looks at preventative and corrective action

A review of BS25999 by Al Berman (Executive Director of Disaster Recovery Institute International) as printed in Baseline Magazine points out some concerns with BS25999. They include:

Admitting to a recovery plan problem during the ACT stage may be construed as "legal discovery" and could lead to a law suit. He is quoted as saying "I've been told that it is discoverable under litigation i.e., you've admitted to a deficiency. So, if you are going to go through this process and you're going to acknowledge you have deficiencies and something happens, that represents negligence at best, gross negligence at worst," Berman says. "I've had this discussion with a number of large corporations and when we get to this point they actually call their general counsel into the discussion and literally turn white when they hear the ramifications."

Mr. Berman's other concern about BS25999 is that it is not completed. If you implemented BS25999 Part 1, you would have had to change your recovery plans when BS25999 Part 2 was introduced. He recommends that you determine the current and future characteristics of the BS25999 evolution before deciding to implement the BS25999 protocol.

According to Berman, businesses need to take it slow with adoption and survey their options, because BS25999 isn't the only holistic framework available and in coming years we should expect to see even more continuity standards emerge. For example, the National Fire Prevention Association 1600 standard has been the official standard in North America for over a decade. And others are coming—currently the American National Standards Institute is charged with overseeing efforts to come up with an even more comprehensive standard in response to lawmaker's directives in the 9/11-spurred Private Sector Preparedness Act 11053.

Even with Mr. Berman's concerns, a company can implement excellent recovery plans by following the recommendations in this document through best practices and accepted recovery plan directions.

National Fire Prevention Association 1600 Standard

In an article by Donald L. Schmidt in the BNET Business Network web site. NFPA 1600 gives businesses and other organizations a foundation document to protect their employees and customers in the event of a terrorist attack.

A sweeping overhaul of the U.S. intelligence community includes provisions to make NFPA 1600, Disaster/Emergency Management and Business Continuity Programs, the national preparedness standard.

The act was approved by the Senate by an 89-2 vote, and in the House on a vote of 336-75. President Bush signed the bill into law on December 17, 2004. The law implements many of the recommendations made by the National Commission on Terrorist Attacks Upon the United States, better known as the 9/11 Commission.

The provision of the law highlighting NFPA 1600 is section 7305, Private Sector Preparedness (B) Sense of Congress on private sector preparedness, which states "It is the sense of Congress that the secretary of Homeland Security should promote, where appropriate, the adoption of voluntary national preparedness standards such as the private sector preparedness standard developed by the American National Standards Institute and based on the National Fire Protection Association 1600 Standard on Disaster/Emergency Management and Business Continuity Programs."

The Commission recommended that NFPA 1600 be recognized as the National Preparedness Standard. The Commission reviewed the need for private sector preparedness during their public hearings and noted that "the private sector controls 85 percent of the critical infrastructure in the nation," and "the 'first' first responders will almost certainly be civilians."

The Commission acknowledged the lack of a standard as a principal contributing factor to the lack of private sector preparedness and asked the American National Standards Institute (ANSI) to develop a consensus on a standard for the private sector. ANSI convened its Homeland Security Standards Panel (HSSP), which held a series of workshops attended by representatives of many industries and associations in the private sector as well as public sector officials. After reviewing available documents and studying NFPA 1600, ANSI's HSSP endorsed NFPA 1600.

NFPA 1600 has become well known in the public sector since the Emergency Management Accreditation Program (EMAP) began using NFPA 1600 as criteria for accreditation of public sector emergency management programs. EMAP is a voluntary, national accreditation process for public emergency management programs at the state, territorial, and local level. Surprisingly, however, the standard has not received as much attention in the private sector. The recommendation of the Commission has shined a bright spotlight on NFPA 1600, and now the document is receiving much more attention from business and industry.

The United States Congress actively addressed the 9/11 Commission's recommendations. HR 4830, the "Private Sector Preparedness Act of 2004," was filed and its purpose is to enhance private sector preparedness. The program elements within this legislation closely mirror those of NFPA 1600 and the bill directs the Secretary of Homeland Security to: "... support the development of, promulgate, and regularly update as necessary national voluntary consensus standards for private sector emergency

preparedness. Such standards include the National Fire Protection Association 1600 Standard on Disaster/Emergency Management and Business Continuity Programs."

NFPA 1600 isn't a handbook or "how-to" guide with instructions on building a comprehensive program. Instead, it outlines the management and elements that organizations should use to develop a program for mitigation, preparedness, response, and recovery. The Technical Committee on Emergency Management and Business Continuity has declined to prescribe a program development process leaving it up to each entity to follow a method that meets the specific needs of the entity.

NFPA 1600 requires development of a documented program that defines the entity's policy, goals, objectives, plans, and procedures. The standard also requires appointment of a program coordinator to work in conjunction with an advisory committee to develop the program. Specific program elements include: hazard identification, risk assessment, and impact analysis; hazard mitigation; resource management; mutual aid; planning; direction, control and coordination; communications and warning; operations and procedures; logistics and facilities; training, exercises, evaluations, and corrective actions; crisis communications and public information; and finance and administration. NFPA 1600 also requires compliance with applicable regulatory requirements.

NFPA 1600 requires an "all hazards" approach. There has been significant emphasis over the past three years on preparedness for terrorist attacks-and much work remains to be done. However, hurricanes, tornadoes, flooding, and other natural and manmade disasters continue to take a significant toll in lives lost, property damage, and business interruption. NFPA 1600 requires assessment of all hazards that might impact people, property, operations, and the environment. Risk assessments should quantify the probability of occurrence and the severity of their consequences. A business impact analysis (BIA) should quantify the impact a disaster will have on the organizations' mission, as well as direct and indirect financial consequences. The business impact analysis enables an organization to evaluate the cost-effectiveness of mitigation efforts and determine how much to invest in preparedness, response, and recovery plans.

Private Sector Preparedness Act

H.R. 4830 – Private Sector Preparedness Act of 2004 is a bill introduced in the U.S. House of Representatives to amend the Homeland Security Act of 2002 and direct the Secretary of Homeland Security to develop and implement a program to enhance private sector preparedness for emergencies and disasters.

Program Elements- In carrying out the program, the Secretary shall develop guidance and identify best practices to assist or foster action by the private sector including:

1) identifying hazards and assessing risks and impacts;
2) mitigating the impacts of a wide variety of hazards, including weapons of mass destruction;
3) managing necessary emergency preparedness and response resources;
4) developing mutual aid agreements;
5) developing and maintaining emergency preparedness and response plans, as well as associated operational procedures;
6) developing and maintaining communications and warning systems;
7) developing and conducting training and exercises to support and evaluate emergency preparedness and response plans and operational procedures;
8) developing and conducting training programs for security guards to implement emergency preparedness and response plans and operations procedures; and
9) developing procedures to respond to external requests for information from the media and the public.

Congress has found

Identifying standards and best practices is necessary to promote emergency preparedness by private sector organizations, in addition to educational activities to effectively communicate such standards and best practices.

As business waits for the Private Sector Preparedness Act to be finalized, business leaders around the country are not standing still. They realize that contingency planning and continuity of operations is imperative for their business survival. We can only hope that no one is waiting around for what the standards body or best practices authority will be. Let's pray that the private sector has gone beyond developing plans and now is exercising Corporate Emergency Response Team (CERT) training in all the facilities deemed to be soft targets. Without this, we will certainly not be as ready as we could be. And once we have trained and tested numerous times, we will know what to improve and how to change the procedures accordingly.

Some areas that should be investigated by corporations include:

1. Recovery disciplines currently employed by the corporation like:
    a. Emergency Management;
    b. Business Continuity Management;
    c. Compliance and Regulatory Requirements and Adherence practices;
    d. Workplace Violence Prevention policies and practices;
    e. Organizational structure associated with Recovery Operations;
    f. Languages and Tools used to support Recovery Operations; and
    g. Command Centers and how they interact during an Emergency event.

2. How to improve Recovery Operations and minimize Business Interruptions.

3. Combination of Recovery Operations to optimize performance and response times.

Once the direction of Recovery Operations has been decided upon, it is imperative to integrate Recovery Operations into the everyday functions performed by personnel. This includes:

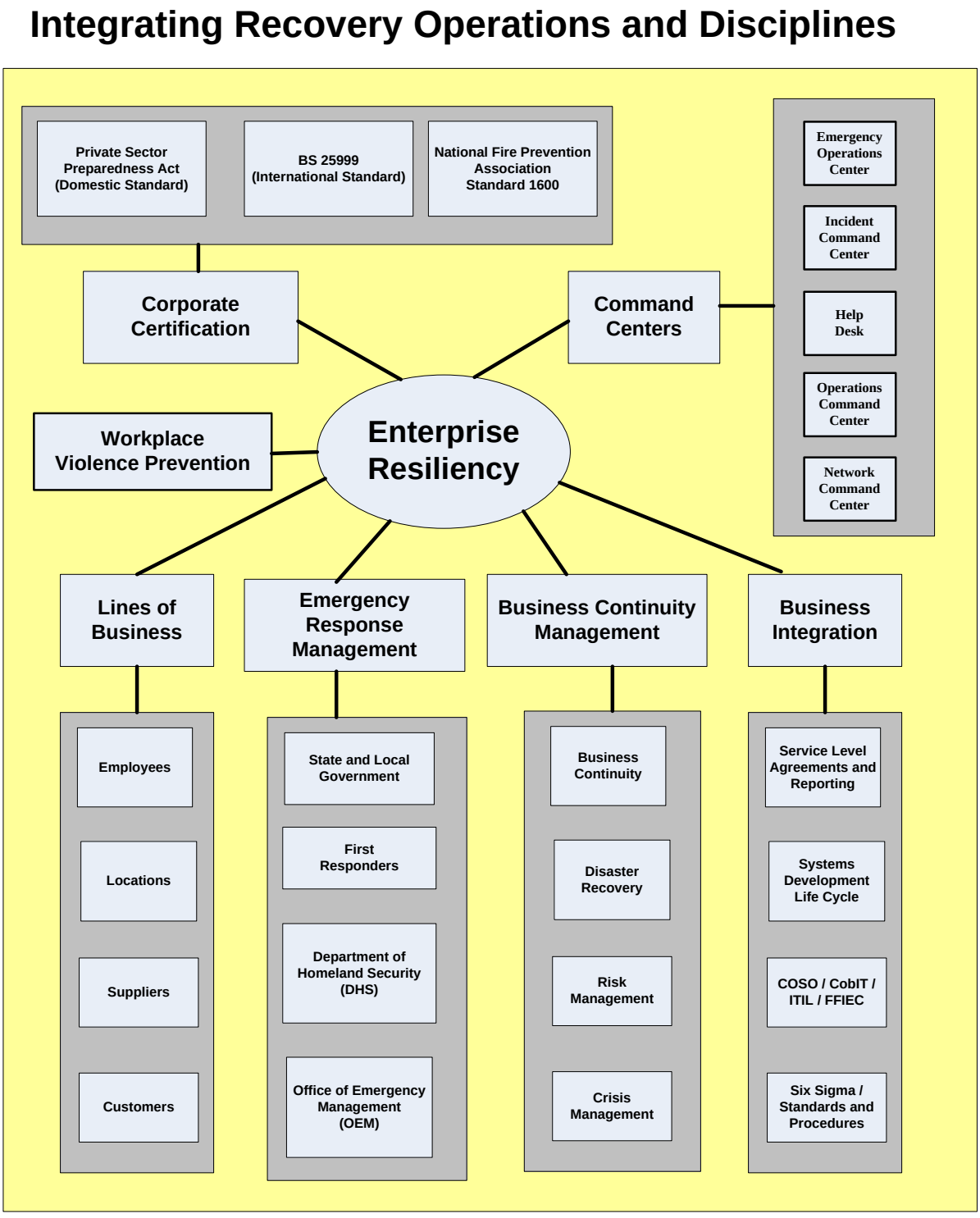
1. Development through Production Acceptance.
2. Support, Change Management, and Maintenance.
3. Standards and Procedures.
4. Documentation and Training.
5. Testing and on-going improvements.

The following section will describe how to integrate Recovery Operations into the everyday workflow used to implement and support business operations throughout the corporation.

Recovery Operations Building Blocks

The building blocks that are used to construct a business environment that can be certified consist of:

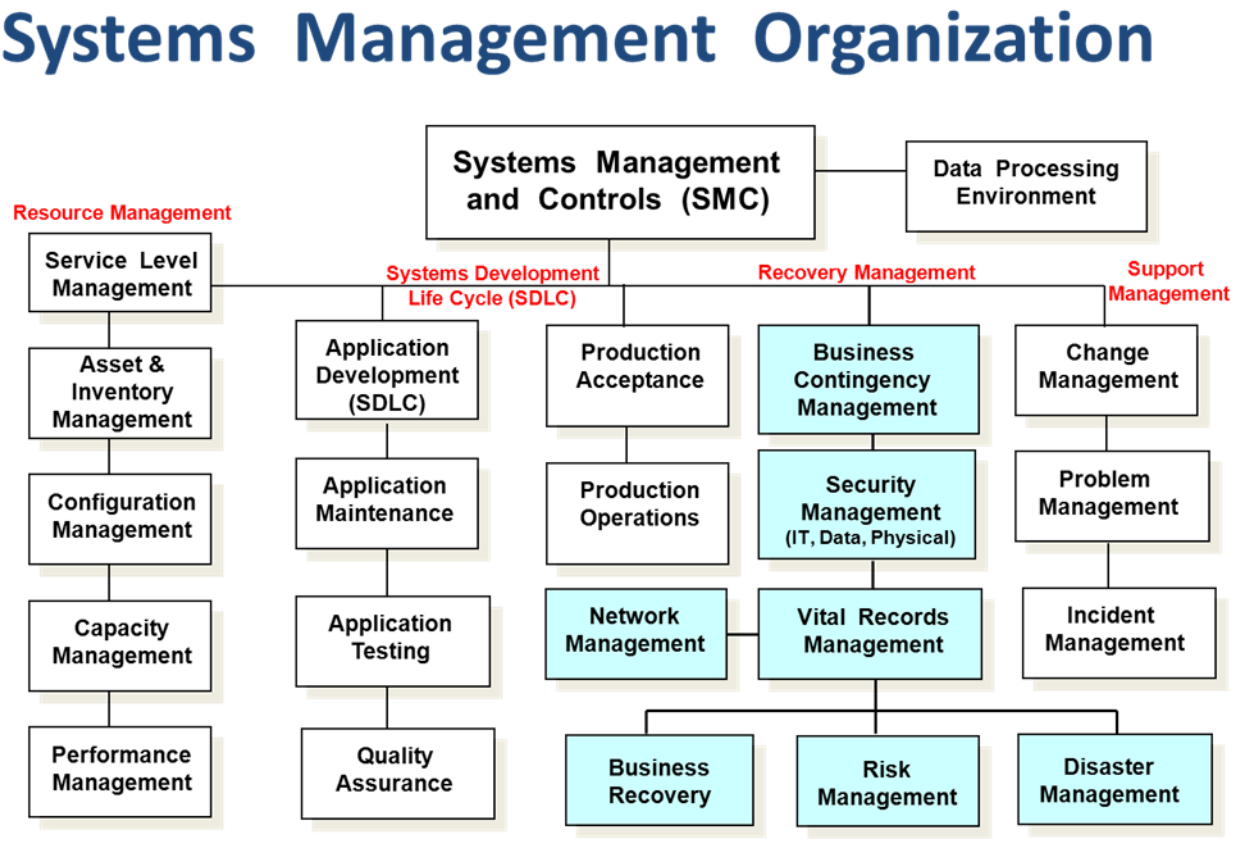
Figure 42 – Introduction to Recovery Operations



Business Integration

The IT Organization

Figure 43 – The IT Organizational Structure

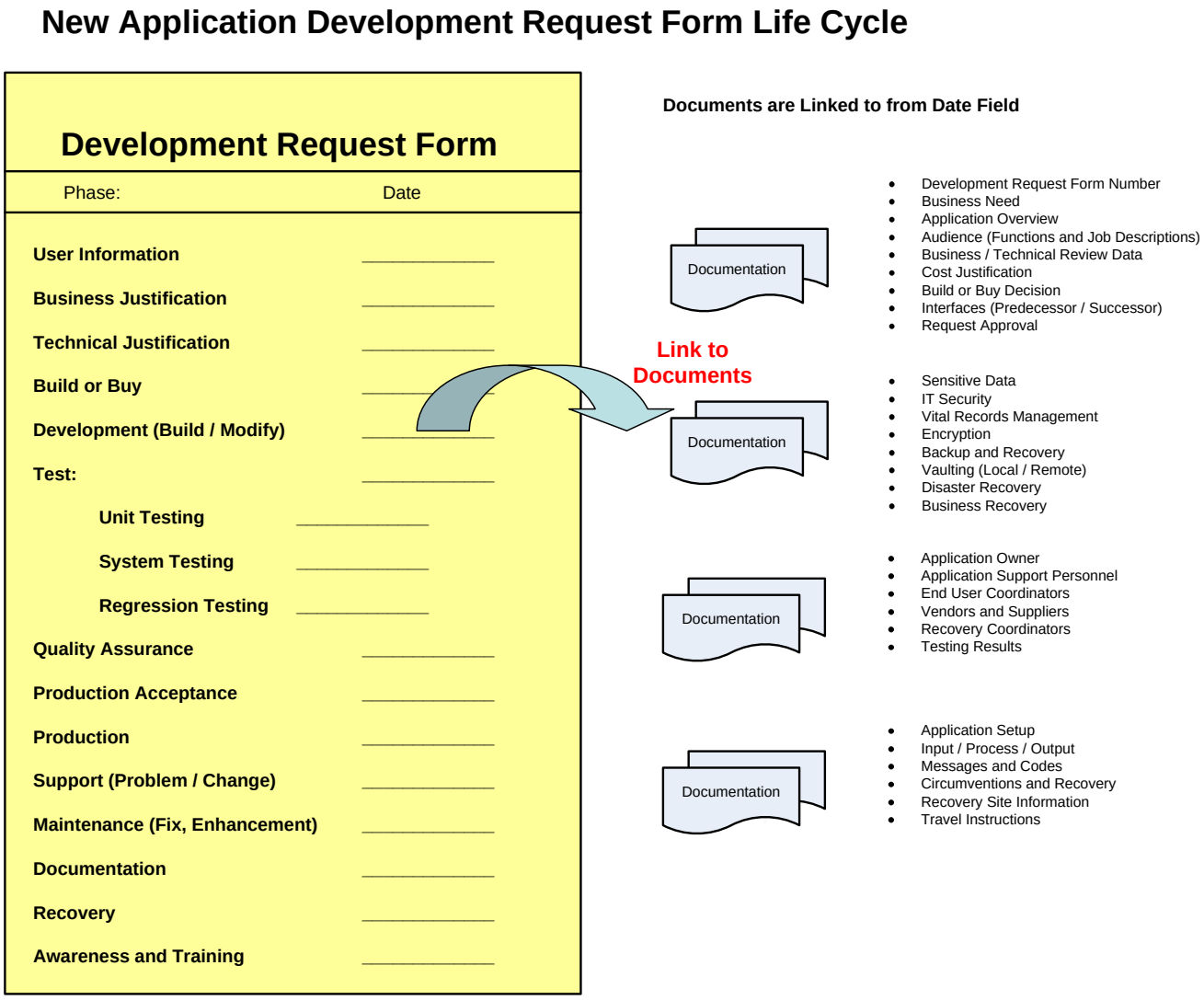


The normal IT organizational structure is shown above. It is divided into functional responsibilities so that redundancy is eliminated and the most efficient organizational structure is achieved. The four lines of responsibilities perform Production Processing (Batch, Online, and Remote); Service Provision (Service Level Management, Inventory Management, Configuration Management, Capacity Management, and Performance Management); Recovery Management (IT Security Management, Vital Records Management, and Business Continuity consisting of Emergency Management Preparedness, Business Continuity Management, Risk Management, and Disaster Recovery Planning) and finally Incident Management (Problem and Change Management).

Applications Development and Maintenance is considered a separate organization, as is Human Resource Management, Financial Services, Sales, and Production. The organization shown above relates to developing Enterprise Resiliency and Business Continuity Management.

Development Request Form and Its Life Cycle

Figure 44 - New Application Development Form



New application development activities are initiated when a New Application Development Form is submitted. The steps needed to complete the development of a new application and have it tested, and migrated into the Production environment are shown above. Types of information created at each stage of development are linked to when a completion date for a development phase has been completed. These forms are listed in a Table of Contents for each completed phase. Specific forms can be linked to from these Table of Contents forms.

This process will make it easy to locate and display forms associated with an application and insure that all personnel have the information they need to build, test, support and maintain the application going forward.

Standards and Procedures Manual Sections

Figure 45 – Standards and Procedures Manual section

i. Table of Contents	7. Application Maintenance.
ii. Benefits from S&P Manual.	8. Application Testing.
iii, Company Overview.	9. Quality Assurance.
iv. Division and Department Overview.	10. Production Acceptance
v. Compliance Requirements.	11. Production Operations
vi. Company Organization.	12. Recovery Management
vii. Department Organization.	13. IT Security Management
viii. Job Functions and Descriptions.	14. Vital Records Management
ix. Forms Library.	15. Change Management
x. Workflow Analysis.	16. Problem Management:
xi. Tools Analysis.	a. Operations Control Center,
xii. Available Training.	b. Network Control Center,
1. Service Level Management	c. Help Desk,
2. Inventory Management	d. Crisis Management,
3. Configuration Management	e. Activating Contingencies,
4. Capacity Management	f. Contingency Command Center.
5. Performance Management	17. Data Processing Environment.
6. Application Development	

Standards and Procedures manuals are used to provide personnel with guidelines and directions for creating and supporting business products and services. It consists of information related to what the corporation is and how it is structured to support specific functions performed by the departments and business units contained within an organization.

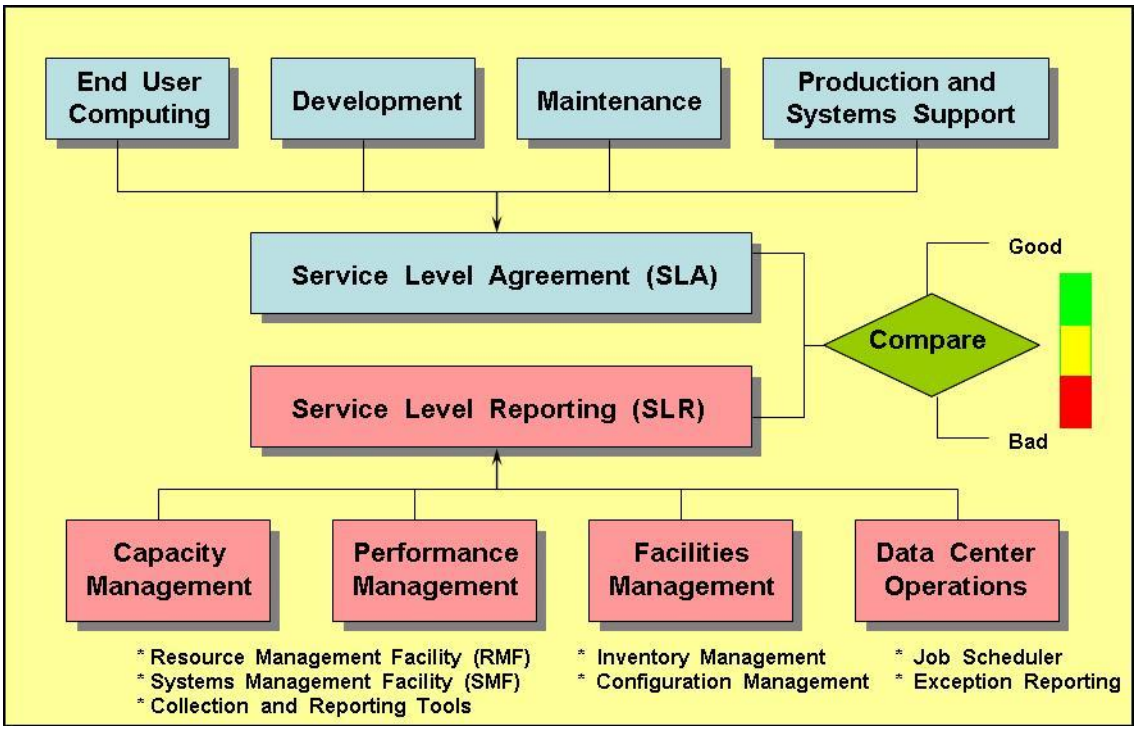
The Standards and Procedures manual sections shown above will be further described in the following pages.

Standards and Procedures manuals are normally contained within the company Intranet site and forms can be linked to from a main page like shown in the New Application Development Form life cycle shown earlier.

Service Level Agreements (SLA) and Service Level Reporting (SLR)

When new applications or business services are introduced they must go through various stages to insure that they work properly and adhere to company standards and procedures. This is initiated by developing a Service Level Agreement (SLA) between the requestor and service supplier and incorporating Service Level Reporting (SLR) to document and insure that service objectives are met as agreed upon. A Green, Yellow, Red color code developed through Service Level Reporting (SLR) can be used to determine if the SLA guidelines are being met. Categories included in SLR are: Capacity, Performance, Facilities, and IT Operations, while SLA's define user requirements for computing power, development, maintenance, and production systems usage and support.

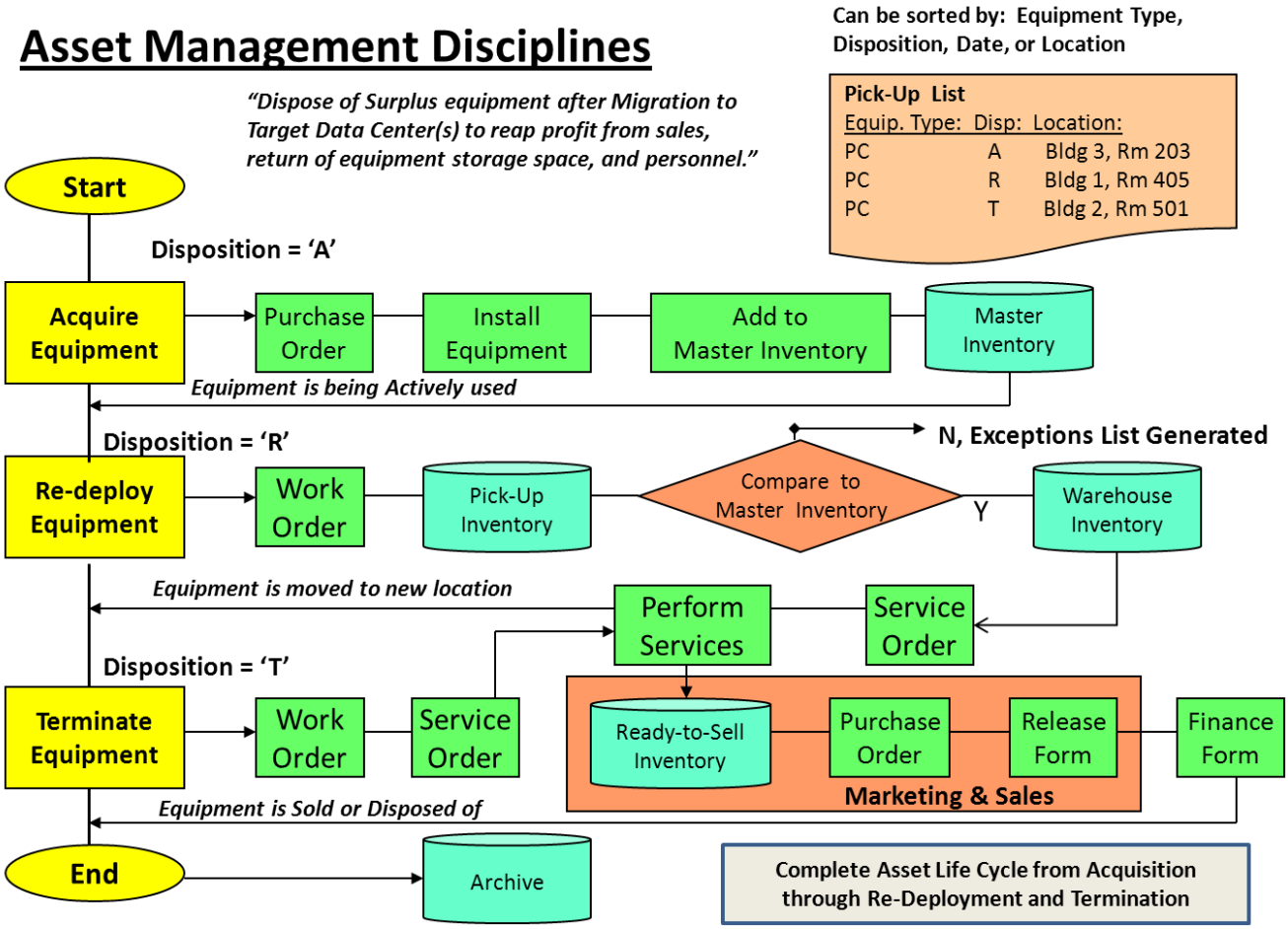
Figure 46 – Service Level Agreements and Reporting



System tools used to support SLR include: Resource Management Facility (RMF); Systems Management Facility (SMF); Inventory Management and Configuration Management; Job Scheduling; Exception Reporting; and Collection and Reporting tools used to gather required information and produce required reports.

Asset Management System (AMS)

Figure 47: Asset Management System



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.

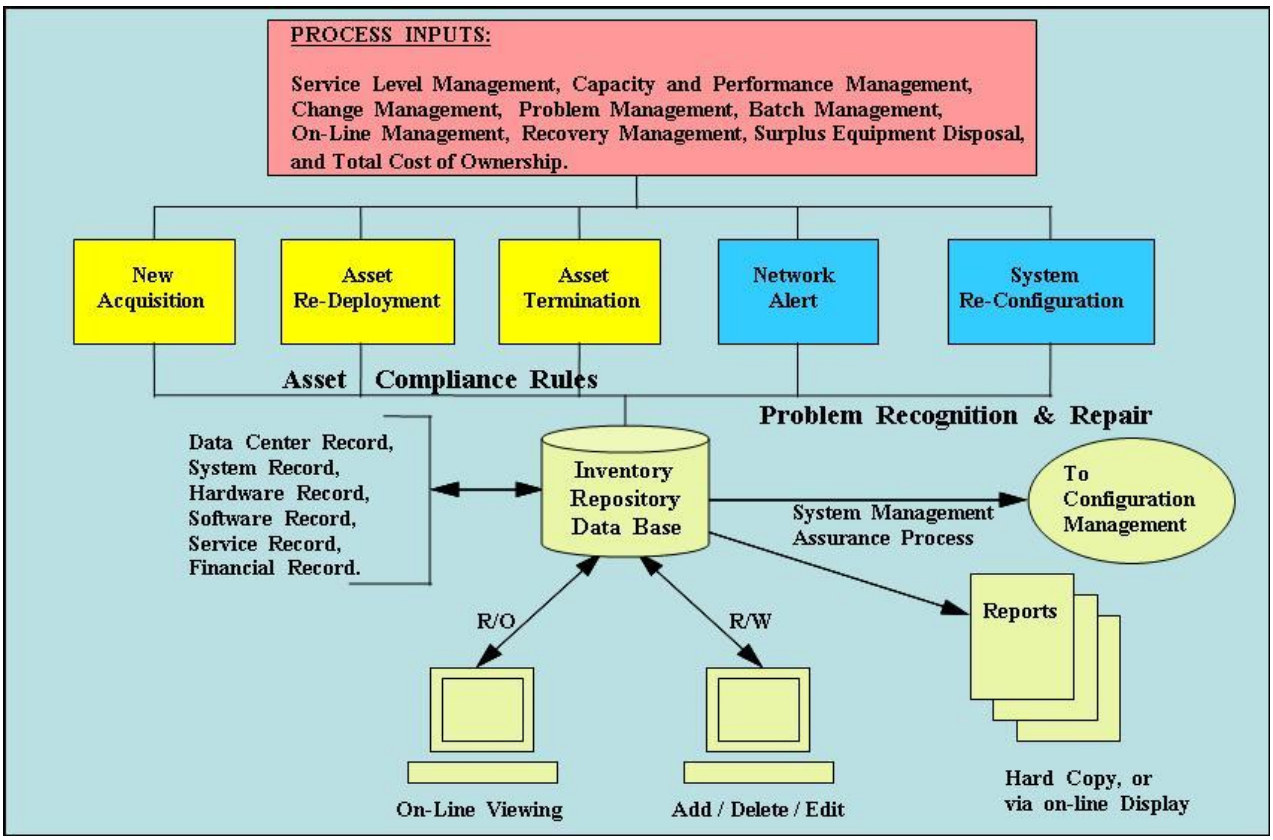
The process for achieving Asset Management is shown above.

An Asset Management System (AMS) can be used to Acquire, Redeploy, or Terminate assets in compliance with corporate and industry standards (i.e., toxic materials must be disposed of in accordance to government requirements). Data contained on assets must be destroyed or cleaned when redeploying equipment so that personal or company information does not move from one user to another unless proper authority is granted. This becomes especially important when terminating or donating equipment because you do not want company information in the hands of unauthorized personnel.

Utilizing an Asset Management System in conjunction with the Infrastructure Department will provide a means to order and implement equipment, applications, and services that adhere to delivery schedules and performance standards stated in the SLA. Remember, people must be trained and available to install equipment, update system programs, and test all related components. Personnel must also be trained to operate the new equipment or service offering.

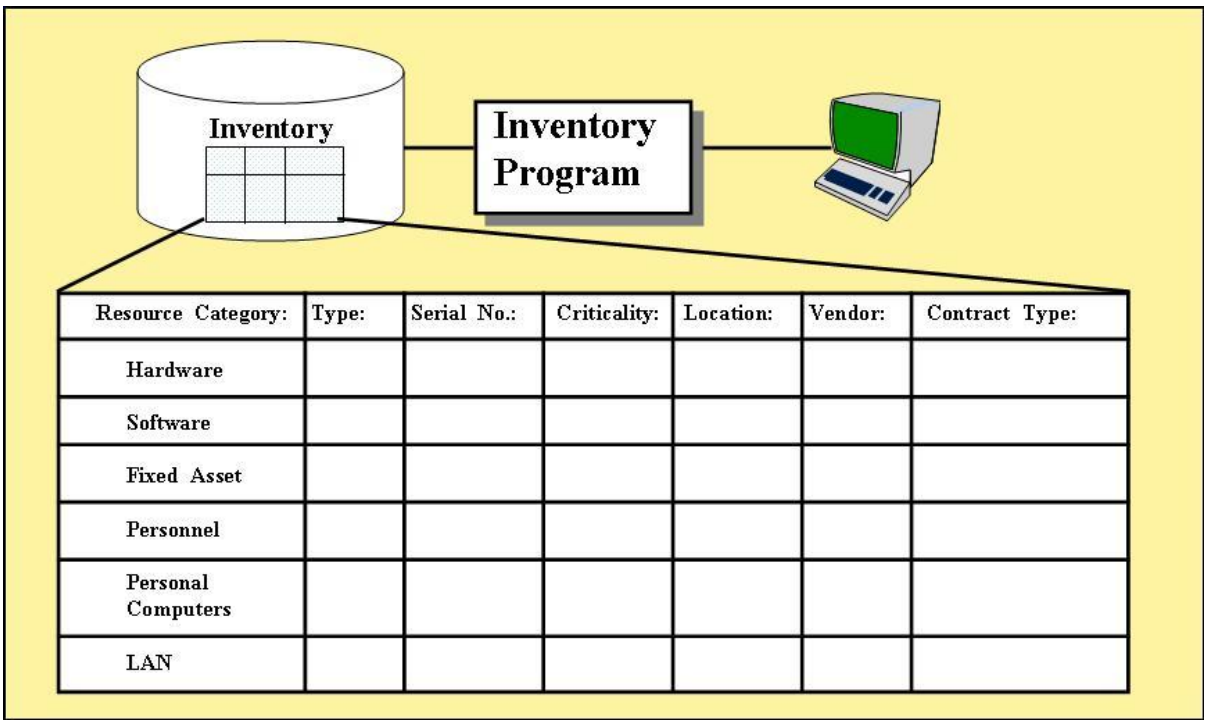
Asset Management System Interfaces

Figure 48 – Asset Management System Interfaces (AMS)



Inventory Management System

Figure 49 - Inventory Management System



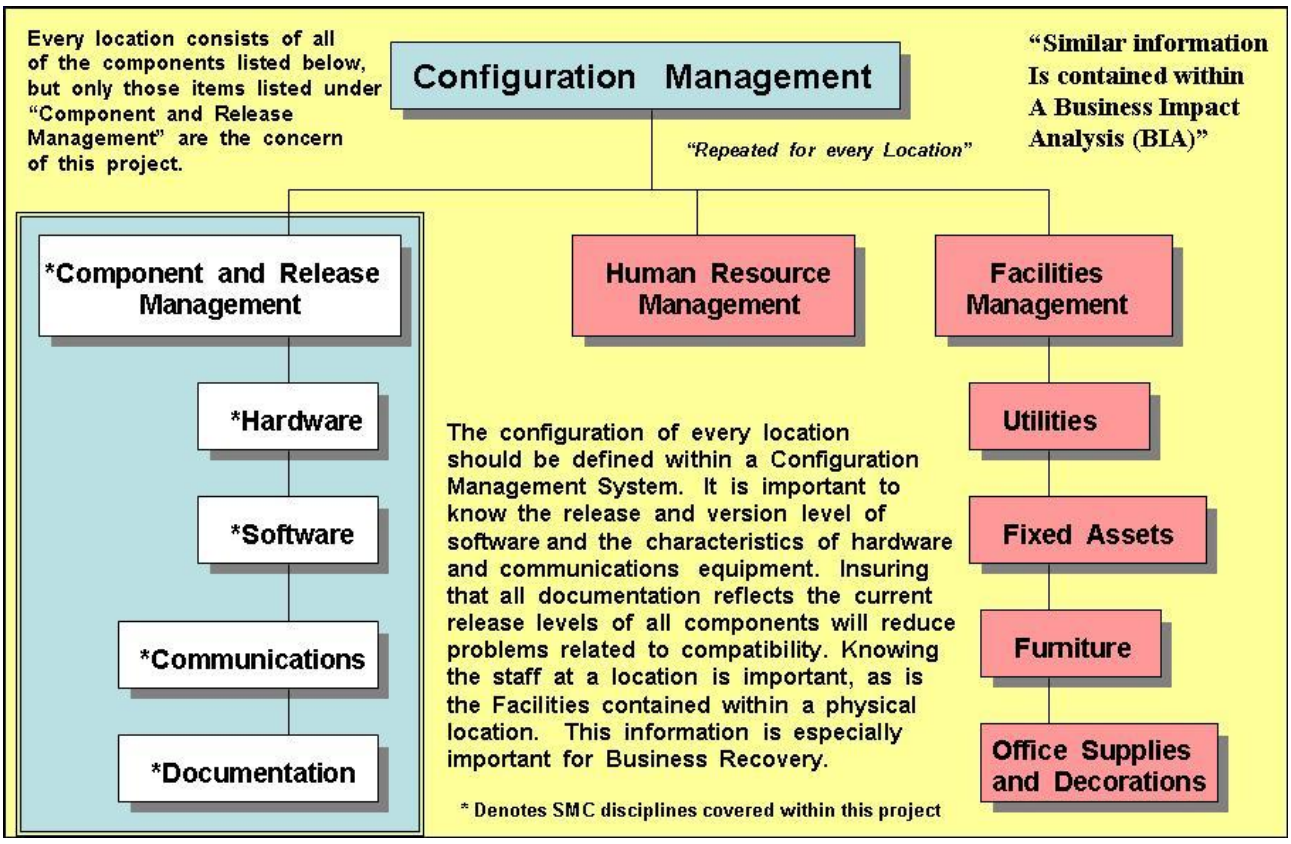
Resource Category:	Type:	Serial No.:	Criticality:	Location:	Vendor:	Contract Type:
Hardware						
Software						
Fixed Asset						
Personnel						
Personal Computers						
LAN						

It is important to record and track assets and where they are located. This information can be used to determine when a piece of equipment needs to have its lease renewed or terminated. It can also be used to determine the amount of equipment located at a specific site so that critical equipment can be replaced during a disaster event.

Monitoring the use of assets and tracking their problem types will allow you to make equipment purchasing decisions and the quality of supporting equipment vendors.

Configuration Management

Figure 50 - Configuration Management



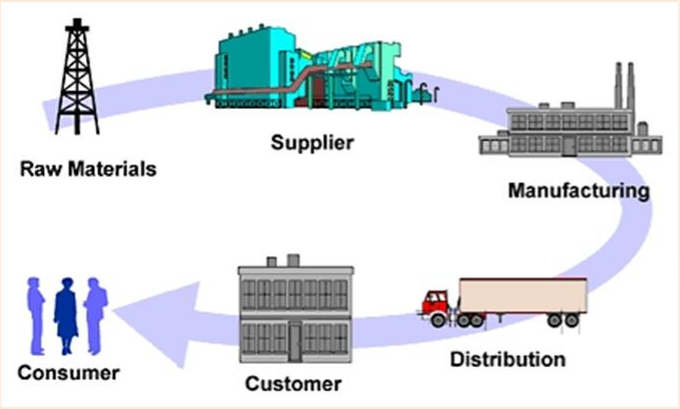
Supporting recovery operations by providing a description of the equipment and assets located at a specific location, Configuration Management will also provide support personnel with an overview of how to connect the system to a site and a means to determine any Single Points of Failure that may require a secondary path to eliminate potential failures through failover operations.

If a site is lost due to a disaster, the Configuration Management data can be used to enquire into the Asset Management System to obtain replacement equipment that may be available through Redeployment and/or Termination. The Inventory Management System may also assist in locating low priority equipment from other locations that can be redeployed to replace equipment lost due to a disaster event. If these systems do not provide replacement equipment, then vendor agreements should be available to replace the equipment lost due to the disaster event.

Supply Chain Management

Figure 51: Supply Chain Management overview

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



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

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.

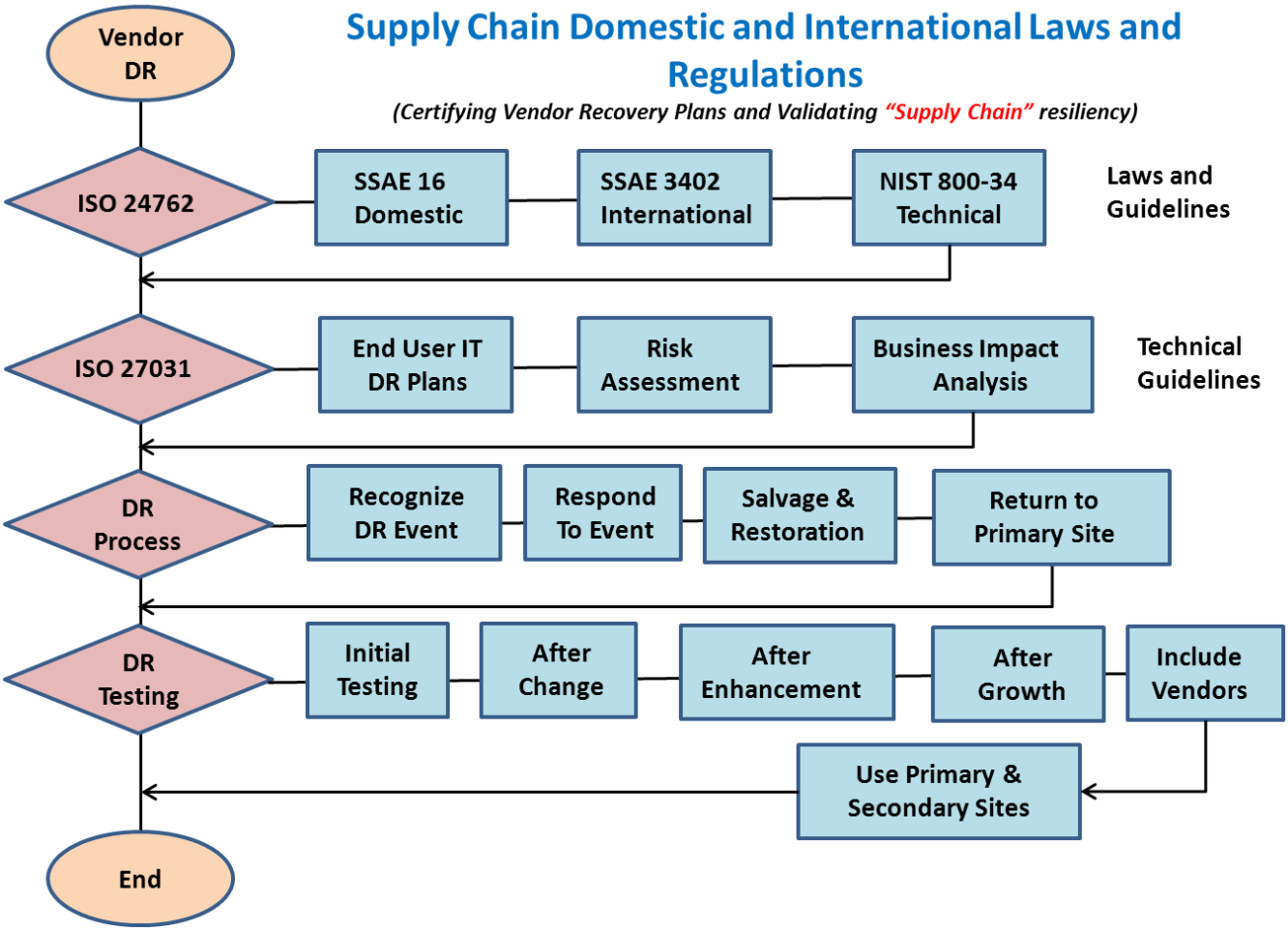
Suppliers accumulate supplies and transport them to their clients via an established schedule, or in respond to demand. Should the Supplier, Manufacturer, or Distributor have a failure and cannot make deliveries as required, then they can contribute to your experiencing a disaster – not because of a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

Supply Chain Management Laws and Regulations

Figure 52: Supply Chain Management Laws and Regulations

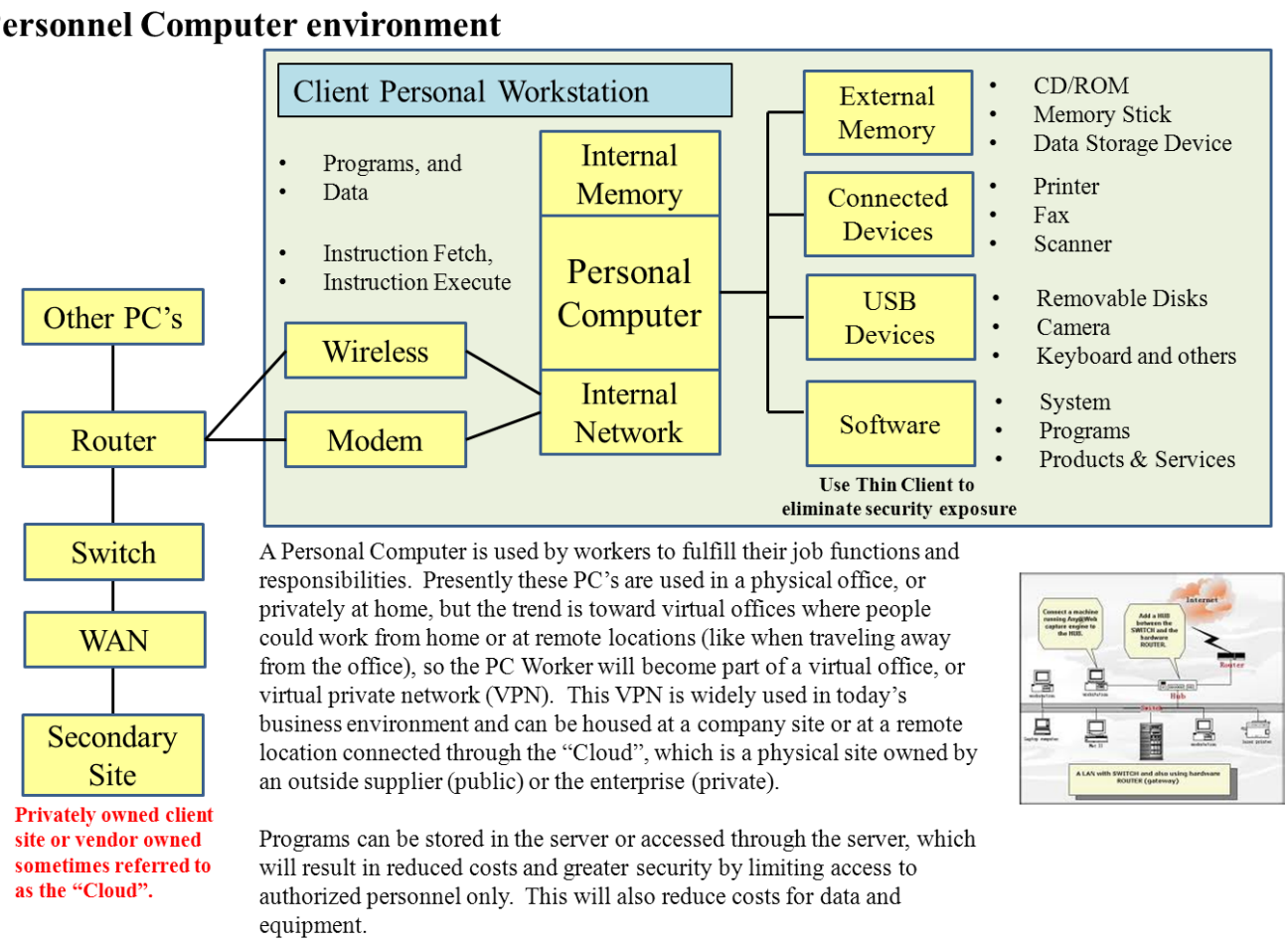


In order to validate that your supply chain complies to domestic and international standards, the above laws have been created.

As you can tell by now, it is essential that you receive your supplies on time no matter which location you are conducting business from and under normal or recovery conditions.

Personnel Computer Environment

Figure 53: Initial Personal Computer configuration



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).

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.

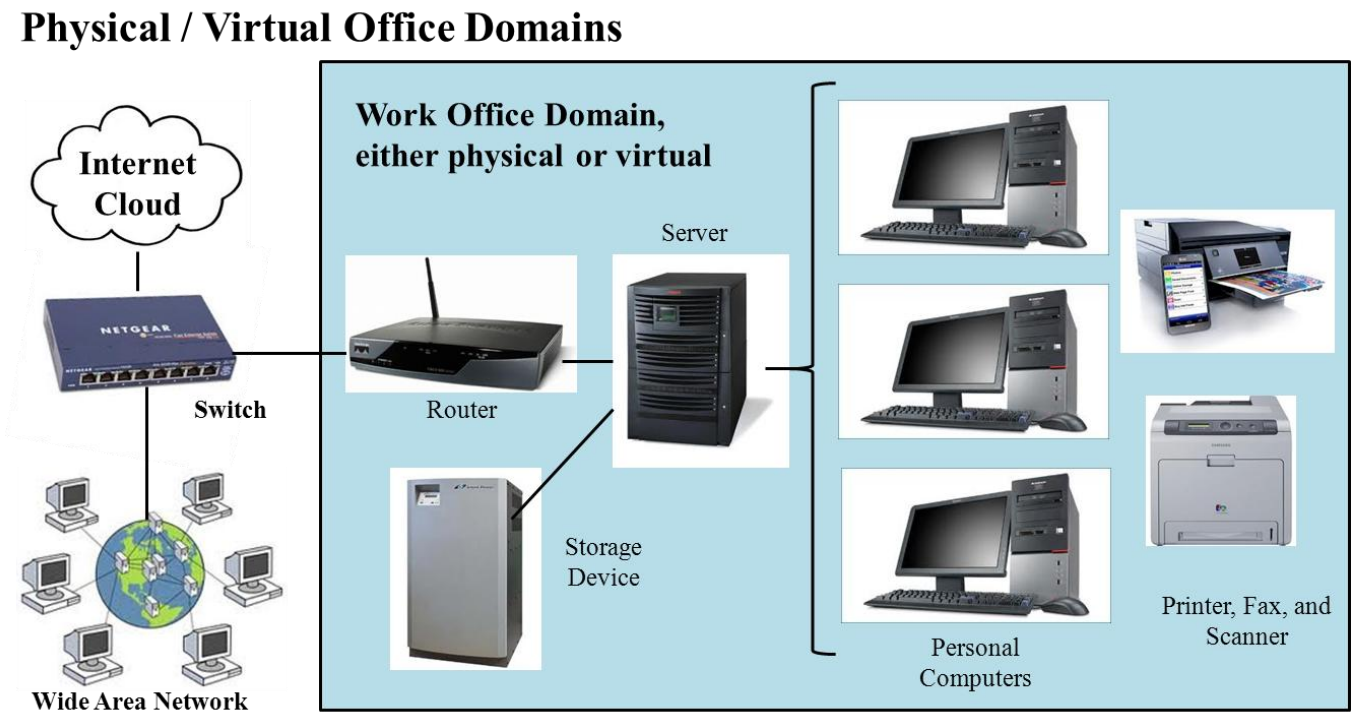
Personnel Computers have grown over the years from a simple Disk Based Operating System (DOS – Disk Operating System) where programs and data had to be loaded into memory via floppy disk drives using a basis 80-80 processing system (computer card based) to a VMware based system using Virtual Memory Partitions 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

Figure 54: Thin Client Personal Computer / Server environment



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.

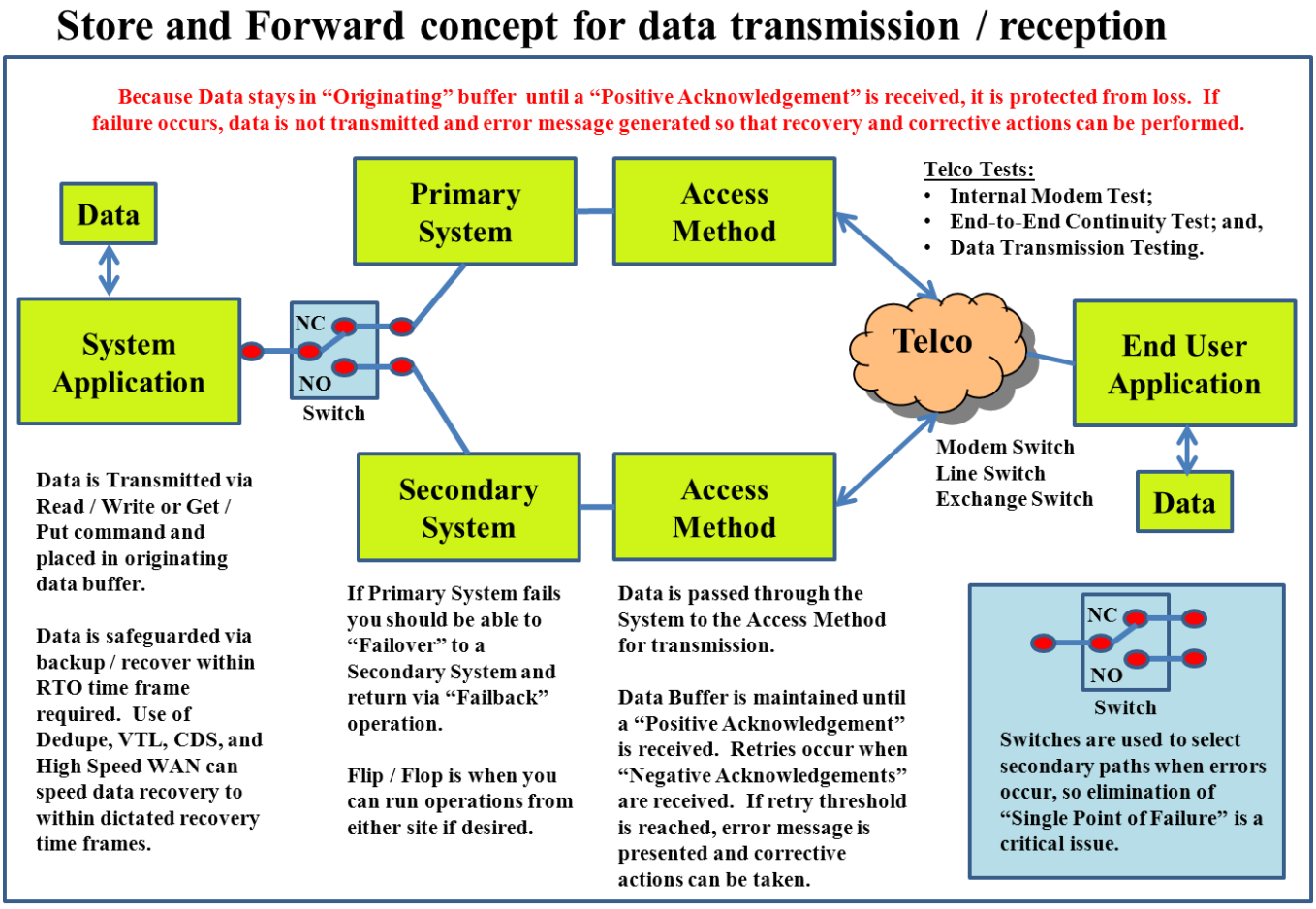
Utilizing this approach eliminates the possibility of personnel downloading data onto transportable media that can be taken off-site and used to expose company secrets or sensitive information. Also, taking personal data away from a protected company environment may result in Identity Theft and large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

Figure 55: Store and Forward concept to protect data



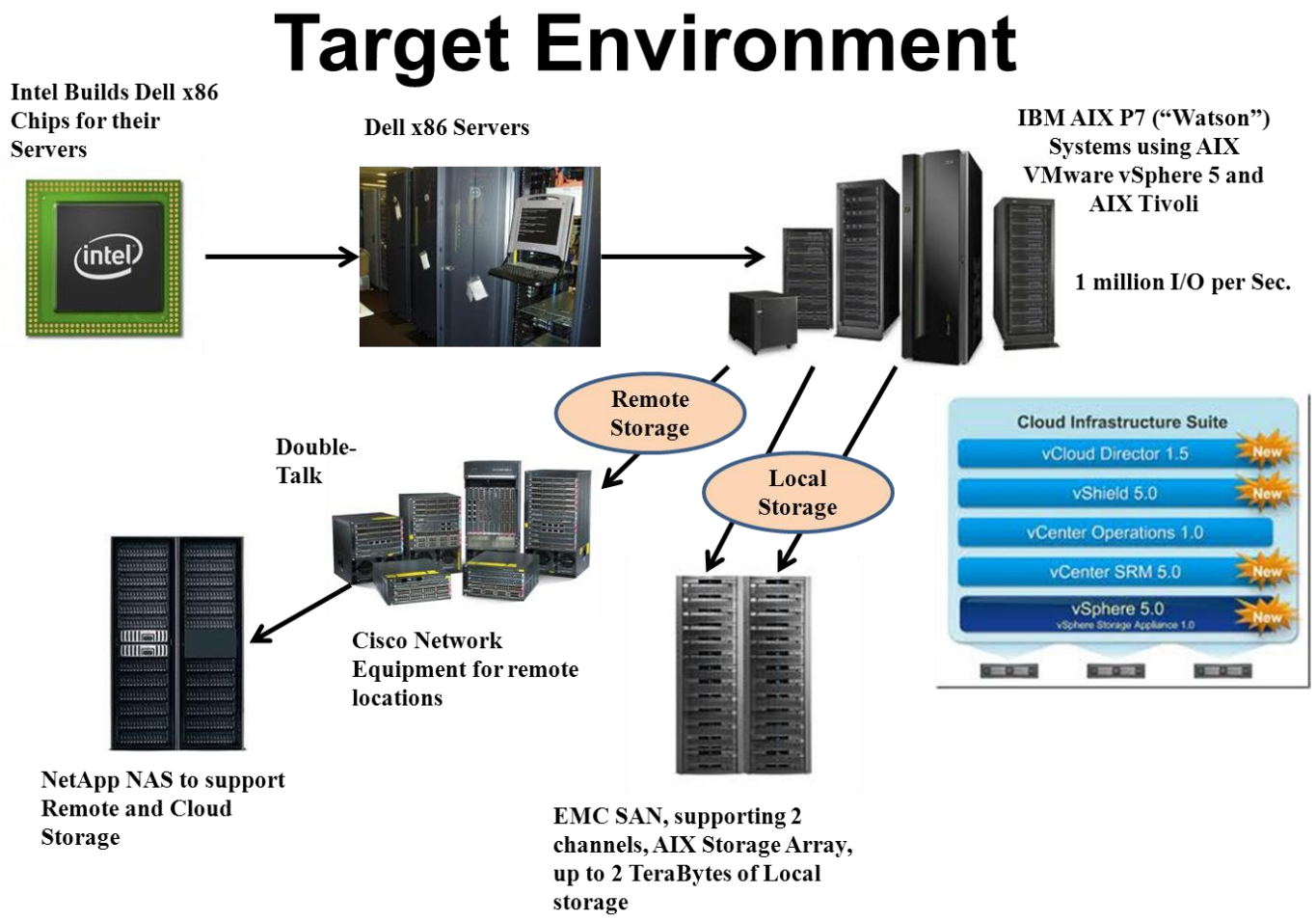
The "Store and Forward" method used to transfer data between programs and devices is shown above and used to ensure the safe arrival of transmitted information.

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

Figure 56: Sample Target IT environment



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.

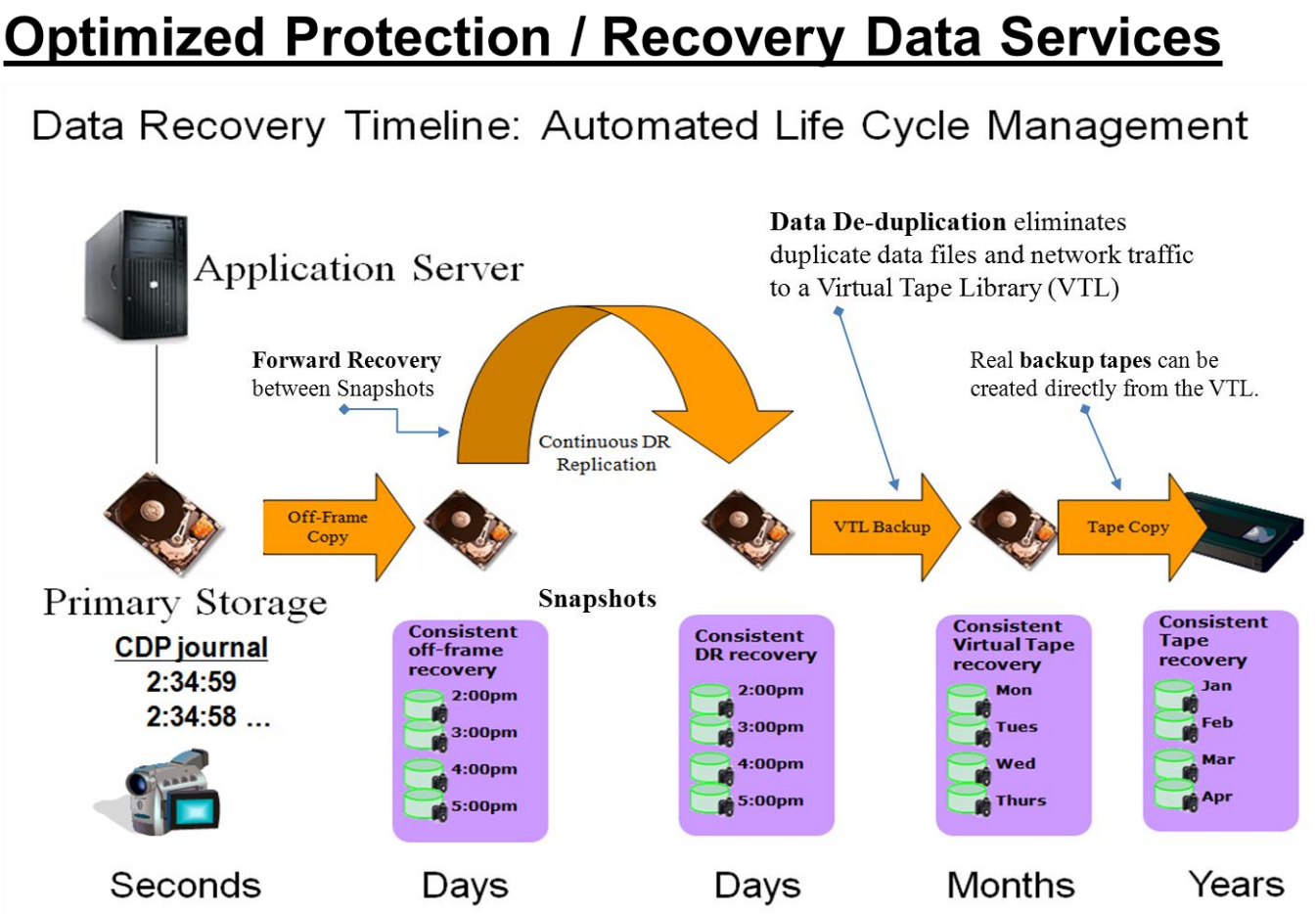
By incorporating the vSphere 5.0 environment the client can host multiple virtual server environments within a single physical server, or server cabinet. The vSphers 5.0 system product directs traffic to the appropriate VMware system, vShield is used to provide security protections, vCenter Operations 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

Figure 57: Optimized Data Protction and Synchronization



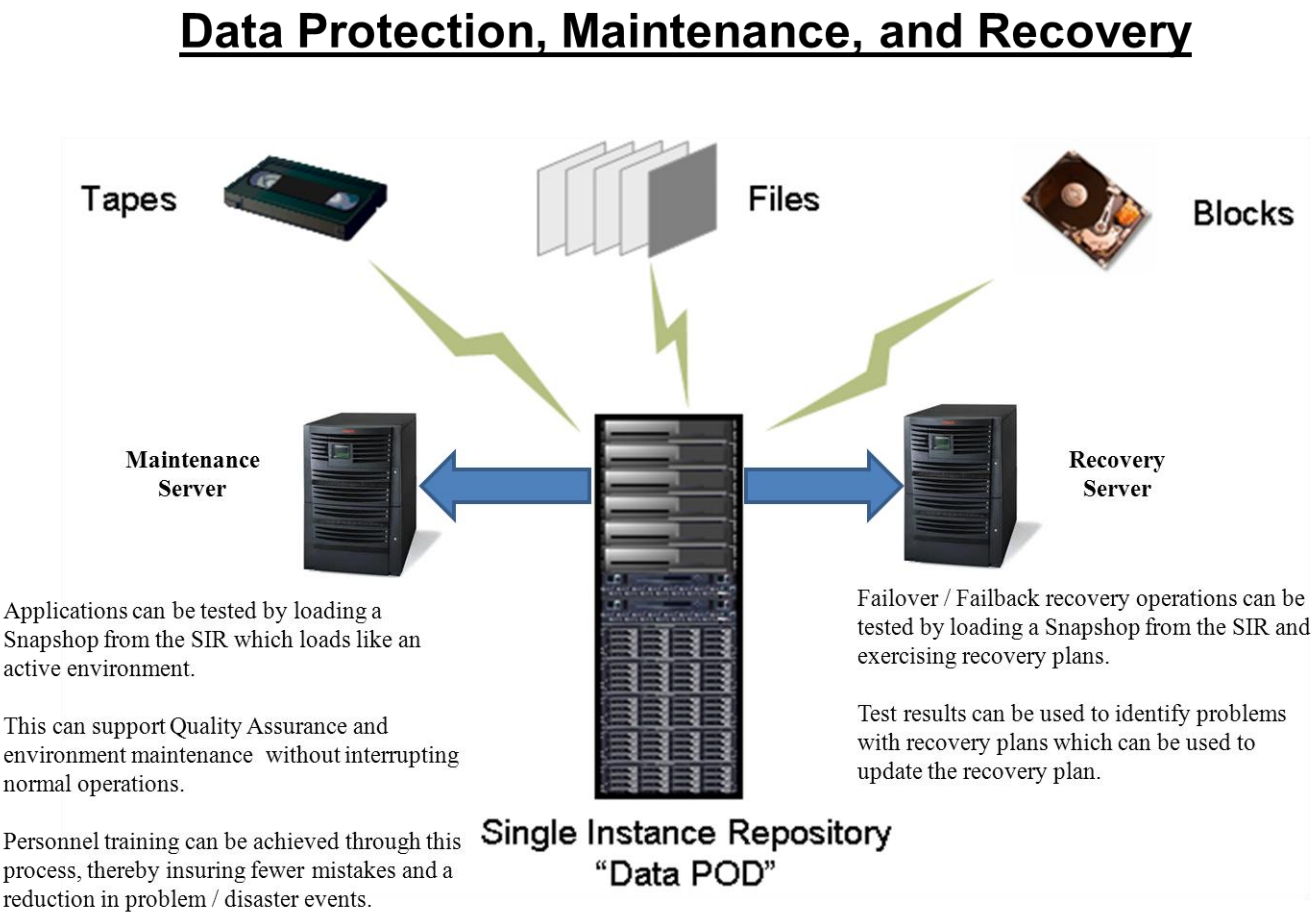
As systems become more important to the business, protecting and restoring data becomes crucial. Today's technology is shown in the above illustrations and includes:

- 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

Figure 58: Optimized Data Synchronization and Recovery



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.

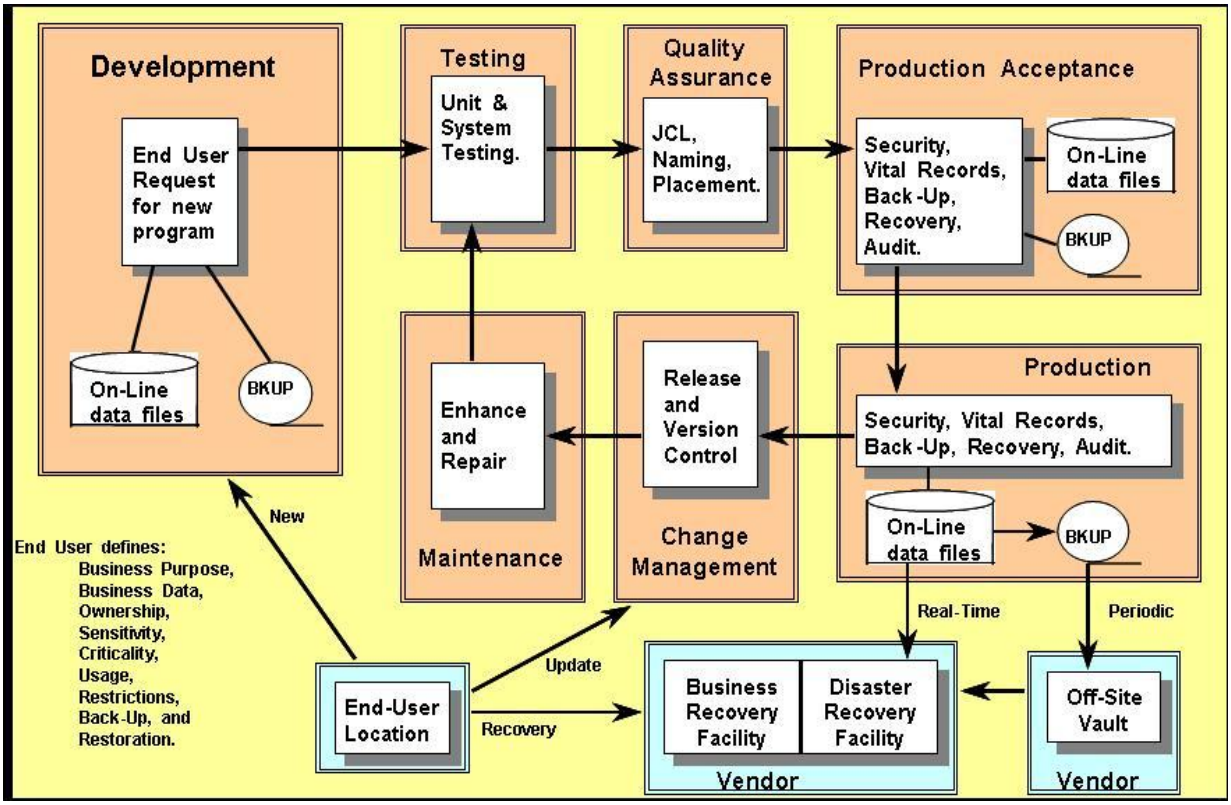
The use of a SIR concept will allow companies to become more efficient without taking a chance on damaging the production environment. An additional benefit is a better trained and confident staff whose morale is high because they know what to do in time of failure and do not have the fear presently 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.

Systems Development Life Cycle (SDLC)

A Systems Development Life Cycle (SDLC) is used to define how applications and their assets are developed in accordance to company standards. The phases contained in an SDLC include:

1. Development;
2. Testing;
3. Quality Assurance;
4. Production Acceptance;
5. Production;
6. Backup and Recovery Operations;
7. Support; and
8. Maintenance.

Figure 59 – Systems Development Life Cycle flow and stages



The Systems Development Life Cycle phases and their purpose are:

Development – The initial starting point for creating new applications that may be created in-house or purchased through a vendor. The user defines the priority of the application and a Service Level Agreement is constructed between the user and the Information Technology department to indicate the amount of computer resources and processing schedules needed by the applications. A Project Plan and Life Cycle is also developed to guide the application through development and into the Production environment.

Testing – Once the application is completed with development, it is tested to company and user standards, including: Walk Through; Unit Testing; System Testing; Scenarios; Scripts; Recovery Tests; Regression Testing; Benchmarks; and Post Mortem discussions.

Quality Assurance – performs Test Validation; Component definitions and naming; Component Placement Requirements; Functionality definition and testing; and Process Definition and Testing.

Production Acceptance – is performed by Operations Personnel and is associated with placing components into designated libraries under approved names. It covers Batch and On-Line programs, IT Security, Operations Guidelines, Recovery Requirements, and IT Audit requirements.

Production – is the day-to-day environment where applications are processed. Batch and On-Line jobs are processed in this environment. Some of the responsibilities associated with the Production Environment include: Set-Up, Processing, Break-Down of Output, Delivery of Output, Vital Records Management; Vaulting (Local and Remote); Disaster Recovery (Recovery Facility or Secondary Site); Business Recovery support (re-routing information to a designated secondary site if a business office or facility is lost); and communications with the Disaster Recovery and Business Recovery Facilities.

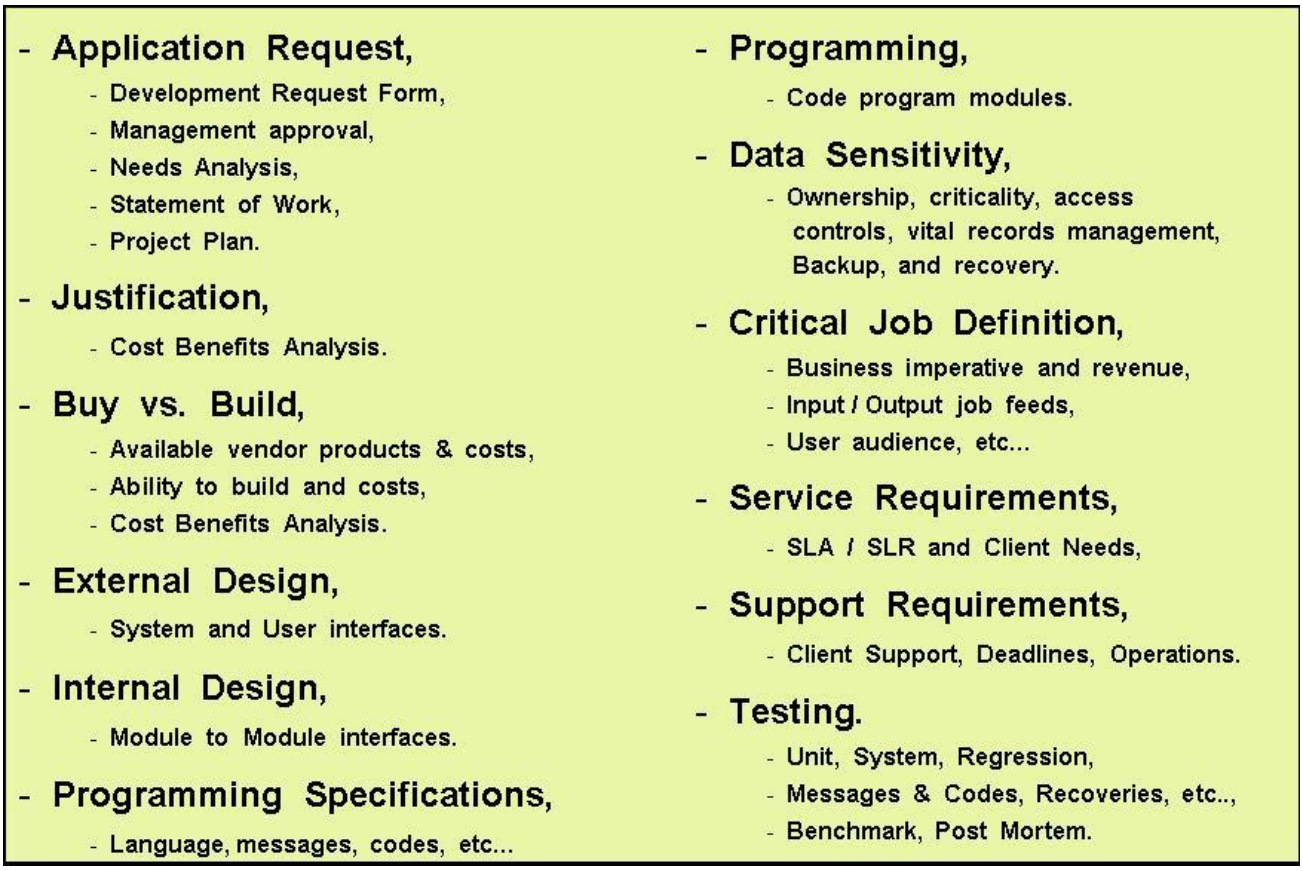
Change Management – When a problem requires a change to an existing component or a new enhancement is requested by a user, a change control must be submitted. To execute a change request, a copy of the production component is copied to the change environment and its release level is raised by one. The change is then moved to the maintenance environment where the required work is performed. This process supports Version and Release Management.

Maintenance – The environment where changes and enhancements are implemented. Once completed, the change is then routed through Testing, Quality Assurance, Production Acceptance, and finally Production where the original component is replaced by the new component.

The Development process is completed once, while the Maintenance process is completed as many times as is necessary.

Application Development Procedures

Figure 60 - Application Development procedures



The steps that must be completed to authorize the development of a new application and move the application from development to the production environment are shown above. They include:

Application Request – A Work Order associated with the development request is created and submitted for approval. It: defines the Development Request; is used to gain Management Approval; generates a Needs Analysis; results in a Statement of Work; and Project Plan detailing the phases and tasks associated with creating the new application. Additionally, all Purchase Orders and Man Hours associated with this Development Request are charged against the original Work Order.

Justification - is achieved through a Cost Benefits Analysis that compares the services delivered through the new application, the new business generated by it, or the problems it responds to against the cost of development. If costs far exceed benefits, then the application will probably not be developed. But if benefits far exceed costs, it will go a long way towards management approval.

Buy vs. Build – is a decision based on in-house talent, costs and product availability, as well as product support and maintenance costs over time. It is usually less expensive to purchase a product than to build one from scratch because of costs associated with personnel, processing power, and related resources over a long period of time. A vendor is more apt to devote more time and effort to an application than a company will which will suggest that a better product can come from the vendor.

External Design – The definition of system and user interfaces and the data that will be exchanged. This is used to define data security and access controls between end users and the application modules.

Internal Design – This is used to define how application modules transfer data and the conditions under which this data transfer is accomplished. The types of data being transferred and error conditions that could arise from these transfers are defined and included in an application Messages and Codes Manual.

Programming Specifications – The programming language and techniques are defined during this development phase. All Messages and Codes, User Manual Requirements, and Recovery Techniques are defined here as well.

Programming – Programs are actually coded during this phase in accordance to previously defined guidelines.

Data Sensitivity – The sensitivity of application data is defined during this phase and includes: who owns the data, what the data is used for, how sensitive is the data, who has access to the data and under what conditions do they have access (Write, Read, Execute, etc.), what access controls should be created to protect the data, how often should the data be backed up (Real Time Shadowing, Incremental, End of Day, End of Job, etc.). Data Security Rules and Firewalls are created and tailored based on the information obtained during this phase. Back-up / Restoration and Vaulting requirements are also defined during this phase.

Critical Job Definition – This phase is used to define the applications criticality and the criticality of jobs associated with the application. This information is used to drive Recovery Operations, Recovery Time Objectives, and Recovery Point Objectives.

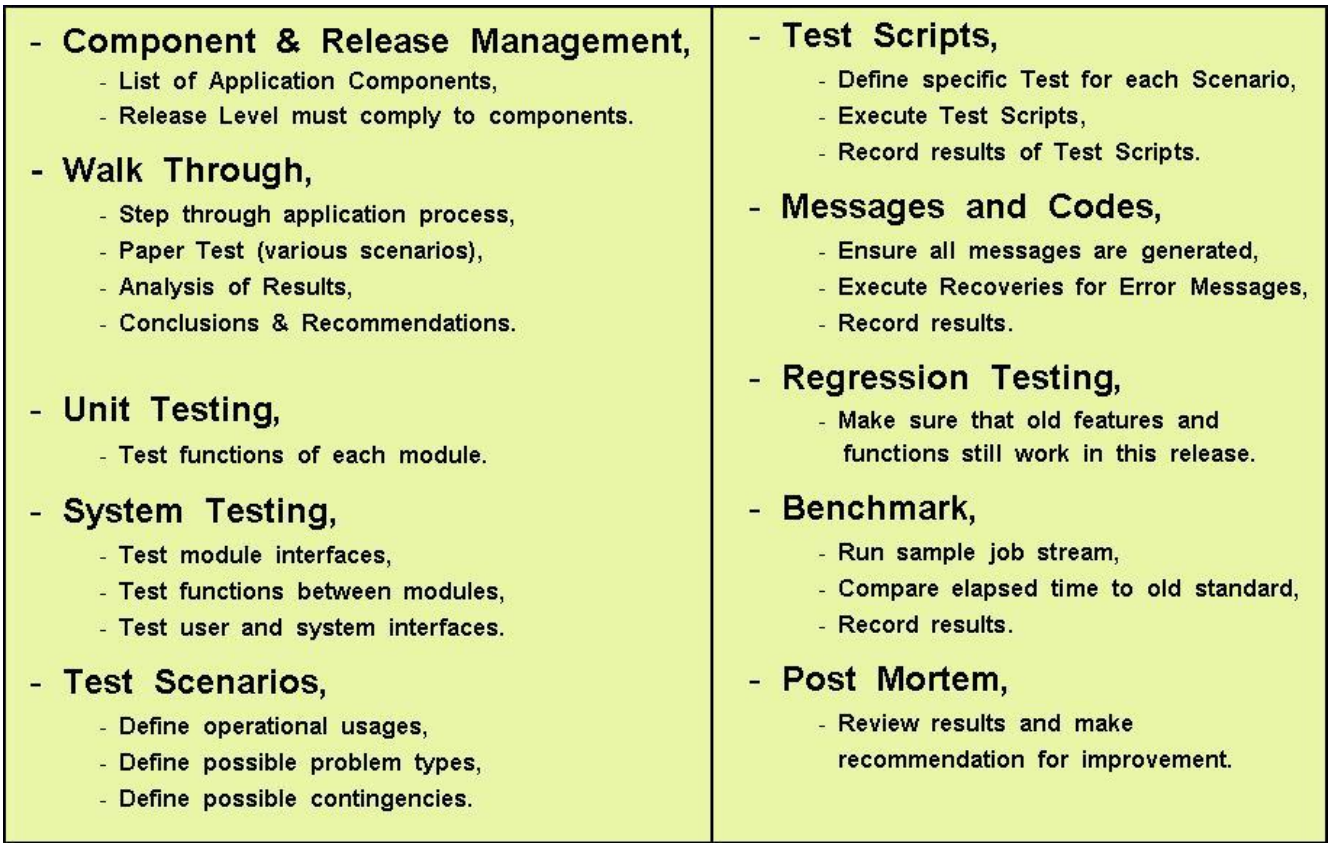
Service Requirements – This phase is used to define the Service Level Agreement (SLA) that the application owner has requested and the Service Level Reporting (SLR) requirements needed to monitor and report on application operations.

Support Requirements – This phase is responsible for defining the Technical Support and Maintenance requirements associated with the application. It is used to define the information needed by the support organization, the personnel in support positions, and their contact information.

Testing – This phase is used to test the application to make sure it operates correctly. During this phase all error messages are generated and recoveries exercised to insure that the operations staff is provided with the information they need to set-up, process, and produce correct output from the application. Test data files are also created and used to drive testing operations on a consistent basis.

Application Testing Procedures

Figure 61 - Application Testing Procedures



The procedures followed when performing application testing are shown above.

Component and Release Management – The phase is responsible for documenting all components included in the Application Release and ensuring that they are all at the same maintenance level. Components should be from designated libraries in the development or maintenance environments and not from the production environment, which will support library management practices.

Walk Through – A step through of the application process is accomplished during this phase with various paper tests to ensure that all application functions have been defined and accessed. Results from these tests are analyzed to ensure that all application functions have been identified and tested. Conclusions and recommendations are formulated as a result of this testing phase and incorporated into follow-on testing procedures.

Unit Testing – Each unit of the application is tested separately during this phase to ensure that they operate successfully. Inputs, processing functions, and outputs are generated and compared to expected results. Any exceptions are documented and repaired as needed.

System Testing – Individual application module interfaces are tested to ensure that all functions operate correctly. User and system interfaces are also exercised to ensure their operation is successful and expected outputs are achieved.

Test Scenarios – Various scenarios are created to simulate how the applications will operate normally and during problem incidents. These exercises are utilized to determine if the application can provide normal operations and respond to error conditions by providing information needed to define and respond to abnormal conditions. Required data used to support scenarios should be generated and used to support testing of normal and error conditions.

Test Scripts – The sequence of events that will be exercised during the pre-defined Test Scenarios will be exercised during this phase through Test Scripts. All conditions resulting from the test scripts are documents and analyzed during the Post Mortem phase.

Messages and Codes – All Messages and Codes (normal and error) are generated during the testing of units and systems through test scenarios and test scripts so that expected results can be verified. Responses by the operations and support staff to the messages and codes are reviewed and verified. All results during this phase are recorded and used during the Post Mortem phase of testing.

Regression Testing – Any and all old functions delivered by this application are testing during this phase to ensure that existing functions still perform correctly and that results match those previously experienced. Again, any exceptions are recorded and reviewed during the Post Mortem phase.

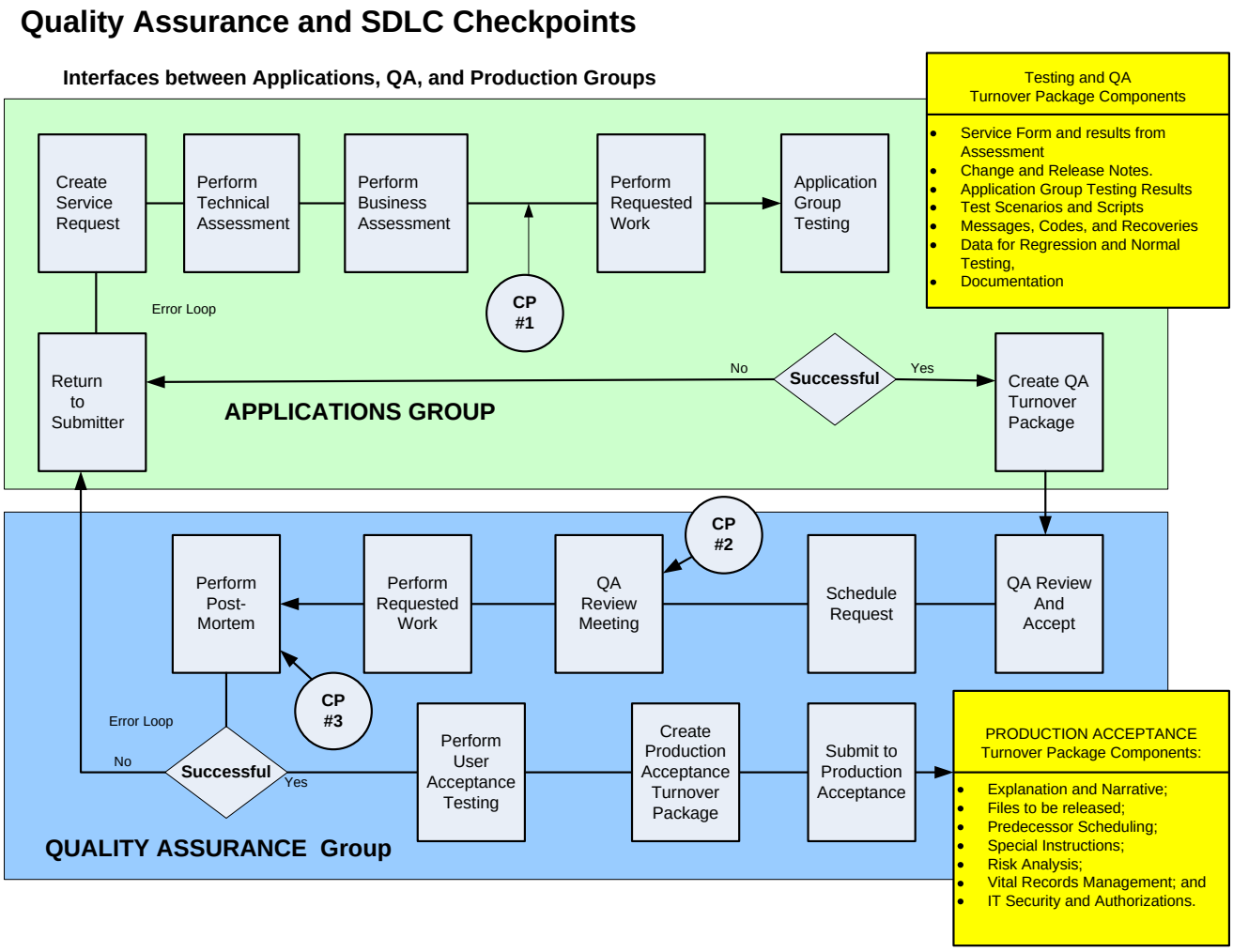
Benchmark – A Benchmark job stream, or exercise, is executed and previous processing times and efficiencies are compared to new times and efficiencies to determine if the new application executes faster or more slowly than the old application. These results are also recorded and reviewed during the Post Mortem phase.

Post Mortem – All results recorded during the previous phases are reviewed and analyzed to determine if the application testing completed successfully. Any exceptions are reviewed and corrective action performed if necessary. A final Post Mortem report is generated and provided to management for review after this phase is completed. If approved, the application will move to the Quality Assurance phase of the System Development Life Cycle.

Testing is extensive and organized to exercise all application functions, both normal and those functions that generate error messages and codes. Test data is generated to drive the testing process and generate normal and abnormal conditions. Old and new functions are tested to ensure their operation and a performance benchmark test is used to compare old efficiencies to new performance results. Finally a Post Mortem is used to formally evaluate the application testing process and experienced results. The Post Mortem can be used to update testing procedures and make recommendations to correct mistakes uncovered during the testing process. Finally, a management report is generated to inform management of the testing results and recommendations generated during the Post Mortem phase.

Quality Assurance and SDLC Checkpoints

Figure 62 – Quality Assurance and SDLC Checkpoints



The process of moving an application from the development to production environment is shown above. Checkpoints are included in the process to quickly identify and respond to critical steps and information. They include:

Checkpoint #1 – Review the decisions made regarding the application request and determine how the application is to be constructed (Build / Buy and Technical Strategy). This checkpoint will provide permission to go forward with the applications development, or not.

Checkpoint #2 – Development and Testing of the application has been completed by the Applications Group and the application has just completed its QA Review. A decision to go forward or reject the application is made during this checkpoint.

Checkpoint #3 – A Post Mortem of the applications Testing and Quality Assurance is completed and the work requested by the application completed. This decision will provide a go / no-go decision for the application to enter the Production environment.

Quality Assurance Procedures

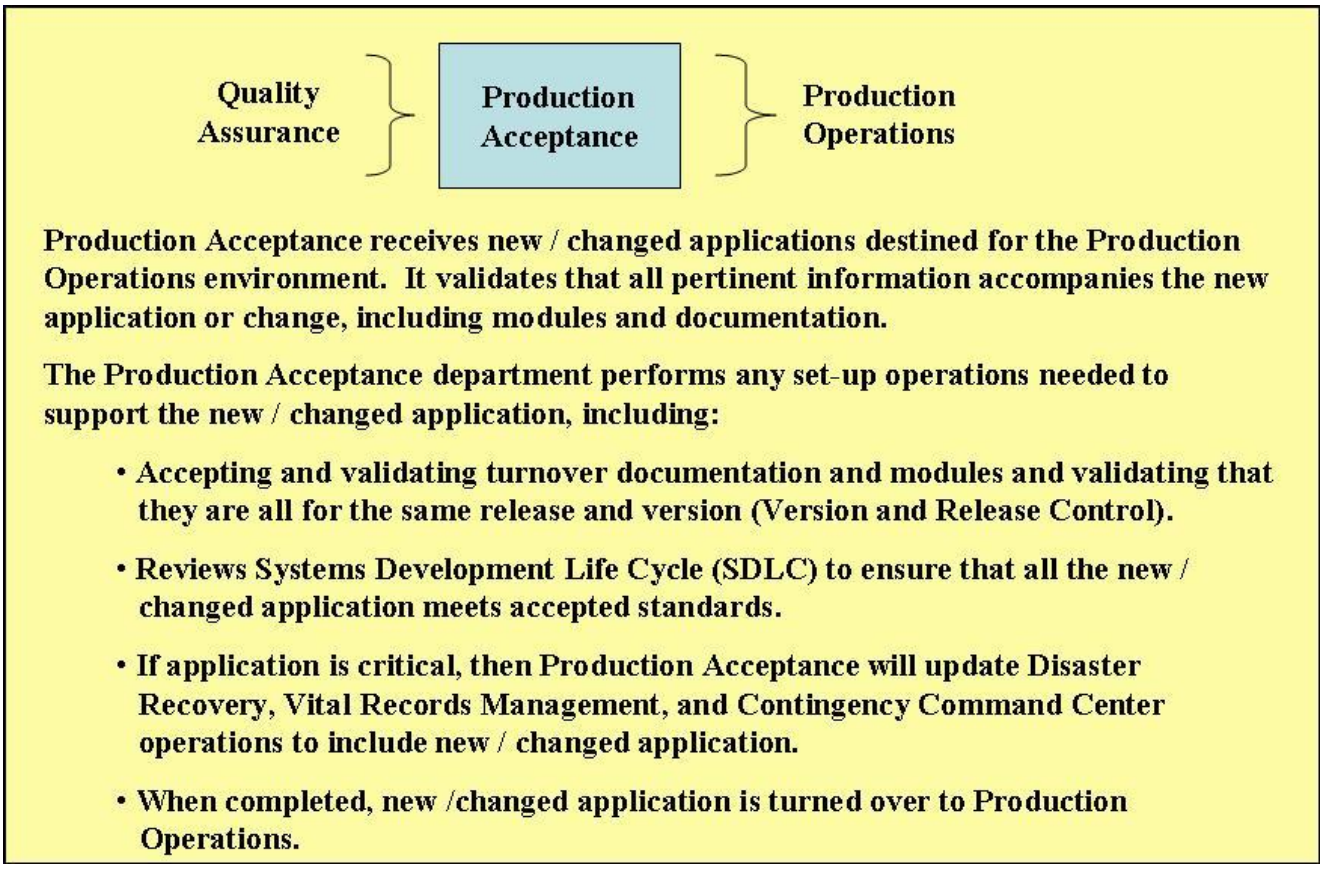
Figure 63 - Quality Assurance procedures

1. **Customer Focused Organization** -- Organizations depend on their customers and therefore should understand current and future customer needs, meet customer requirements, and strive to exceed customer expectations (see Service Level Agreement).
2. **Leadership** -- Leaders establish unity of purpose and direction of organization. They should create and maintain the internal environment in which people can become fully involved in achieving the organization's objectives.
3. **Involvement of People** -- People at all levels are the essence of an organization and their full involvement enables their abilities to be used for the organization's benefit.
4. **Process Approach** -- A desired result is achieved more efficiently when related resources and activities are managed as a process, hence QA is essentially a process.
5. **System Approach to Management** -- Identifying, understanding, and managing a system of interrelated processes for a given objective improves the organization's effectiveness and efficiency.
6. **Continual Improvement** -- Continual improvement should be a permanent objective of the organization.
7. **Factual Approach to Decision Making** -- Effective decisions and actions are based on the analysis of data and information. "If you can't measure it, you can't manage it!"
8. **Mutually Beneficial Supplier Relationships** -- An organization and its suppliers are inter-dependent, so a mutually beneficial relationship enhances the ability to create value.

Quality Assurance is a Company Philosophy that defines the desired level of quality sought by a company and the procedures followed to achieve these goals. During this phase test results are reviewed and the Post Mortem report analyzed to determine if the application meets company Quality Assurance objectives. The above functions are performed during the QA phase and if successful the application is allowed to proceed to the Production Acceptance phase of the System Development Life Cycle.

Production Acceptance

Figure 64 - Production Acceptance procedures

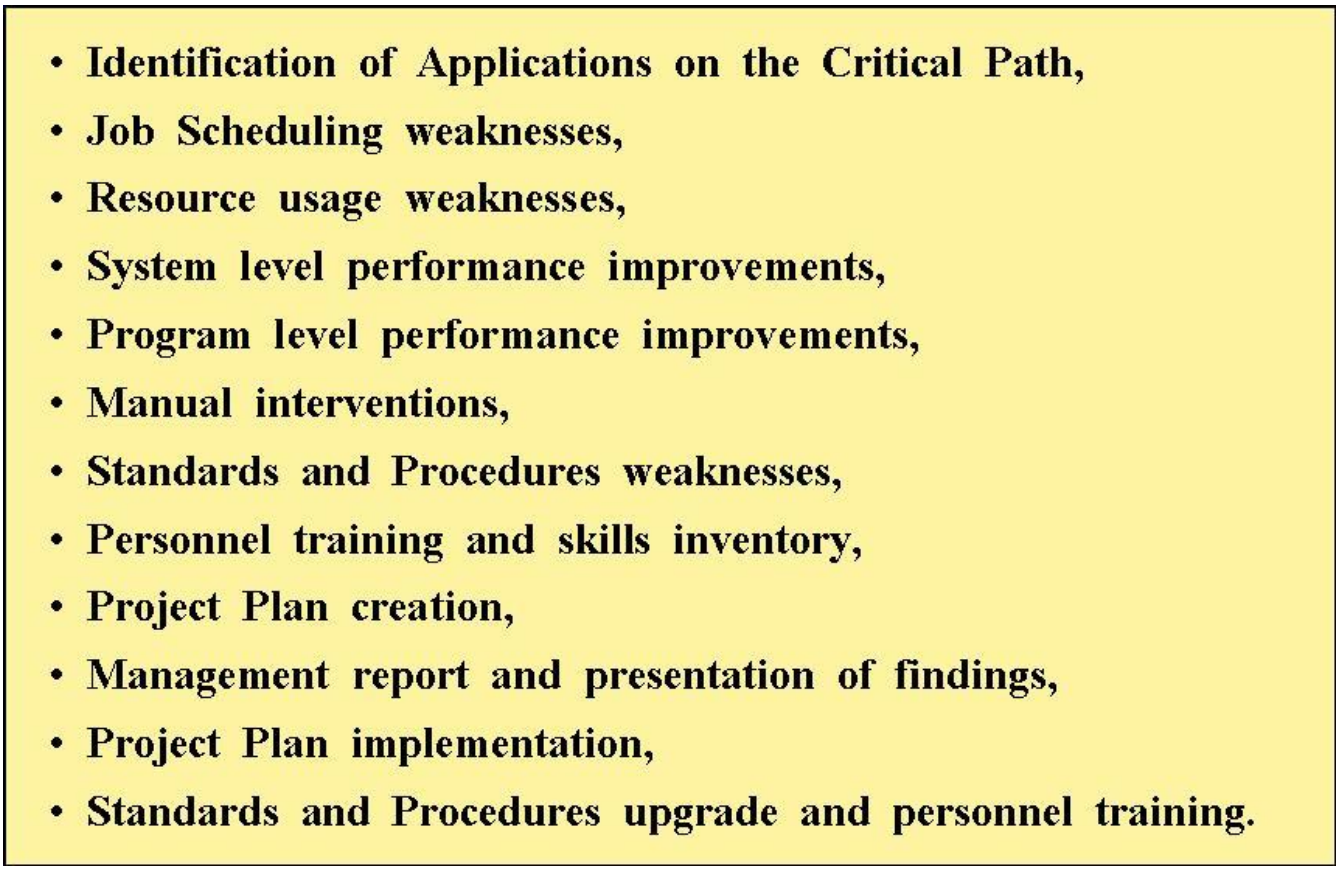


Production Acceptance is the last step before an application is allowed entry to the Production environment. It is responsible for reviewing application components and following the procedures needed to integrate the application and its components into the Production environment through disciplines like:

- Data Sensitivity and IT Security Access Controls;
- Vital Records Management;
- Backup / Recovery / Vaulting (Local and Remote);
- Job / Application documentation, including:
  - Job Run Book;
  - Support personnel and their contact information;
  - Messages and Codes; and
  - Expected Results.
- Job Set-up instructions;
- Messages and Codes, with Circumvention and Recovery procedures; and
- Recovery Procedures.

Capacity and Performance Optimization

Figure 65 - Capacity and Performance Management



Capacity and Performance Management is responsible for defining resource usage associated with an application and its efficiency. Applications are also reviewed to determine if they are critical and what their processing sequence should be based on dependencies. This information is used to define at what point an application should be backed up and restored during recovery operations.

Some of the functions achieved during this process are:

- Is the job / application a critical component requiring disaster recovery operations support;
- When the application / job should be scheduled base on runtimes and deadline scheduling;
- Resource usage and associated Input / Output processing times;
- System and Program processing times and Manual Interventions affecting completion times;
- New and Old processing time comparisons; and
- Impact on existing processing schedules (good or bad).

Information Technology Security

Figure 66 - IT Security procedures

1. IT Security Organizational Structure.

2. IT Security personnel and their functional responsibilities:
   a. Data Owner definition.
   b. Data Sensitivity.
   c. Data Usage guidelines.
   d. Data Access Controls.
   e. Violation Capturing.
   f. Violation Reporting.
   g. Required Forms.
   h. Procedures for completing forms.
   i. Forms submission and processing.

3. Existing Documentation.

4. Standards and Procedures manual sections.

5. Process descriptions.

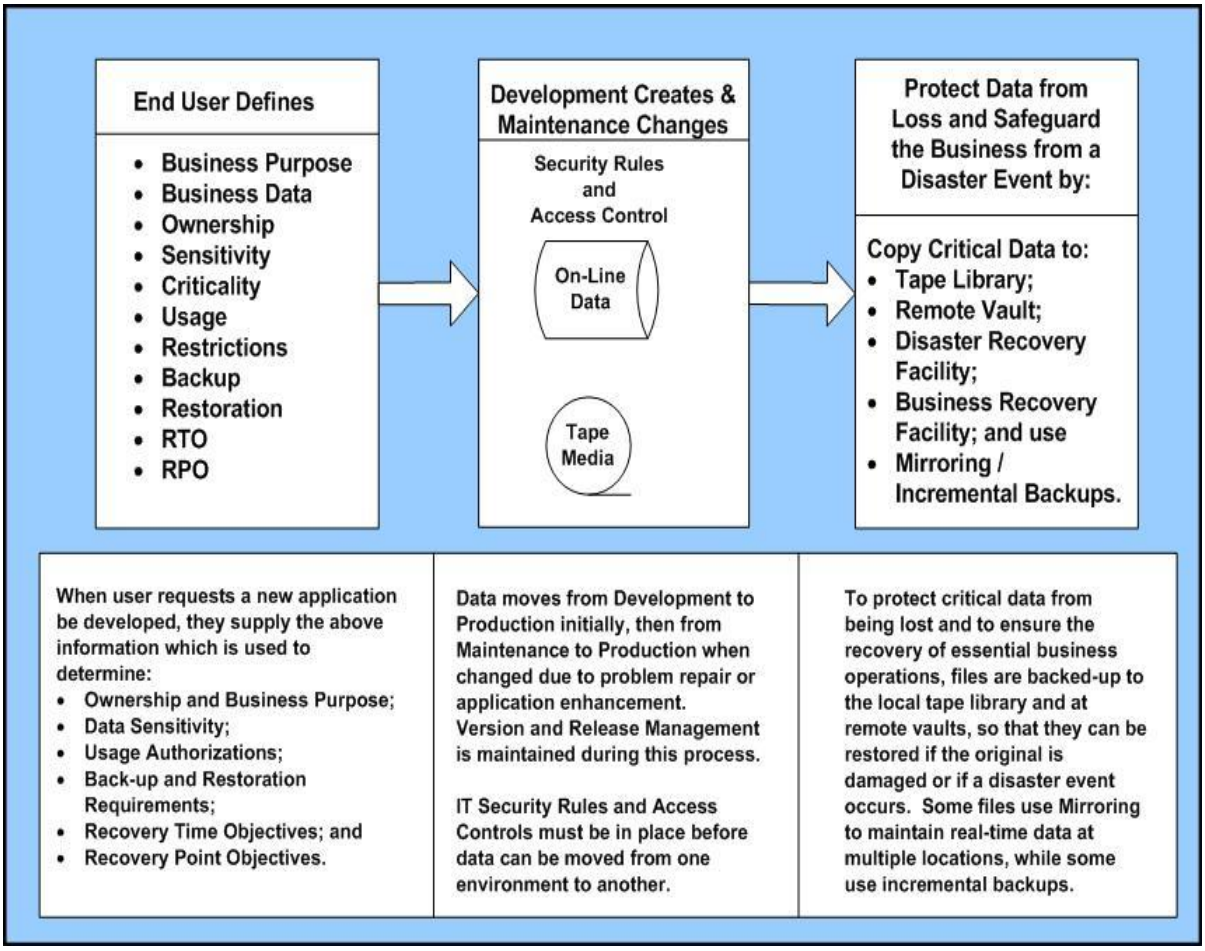
<NOTE>: The IT Security Management discipline will be included as needed in the SMC processes documented within the S&P Manual.

The responsibilities of the IT Security department are shown above. Its primary responsibility is to respond to Data Sensitivity requirements and insure that unauthorized access to sensitive data is not accomplished. It is also responsible for monitoring and reporting on access to IT assets so that security violations are identified and supportive documentation needed to pursue legal action or repair access rules is obtained. The control of Entitlements that allow personnel access to assets must be maintained so that access controls are updated when personnel leave the firm or change positions.

Vital Records Management procedures associated with library management and vaulting are based on data sensitivity associated with data, a job, or an application. Storage Management procedures are implemented in support of Library Management requirements and responsible for real-time and incremental backup of data and the control of data encryption to safeguard information from unauthorized access, even when contained on a tape / cartridge that is lost in transport.

Protecting Critical Data through Security and Vaulting

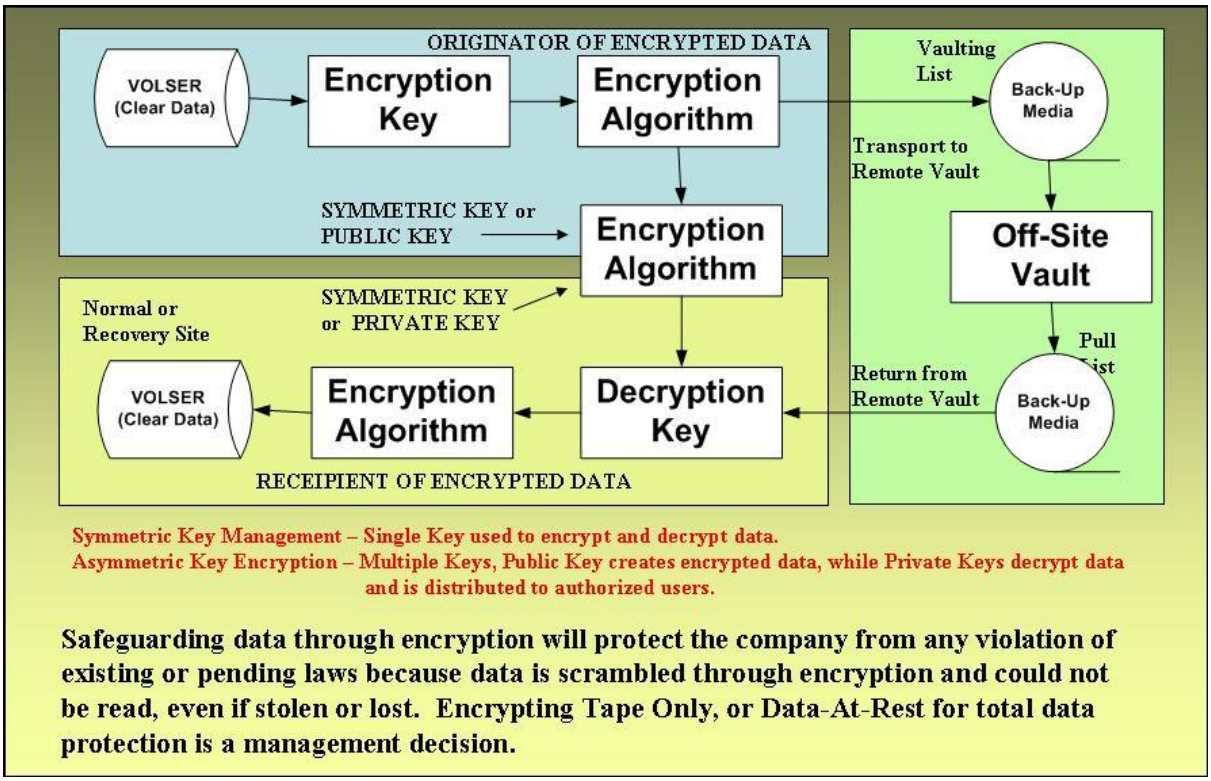
Figure 67 - Protecting Critical Data through Security and Vaulting



Data Sensitivity through Vital Records Management is described above. These guidelines are used to establish back-up and restoration guidelines associated with data.

Protecting Data through Encryption

Figure 68 - Protecting Data through Encryption

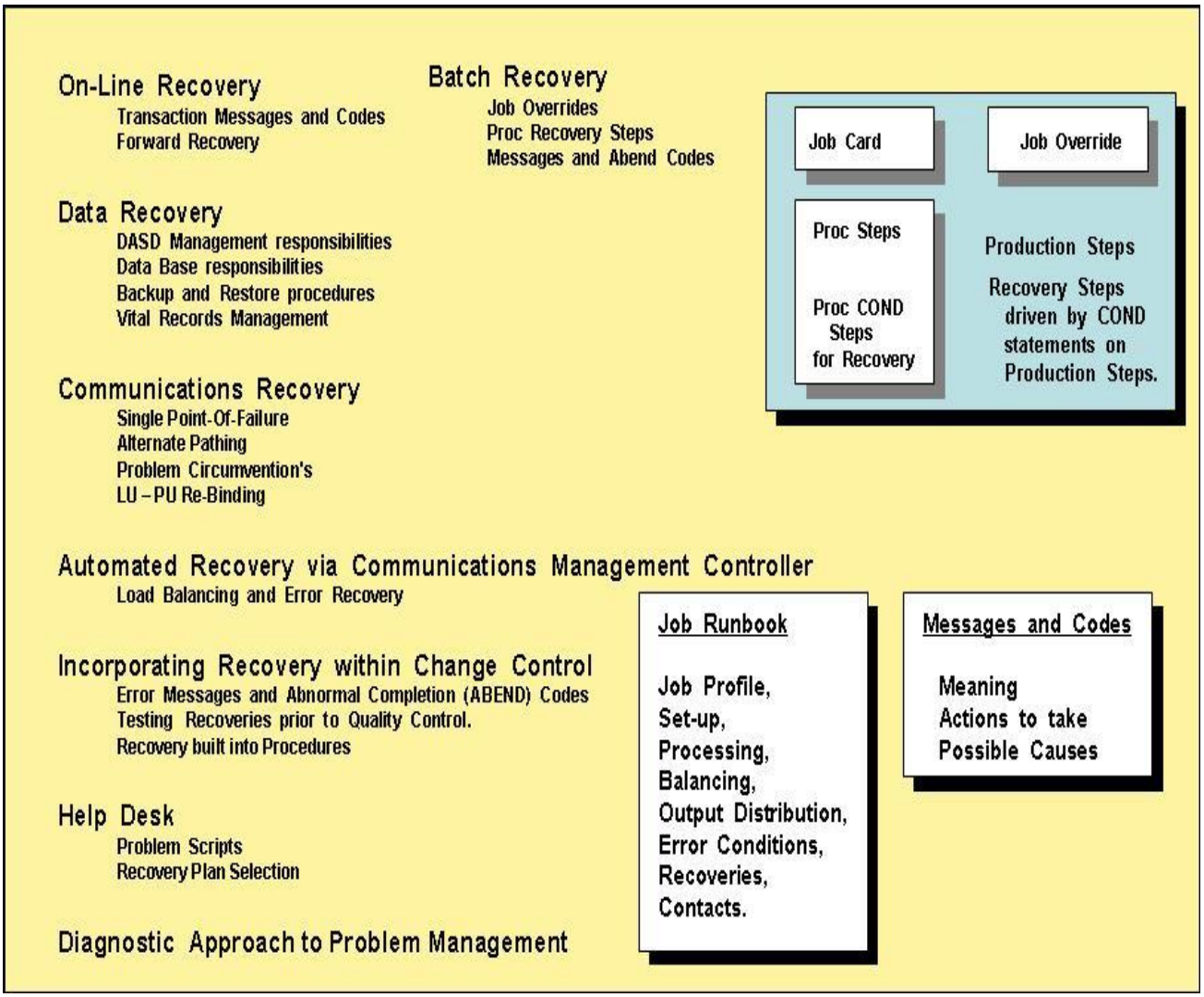


Encryption protects data by scrambling data through encryption formulas identified as keys. Public and Private keys can be used to scramble and unscramble data as needed. Encryption can now be accomplished in hardware devises with little or no overhead. Because of this, its use is growing.

Encryption information contained on Tapes / Cartridges being stored at a remote vault or transported to another site will protect against Identify Theft and fines should a media be lost during transport, because the data is encrypted and therefore safeguarded from unlawful access.

Specific Recovery Techniques

Figure 69 - Specific Recovery Techniques



Suggestions for recovery in various environments are shown above and should be considered when defining Job Turnover documentation requirements, so that the Operations Staff knows how to recognize and recovery from encountered problems.

Vital Records Management

Figure 70 - Vital Records Management procedures

1. **Define Vital Records Management Organizational Structure.**

2. **Define Vital Records Management personnel and their functional responsibilities.**

3. **Vital Records Management Standards:**
   a. Vital Records definition (Forms Management and Control);
   b. Library Management for Vital Records,
   c. Backup requirements;
   d. Vaulting requirements; and,
   e. Recovery requirements.

3. **Vital Records Management procedures:**
   a. Identification;
   b. Classification;
   c. Back-up procedures;
   d. Local Vaulting;
   e. Remote Vaulting, Retention, and Archiving;
   f. Restoration, Re-Use, and/or Destruction procedures;
   g. Interface with Tape Management System; and
      - Vault Management,
      - Encryption.

4. **Vital Records Management Standards and Procedures Manual sections.**

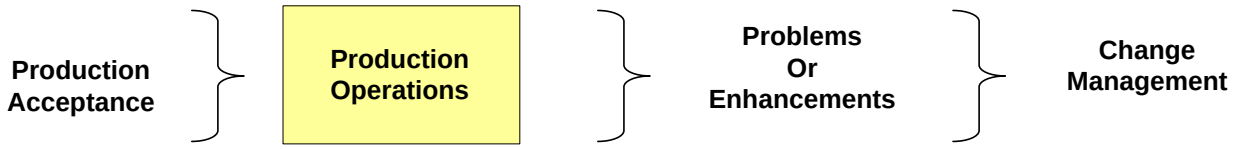
5. **Vital records Management process descriptions.**

<NOTE>: The Vital Records Management discipline will be included as needed in the SMC processes documented within the S&P Manual.

Vital Records must be backed up so they can be restored to local devices when Equipment or Data Checks occur, or remotely when responding to a disaster. Vital records can include financial, compliance, and application required information.

Production Operations

Figure 71 - Production Operation procedures



Production Operations is responsible for:

- Online Operations;
- End-User Operations;
- Batch Operations;
- Start of Day, Start of Week, Start of Month, and Start of Year processing;
- End of Day, End of Week, End of Month, and End of Year processing;
- Backup and Restoration;
- Job Set-Up, Processing, Output Control, and Recovery Operations; and
- Production Operations environmental Disaster Recovery.

Its control areas include:

- Input Control;
- Job Setup;
- Job Processing;
- Output Control;
- Report Distribution; and
- Library Management.

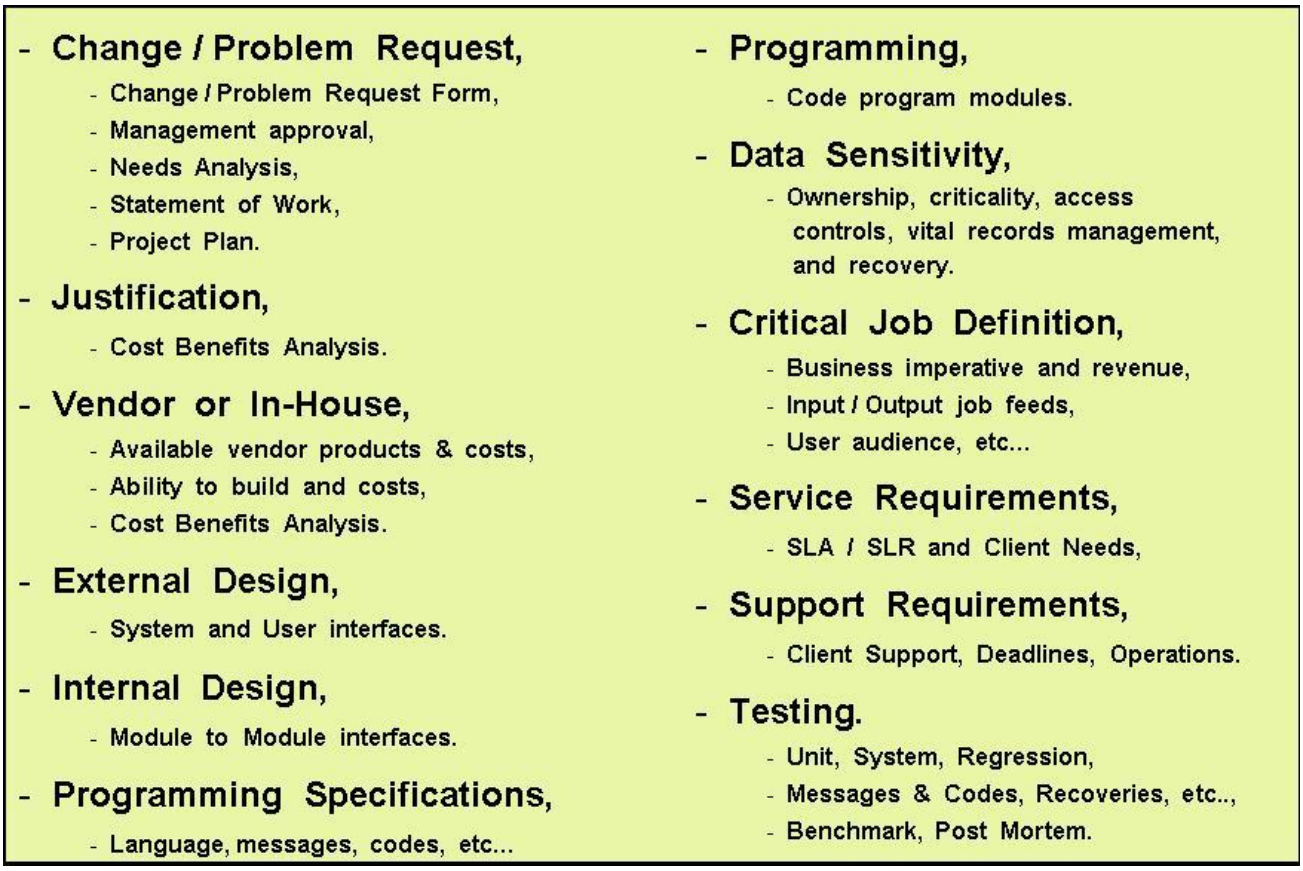
Production Operations is the final destination for an application and when it is approved for Production the above procedures are performed by the Production Operations Staff.

Start-of-the-day operations are responsible for activating data bases and online systems so that office personnel can perform their job functions. At the end of the day, or periodically throughout the day, backup of production data is accomplished on a real-time or incremental manner so that recovery operations can be accomplished within the Recovery Time Objectives.

Job Set-Up, Processing, Breakdown, and Delivery are performed by Operations Control personnel, while Technical Support personnel respond to encountered problems and make necessary repairs. Problem resolutions can generate Change Management requests and are passed on to Maintenance for incorporation into the next release of the program.

Maintenance Procedures

Figure 72 - Maintenance procedures



The procedures that must be followed when performing maintenance on an existing application are shown above. Changes are made when a problem resolution of enhancement is requested.

Maintenance procedures are almost exactly the same as those performed during the development process, except that maintenance data is copied from the production environment and its release level is raised by one. This process supports component and release management and allows for testing to be accomplished for the newly updated application.

Maintenance is the result of a user requested enhancement or to make a change needed to correct a problem.

Industry Best Practices

Over time the Information Technology industry has developed best practices to incorporate new and enhanced services within a corporate environment that is most efficient and adheres to compliance regulations. These practices are defined as:

1. COSO – Committee of Sponsoring Organizations;
2. CobIT – Control Objectives for Information Technology;
3. ITIL – Information Technology Infrastructure Library; and
4. ISO 17799 – Information Security Objectives.

COSO was developed to incorporate Risk Management and Mitigation Guidelines throughout an organization to best protect Stakeholders from uncertainty and risks that could erode value. It provides a framework for Organizational Structure, Standards and Procedures, and Employee Awareness and Training requirements.

CobIT is designed to extend COSO controls over IT environments by providing guidelines, integrating new acquisitions, delivering new acquisitions, monitoring IT activity, and helping management meet business objectives. It contains three levels of detail, including: Board of Director briefings; Management Guidelines; and the Staff receives briefings on CobIT Framework, Control Framework, Control Practices, Audit Guidelines, and Implementation Guidelines.

ITIL provides a framework to integrate Service Delivery and Support Services. The Service Delivery section provides guidelines for Availability Management, Capacity Management, IT Service Continuity Management, Financial Management for IT Services, and Service Level Management. ITIL Service Support provides guidelines for Problem Management, Change Management, Configuration Management, Versions and Release Management, and Service Level Management.

ISO 17799 provides guidelines for Change Initiation, Change Readiness Reviews, Operations Review, and SLA Reviews.

These disciplines are illustrated in pictures on the following pages.

COSO

Figure 73 - COSO Risk Assessment Overview

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.**

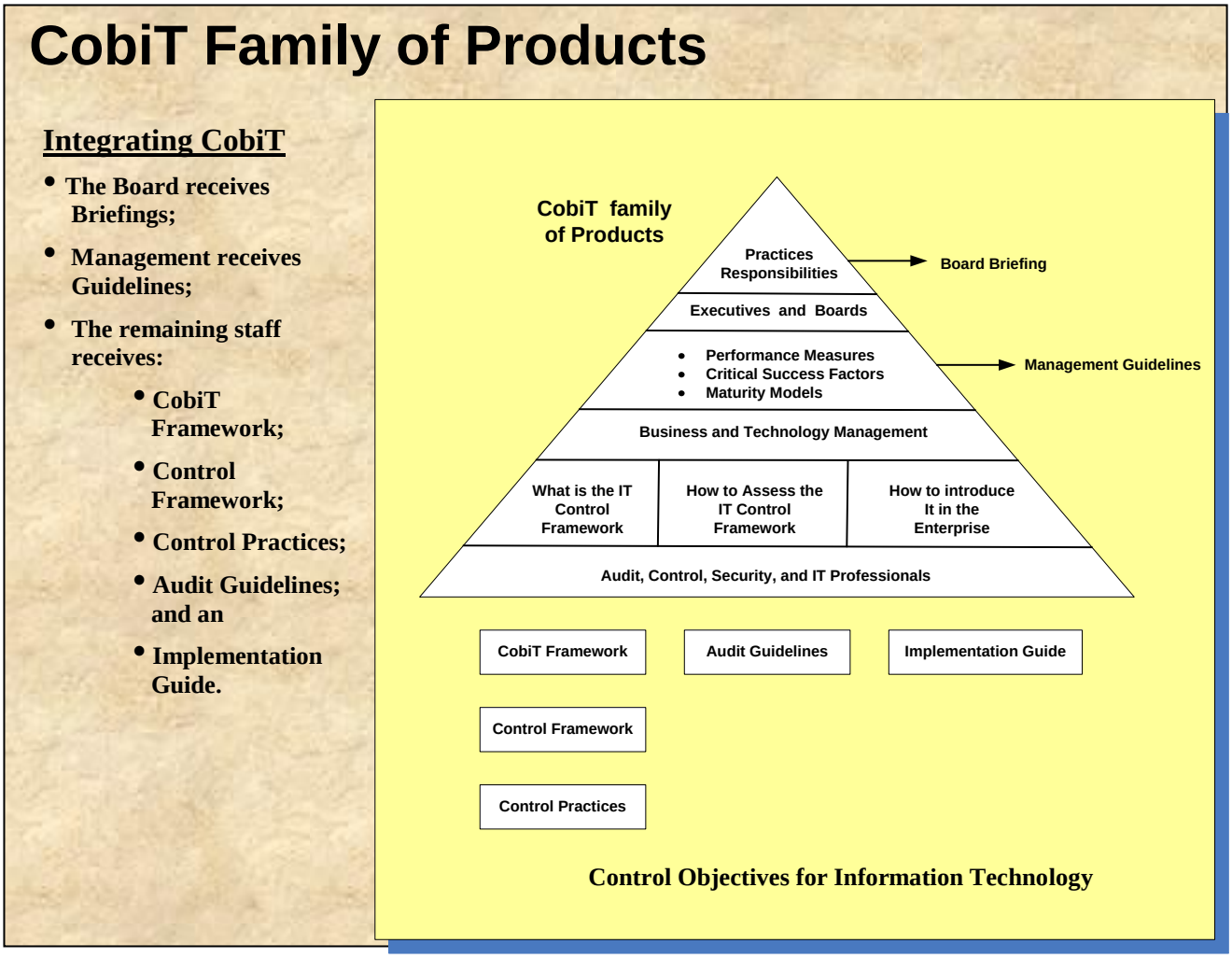
Creation of Organizational Structure, Personnel Job Descriptions and Functional Responsibilities, Workflows, Personnel Evaluation and Career Path Definition, Human Resource Management.

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

For more details about COSO go to www.erm.coso.org. From the above picture you can see that COSO is used to identify risks, but is also used to integrate operations within a company by defining Job Functions and Standards and Procedures that can be used to ensure that best practices are not only integrated within the business but are also supported and maintained going forward.

CobIT Family of Products

Figure 74 - CobIT Family of Products

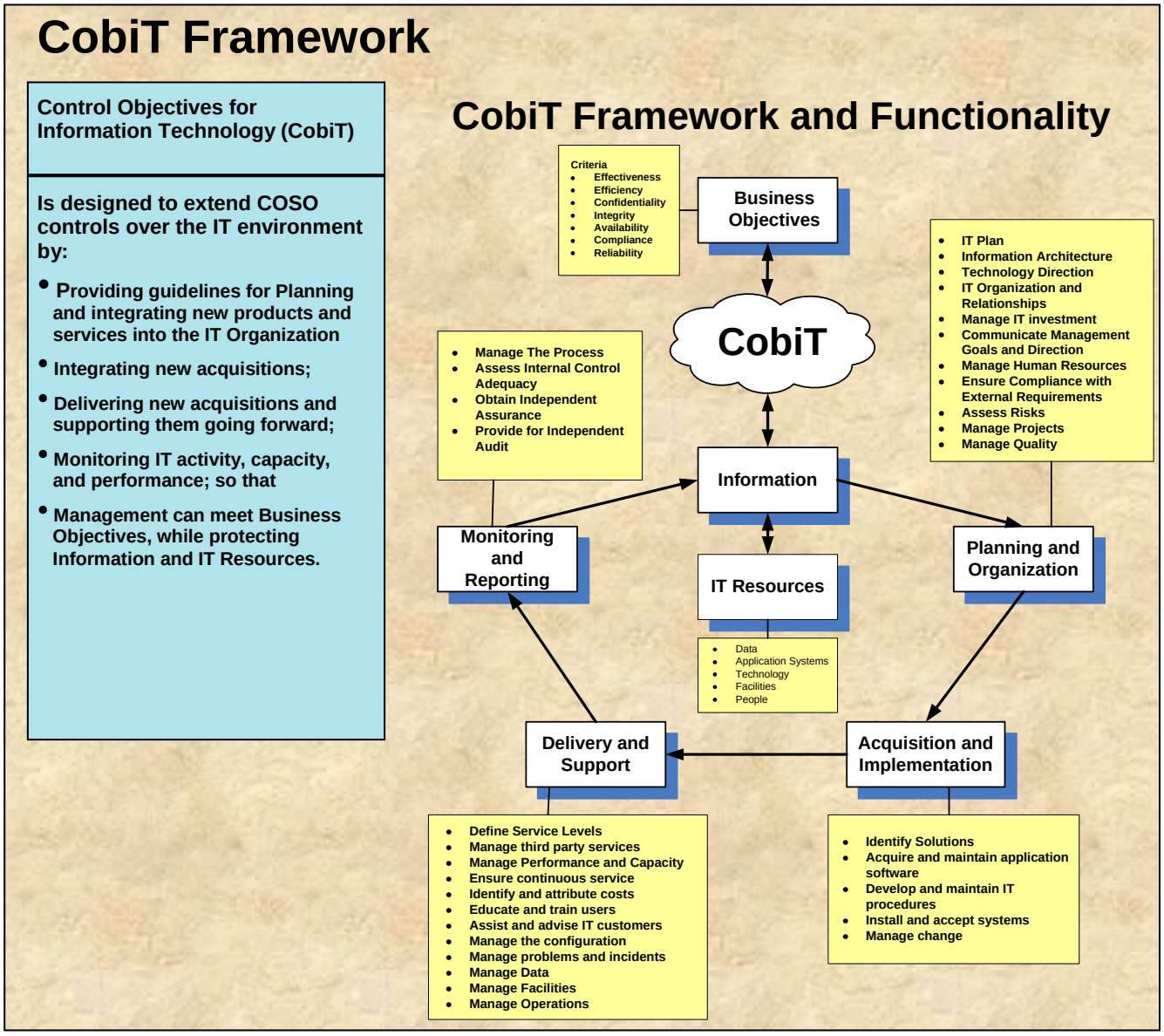


How CobIT is integrated into an Information Technology environment is illustrated in the above picture by showing the three levels and various components that are included in the CobIT framework.

CobIT is used to support integrating applications into the Information Technology environment in accordance to corporate and industry standards. It crosses all levels of management and supportive personnel so that a common language and process is adhered to. CobIT is widely used and has gained acceptance throughout the IT and Business community.

CobIT Framework

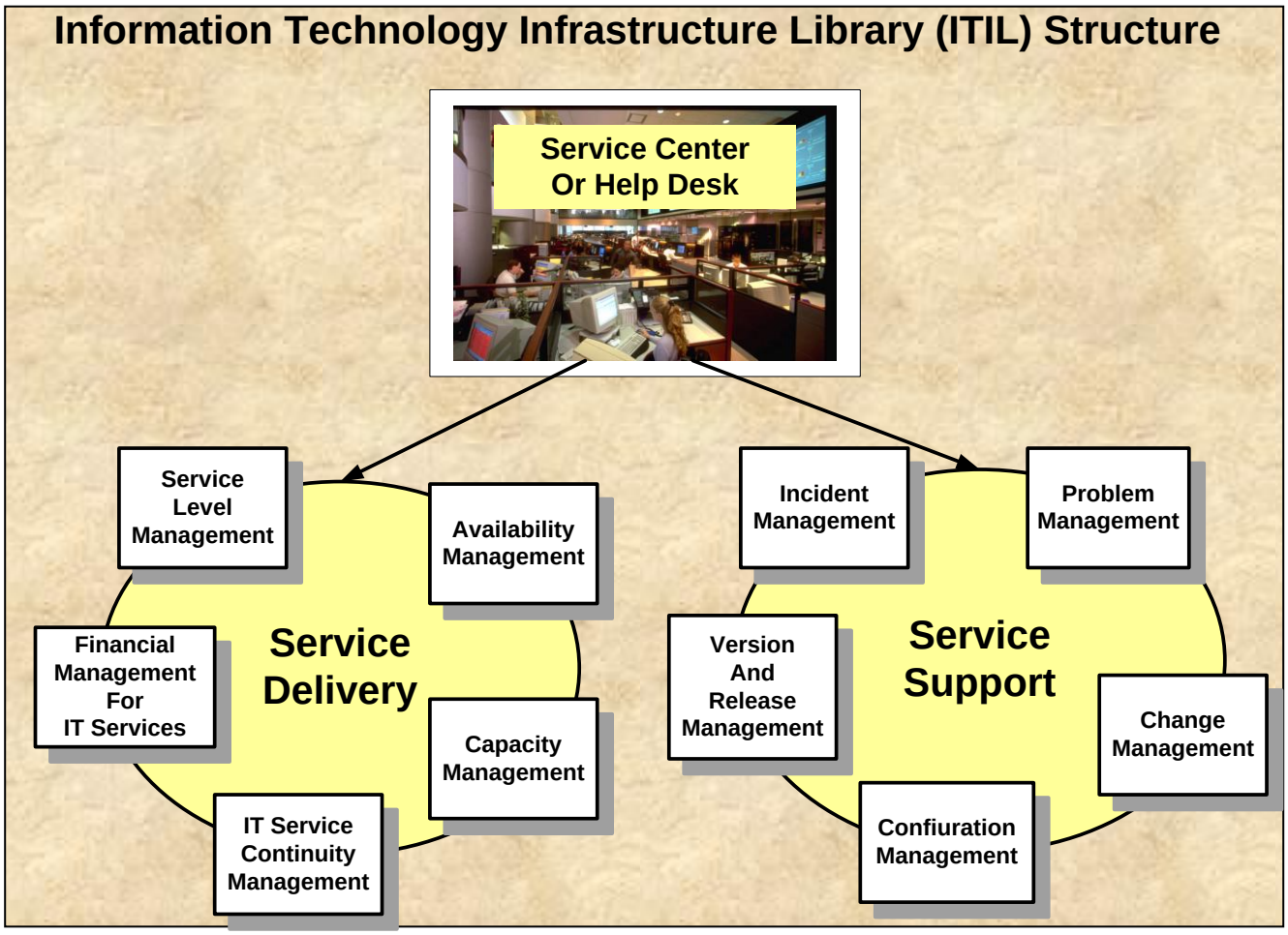
Figure 75 - CobIT Framework



How CobIT is integrated into a company is detailed above. It is agreed that CobIT should be followed when integrating an application into the business environment, but it is too complicated to fully explain within the document. Many reference materials can be located by online searches, which may be more current than any information contained within a printed document.

ITIL Framework

Figure 76 - ITIL Framework



ITIL is an evolution of Systems Management and is responsible for Service Delivery and Service Support. Again, ITIL is a complicated topic too large to fully cover within this document and should be researched via online searches. Additionally, ITIL is evolving and new releases are already being introduced to the industry. The use of ITIL is highly recommended because it truly addresses the problems previously experiences in a forms based operation, which was the single greatest loss of productivity in older IT and business organizations. As you can see from the ITIL components, most of them have been addressed in earlier sections of this document.

Figure 77: ITILv3 Overview and Enhancements

Information Technology Infrastructure Library (ITIL) v3 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

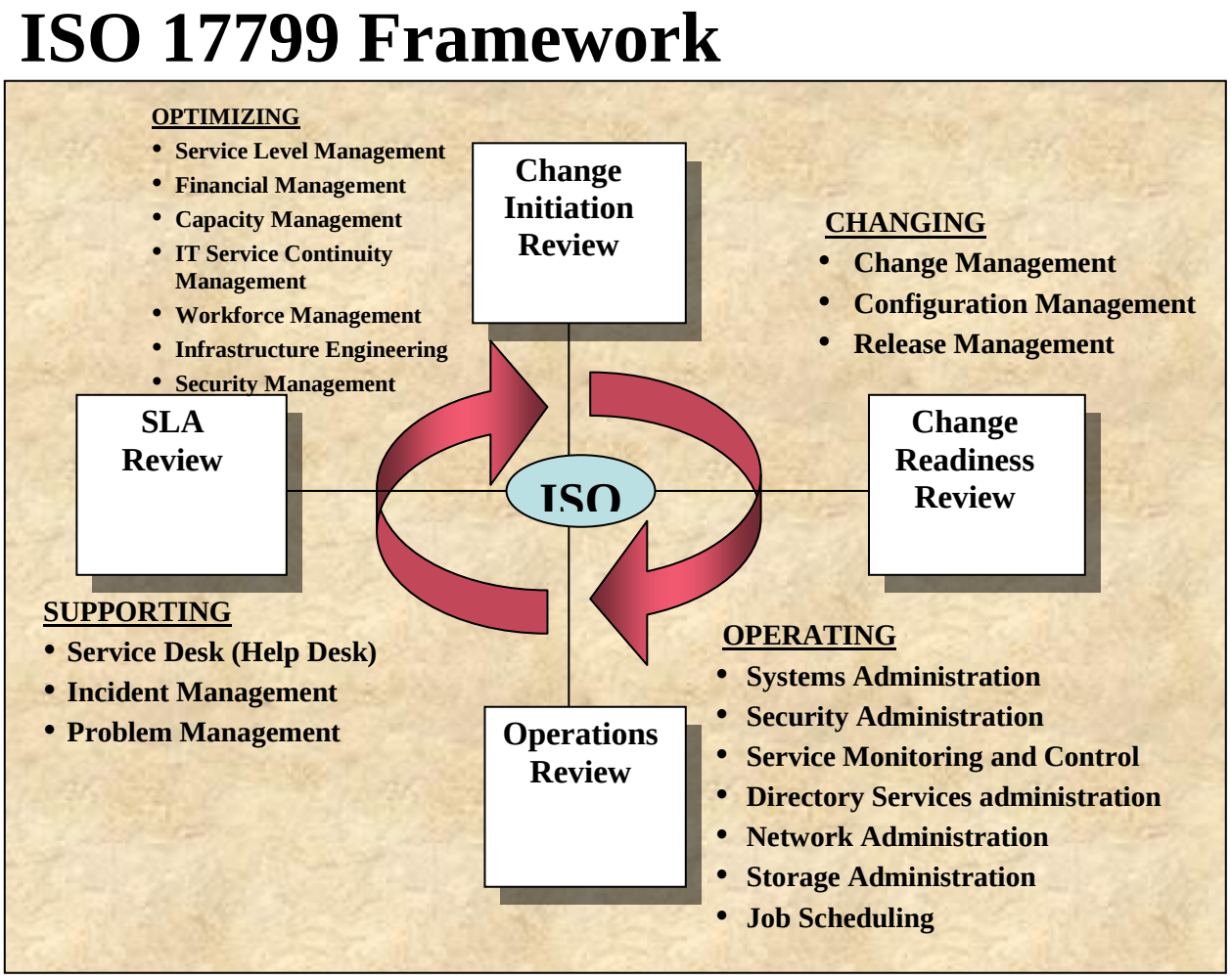
ITIL provides Forms Management and Control functions and is used to maintain libraries and support service delivery and maintenance. Information contained in ITIL Libraries can be used to satisfy a wide range of functional responsibilities from documentation, to performance, to auditing, and compliance.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

ISO 17799 Framework

Figure 78 - ISO 17799 Framework

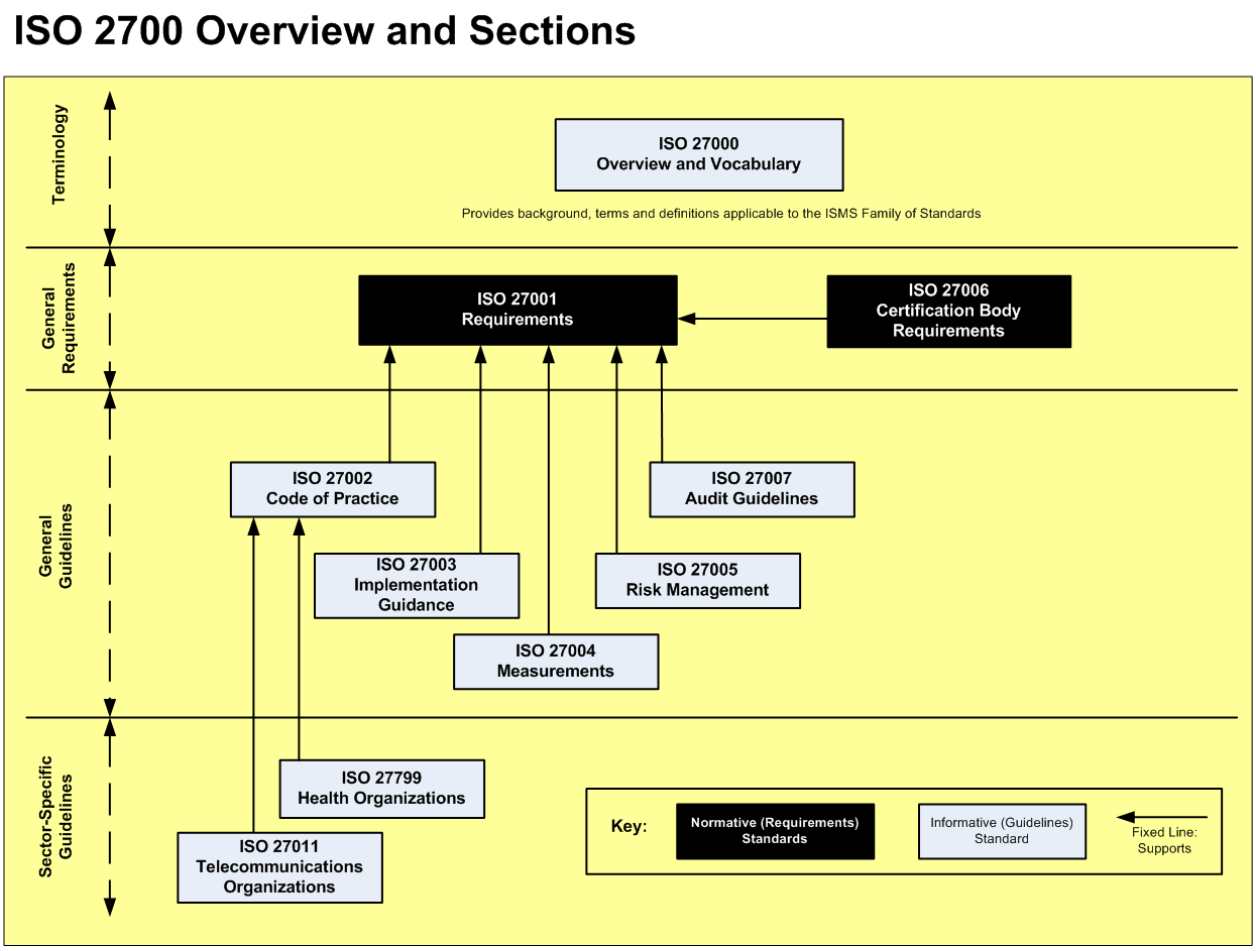


ISO 17799 is responsible for ensuring that changes to the Production Environment follow established standards and procedures designed to safeguard the company and adhere to compliance requirements. When used, it will optimize operations and reduce problems.

Again ISO 17799 is too large of a topic to be fully addressed in this document, but you see from its sections that most ISO 17799 functions have already been addressed in earlier sections of this document.

ISO 2700 Information Security Management System (ISMS)

Figure 79: ISO 27000 new Information Security Management System



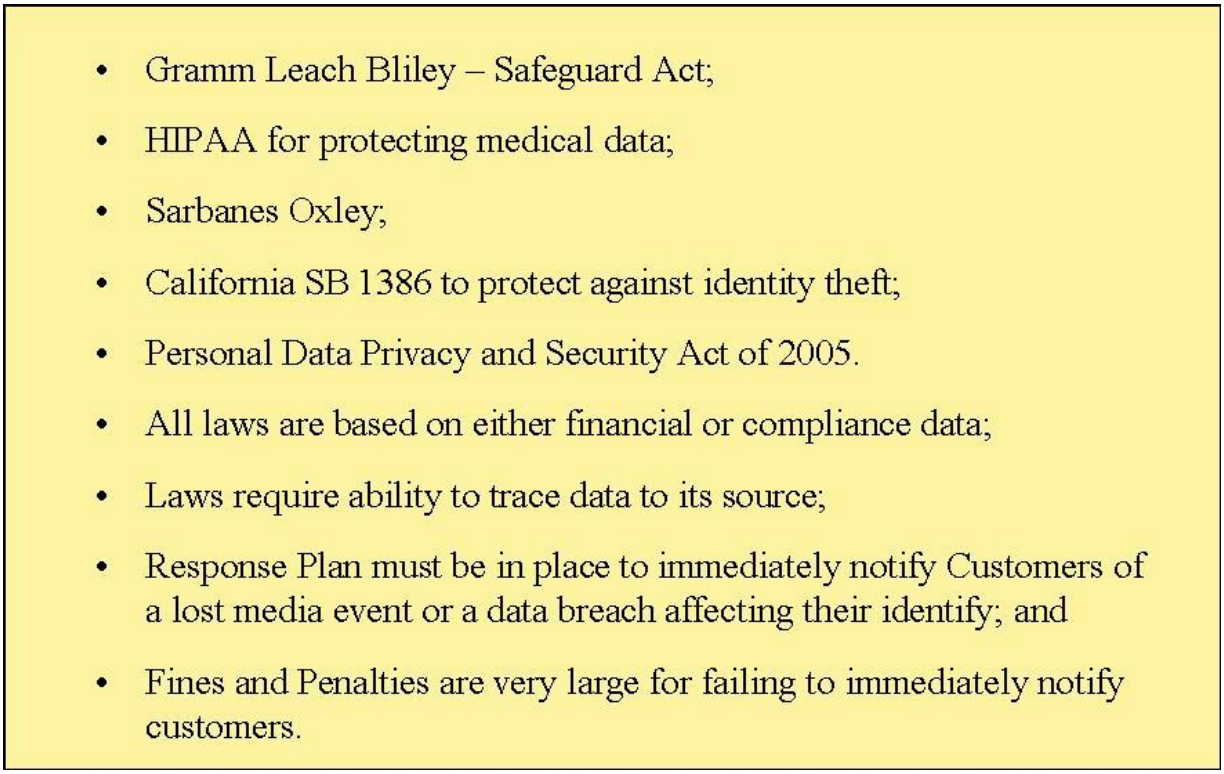
The new Information Security Management System (ISMS) guideline has been developed by beginning with a Glossary of Terms and then the following sections

ISO 27001 – Requirements Definition*;
ISO 27002 – Code of Practice;
ISO 27003 – Implementation guidelines;
ISO 27004 – Measurements;
ISO 27005 – Risk Management;
ISO 27006 – Certification Body Requirements*;
ISO 27007 – Audit Guidelines;
ISO 27799 – Health Organizations; and,
ISO 27011 – Telecommunications Organizations.

*Normative (Requirements) Standards which can be considered as guidelines.

Compliance Laws Pertaining to Data

Figure 80 – Laws pertaining to data



Some of the laws governing Information Technology and Business Recovery are listed above with more details to follow. Most of these laws are based on compliance data and its protection.

Each of the major compliance regulations, their components, and penalties are addressed in more detail in the following sections of this document.

Overview of Compliance Laws and their Penalties

Figure 81 - Review of Compliance Laws and Penalties

	Graham-Leach-Bliley Safeguard Rule	HIPAA Security Rule	Sarbanes-Oxley 404 Rules	California SB 1386
Effective Date:	**May 23, 2002**	**April 21, 2003**	**June 5, 2003**	**July 1, 2003**
Compliance Deadline	**May 23, 2003**	**April 21, 2005**	**June 15, 2004** (for public companies with market cap. of $75 million or more) **June 15, 2005** (for other SEC reporting companies)	
	Existing Laws and their Consequences			
Covered Entities	Financial Institutions as defined in the Bank Holding Company Act that possess, process, or transmit private customer information.	Organizations that possess, transmit, or process electronic protected health information (EPHI).	Publicly owned companies that file periodic reports with the SEC.	Any public or private entity that has unencrypted electronic personal information of California residents.
Purpose	Protect Customer Information from unauthorized disclosure or use.	Protect EPHI from unauthorized disclosure or use.	Provide senior management assessment of effectiveness of company's "internal controls for financial reporting" and attestation by independent auditors.	Protect California residents from Identity Theft.
Operative Mechanisms	**Information Security Program:** ▪ Responsible Employee Selection, ▪ Risk Assessment, ▪ Information Safeguards and Controls, ▪ Oversight of "Service Providers", ▪ Testing and Monitoring.	**Security Safeguards:** ▪ Risk Assessment, ▪ Policies and Procedures to control access, ▪ Physical Security Measures, ▪ Contingency Plan, ▪ Appointment of Security Officer, ▪ Training and communication to increase awareness, ▪ Audits and maintenance of Audit Trails, ▪ Agreements with "busines associates", ▪ Testing and Evaluation.	Internal Control Framework: ▪ (Coso Framework or Equivalent) ▪ Control environments – Compliance and Ethics, ▪ Risk Assessment and Analysis, ▪ Control Activities – policies, procedures, controls, ▪ Information and Communications, ▪ Monitoring or operations and control activities to determine continuing effectiveness of internal controls.	
Criminal Consequences of Noncompliance	Fines and Imprisonment for up to 5 years.	Fines to $250,000 and imprisonment for up to 10 years.	Fines up to $5 million and prison sentences for up to 20 years for deliberate violations.	Civil liability to any injured California resident.

A summary of the compliance acts is provided above with the entities they cover, their purpose, their operative mechanisms, and penalties associated with the laws. A more detailed description of each of these laws follows.

Use the above chart to gain an overall understanding of the Compliance Laws and their Penalties along with what is required to be in compliance.

Sarbanes Oxley Act

Figure 82 - Overview of Sarbanes Oxley

Sarbanes Oxley Act

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

The Sarbanes Oxley Act was designed to insure that corporations have current financial information available for review by auditors and to ensure that financial problems are addressed before they cause catastrophic problems. Its initial objective (section 302) is to define reporting requirements, then to gather all financial information into a common repository (section 404) for reporting and to eliminate security exposures. The final goal of the Sarbanes Oxley Act (section 409) is to have an automated financial reporting system available for instant auditing, if necessary, and to improve financial controls.

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

Graham, Leach, Bliley Act

Figure 83 - Overview of Graham, Leach, Bliley Act

Graham, Leach, Bliley Act

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

To adhere to the Graham, Leach, Bliley Act (GLB) a company, must implement and maintain an in-depth IT Security program that will protect Customer Information from unauthorized access. Its main purpose is to stop Identify Theft and any unauthorized use of Customer Data.

An IT Security audit is initially performed to detect where customer data is stored and how it is being protected. Any Gaps and Exceptions uncovered during this audit must be corrected to adhere to GLB and IT Security Audit Trails must be maintained to document any security flaws and provide information to assist in the prosecution of violators.

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

HIPAA

Figure 84 - Overview of HIPPA

HIPPA

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

HIPPA was introduced to protect personal medical information from unauthorized access and use. IT Security access control rules are created to isolate personal medical information from unauthorized access and use. Security audit trails must be maintained to identify unauthorized access to personal medical information and is used to assist in the prosecution of violators. Heavy fines are associated with violators of HIPPA.

Like GLB, HIPPA security rules and procedures are periodically reviewed to identify improvements and new procedures and products that may assist in the protection of personal medical information. These new products and procedures are implemented as deemed necessary to continually increase protection of medical information.

Patriot Act

Figure 85 - Overview of Patriot Act

Patriot Act

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

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

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

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

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

EPA Superfund

Figure 86 - Overview of EPA Superfund Act

EPA Superfund Act

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

The EPA Superfund Act was designed to help identify and clean-up toxic sites, but has evolved to include the disposal of electronic equipment like computers, cell phones, batteries, and the like. This problem has world-wide implications because of the materials contained in computers from gold to a range of toxic materials. Some computers are discarded and sent overseas for breakdown and material processing. Unfortunately, the methods used to dispose of computers have resulted in poisoning and pollution on a large and dangerous scale.

Many companies have developed a "Total Cost of Ownership" concept for purchasing, deploying, and terminating their computer equipment. The vendors are responsible for supplying and disposing of computer equipment in a manner that adheres to EPA Superfund guidelines. This also includes the erasing of any data from the memory of disposed or redeployed equipment thereby eliminating the chance that personal or business data would be access by unauthorized personnel.

FFIEC - Federal Financial Institutions Examination Council

The Table of Contents of the FFIEC Standards Manual is:

Figure 87 - FFEIC Table of Contents

The FFIEC is the most robust and recognized method for implementing recovery operations within a firm. It has been used domestically and internationally and has a wide audience of followers.

Crisis Management

Figure 88 - Crisis Management Charter

Charter

"Crisis and Situation Management is responsible for the establishment of Standards and Procedures that maximize operational responses to encountered problems and minimize business interruptions."

"By categorizing problems and their established recoveries within a matrix, the appropriate contingency plan can be activated that best responds to exceptional situations – before they become a crisis."

"Much as Battle Stations are assumed within a military organization, when crisis situations occur personnel assume recovery team functions and management enacts a contingency organization to coordinate business operations."

"Through these efforts, business services are continued in a planned fashion and reactions are kept under control."

"The results obtained from this Systems Management discipline are fewer interruptions and a safeguarded environment that is capable or responding to a wide-range of disaster events"

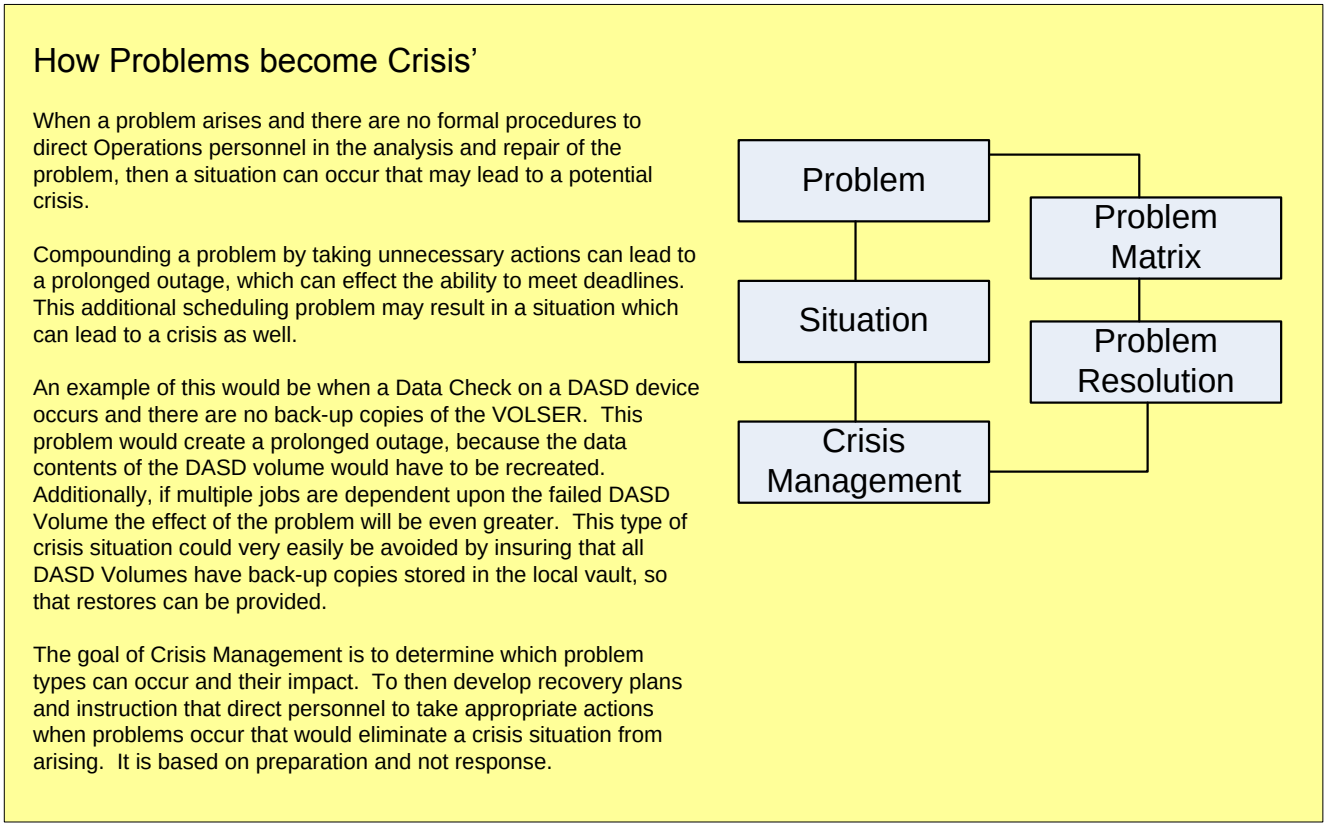
A Crisis occurs when encountered problems are not anticipated and responses to the problem are not planned and documented. This leaves personnel without a definition of the problem or instructions on how to respond to the problem, including circumvention and recovery procedures. To avoid a Crisis Situation, all types of problems should be defined, their possible causes outlined, circumvention procedures documented, and recovery procedures detailed.

Before applications are permitted into the production environment, all problem types must be defined, the possible causes of these problems listed, circumvention procedures provided, and recovery procedures documented. All related personnel should be made aware of these problem types and their recovery procedures. Operations personnel are responsible for providing back-ups to data during the Production Acceptance process.

To adhere to Crisis Management requirements, all error conditions producing messages and codes should be exercised during the Testing process. Operators should be able to look-up the message or code and perform the circumvention and problem management instructions included in application documentation should be submitted to Production Acceptance.

How Problems Become Crisis'

Figure 89 - How problems become Crisis'



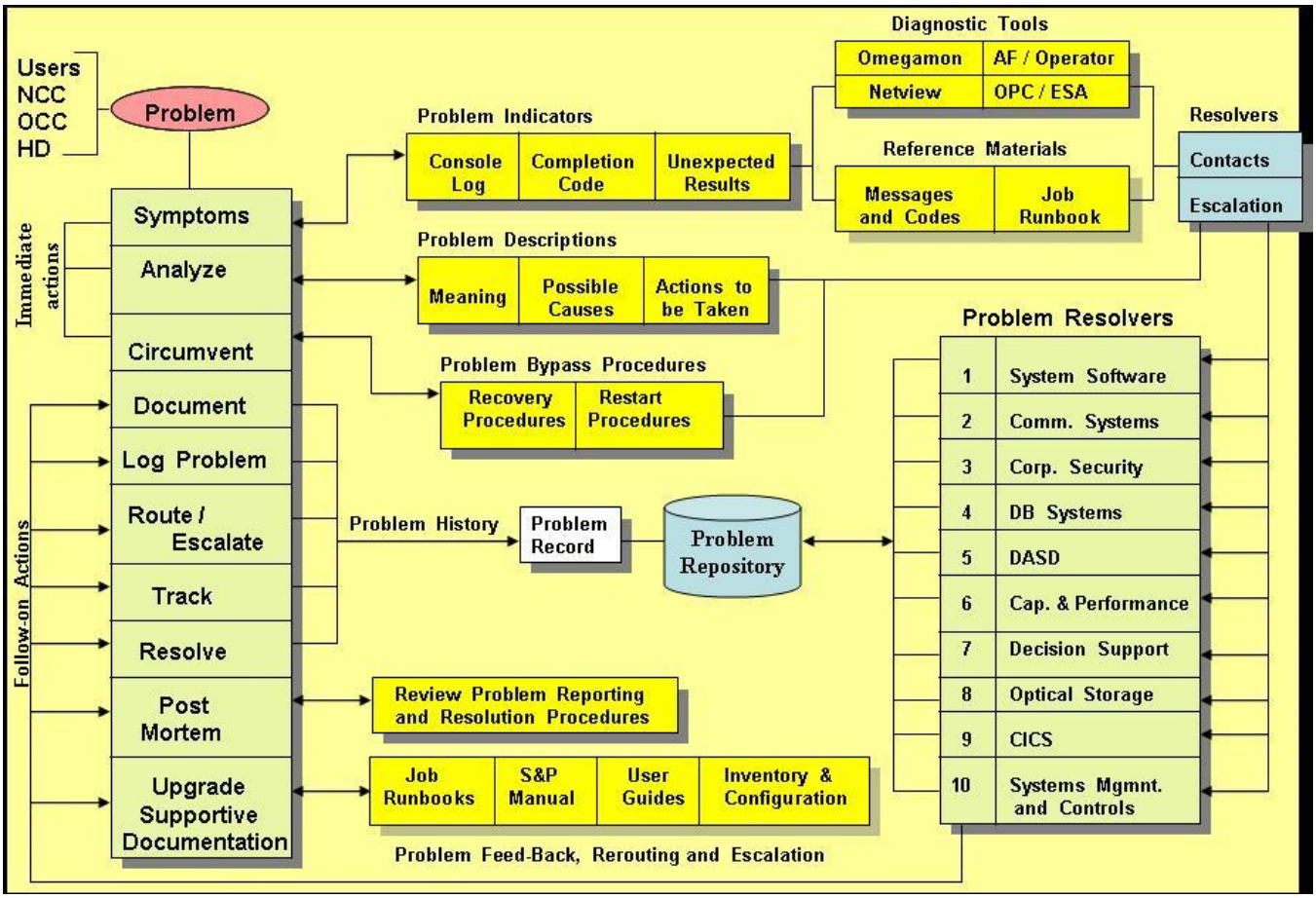
The above illustration shows how a problem can elevate to a Crisis situation because the problem type is not defined and instructions for circumvention or resolution are not provided.

If problem types are defined and procedures to identify, circumvent, and recover from the problem are provided it is very likely that if the problem occurs it will be easily resolved and not lead to a crisis. In a crisis situation people improperly react and compound the problem.

To avoid a crisis situation make sure that all problem types are defined and that circumvention and resolution documentation is provided during the testing and production acceptance process.

Support and Recovery Techniques

Figure 90 - Support and Recovery Techniques



The steps associated with problem definition, reporting, and resolution are shown in the above illustration.

First Level Problem recovery is when a reported problem can be resolved by the Help Desk technician, usually because the problem is a reoccurrence and has been recorded in the problem data base. If the Help Desk technician can not resolve the problem, it is escalated to **Second Level** support who is usually the internal person responsible for the failing components. If the Second Level responder cannot resolve the problem it is escalated to **Third Level** support which is usually the vendor who owns the product.

Problem Management

The Problem Management process, as shown above, begins when a problem event occurs. Problems can be submitted by Users, The Network Control Center (NCC), the Operations Control Center (OCC), Incident Command Centers (ICC), or the Help Desk (HD). A problem description and its impact accompany any submitted problem reports, along with any supportive information that may be available.

Immediate Actions associated with problem submissions include:

Symptoms – obtained through Problem Indicators, Diagnostic Tools and Reference problem symptoms include a Console Log Message, Completion Codes or Messages, or Unexpected Results. Additional problem information can be obtained through Diagnostic Tools like Omegamon, AF / Operations displays, Netview, or OPC / ESA. Reference Manuals can be used to further define the problem. These manuals include the Messages and Codes Manual, User Manuals, and Job Runbooks.

Analyze – the problem through Problem Descriptions like those contained within the Messages and Codes Manual that relate a Problem Message or Code to: the Meaning of the Message or Code; Its Possible Causes; and Actions to be Taken to resolve the problem.

Circumvent – whenever possible problem bypass procedures, work-arounds or problem circumventions should be performed so that operations can continue while researching the problem and its resolution. Problem bypass procedures should be found in Job Runbooks, Recovery Procedures, or Restart Procedures associated with the job.

At this point the problem has been identified, analyzed, and circumvented whenever possible.

Follow-On Actions should be initiated at this point, including:

Document – the problem is documented and added to the problem repository. A Problem History tracking record is also created and used to record all actions taken to resolve the problem. This History Record is displayed whenever a reoccurrence of this problem should happen, thereby eliminating the need to repeat the problem resolution process from its beginning.

Log Problem – The Problem History Record is provided with a Tracking Number so that actions performed to resolve the problem can be stored under the tracking number in the problem repository and later used for reporting.

Route / Escalate – If the problem can not be resolved by the Help Desk worker (Level 1) it is routed to the individual, or group, responsible for repairing the problem type (Level 2). Groups shown include:

1. **System Software** – Operating system and sub-systems are supported by this group. This group is associated with the Operations Control Center (OCC).
2. **Comm. Systems** – Communications Systems and Networks are supported by this group. They are associated with the Network Control Center (NCC).
3. **Corp. Security** – Corporate Security is responsible for creating access control rules that limit use of assets to those that have appropriate levels of security.
4. **DB Systems** – Data Base Systems are responsible for creating and administrating company data base systems.
5. **DASD** – Direct Access Storage Devices (DASD) and all Storage Management System requirements are addressed by this group.

6. **Cap. & Performance** – The Capacity of systems and their Performance is the responsibility of this group.
7. **Decision Support** – This group provides management with assistance by gathering information needed to make accurate decisions.
8. **Optical Storage** – This group is responsible for implementing and supporting all optical storage devices.
9. **CICS** – Customer Information Control System is the online system used by the company and this group is responsible for its support.
10. **Systems Mgmnt. And Controls** – Systems Management and Controls are supported by this group. Systems Management includes Problem, Change, and other supportive activities. The Information Technology Infrastructure Library (ITIL) discipline is presently used to support these functions and more.

If these groups can not repair the problem within a period of time, or if the problem is critical in nature, it will be escalated and routed to the external support group associated with the problem type (Level 3), which is usually the product owner or designated repair authority.

Track – The problem is tracked from initial report through final resolution. Each technician will complete a description of the activities they performed when addressing the problem. All of the information will be contained in the Problem History record and eventually the Problem Repository.

Resolve – The final problem resolution is entered into the tracking record and stored in the Problem Repository. This record is displayed should a reoccurrence of the problem be reported.

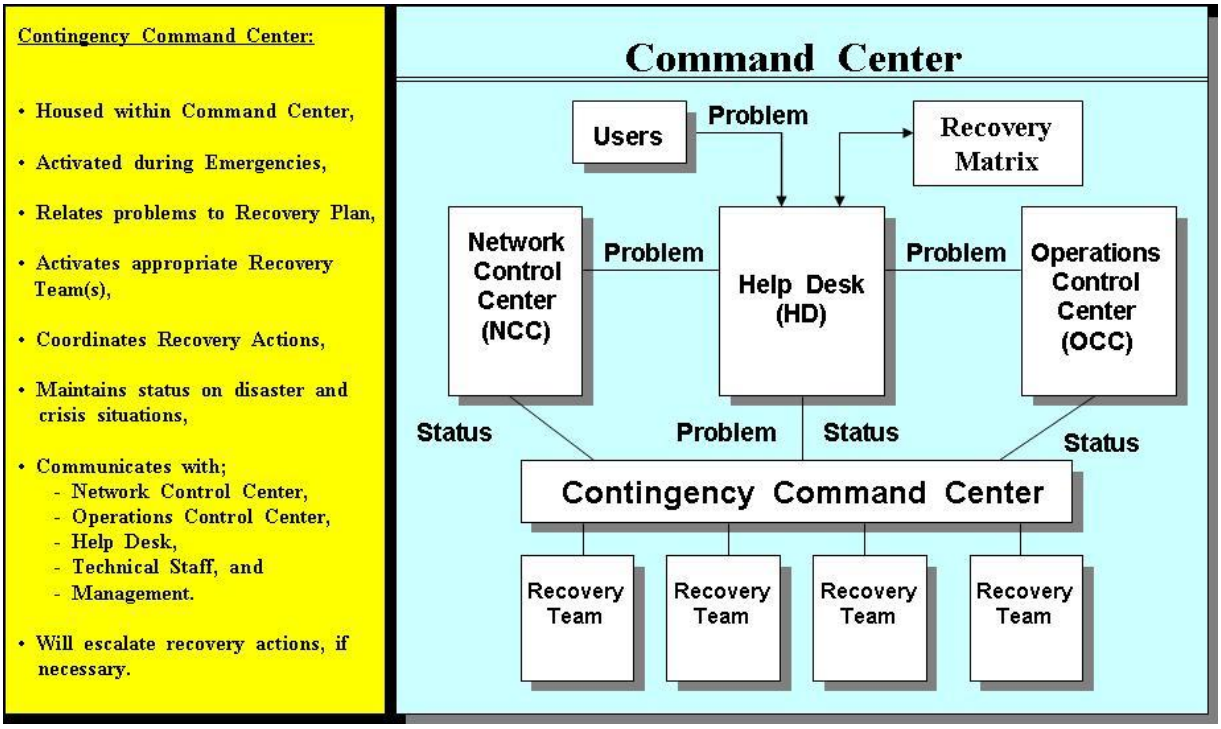
Post Mortem – A Post Mortem is conducted to review encountered problems, the actions taken to repair problems, and improvements that should be made when addressing this type of a problem in the future.

Upgrade Supportive Documentation – All documentation associated with a problem will be reviewed and upgraded is deemed necessary.

Command Centers

Command Center Environment Overview

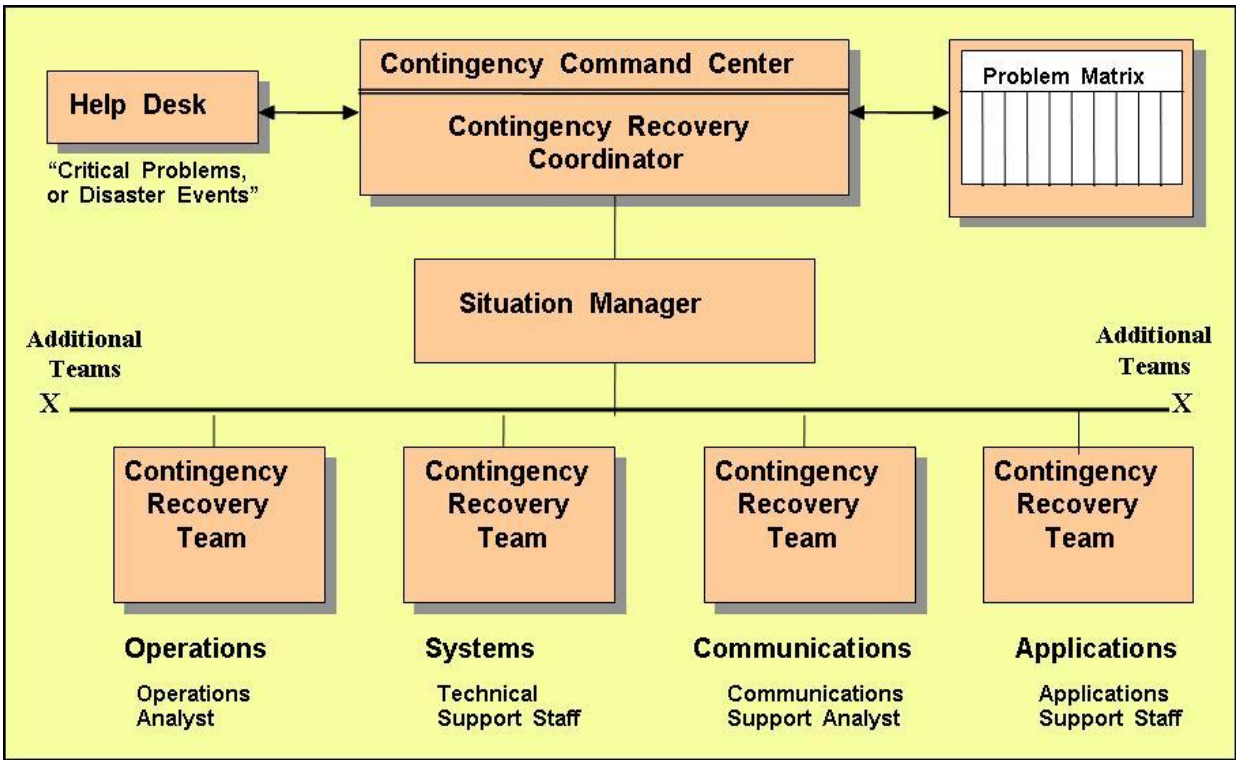
Figure 91 - Contingency Command Center



When problems are reported to the Help Desk, they are compared to the Recovery Matrix and the appropriate recovery operations initiated. The NCC is responsible for identifying and reporting communications problems, while the OCC is responsible for identifying and reporting problems related to operations. The Contingency Command Center is established when a problem becomes a disaster. It is used to direct recovery teams in responding to and recovering from disaster events.

Contingency Command Center

Figure 92 - Contingency Organization in Action



The Problem Matrix can house all recovery plans, so that when a problem is reported it is compared to the Recovery Matrix and the appropriate Recovery Plan selected. Once selected, procedures included in the Recovery Plan are executed from call out of recovery personnel to execution of recovery procedures.

Recovery teams are grouped by area of responsibility to optimize recovery operations. They communicate to the Situation Manager who coordinates all activity across teams. The Help Desk is made aware of recovery operations and is kept informed throughout the recovery process.

Post Mortems are conducted when recovery actions are completed so that improvements can be made to recovery plans and activities.

Help Desk

Figure 93 - Contingency Recovery Operations

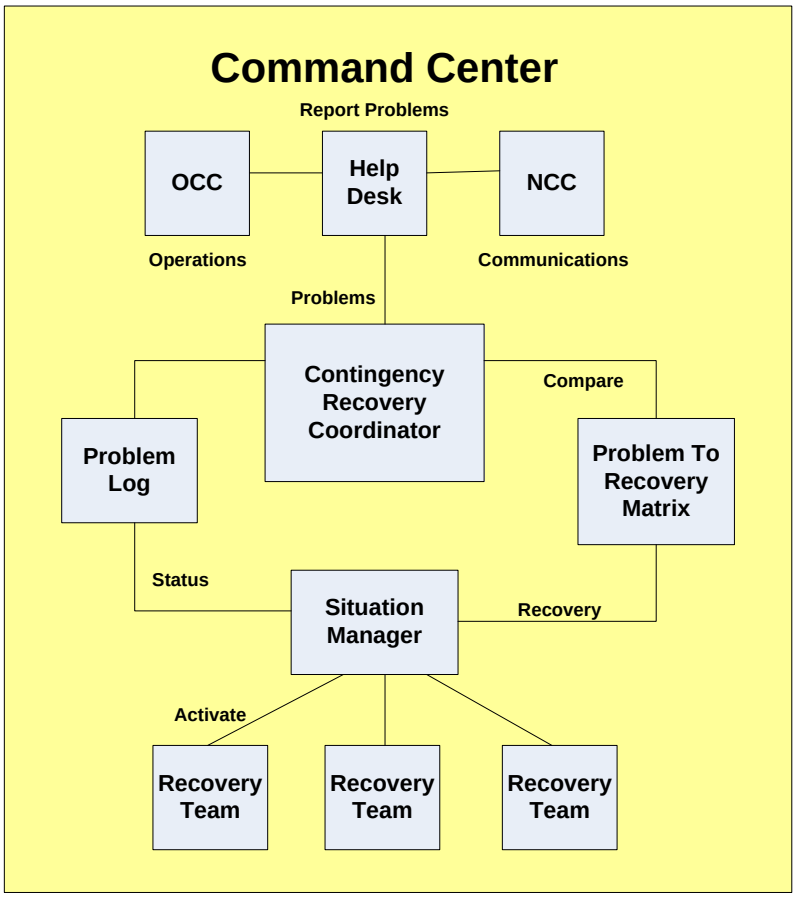
Contingency Recovery Coordinator

Responds to problems classified as "Potential Crisis Situations: by:

- Logging the Problem within the Problem Log;
- Comparing the problem to the Recovery Matrix;
- Selecting the corresponding Recovery Plan;
- Activating the Recovery Plan and Recovery Teams contained in the Recovery Plan; and
- Monitoring recovery operations and reporting on recovery status.

Situation Manager

Reporting to the Contingency Coordinator, the Situation Manager is responsible for activating and monitoring Recovery Team operations and for providing assistance through any mechanisms at their disposal. When situations become overly complex and a potential crisis can occur, the Situation Manager will take appropriate escalation actions needed concentrate more resources on the resolution of the problem.



Recovery Teams

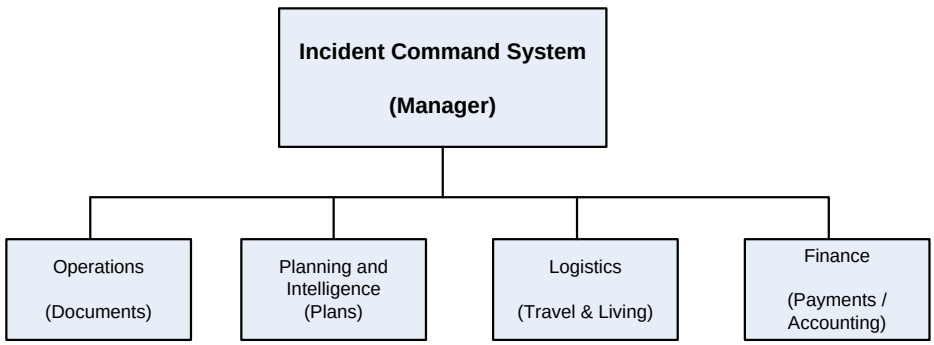
Designed to pull expertise together so that specific talents can address problems that require recovery operations, before normal processing can be resumed. Each Recovery Team consists of a Team Manager and Team Members. The organization of a Recovery Team is supplied to the Situation Manager and Contingency Recovery Coordinator. This organizational description includes functional responsibilities and alternate personnel for each of the recovery positions. Recovery Teams may require Recovery Tools as an aid in the performance of their assigned tasks.

The Help Desk is responsible for accepting problem calls, logging them, providing first level responses to problems, and escalating problems that can not be resolved through first level responses. In most organizations, the Help Desk will also be responsible for identifying disaster events, pulling recovery plans, and executing recovery operations by calling personnel associated with the recovery plan.

The Contingency Recovery Coordinator is responsible for global management of disaster responses, while Situation Managers and Recovery Teams actually perform recovery tasks as defined in the recovery plan.

Incident Command Center

Figure 94 - Incident Command Center overview



Incident Command Center Teams:

IAT – Initial Assessment Team

Assesses Damages and Determines Impact.

LIRT – Local Incident Response Team

Manages event Locally;
Determines how long event will last; and
Declares Local Disaster Recovery Activation.

CIRT – Corporate Incident Response Team

Manages event throughout corporation;
Determines Disaster Recovery event global impact; and
Declares and manages Disaster Event Globally.

The Incident Command Center is comprised of a Initial Assessment Team (IAT) who identify and analyze problem incidents to determine the criticality of the problem and what resources may be needed to respond to the problem incident. Normally the problem is turned over to Local Incident Response Teams (LIRT) who will be responsible for repairing local incidents. If the LIRT does not have the resources needed to repair a problem, the Corporate Incident Response Team will provide the needed resources. The CIRT is also responsible for overall management of encountered incidents and making any improvements needed to better respond to incidents going forward.

Workflow and Job Descriptions

Figure 95 - Workflow Overview used to create Job Descriptions

Functions	Inputs	Drivers	People	Procedures
GENERAL FUNCTIONS:				
New Contract	Contract	On-Going	Salesman	Marketing & Sales Prospecting
Customer Information	Customer Information Form		Salesman	Providing Jonas with Customer Information
Types of Work				Defining Our Work by Categories
HVAC/R		Concept		
Service		Offset		
Life Protection Services		Offset	Gary Kull	
Sprinkler				
Fire Extinguisher				
Fire Alarm System				
Store Survey Results	Work Order for Survey	Periodic		Technicians Handbook
Pictures	Pictures		Field Technician	
Category				
Proposal		Pictures / Customer	Salesman	Generating Customer Proposals
Proposal Agreement	Intranet			Proposal Replies & Library History
Video Proposal			Business Development	
Picture Proposal			Sales & BusiDev	
Customer Work Order				
Unsolicited Service Call	Prospect Service Call	Provide Lead to Sales	Service	Creating Customer Work Orders in Jonas
From Store Manager	Customer Service Call	Offset	Marketing & Sales	Closing Prospect
Request For Proposal	RFP	Projects	Project Office	History of RFP Responses
From Building Manager	RFP	Concept	Project Office	Building Managers - Types of Work
Scheduled PM or Survey	PM or Survey Work Order		Service Department	
Interfacing with				
Jonas	Jonas			Jonas Procedures
Services				Service Department Procedures
Projects				Project Department Procedures
Accounting				Accounting Department Procedures
Marketing & Sales				Marketing & Sales Procedures
Customers				Customer Communications Guidelines
Communicating				
Work Request	Service Request	PM's or Surveys	Service Dept.	Creating a Work Request
Work Forwarded		Skills Required		Routing a Work Request
Work Completed	Pictures from Technicians		Service Dept.	Completing a Work Request
Information	Pictures, Work Order		Service Dept.	Company Interfacing and Communicating
Customers	Salesmen			Customer Communications Guidelines

Job Descriptions are formulated from the Functional Responsibilities assigned to an individual or job category. The above figure is used to illustrate how a department can divide its Functional Responsibilities into sub-categories where personnel are assigned to a specific area. It breaks job functions into general functions, provides the inputs needed to support job activity, the drivers that the job functions provides to other personnel, the people manning the position, and a link to the procedures associated with the job function. Job Descriptions can easily be created from this spreadsheet.

Another category that can be added to this spreadsheet would be a listing of assigned personnel and their backup should they be absent or resign. This is illustrated on the following page.

Defining Primary and Secondary Personnel Assignments

Figure 96 - Personnel assignments and their backups

Functions to People	Manager	Supervisor 1	Clerk 1	Employee 1	Employee 2	Employee 3	Supervisor 2	Clerk 2	Employee 4	Employee 5	Employee 6	Procedures
New Contract	1	2					3					Writing a Contract
Customer Information			1					2				Completing Custoemr Information
Types of Work		1						1				Defining types of work
HVAC / R				1	2				3			HVAC / R definitions
Service					1	1				3		Service offerings
Life Protection Services						1			1		3	Life Protection Service definitions
Sprinklers			1					2				Sprinkler services and laws
Fire Extinguisher				1					2			Fire Extinguisher services and laws
Fire Alarm System					1					2		Fire Alarm services and laws
Store Survey Results	1	2					3					Performing a Store Survey
Pictures				1					2			Creating Store Pictures
Category					1					2		Categories of pictures
Proposal	1	2					3					Writing store proposals
Proposal Agreement	1	2					3					gainsin proposal agreements
Video Proposal												Creating a Video Proposal
Picture Proposal												Creating a Picture Proposal
Customer Work Order	1	2					3					Creating a Customer Work Order
Unsolicited Service Call			1					2				Responding to an unsolicited service Call
From Store Manager			1					2				Responding to Store Manager requests
Request for Proposal	1	2					3					Responding to a Request for Proposal
From Building Manager			1					2				Responding to Building Manager requests
Scheduled PM or Survey		1					2					Scheduling PM or Survey calls
Interfacing with	1	2					3					Interfacing with tools and departments
Jonas			1					2				Interfacing with the Jonas System
Services		1					2					Interfacing with the Service Department
Projects		1					2					Interfacing with the Projects Department
Accounting			1					2				Interfacing with the Accountign Department
Marketing & Sales	1	2					3					Interfacing with Marketing & Sales
Customers	1	2					3					Interfacing with Customers
Communicating	1	2					3					Communicating throughout the company
Work Request		1						2				Creating and Logging a Work Request
Work Forwarded			1						2			Forwarding a Work Request
Work Completed				1						2	3	Closing a Work Request when completed
Information		1	2				3	4				Reporting Work Request activity
Customers	1	2					3					Providing Customer with required reports

By creating a spreadsheet of functions and personnel assigned to complete the function management will be able to determine who should be trained for a specific function. Should a disaster event occur, or if an employee is absent, management will know who the backup is for a specific employee performing a specific function. This spreadsheet will also allow management to see how work is divided among employees within a department and it will serve as a quick reference when reviewing work flow.

The procedures associated with a job function can also include any recovery operations that the employee is responsible for.

Job Description Database Form

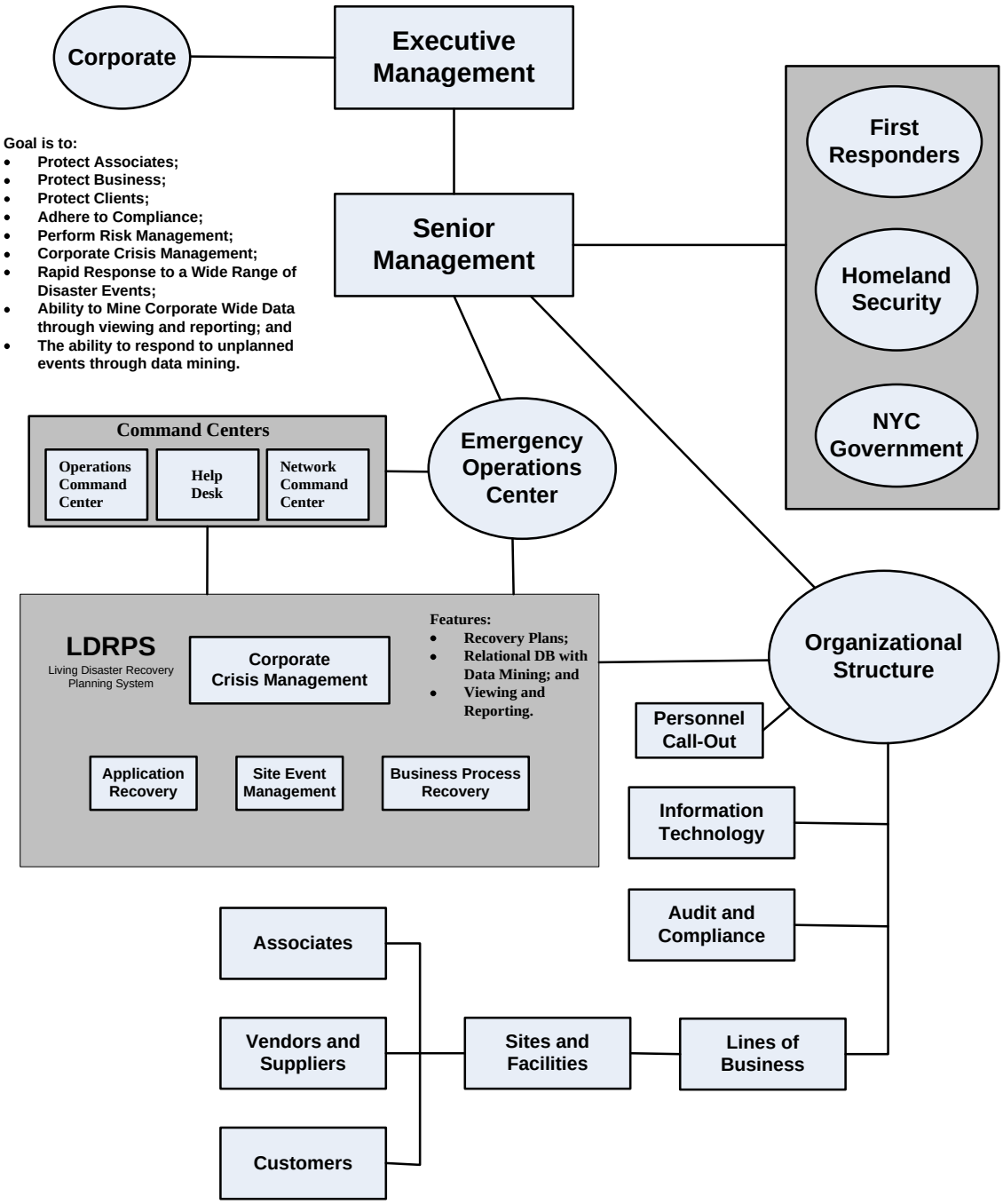
Figure 97 - Employee Job Description Database Screen

Instead of using an Excel Spreadsheet, you may want to use a data base system to create employee records and the functions that they are assigned to. I personally believe that a data base system is better than a spreadsheet, but everybody has their own likes and dislikes. The decision is your to make.

Emergency Management Preparedness Environment

Figure 98 - Emergency Management environment

Emergency Management Preparedness Environment and Tools



A fully implemented Enterprise Resiliency Organization is displayed above and explained below.

The **Emergency Management Preparedness** environment is centered in the Emergency Operations Center (EOC) and reports to Senior, Executive and Corporate Management. When an emergency event occurs, the EOC is activated and manned by members of the various recovery disciplines (Emergency Management, Business Continuity, Workplace Violence Prevention, etc.). The EOC interfaces with:

First Responders – Consisting of Fire Department, Police Department, Hazardous Materials Handlers and other disciplines that are first on scene and usually take command of the area affected by a disaster event. For example, the Fire Department will not allow people into a building that is still on fire, nor would a Policeman allow personnel into an active crime scene. The First Responder must allow access into a disaster event scene when the area is clear of danger. Knowing how long it will be before a scene is going to be closed to access could dictate the initiation of a recovery plan to move operations to a secondary site.

Homeland Security – will take command of a scene or dictate recovery operations in some instances. They are primarily responsible for terrorist activities, but can also provide assistance during natural disasters.

NYC Government (or local city government) – is responsible for controlling local responders and communicating recovery activities to public organizations. The local government can provide many assets to assist companies respond to emergency events.

EOC personnel also communicate with the other **command centers** contained within the organization as described earlier in this document. The command centers include:

- Help Desk (HD);
- Incident Command Center (ICC);
- Operations Command Center (OCC); and
- Network Control Center (NCC).

Disaster Recovery Tools are used to provide the EOC team with information vital to the performance of their functions. One of these tools could be Living Disaster Recovery Planning System (LDRPS) from Strohl Systems, recently purchased by Sungard. Other tools are also available for use by the EOC team to provide a wide range of information used to identify, analyze, define, and respond to disaster events.

The EOC also communicates with the **Organizational Structure** by using **Personnel Call-Out** programs to notify personnel that a disaster event occurred and that they should take pre-planned actions contained in the Recovery Plan for the disaster event.

The Information Technology (IT) Line of Business performs actions and executes Disaster Recovery Plans in conjunction with the EOC so that IT resources and data centers can be repositioned to supply business services to areas affected by the disaster event. The language and tools used by the IT LOB are different than those used by the EOC staff and communications between the two areas must be coordinated in a manner that provides an interface that is understandable between the two areas.

Audit and Compliance must be included in any recovery action to insure that compliance requirements are met and that controls are put in place to mitigate any uncovered weaknesses.

All **Lines of Business** (LOB's) within the organization must be informed of disaster events and directed to execute recovery plans as necessary. These plans are considered Business Continuity Plans and fall under the Business Continuity Management discipline, which also speaks a different language than the EOC Staff. Communications and coordination must be established to provide an interface between these two areas in order to reduce confusion and improve recovery operations.

Business Recovery Plans cover recovery operations for the LOB's and include:

> **Sites and Facilities** – This important section of Business Recovery is responsible for evacuation of personnel should a site experience a disaster event and for recovery actions that include salvage and restoration along with moving operations to a recovery facility should an outage be of sufficient time to deem the move necessary.
>
> **Associates or Personnel** – The most important asset to any company is its staff, Business Recovery Plans must take the safety of personnel into consideration.
>
> **Vendors and Suppliers** – Recovery operations must be coordinated with Vendors and Suppliers so that needed resources can be redirected to a recovery site should the primary site be lost and the staff has to move to an alternate facility. This includes communication and equipment supplies.
>
> **Customers** – Coordination with customers is imperative because you do not want to affect the services provided to customers.

Should a **Workplace Violence** event occur, like a shooting at a work site, the Workplace Violence Prevention plan is activated to coordinate actions with Employees, Police, Fire Department personnel, and the general community. Every effort should be made to prevent an act of violence, but should one occur every possible action should be made to safeguard personnel and the surrounding community.

Other areas where Emergency Management assistance can be sought and obtained include:

State and Local Government

Companies must adhere to governmental regulations in order to be in compliance. It is therefore necessary to identify the laws and regulations that your company must adhere to and to then implement responses to these needs that guaranty compliance.

First Responders

Fire and Police personnel are usually the first people to respond to a disaster situation. They are therefore defined as First Responders. These people can put out a fire, respond to a Hazmat situation, or simply arrest an offender, but they command the ground and will restrict entry to a disaster area until the situation is fully responded to and all required evidence is collected. It is very important to get to know the First Responders in your area so that you understand their procedures and can coordinate recovery operations with them.

Department of Homeland Security (DHS)

The DHS is responsible for responding to terrorism, national disaster events, and for establishing guidelines that local responders must adhere to.

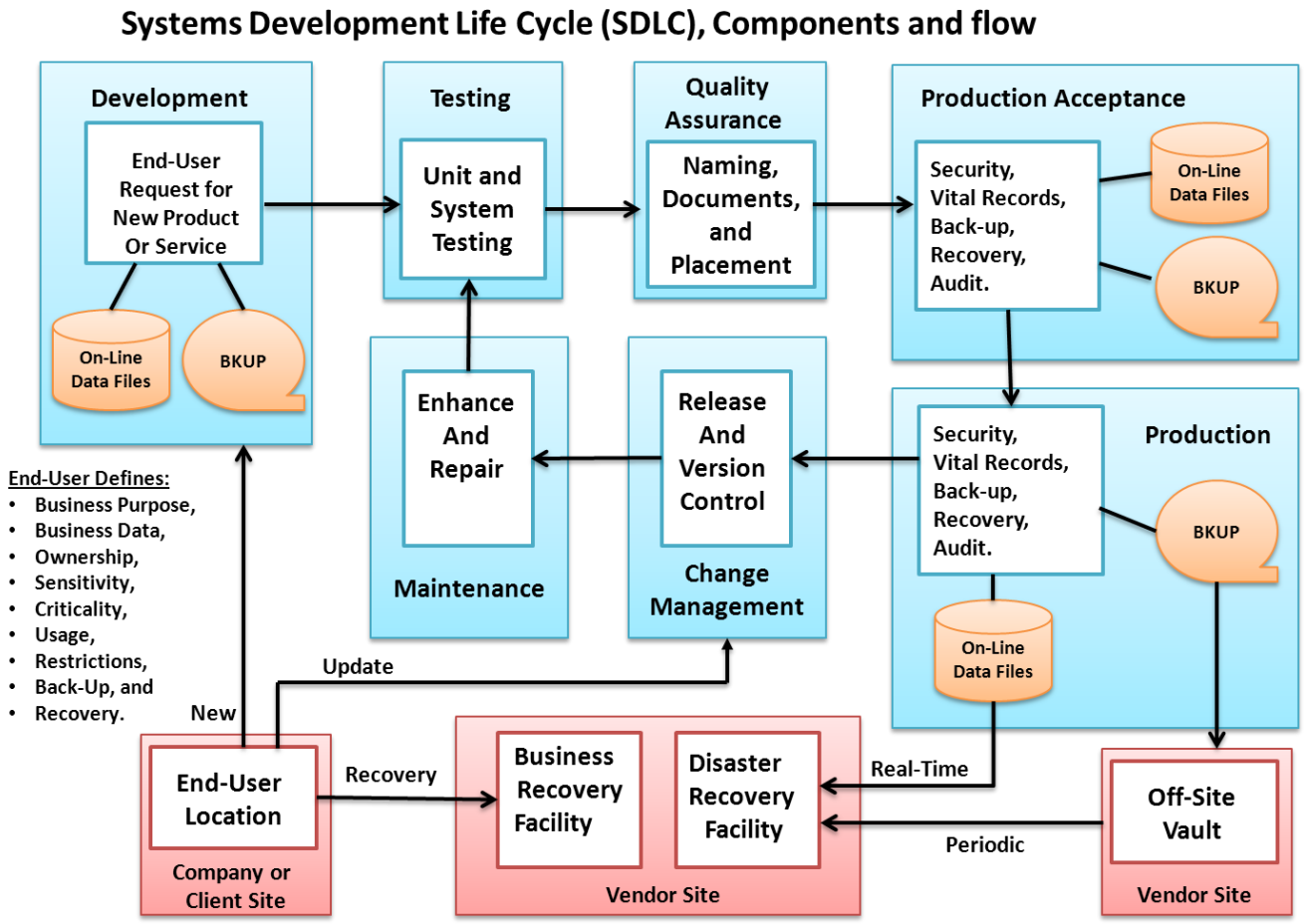
Office of Emergency Management (OEM)

The OEM is more responsible for local disaster events and coordinating recovery efforts with the business community.

Appendix A – Integrated Emergency Management Organization

The Systems Management Development Life Cycle

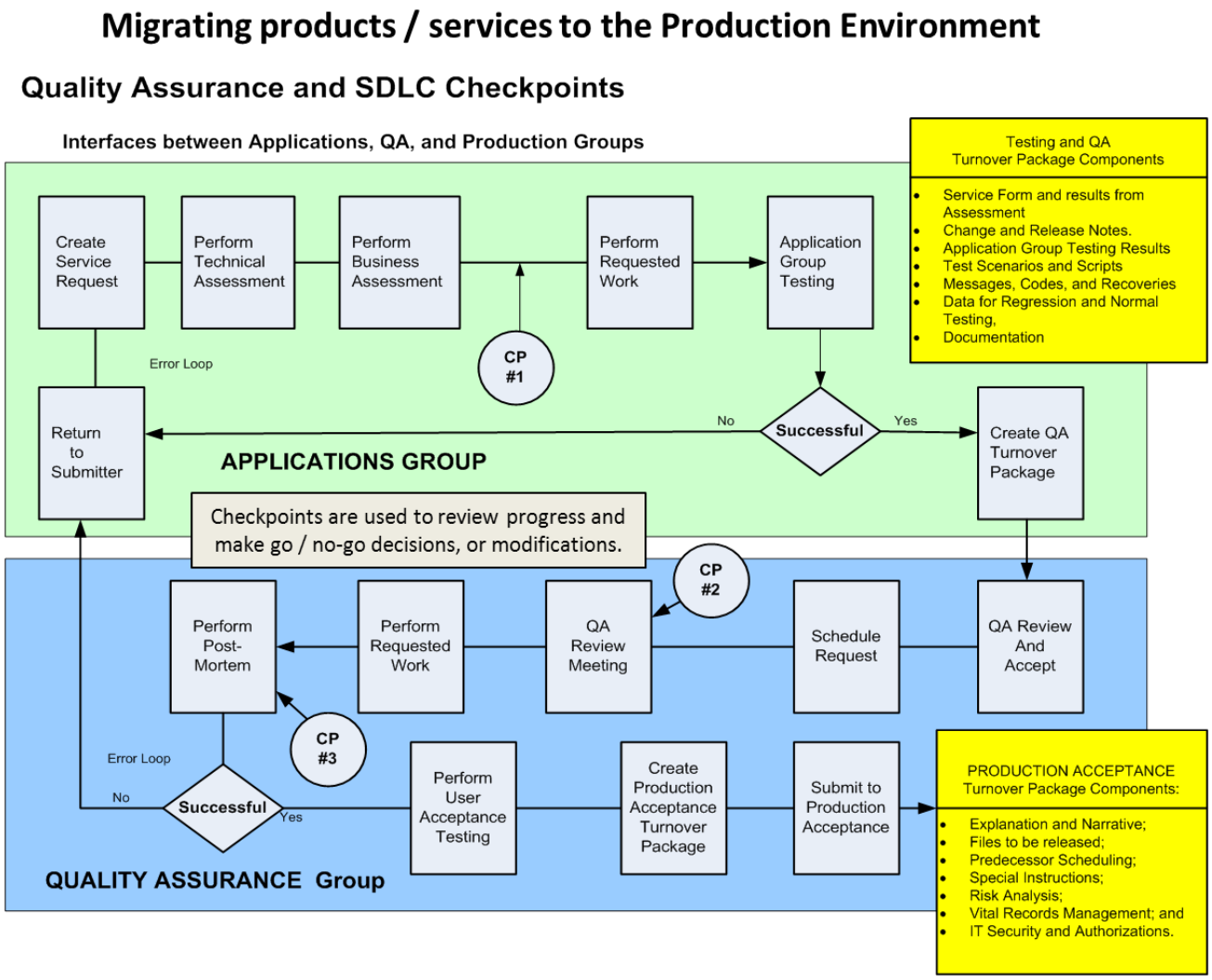
Figure 99: Systems Development Life Cycle flow



The steps followed to introduce newly developed products an services is shown above. Starting with the client making a development request, the product is developed, tested, passed by Quality Assurance, and sent to Production Acceptance where is set-up and made ready to be processed in the production environment. Once in Production, the application is monitored for errors and successful completions. Errors are identified and resolutions created that are then sent to maintenance along with client enhancements. Maintenance is performed by taking a copy of the production environment, applying the changes, and then going through testing, QA, and Production Acceptance again. This Maintenance Loop is performed on a periodic basis, with individual changes having the ability to be backed off by individually without harming other changes.

Application Migration into Production

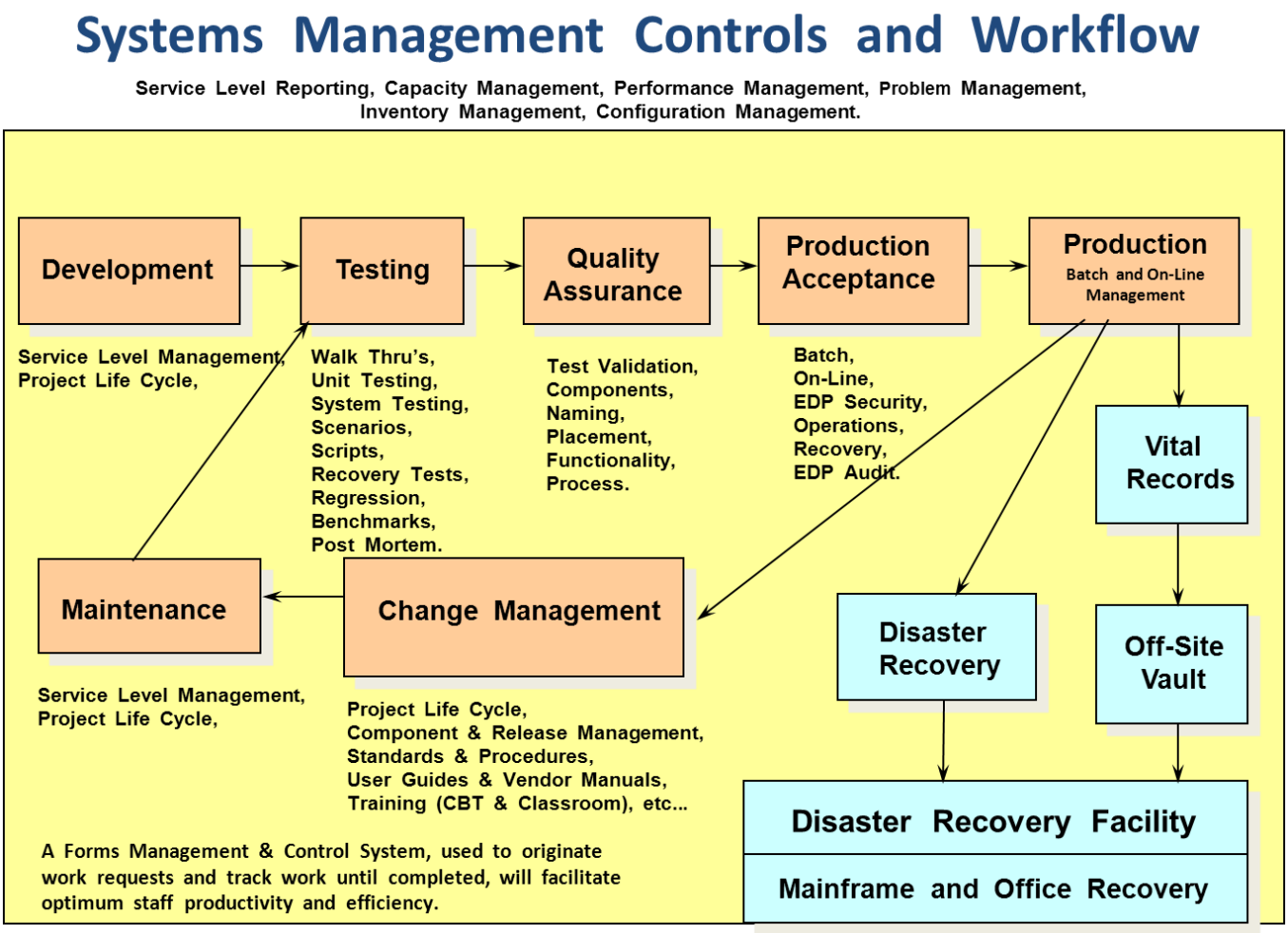
Figure 100: Application Migration Pathway to Production



Application are created in development after a decision is made to build internally or purchase. Then testing, QA, and Production Acceptance becomes envolved until the product is introduced into the production environment. Checkpoint are used to review status, make alterations, and make go / no-go decisions.

Systems Management and Controls

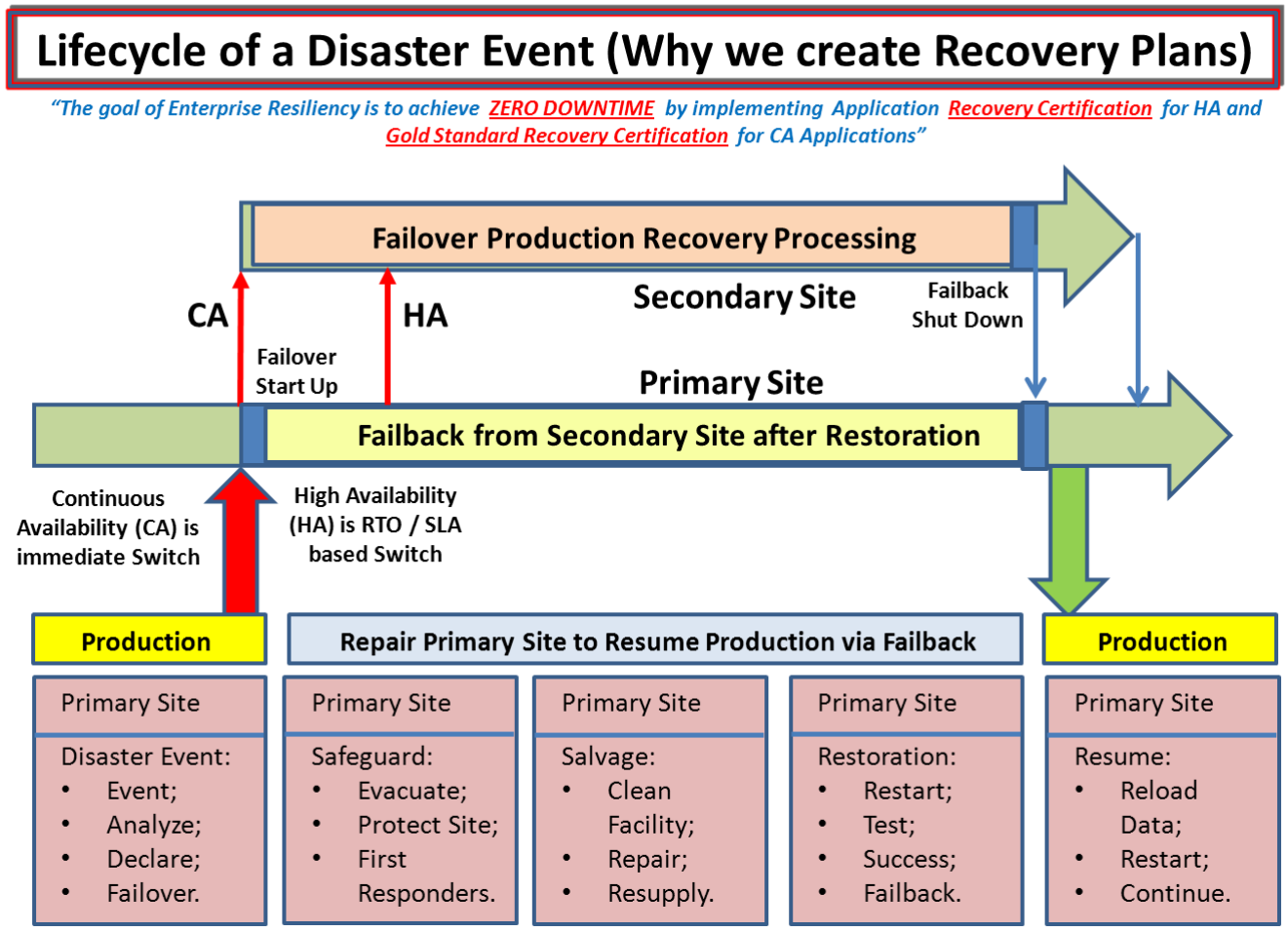
Figure 101: Systems Management and Controls overview



The functions performed in order to control systems operation and manage applications entering the production environment from Development or Maintenance is shown above.

The Disaster Life Cycle

Figure 102: The Disaster Recovery Life Cycle



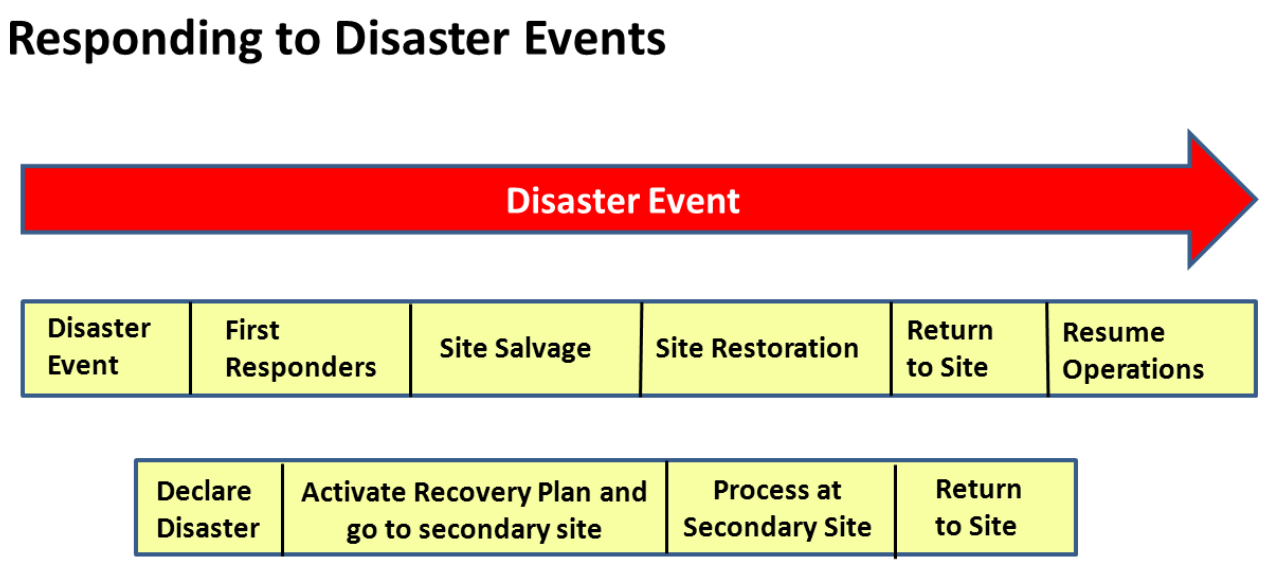
Disasters have a Life Cycle that is shown below. When a disaster event occurs, it must be recognized and acted upon appropriately. This initial action is included in a recovery plans initial problem analysis section. Once recognized, the problem is reported to management and the Help Desk. Management 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

Figure 103: Responding to Disaster Events at primary 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.

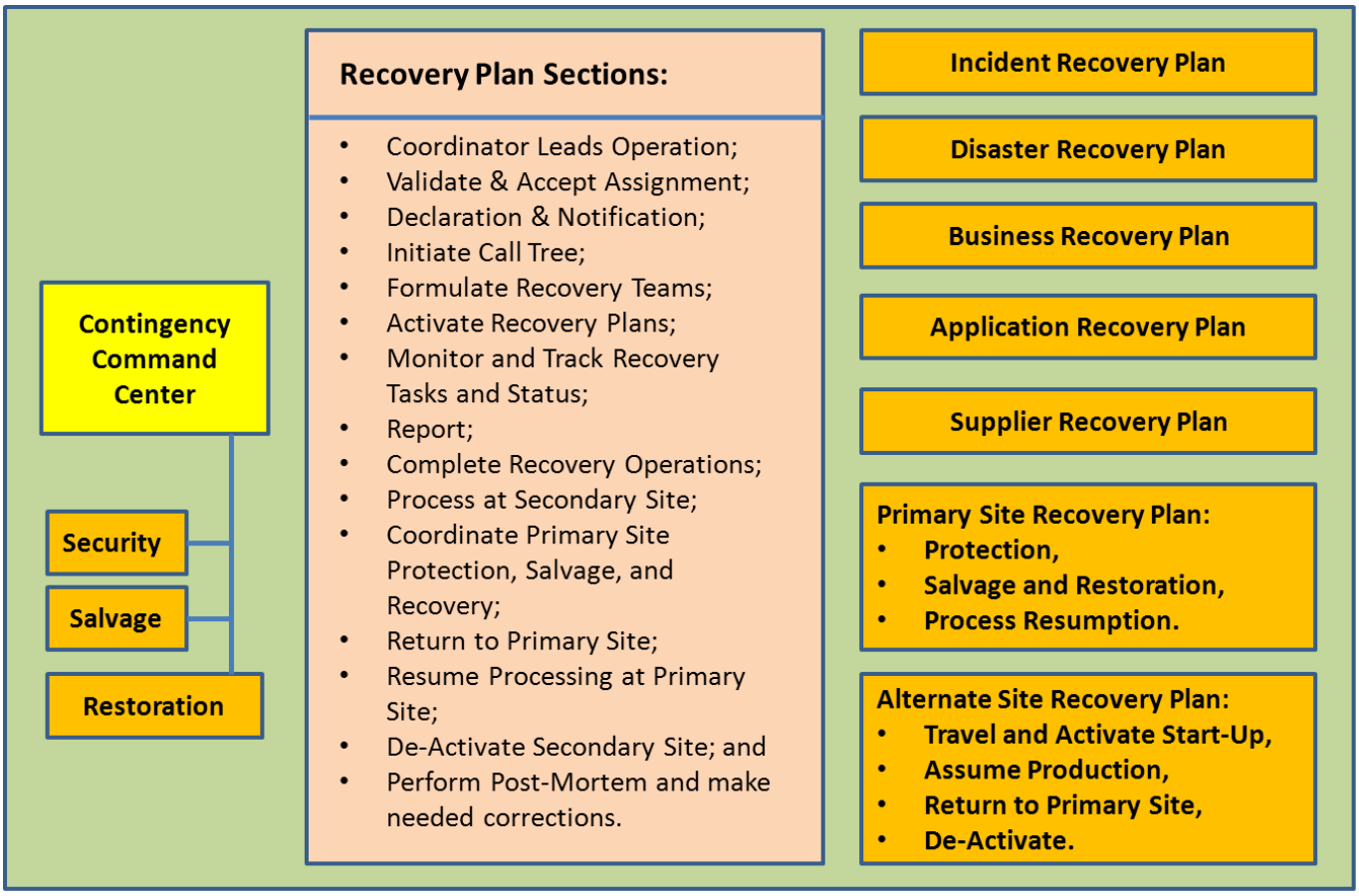
First Responders (consisting of the police, fire department, and emergency medical technicians) will perform their tasks immediately upon arrival on the scene. In some cases the building or affected area will be cordoned off which would interfere with normal business operations. You can usually be assured 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

Figure 104: Types of Recovery Plans



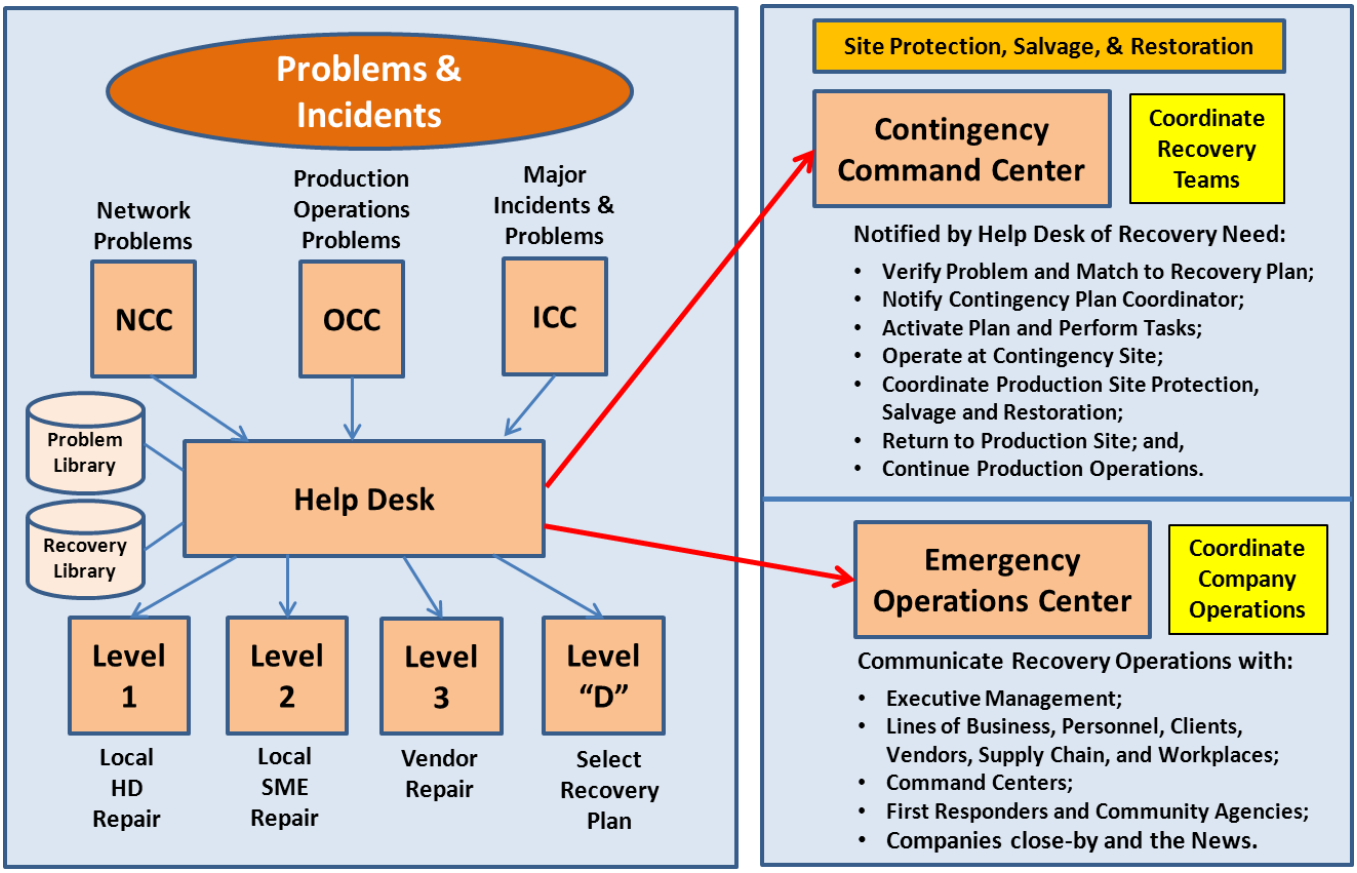
Once recovery plans are created, they must be identified, declared, and acted upon which requires interactions between end-users, command centers, and management.

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

Figure 105: Relating Disaster Events to Recovery Plans



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.

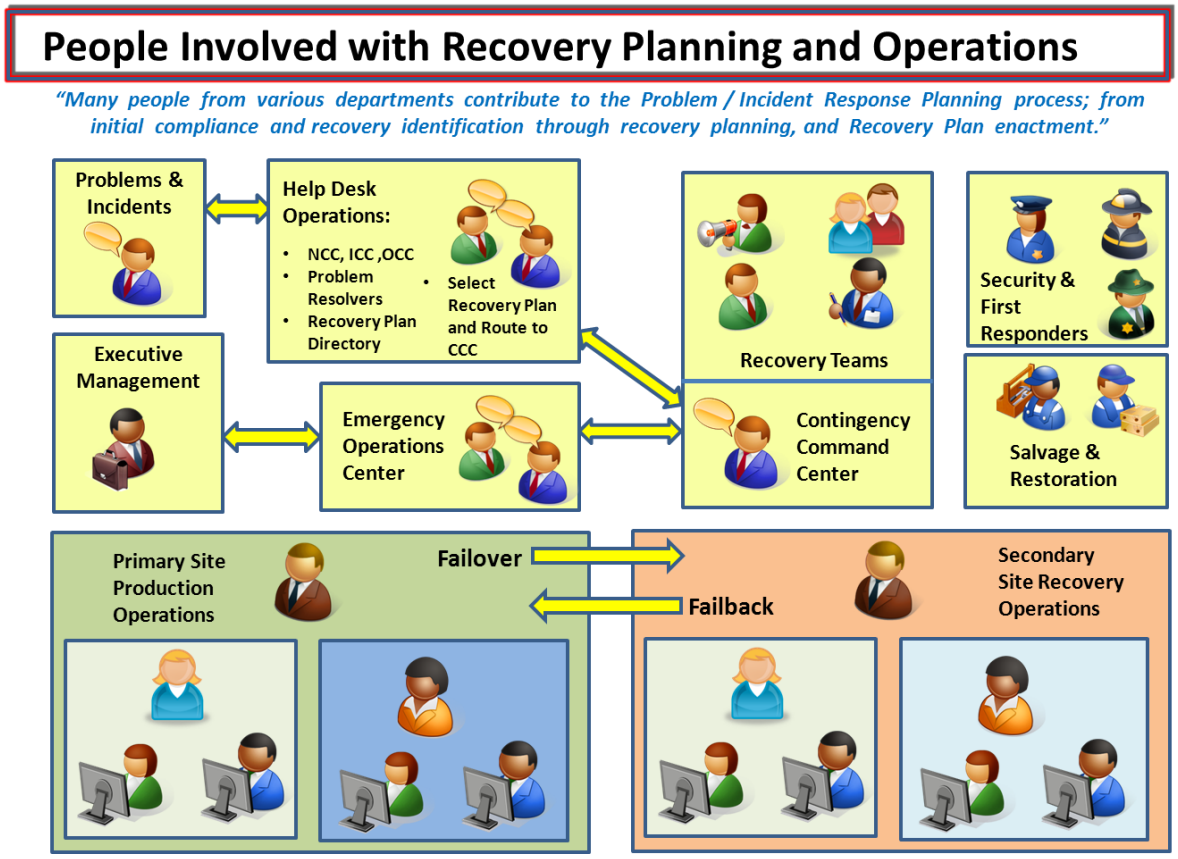
The Contingency Coordinator would activate the recovery plan and perform all tasks contained in the plan from notification through relocation to the secondary site and the resumption of production processing at the secondary site. Once the primary site has been repaired and is ready to receive personnel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

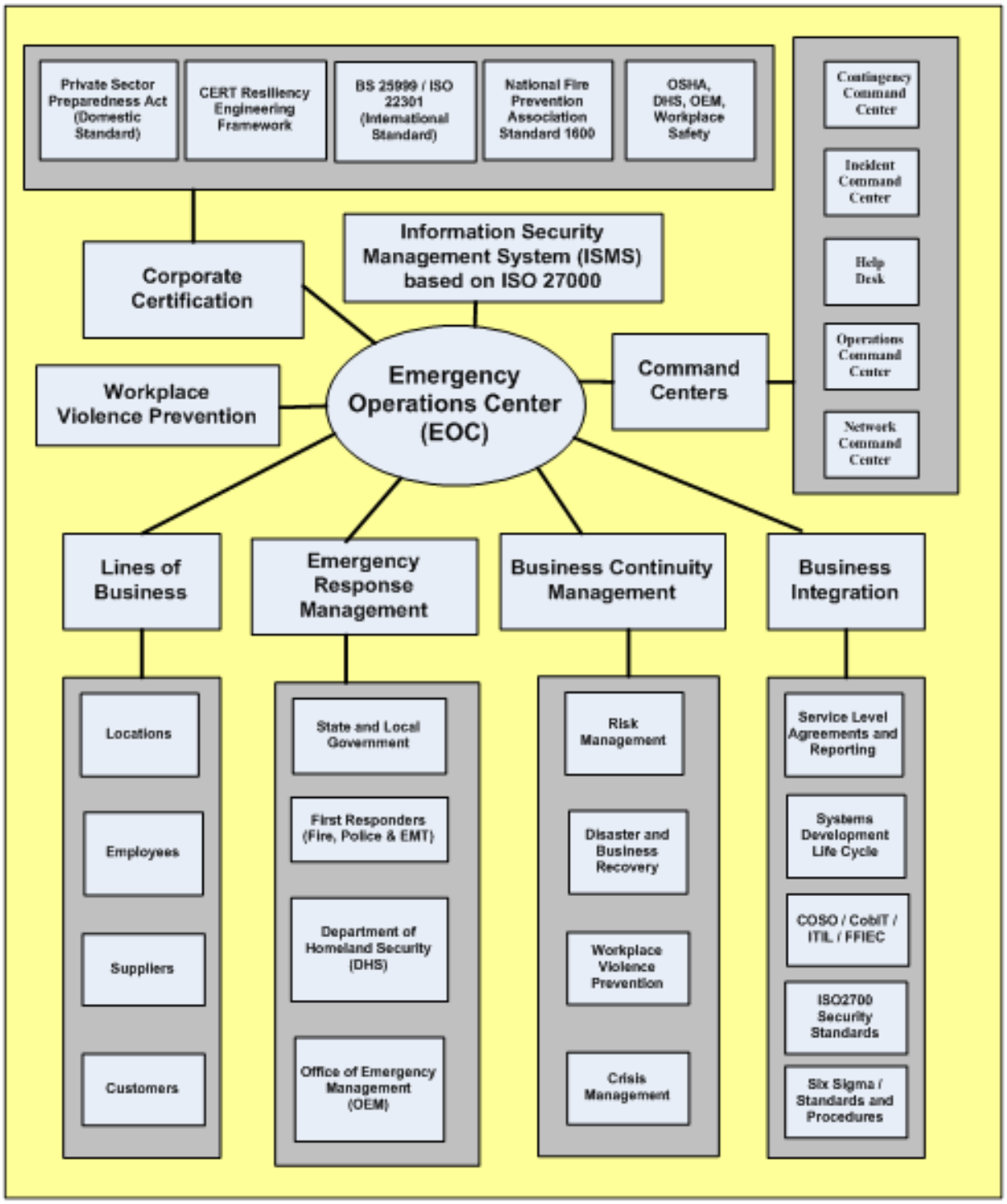
Figure 106: People envolved in Recovery Operations



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)

Figure 107: Fully integrated EOC environment (Physical Goal)



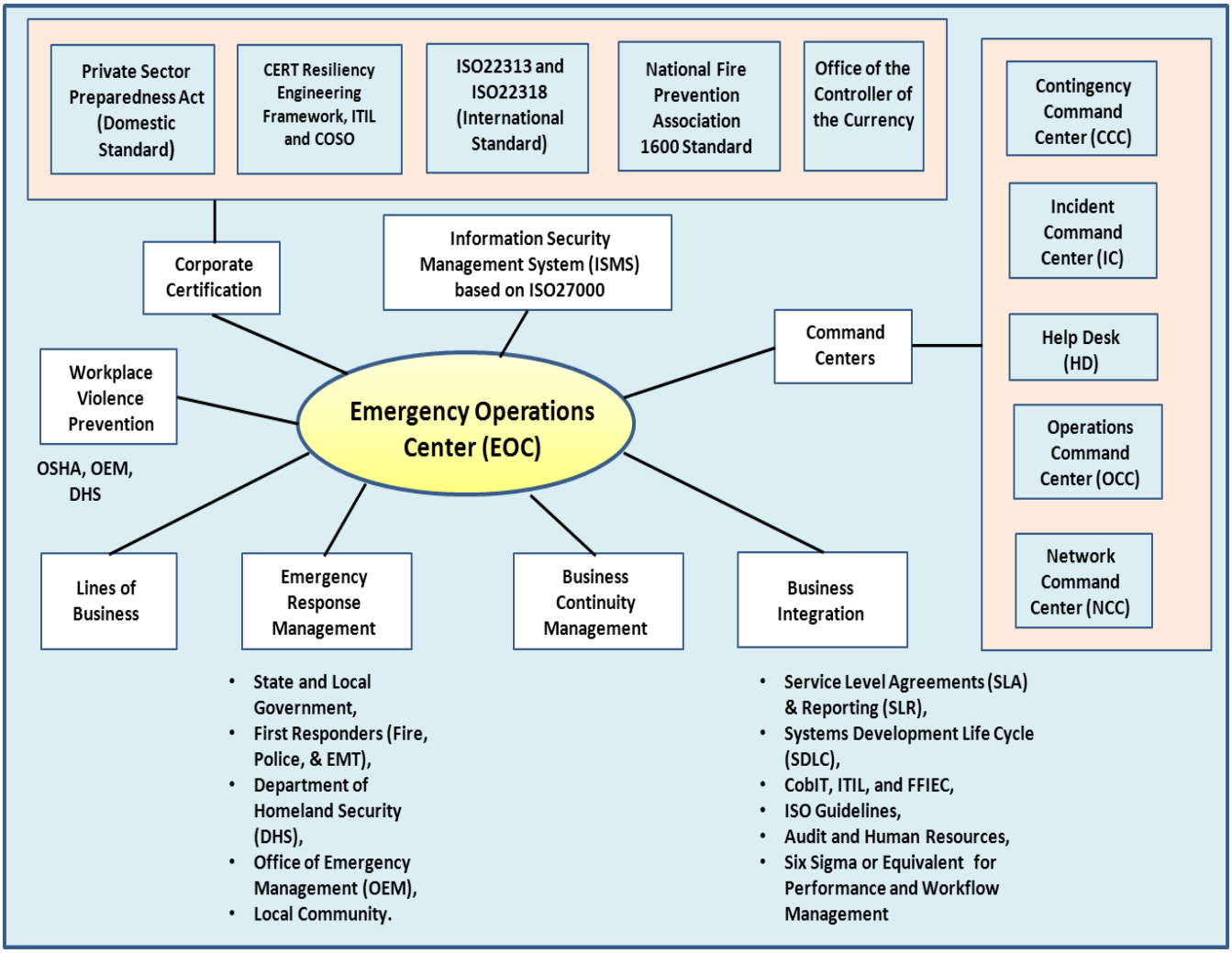
The EOC is activated when a disaster event occurs. It communicates with the Help Desk, Contingency Command Center, Business Units, and Executive Management in order to coordinate recovery operations and maintain business requirements associated with Corporate Certification and Enterprise Resiliency.

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)

Figure 108: Fully integrated EOC environment (Logical Goal)



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.

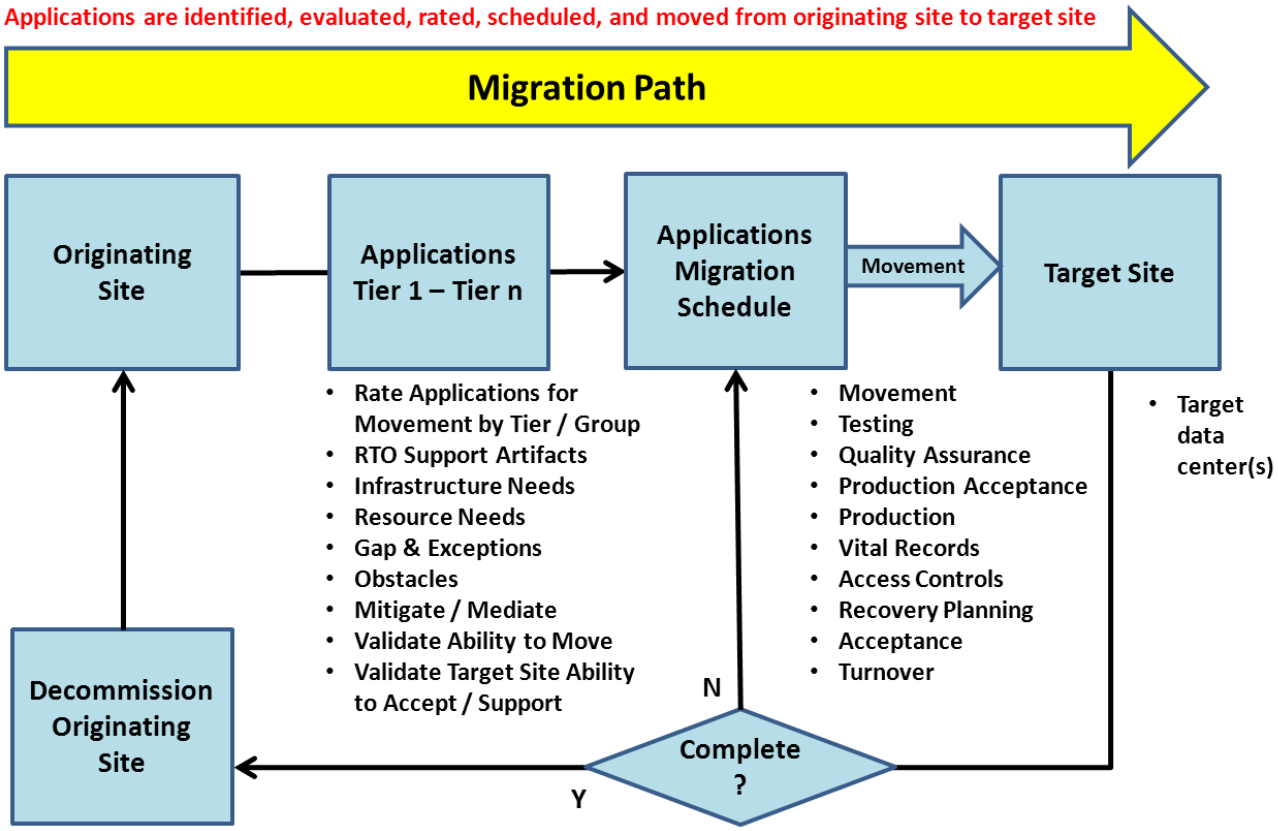
Achieving Enterprise Resiliency and Corporate Certification will allow a company to optimize production operations and enhance its reputation world-wide. It is the direction that all companies will eventually have to achieve in order to stay competitive, so why wait when you can be considered as an industry 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.

Migrating Applications between sites

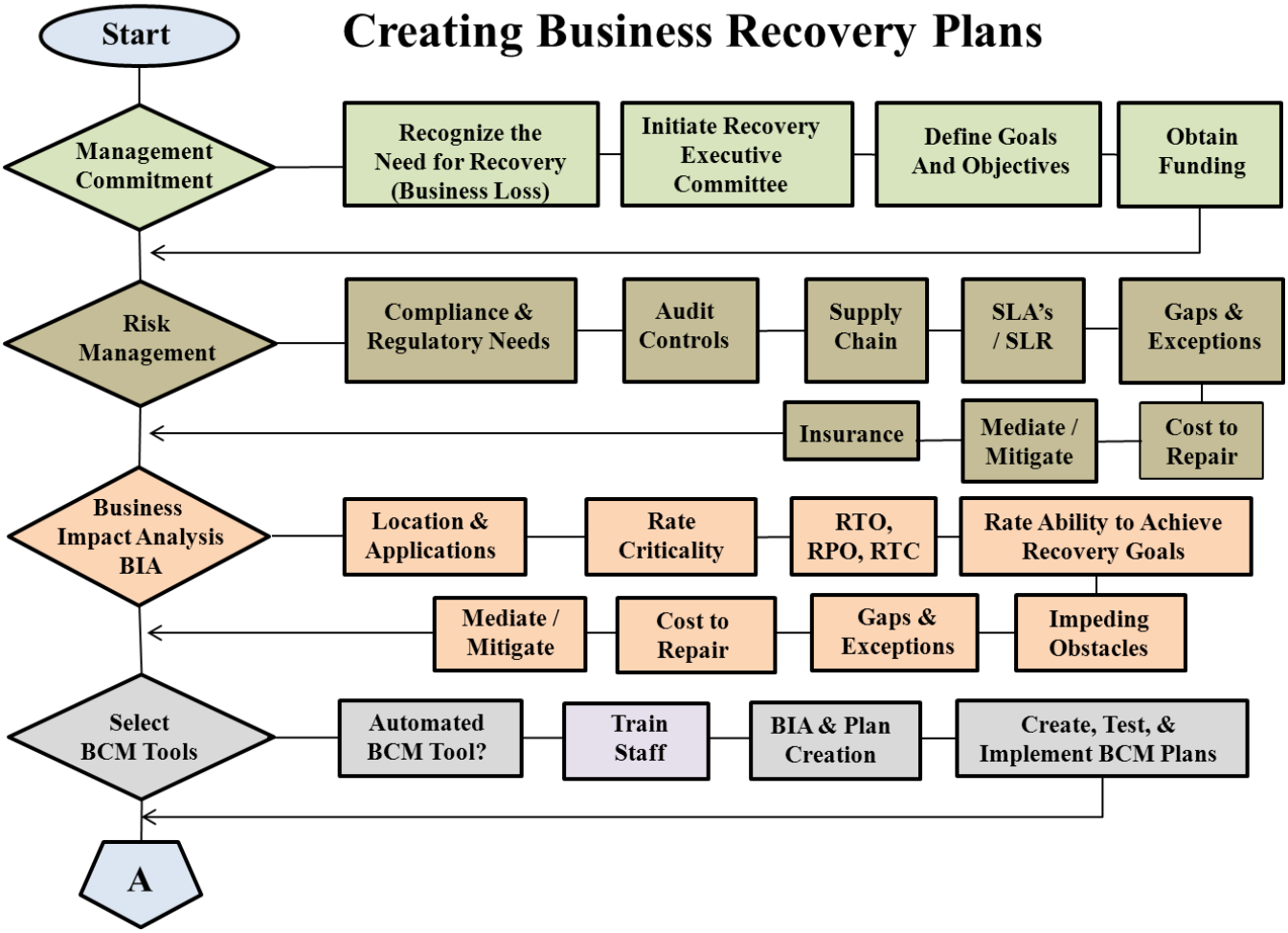
Application Migration can occur when:

- 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.

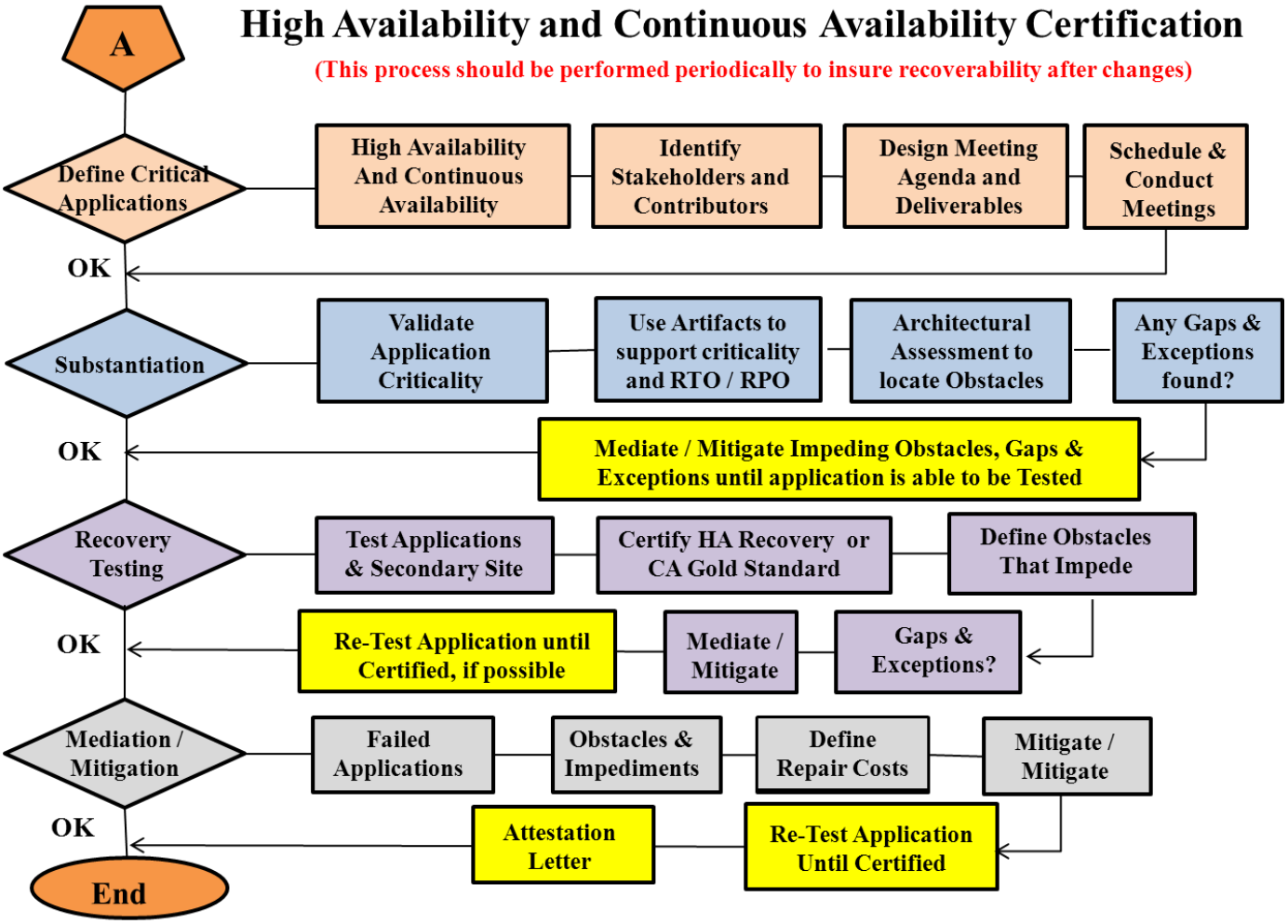
Creating Recovery Plans (Flowchart)



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)



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

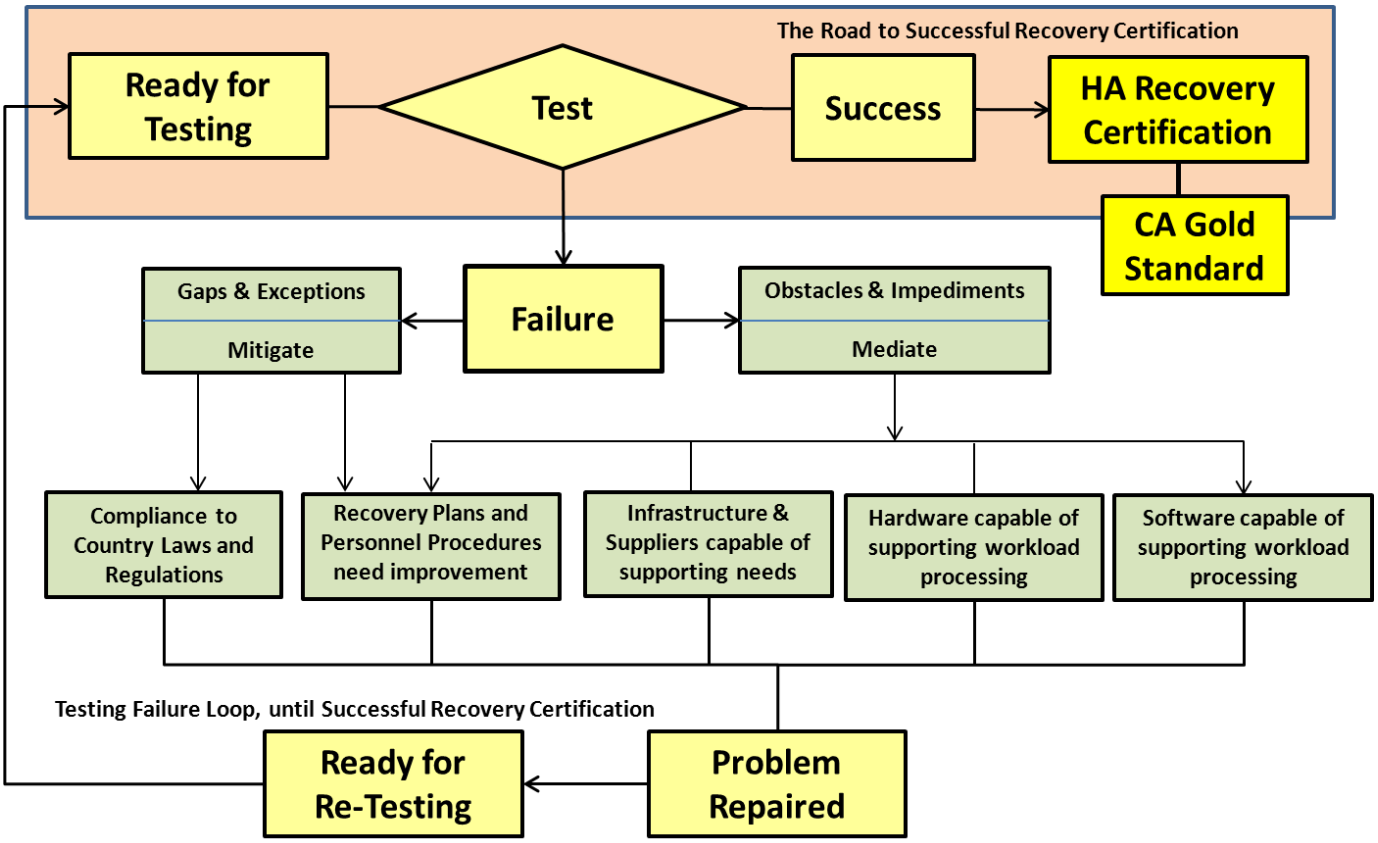
1. Identify and rate applications based on recovery criteria (Tier-1 through Tier-n, where Tier-1 is most critical and requires Continuous Availability (CA) and Gold Recovery Certification via immediate Flip / Flop recovery operations in either the primary or secondary site for prolonged times and without 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.

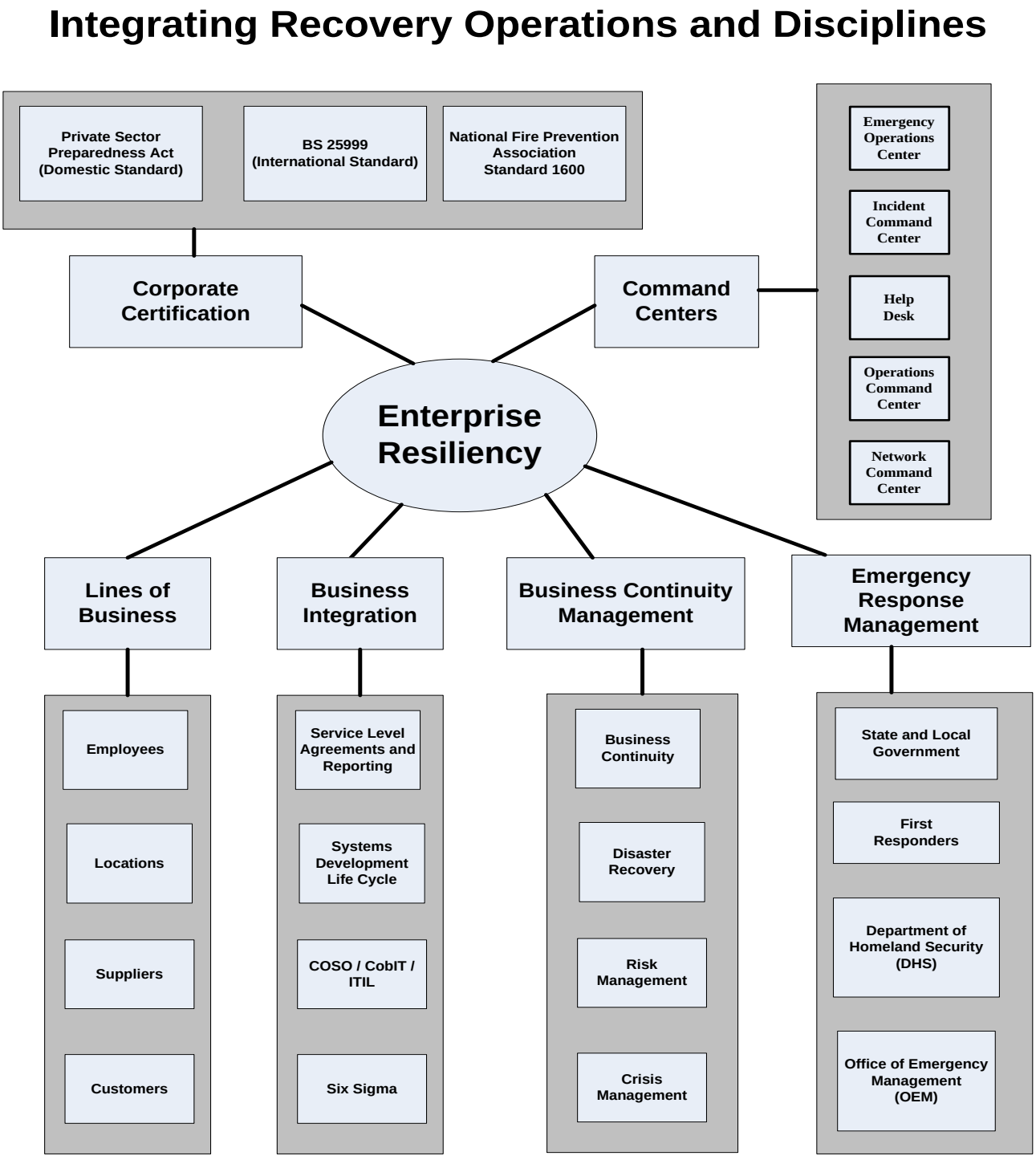


Steps include:

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.

Emergency Operations Center (EOC) overview

Figure 109 - Enterprise Resiliency and Corporate Certification



Another example of how Emergency Management and Business Continuity are integrated within a company is shown above.

Appendix B - Technology Risk Management Flow Chart

Figure 110 - Technology Risk Management (part 1)

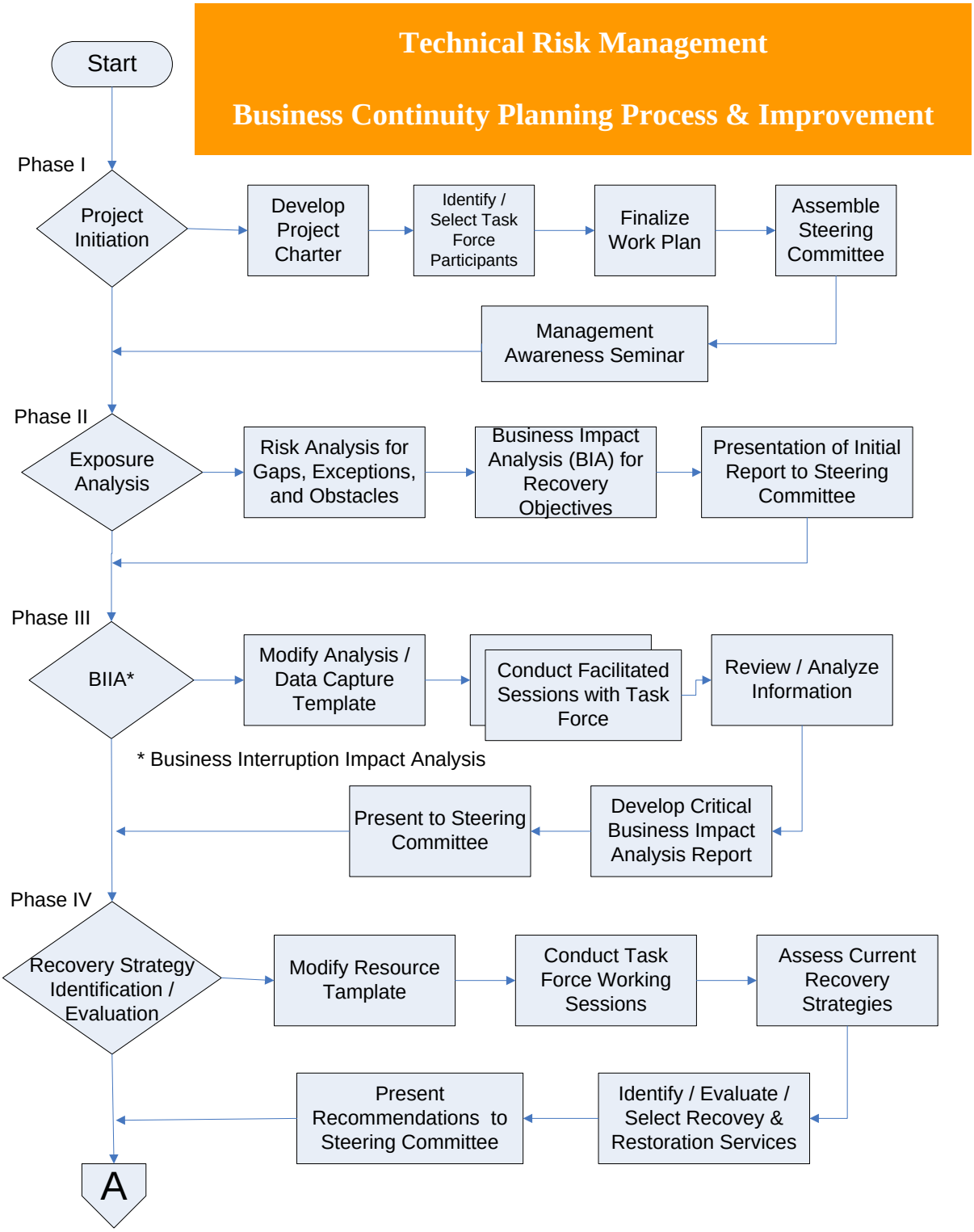
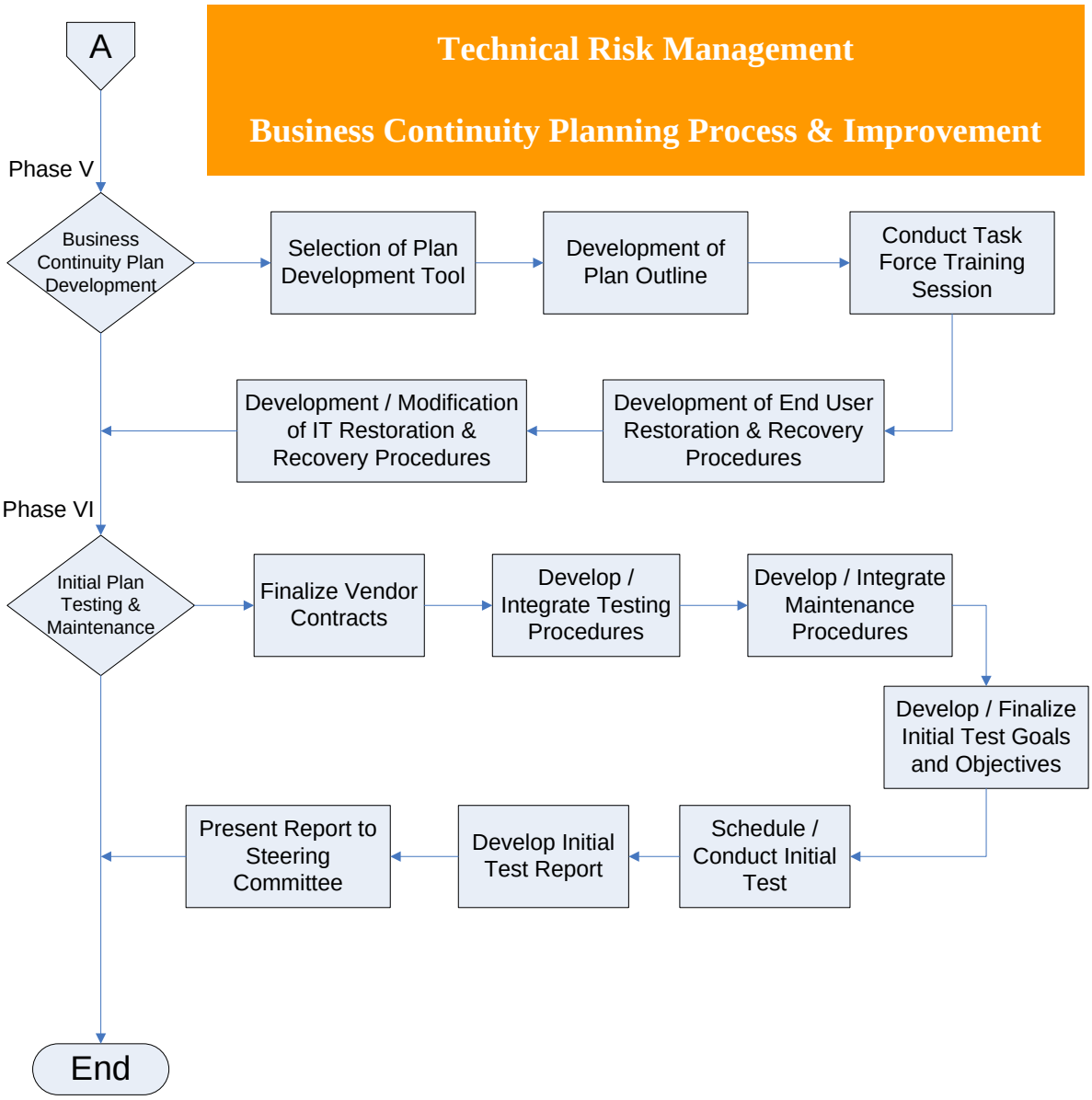


Figure 111 - Technology Risk Management (part 2)



The above flow chart is an example of how recovery operations can be implemented within a company.

Appendix C – Universe of Disruptive Threats

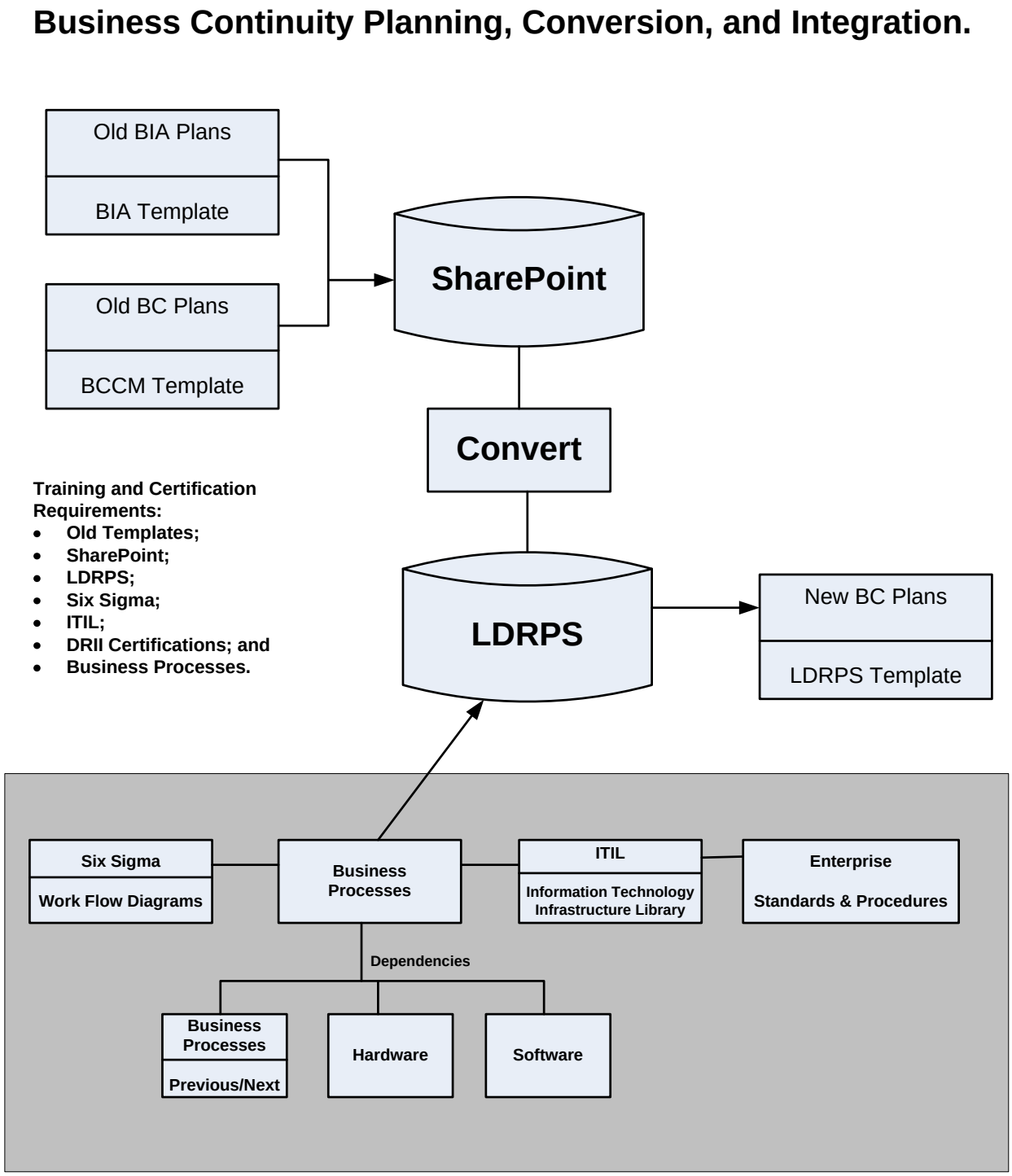
Universe of Disruptive Threat Events

Category	Disruptive Threat Events Considered for Assessment
	Note: Items in red are global threats
Natural Hazards	• Earthquake • Hurricane • Tidal Wave • Tornado • Landslide • Flood • Heat Wave • Blizzard / Ice Storm • Lightning Storm • Nor'easter • Wildfire • Pandemic • Drought • Sand Storm • Climate Change • Volcano
Accidental Hazards	• Building Fire • IT Hardware Failure • Errors / Omissions • Airplane Crash • Hazmat Release – Chemical Plant • Hazmat Release – Railroad Tank Car • Hazmat Release – Commercial Truck • Nuclear Power Plant Radiation Leak • Building Collapse • Dam Collapse • Bridge Collapse • Explosion
Intentional Acts	• Bombing • Civil Disorder • Vandalism • Arson • Bio-Terrorism • Dirty Bomb • Brute Force Attack • Embezzelment • War / Invasion • Misinformation • Cyber Attack • Electromagnetic Pulse
Utility Disruptions	• Power Utility Disruption • Telecom Utility Disruption • Water Utility Disruption • Natural Gas Disruption • Airport Closure • Railroad Service Disruption • Bus Service Disruption • Roadway Closure • Diesel / Gas Disruption • Oil Supply Disruption

Categories of threats and global influences are provided above. These threat categories should be addressed within your recovery plans.

Appendix D - BCP Conversion and Implementation

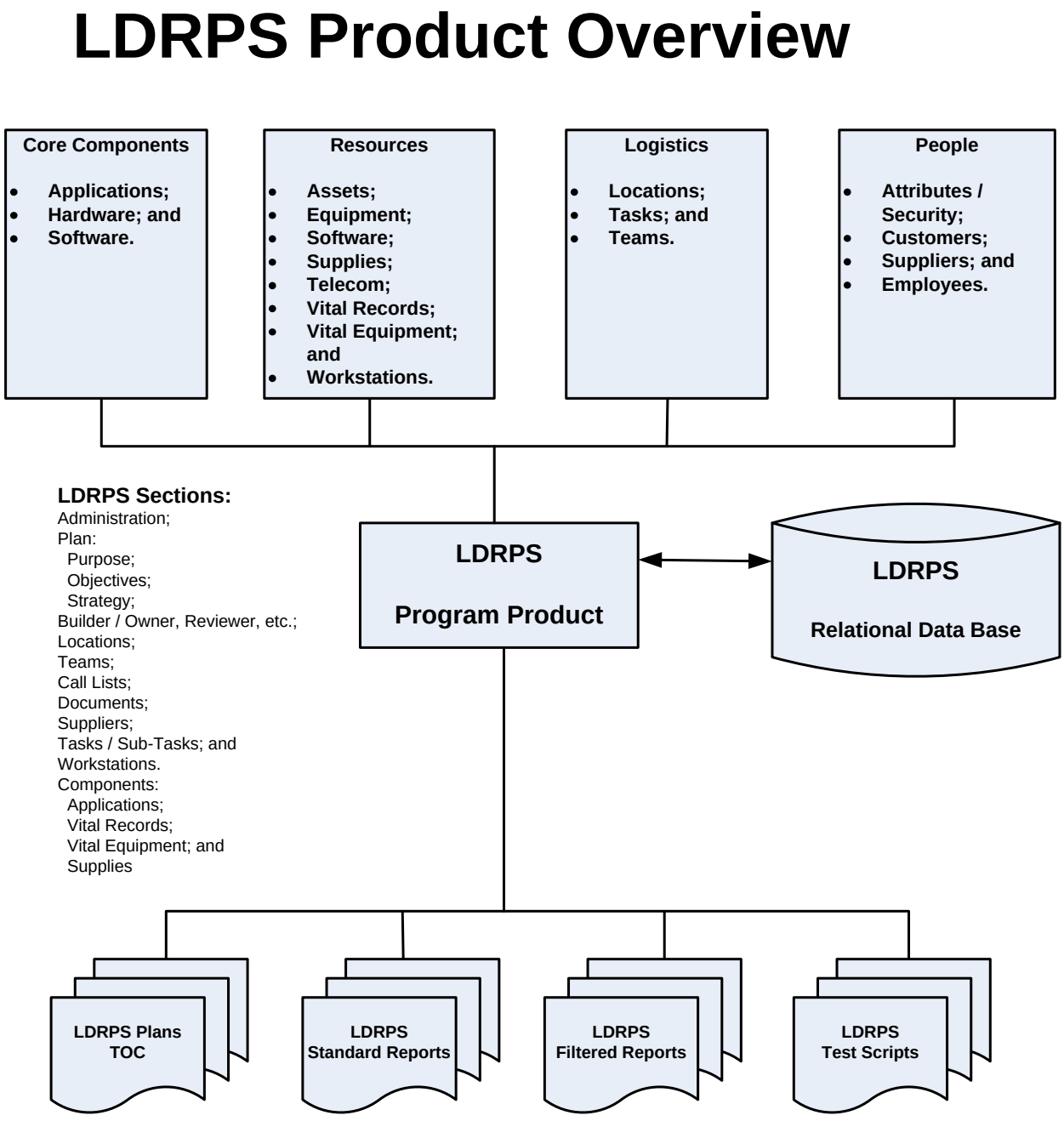
Figure 112 - BCP Conversion and Implementation



The process of converting recovery plans to the LDRPS system is shown above and an overview of the LDRPS product is shown below.

Appendix E - LDRPS Product Overview

Figure 113 - LDRPS Product overview



LDRPS Product Features:

- **Comprised of Core Components, Resources, Logistics, and People.**
- **Relational Data Base which allows for Data Mining;**
- **Web Based Enterprise capable system;**
- **Recovery Plans are based on a Table of Contents defining plan sections;**
- **Standard Reports included with program product;**
- **Filtered / Specialized Reports based on Filtered Searches (Data Mining); and**
- **Test Scripts for Plan Testing.**

Appenix F: - About the Author

THOMAS BRONACK, CBCP
DRII Certified Business Continuity Professional
Member ACP Board of Directors and Director of Vendor Relations

Possessing over 30 years of technical, managerial, sales, and consulting experience implementing safeguarded environments that comply with business/regulatory requirements and skilled in operations analysis, creating disaster recovery and business continuity plans, writing standards and procedures governing business operations and personnel accountability, adept in planning and improving the efficiency of data processing systems/services; optimizing information technology productivity through system implementation, quality improvements, and technical documentation. I have developed, migrated, and dissolved data center and their associated applications.

SELECTED ACCOMPLISHMENTS

- Formally trained by IBM on mainframe hardware and software products including a range of mainframe types and operating systems.
- Conducted IT Technology and Security Risk Assessments for a wide variety of firms.
- Implemented Business Continuity Plans for major organizations in the Banking, Brokerage, Insurance, Service and Product Vendors, Pharmaceutical, Manufacturing, and International industries.
- Sales Agent for IBM Business Recovery Services, bringing Chase, Citibank, and Salomon Brothers in as clients.
- Provided consulting and established offsite recovery facilities for clients of IBM Business Recovery Services.
- Provided offsite vaulting and professional consulting services for Zurich Depository Corporation clients.
- Merged ADP Proxy and IECA into new $9.3 million facility, while consulting to Brokerage Division President.
- Implemented a Communications Management Controller for the EAB Mainframe environment that provided automated load balancing and recovery, like VMware does today for server level products.
- Created Five Year Business Plan for IT Division of European America Bank.
- Implemented Network Control Center, Operations Control Center, Help Desk, and Contingency Command Center.
- Developed and presented educational classes on Business Continuity and general Information Technology topics.
- Provided presentations and workshops to major industry groups like IFSA, ISACA, ISSA, ACP, and CPE.
- Implemented, supported and maintained Recovery Plans for Banks, Brokerage Firms, Pharmaceutical Firms, Manufacturing Companies, and other types of firms.

Education

- A.A.S., Electrical Technology, New York City Community College;
- B.S. Coursework, Computer Science, City University of New York;
- Certificates in Systems Programming and Project Management from IBM;
- Certified Business Continuity Professional from Disaster Recovery Institute International;
- Member of the New York Contingency Planning Exchange (CPE) and Association of Contingency Planners (ACP).

Contact Information:

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