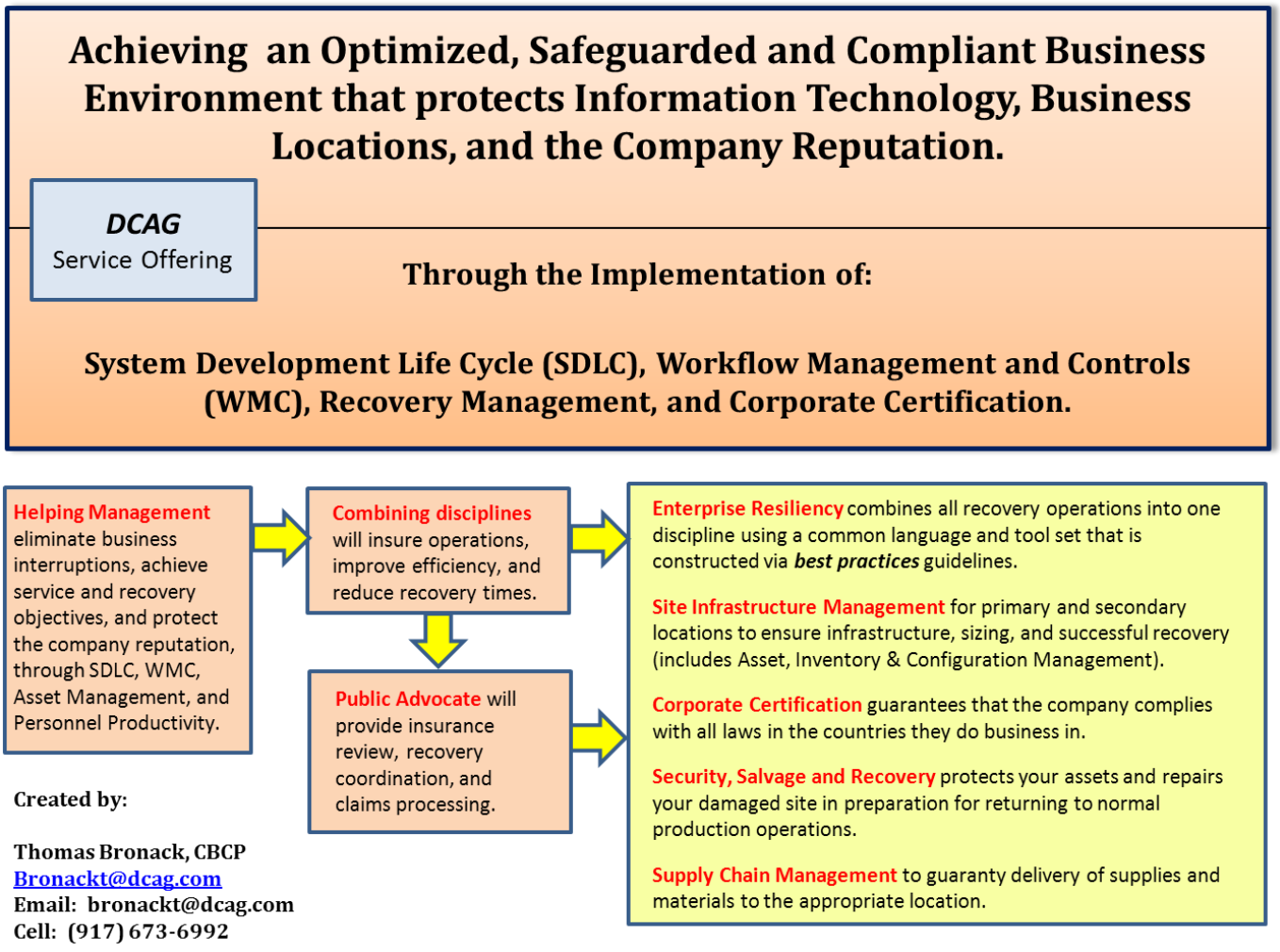


The following article was created to explain how a company can achieve more effective recovery and compliance through Enterprise Resiliency and Corporate Certification. It is intended to provide a solid foundation upon which your company can produce an optimized, safeguarded, and compliant environment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

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

Table of Contents:

Table of Figures

The purpose of this paper

Management is responsible for achieving their assigned business goals and for providing uninterrupted operations even if a disaster event occurs. Failure to achieve these goals 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 addresses the many operational, recovery, and compliance concerns and responsibilities that management must be aware of and respond to - as shown below:

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 (Gaps, Exceptions, and Obstacles).
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 an Infrastructure and 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 complied with for the countries that the company does business in.
11. Develop an Organizational Structure that will perform all functions associated with Infrastructure Management, 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 Usage 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 all the countries where you do business.
17. Integrate procedures associated with business operations, audit, and recovery within the everyday functions performed by personnel, and have documentation requirements validated during the Quality Assurance process to guaranty Version and Release Management practices have been followed.
18. Develop methods for identifying and Mitigating Audit Gaps, Exceptions, while Mediating Obstacles that impede operations and compliance.
19. Implement compliance reporting, including mitigation of encountered gaps and exceptions, and mediation of any uncovered obstacle that would impede production or recovery operations.
20. Continue to monitor and improve operations going forward.

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 * number of clients * 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 very 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.

Figure 1: Objectives Management must achieve

Objectives to be achieved, include:

- **Safeguarded and Optimized IT and Business Environments 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).**

Should an outage occur, whose potential had previously been reported, then the company, Executive Management, and clients are 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, 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 events while complying with the laws and regulations of the countries your company does business in." The purpose of this document is to show you an approach that will help you achieve that goal, including:

- Both safeguard and optimize the Business and IT environments against outages or performance degradations.

- Utilize industry accepted "Best Practices" for analyzing and improving operations.
- Integrate improvements within the everyday functions provided by the staff.
- Fully document all standards and procedures and train staff.
- Include and update clients and the community on improvements and obtain their feedback.
- Ensure client recovery time and performance objectives are continuously met.

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 objectives? What guarantees 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 resolution of encountered problem? Has the Messages & Codes been tested? Do you have Standards and Procedures documenting on 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 following this path 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. This will lead to a win-win-win situation – 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 and Business Impact Analysis can 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 optimization of services. 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, product processed, supported, maintained, and changed in accordance to Version and Release Management concepts. Following this direction will insure that supportive documentation is included and related to any changes so that a high degree of confidence will be achieved in the instructions and guidelines provided.

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 created), **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, protecting the bottom line 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.
- The EOC is sometimes called a **"War Room"** since all of the personnel needed to identify and rate encountered problems are present so that rapid evaluations and responses can be planned and acted upon and the best protection can be provided to the business and its clients.
- **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 III** 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 Recovery 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, CCC and EOC as necessary.
- **Operations Control Center** (OCC) is responsible for monitoring business processing and the status of jobs, services, and products utilizing information technology resources. They will respond to application operator requests (WTOR – Write to Operator with Request command), perform supportive services like tape mounts etc., identify errors and respond to them, and coordinate with the Help Desk, CCC, and EOC as necessary.
- **Incident Command Center (ICC)** is responsible for responding to incidents (which are not the same as a problem and cannot always 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 the 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 / CERT (for Risk Assessment), CobIT (for integrating Information Technology with the Business Operations), and ITIL (for Service Delivery and Support) 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 recovery time and 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.

Figure 2: Protecting your environment

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

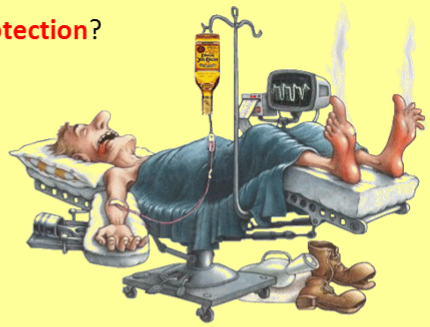
Achieving the above goals will lead to a more efficient operation and a happier staff and client base. The company reputation will be enhanced through these efforts, which will make it easier to retain and recruit new business and personnel.

Why Recovery Management should be accomplished by experts

Figure 3: Recovery Management is difficult 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 for HA, provide Flip / Flop operations for CA, 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), ISO 24762 (Guidelines), and ISO 27301 (Technical Procedures)?
- 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 HA (2 hours – 72 hours) or Continuous Availability CA (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 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.

Recovery Management Objectives include:

Figure 4: Recovery Management possible achievements

- **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 achieved 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 5: Objectives to be achieved

Service Offering Objective **("protecting a Chick in an Alligator Nest")**

- **Help management protect their business and reputation;**
- **Provide a single source to help fulfill / manage recovery and insurance needs;**
- **Review existing recovery and insurance profile;**

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

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.

Explaining 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.

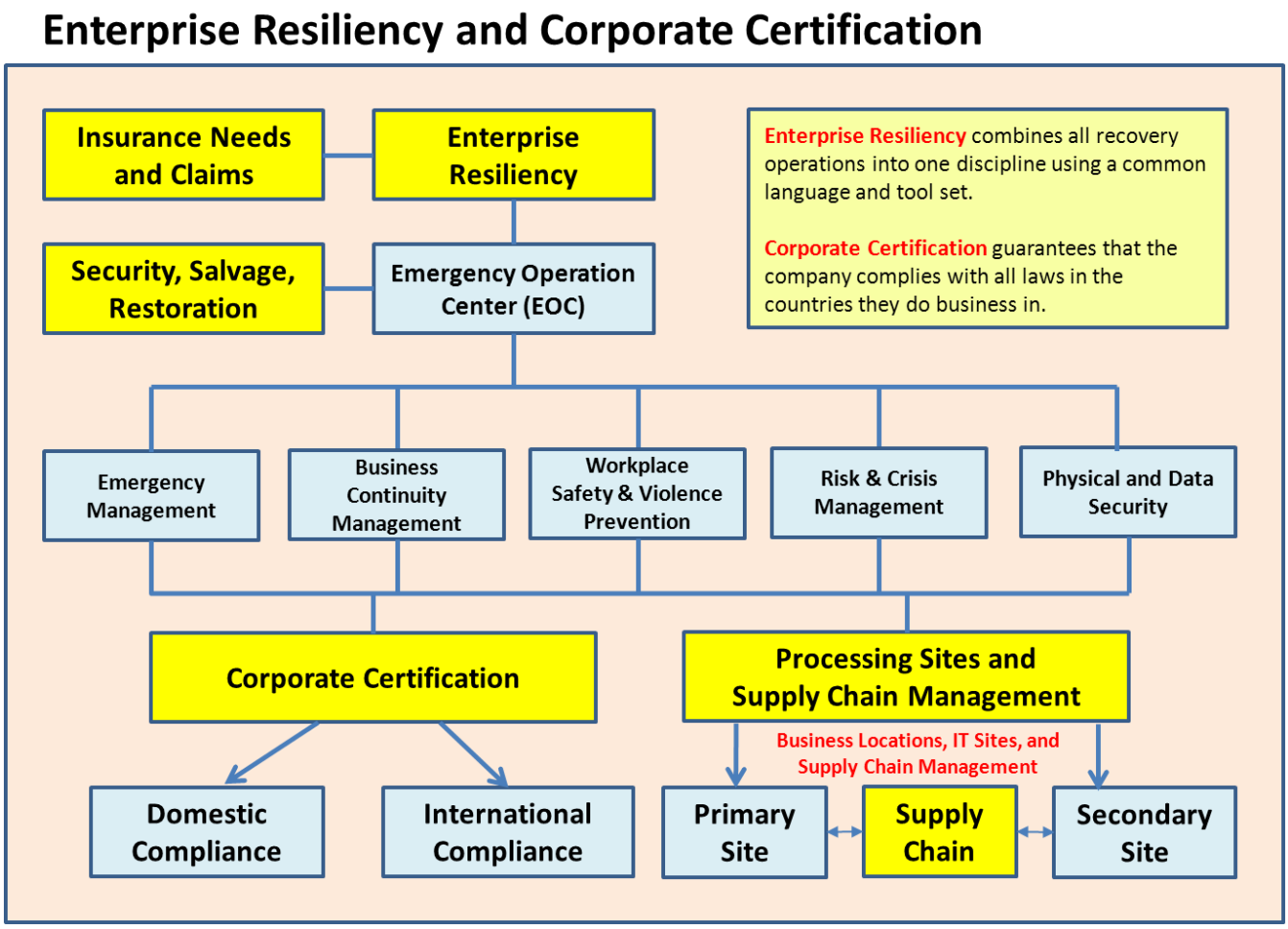
A company can be sanctioned for failing to meet recovery and security objectives, but it could also suffer a loss of reputation that would harm them in the public's eyes and result in a loss of trust and business, sometimes so great that the company would never recover if a disaster event interrupts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

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 an 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.

Figure 6: Enterprise Resiliency and Corporate Certification includes



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

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

Insurance covering management and an interruption to business must be obtained so that outages can be resolved without interrupting the profit or any new line of business. It is important to have a public advocate assist you in reviewing your insurance needs and obtaining the appropriate level of insurance best suited to protecting your business. Public advocates will also assist you in time of disaster by formulating recovery

strategies, hiring companies to provide recovery services, and submitting claims for work that had to be performed to resolve the disaster event.

Site Security, Salvage, and Restoration, must be achieved when a disaster event results in First Responders being called (i.e., Fire, Flood, Workplace Violence, etc.) and the loss of access to the site for a prolonged period of time due to police action, or damage due to resolution of a disaster event by the First Responders. **Site Security and Protection** must be provided to protect company assets and company security personnel should coordinate site protection with the First Responders until they have completed their work. Then company security personnel must protect the site through Salvage and Restoration until the site has been re-occupied by normal personnel after the disaster event and the site is fully functional again. **Salvage** is responsible for cleaning the site and removing any damaged articles. Salvage also removes water and mold damage, recovers paper items, and makes the work place safe for occupation again. **Restoration** is responsible for repairing, or replacing, damaged equipment and facilities. Restoration also helps recover the facility and the supplies needed to perform normal operations again.

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).

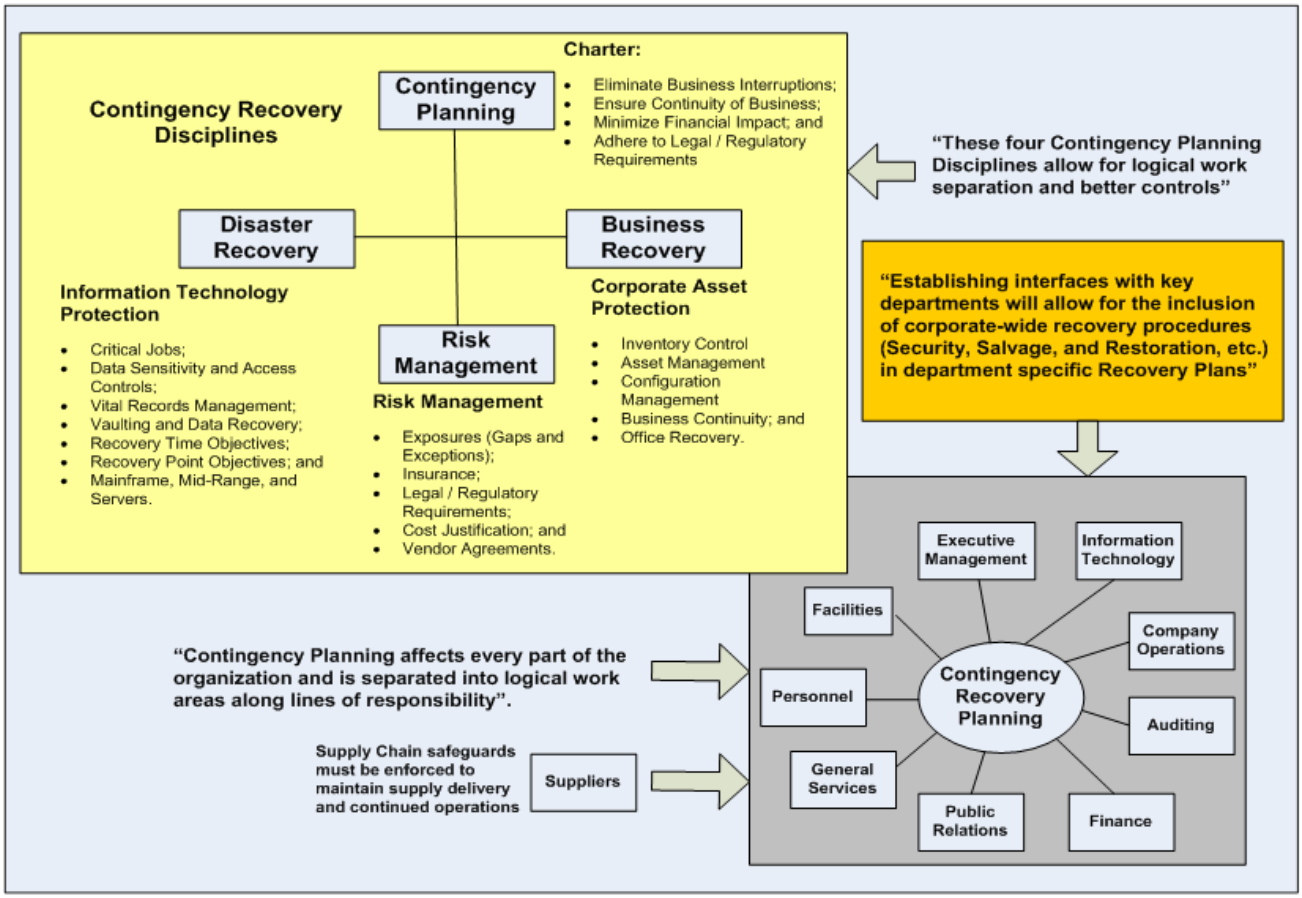
The disciplines included in Enterprise Resiliency and Corporate Certification are shown above, but how you get to that structure requires many people combining their knowledge of the business, its products and services, its clients, and the procedures needed to more efficiently support and maintain clients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

Communications with government agencies and First Responders must be accomplished before a disaster event occurs, so that their knowledge base and requirements can be included in any recovery plan that the company develops. Coordinating recovery planning with the general community is essential as well, so that a disaster event within a single company does not interfere with normal operations of companies that may be sharing facilities (like a building or corporate business park). Being a good neighbor is an essential part of recovery planning and will go a long way to protect personnel, business operations, and the reputation of the company. A lot can be gained through shared community information that will help a company protect its assets and comply with community standards of excellence.

How to integrate Business Continuity Management within the organization

Figure 7: Recovery Charter, Disciplines, and personnel



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 achieve Recovery Management and Enterprise Resiliency

Figure 8: Steps leading to Recovery Management and Enterprise Resilience

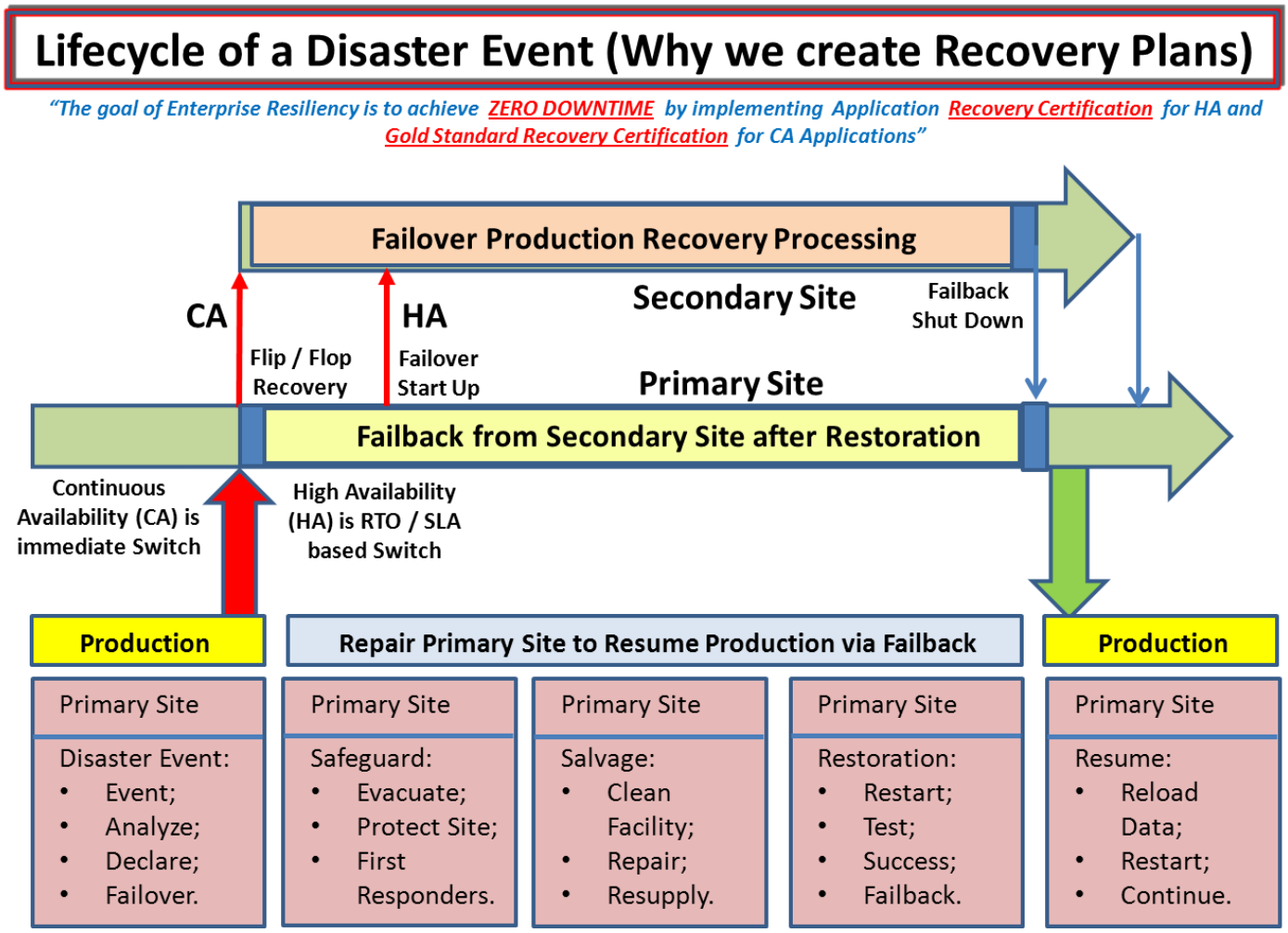
- **Formulate Recovery Management Charter, including:**
  - Charter, Mission Statement, Business Plan;
  - Project Plan, Goals and Objectives, Functional Requirements and Skills, Task Descriptions, Timeline;
  - Management Support, Funding, and Announcement.
- **Project Plan, Organization Structure,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

The above illustration demonstrates the direction to take in order to achieve the goals of Recovery Management and Enterprise Resiliency. Recovery Management is concerned with the restoration of business operations as shown in the Charter statement, 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 cohesive unit following the same culture 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 achieved and maintained.

Lifecycle of a Disaster Event

Figure 9: Lifecycle of a Disaster Event



A disaster event can be plotted from the above illustration. It shows when a disaster event occurs, the ability to instantly flip / flop Continuously Available (CA) applications from a primary site to a secondary site, or Failover / Failback High Availability (HA) applications within a 2 – 72 hour time frame. After transfer to the recovery facility, the primary facility must be made ready for return through protection, salvage, and restoration operations. When completed and the disaster event is over, the staff and applications can return to the normal site to continue processing as before the disaster event.

It is necessary to be able to use current data when processing, so data synchronization must be accomplished for both CA and HA Applications. Today's data synchronization techniques can support this requirement, along with the use of a hosted cloud facility that is maintained at either a public or private site.

After switching locations, data must be synchronized instantly via Continuous Data Protection, or Incrementally via Data Protection (last vital record backup) with a Forward Restore of Data from the last checkpoint or backup copy.

Creating a Business Plan

Figure 10: Charter and Mission Statement

Charter and Mission Statement

1. Achieve "**Enterprise Resilience"** to optimize recovery operations;
2. Insure **"Corporate Certification"** in countries where you do business*;*
3. Adhere to Service Level Agreements (**SLA / SLR**) and Client Performance Contracts (Time and Service based);
4. Guaranty **Data Security and Recovery (RTO / RPO)** objectives;
5. **Protect Personnel** through Physical Security and a Workplace Safety;
6. Utilize **"Best Practices"** to achieve goals;
7. Achieve "**Zero Downtime**" through "**Certified Recovery"** via Failover / Failback for HA (High Availability) applications and Flip / Flop for "**Gold Standard Certification"** of CA (Continuous Availability) applications;
8. **Integrate Enterprise Resiliency and Corporate Certification World-Wide;**
9. **Update Documentation** and adhere to **Version and Release Management;**
10. Provide **educational awareness and training** programs; and,
11. Provide ongoing **Support and Maintenance** going forward.

It is necessary to create a Business Plan to accompany the creation of an "Enterprise Resiliency and Corporate Certification Organization" because it affects everybody associated with the company from employees to clients and the community. This plan would define:

- Mission Statement;
- Charter;
- Scope;
- Objectives and Goals;
- Resource Requirements;
- Deliverables and their Dependencies;
- Costs and Time Frame;
- Validating Results;
- Roll-Out of services and products;
- Support and Maintenance; and
- Version and Release Management.

The Business Plan would establish a direction to follow and allocate people, resources, and funding to implement and maintain the new environment going forward and allow for growth in accordance with support of new business and technology improvements.

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 11: 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.

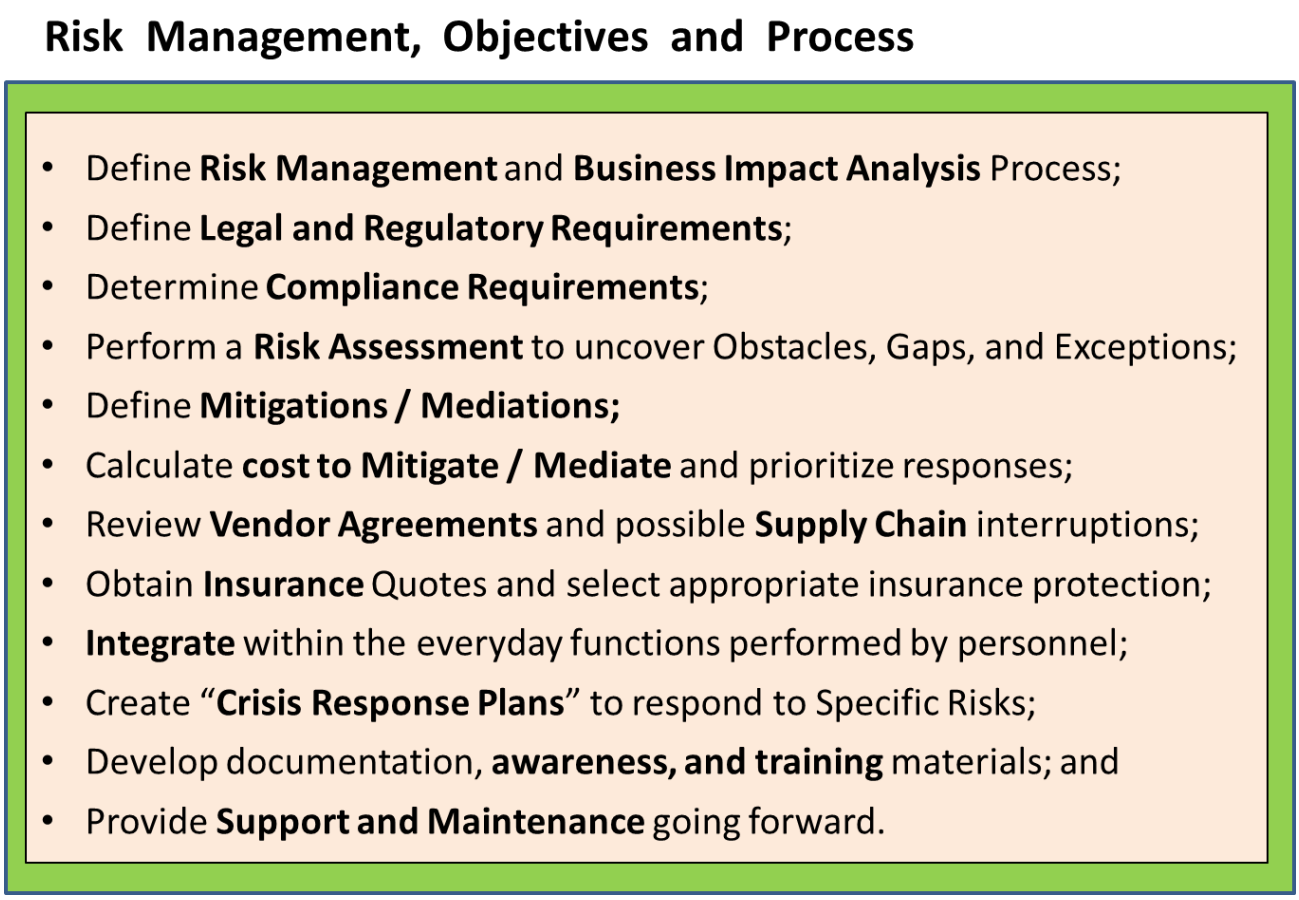
The guidelines formulated through this process will require input from all recovery management disciplines so that the best results can be achieved through their combined knowledge and experience. **Emergency Management** personnel would help define methods for protecting the Workplace, **Disaster Recovery** 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 12: Risk Management objectives and process



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".

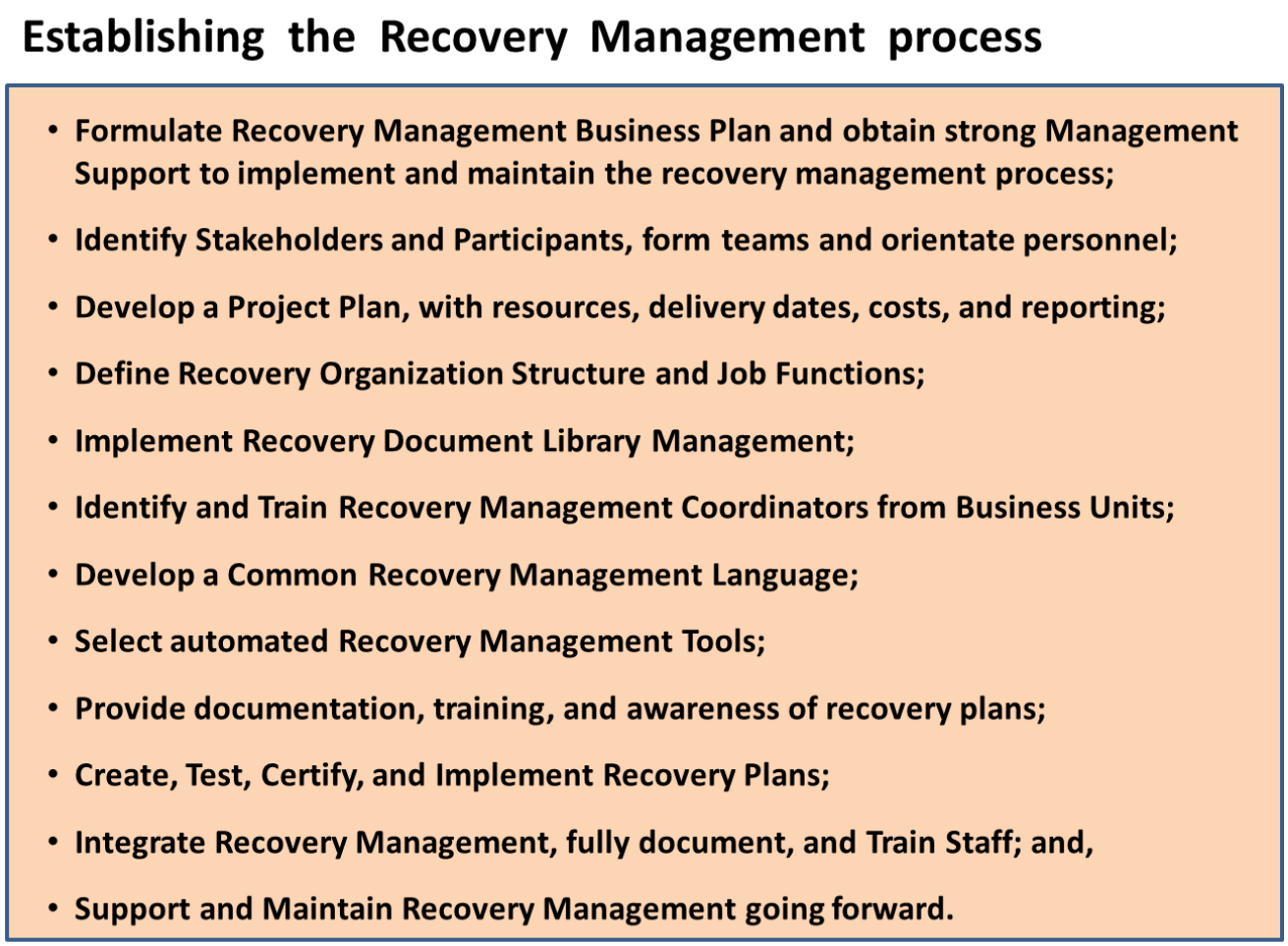
Once identified impediments and obstacles are rated as to their relative cost and likelihood of occurrence and reported to management, where a decision is made to either repair the problem or seek insurance to protect against the occurrence.

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

Figure 13: 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.

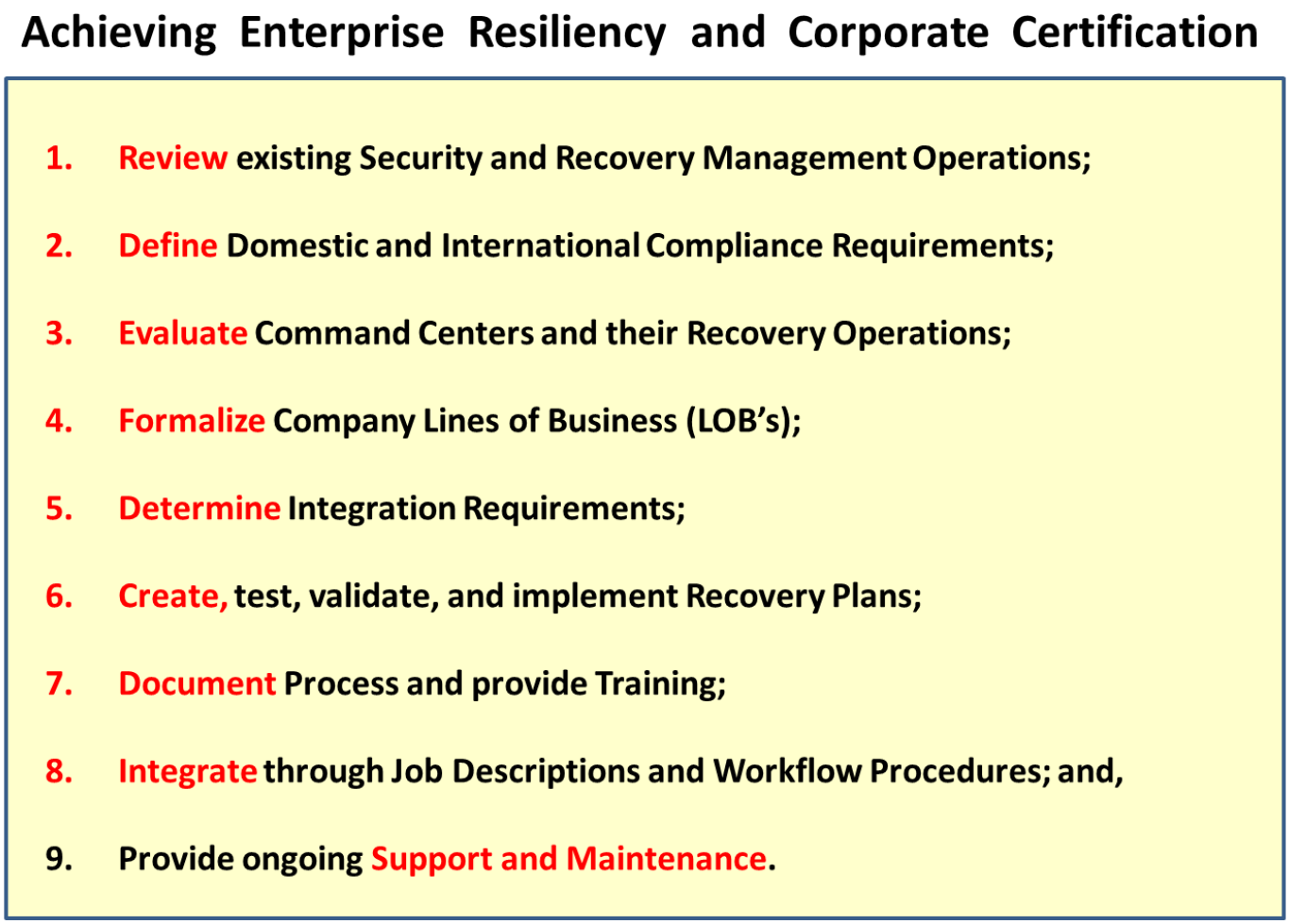
The Recovery Management process includes people who need to have their **functional responsibilities** and job descriptions modified / updated to meet their new responsibilities. Documentation used by affected people must be upgraded to reflect their new responsibilities and procedures used to achieve 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 that they 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

Figure 14: 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 recover operations within required time limits;
- Assign the **Disaster Declaration** Process to responsible management;
- Establish **Recovery Teams** for disaster or business recovery operations;
- **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 on an on-going basis. It will eliminate / reduce disaster events, safeguard the company reputation, improve workflow and operations, lead to better retention and attraction of staff and clients, and thereby improving business profitability and the company's reputation.

Potential threats and their impact on the business

Figure 15: Potential threats and their impact on the business

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

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

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

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

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

Recovery Management plans for loss of a location, service, vendor, or personnel due to a disaster event, while safeguarding the company reputation.

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

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

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

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

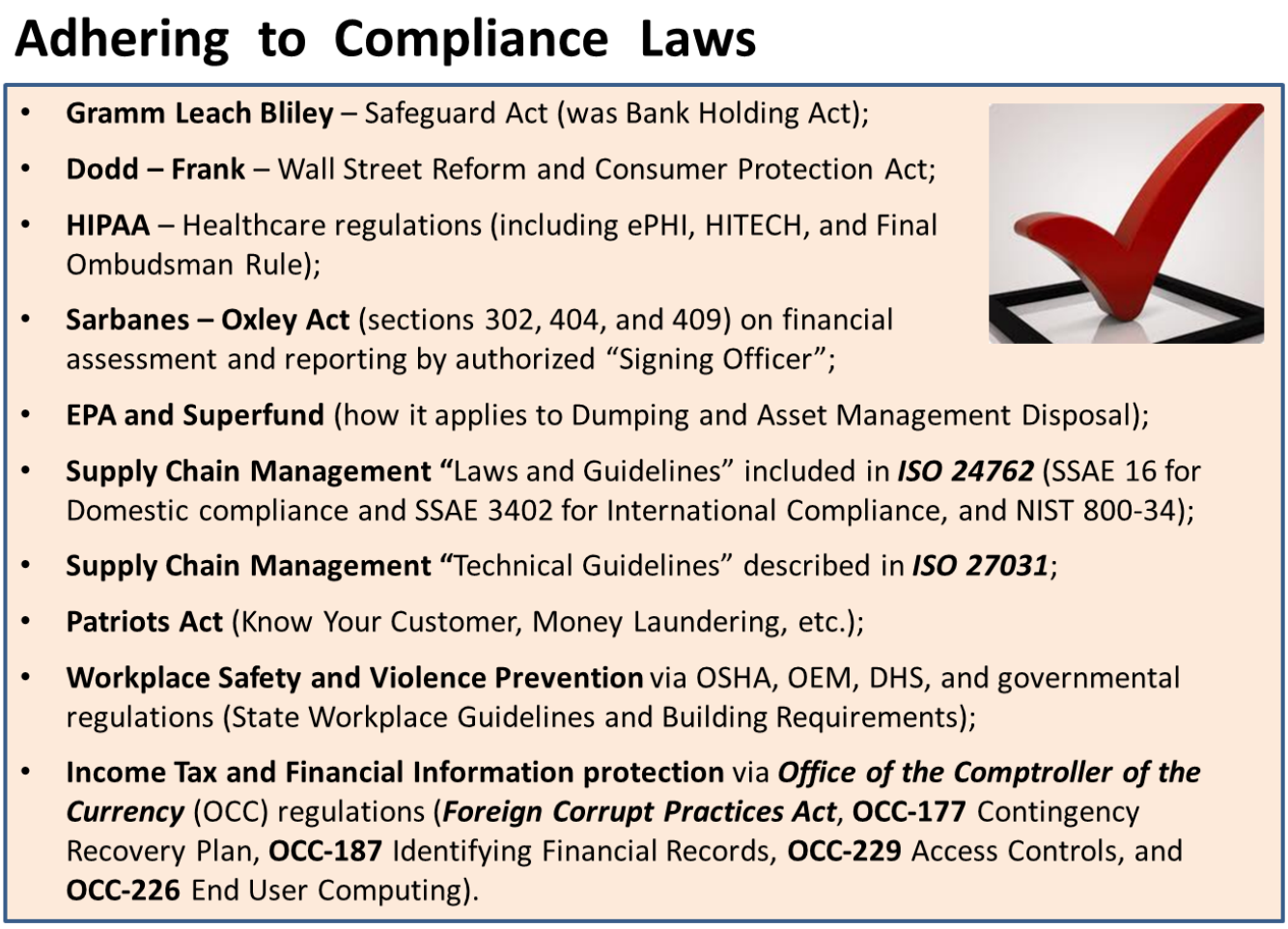
The goal of Recovery Planning within a company is to be aware of the potential events that could lead to a disaster, ranging from Malicious Activities, Natural Events and Disasters, Technical Disasters, External Threats, and Facility Failures.

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

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

Adhering to Compliance Laws and Regulations

Figure 16: Adhering to Compliance Laws



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

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

10. **Office of the Comptroller of the Currency** (OCC), including Foreign Corrupt Practices Act, OCC-177 requiring a Recovery Plan, OCC-187 identifying Financial Records, OCC-229 governing Access Controls, and OCC-226 covering end user computing compliance.

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

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

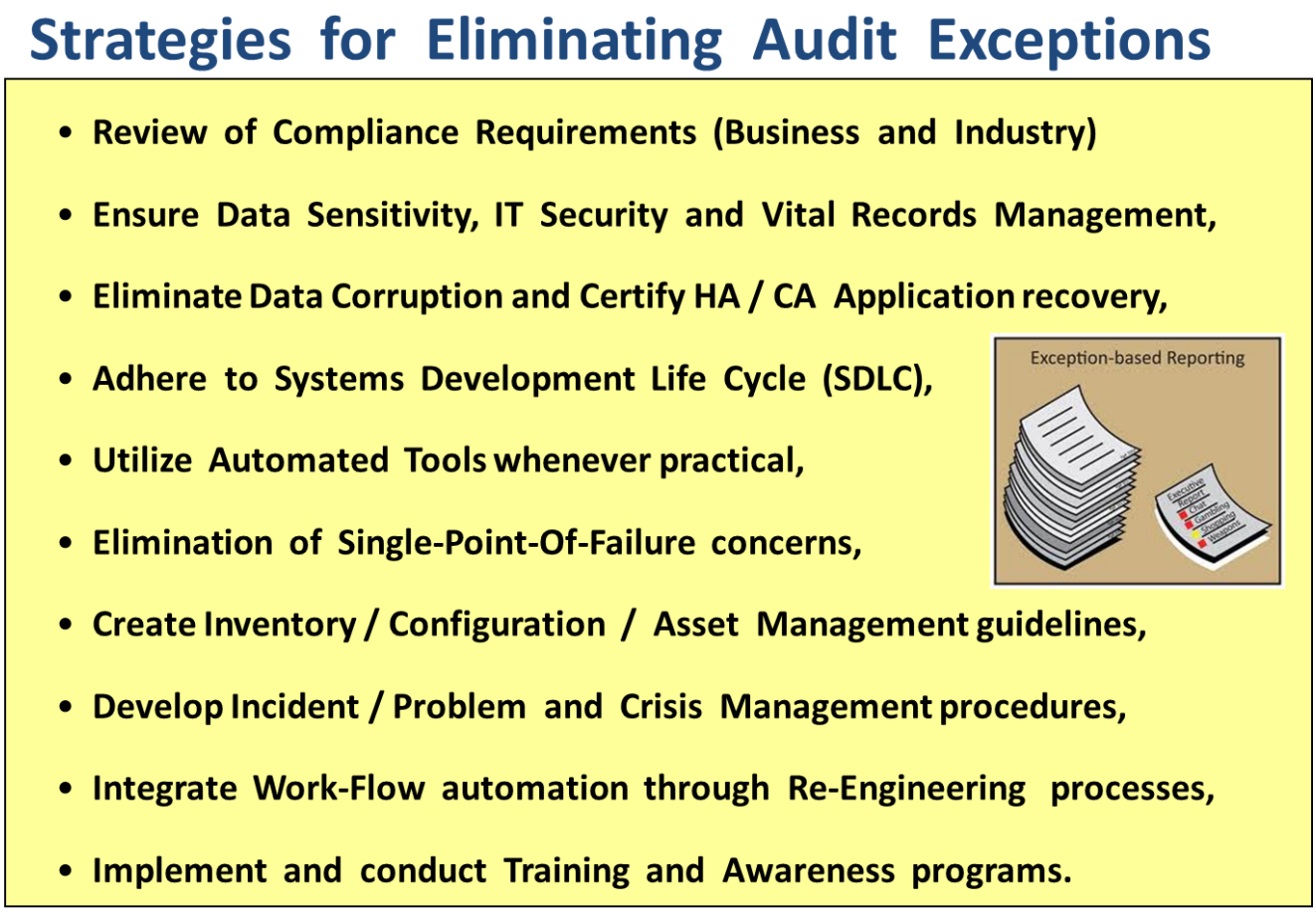
It is therefore crucial to maintain adherence to laws and regulations in the countries that your company does business. It is just as critical to be able to recover your business if a disaster event occurs because clients will leave if you cannot meet the service delivery goals outlines in the Service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

Strategies for eliminating Audit Exceptions, Gaps, and Obstacles

- **Review** Business and Industry Compliance Requirements, both domestically and internationally;
- **Ensure** Data Sensitivity, IT Security, and Vital Records Management;
- **Eliminate** Data Corruption, Certify High Availability (HA) applications and 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 and Business Environment;
- **Create** Asset Management / Configuration Management / Inventory Management procedures;
- **Implement** Facilities Management to create and maintain business locations;
- **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.

Figure 17: Strategies for eliminating audit exceptions



The process of eliminating audit gaps and exceptions is shown above and starts with first reviewing your company's compliance demands. It continues by ensuring that you adhere to data protection through a data sensitivity analysis, defining access controls, establishing IT data security, and finally insuring your adhere to Vital Records management guidelines. One of the goals of this step is to insure that you can recover data within the time objectives established by the client, company, and regulations.

You would then establish a Systems Development Life Cycle (SDLC) and define the functions to be performed by personnel involved with the SDLC. An organizational structure should be created and personnel assigned to positions. The personnel should be trained on their functions and a Standards and Procedures Manual created to illustrate how they should perform their functions and the expected outcome from them.

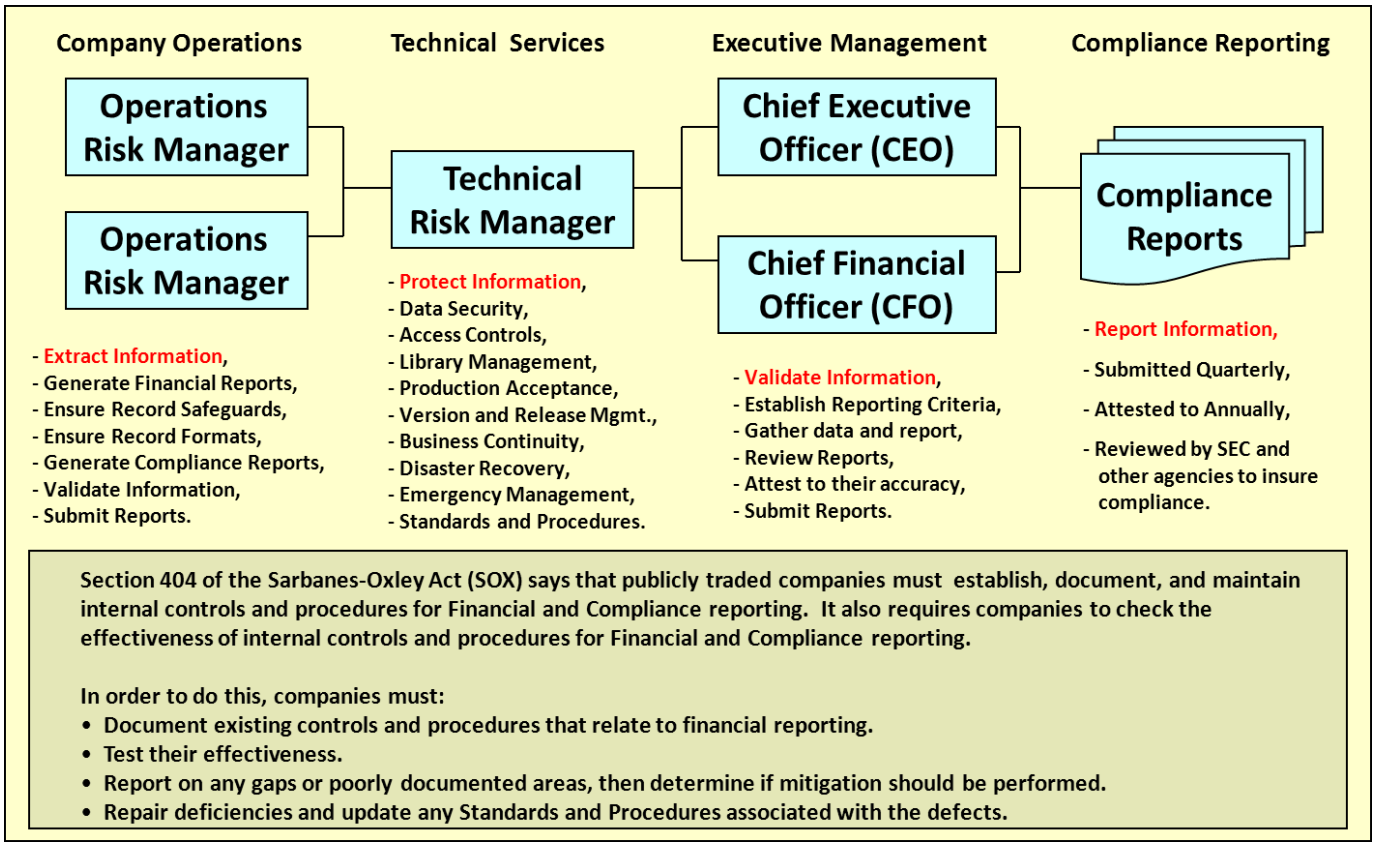
Automated tools should be used whenever feasible to reduce manpower requirements and enhance performance. All "Single Points of Failure" should be located and, when necessary, alternate paths established. Asset Management, Inventory Management, and Configuration Management, and Facilities Management should be used to obtain and assign equipment and supplies as needed. Finally support and maintenance

procedures should be established and everything should be integrated into the everyday functions performed by the staff.

Compliance Reporting Technique

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

Figure 18: Compliance Reporting Technique

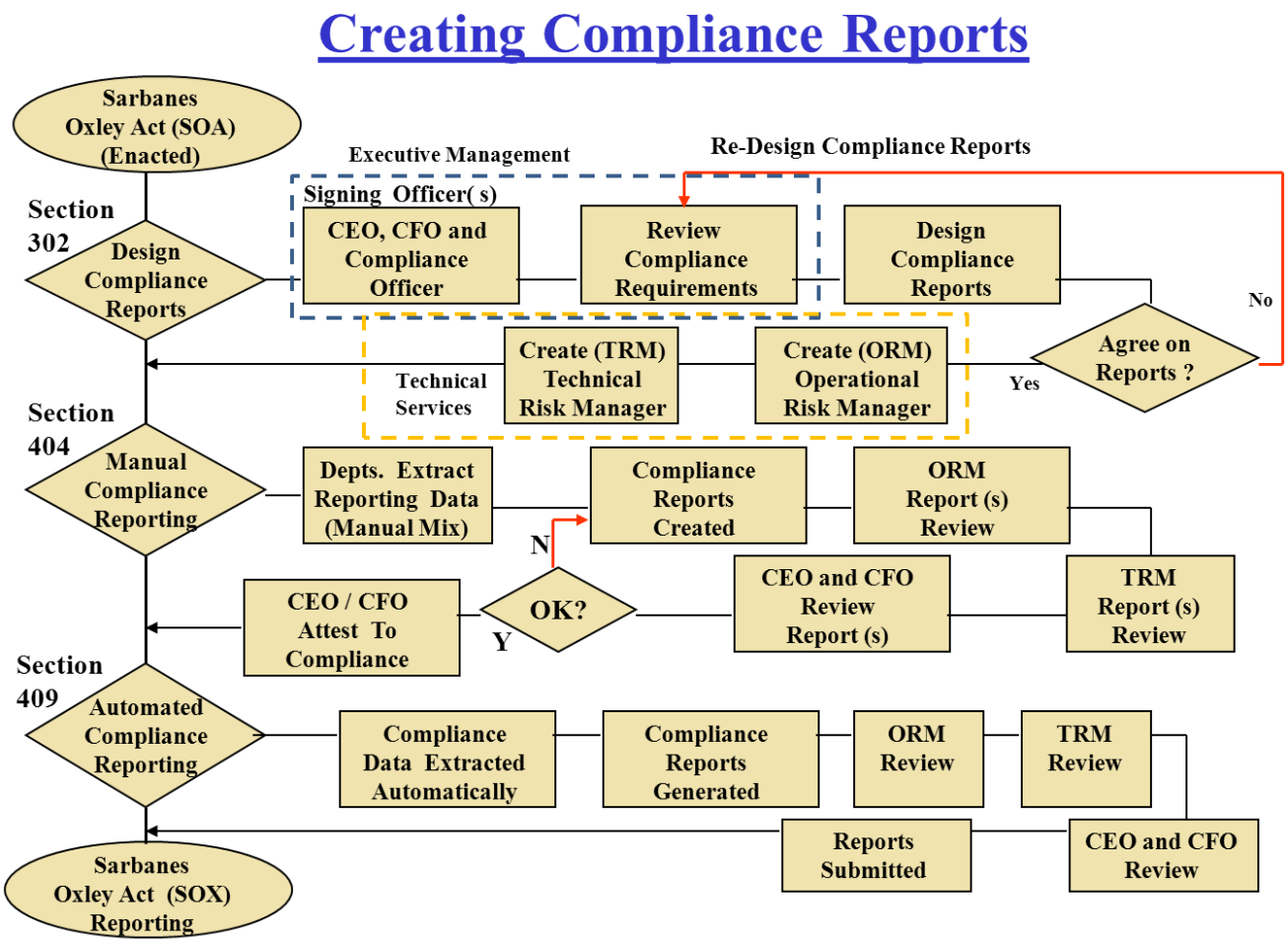


Capturing and gathering compliance information is a corporate endeavor whose pathway is shown above. It starts with the Business Units Operations Risk Manager, who provides the Technical Risk Manager with their reports. The Technical Risk Manager validates reported information and compiles a Compliance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

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

Creating Compliance Reports and a Letter of Attestation

Figure 19: Creating Compliance Reporting (SOX used as an example)



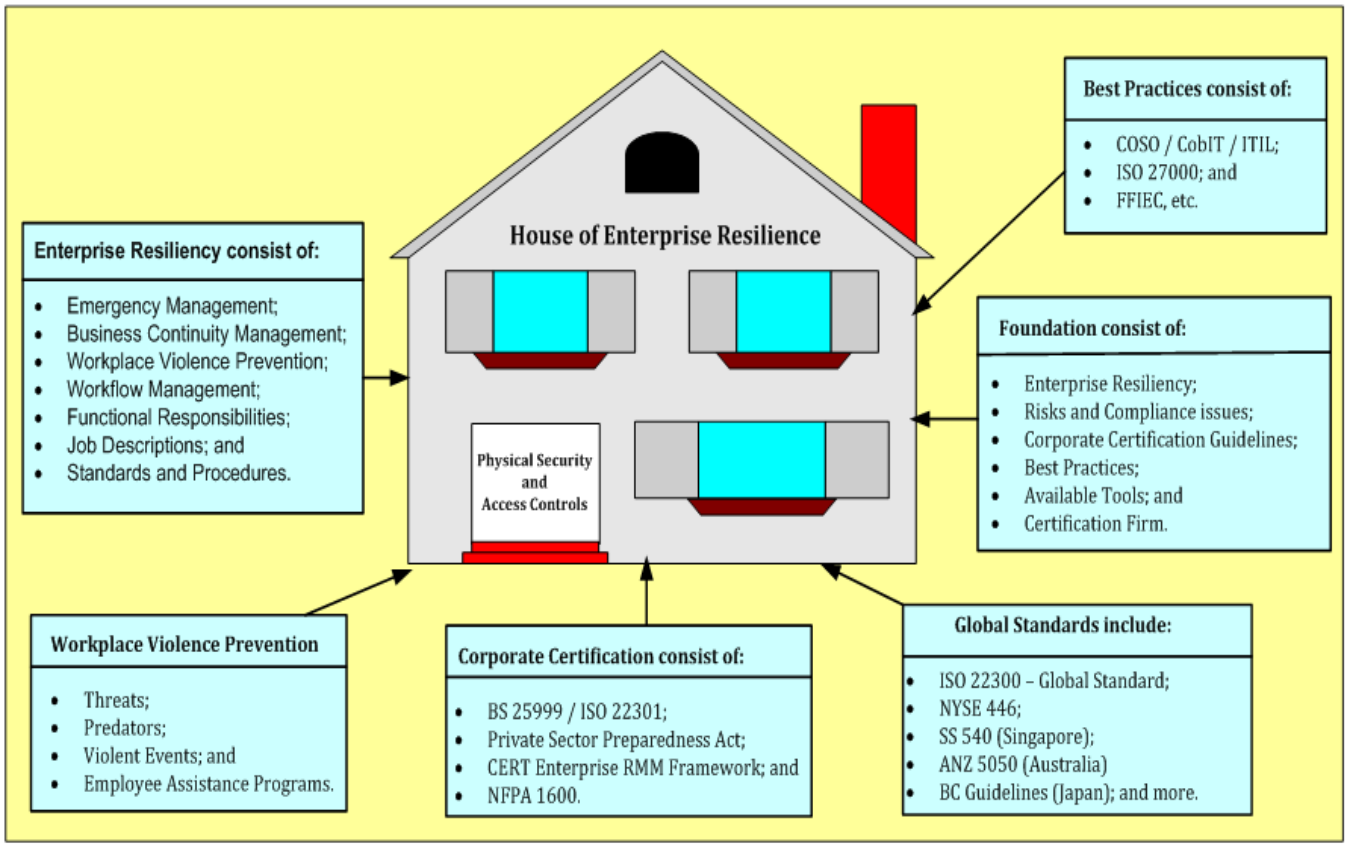
The above illustration is how Compliance Reporting is performed within a business organization with the Sarbanes Oxley (SOX) act being used as an example. The Sox Act was created after the financial crisis to ensure that financial organizations maintain current accounting methods that can be reviewed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

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

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

Enterprise Resiliency and Corporate Certification must be built on a solid foundation

Figure 20: Enterprise Resiliency is built on a solid foundation



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

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

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

The immediate goal of achieving Enterprise Resiliency and Corporate Certification is to protect the company and its reputation from: threats; predators; violent events; and unauthorized access to physical environments or sensitive information. Building this "***Dome of Protection***" over the company will keep business operations safe

from interruptions caused by outside disturbances, while improving the efficiency of the staff and supporting participants (i.e., sub-contractors and business associates).

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

COSO Risk Assessment Guidelines

Figure 21: 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.

Employee awareness training, support, and maintenance going forward.

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

CobIT Framework review

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

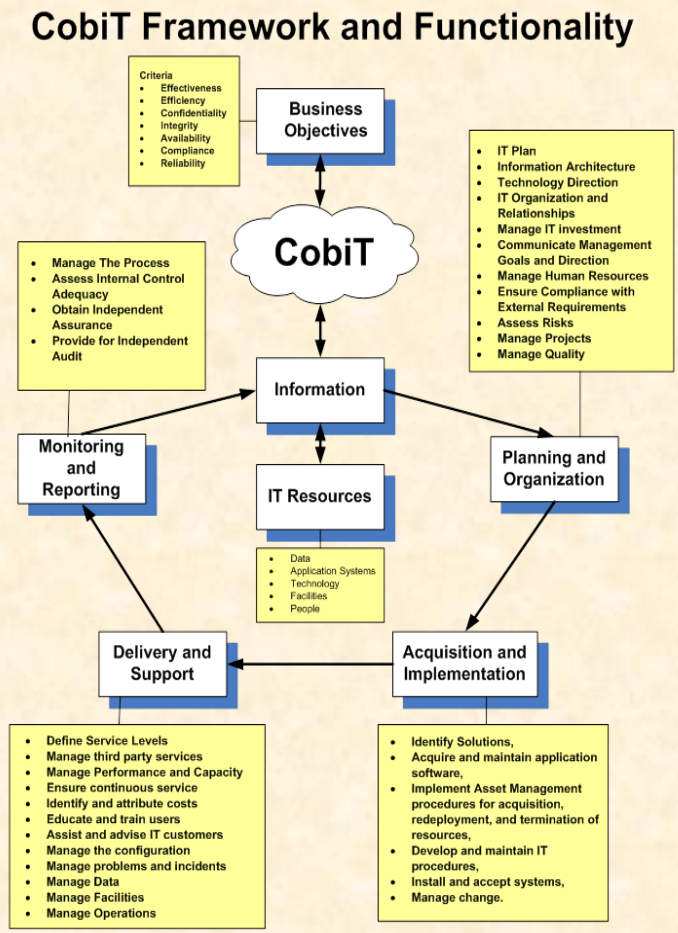
Figure 22: CobIT Framework Overview

CobiT Framework

Control Objectives for Information Technology (CobiT)

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

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



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

Information Technology Infrastructure Library (ITIL) structure.

Figure 23: ITIL v3 Overview

Information
Technology
Infrastructure
Library (**ITIL**)

ITIL Five Phase approach to IT Service Support

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

ITIL Available Modules

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

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

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

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

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 an excellent tool and highly recommended. ITIL files are Relational Data Bases (RDBS) that can be queried to extract information needed for analysis, reporting, and management. Having a RDBS allows for ad-hoc reporting and data extraction, which can to support information requirements for unforeseen events that can occur during a disaster or audit. This makes it easier to create and maintain information, since only a single copy of specific information is created and then appended to other files through a relationship (e.g., on customer name and address used for reports). ITIL also tracks forms from origination to completion.

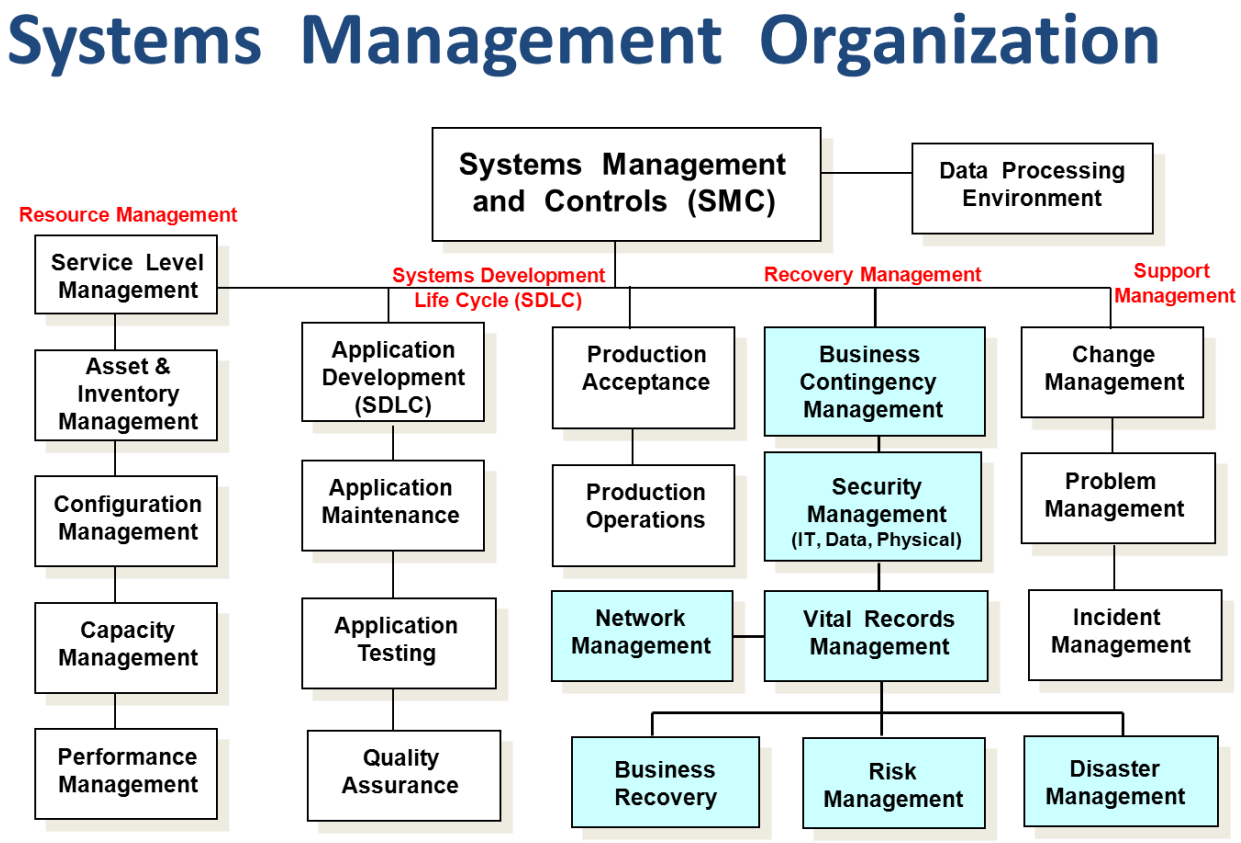
Combining the Risk Assessment of COSO with the implementation techniques of CobIT will help you successfully implement business products and services within the production environment. After that is accomplished, you will need to monitor and respond to problems, while supporting workflow and personnel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

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

The Systems Management Organizational Structure (SMC)

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

Figure 24: Systems Management Organization Chart

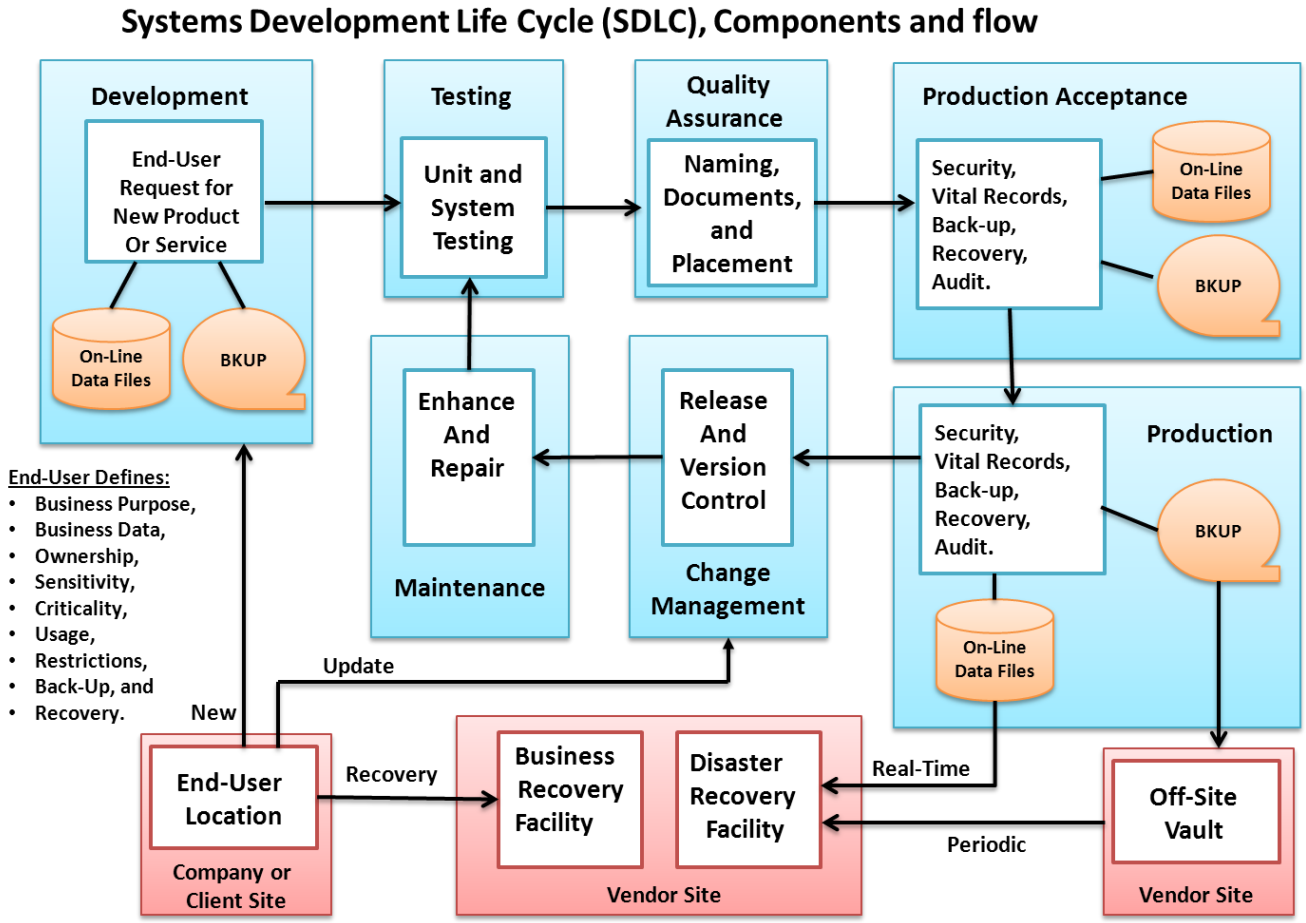


All of these functions are performed to maintain the production and recovery environments in an efficient and safeguarded manner, thereby supporting and protecting business operations and the company reputation.

The Systems Development Life Cycle (SDLC)

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

Figure 25: Systems Development Life Cycle Overview



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

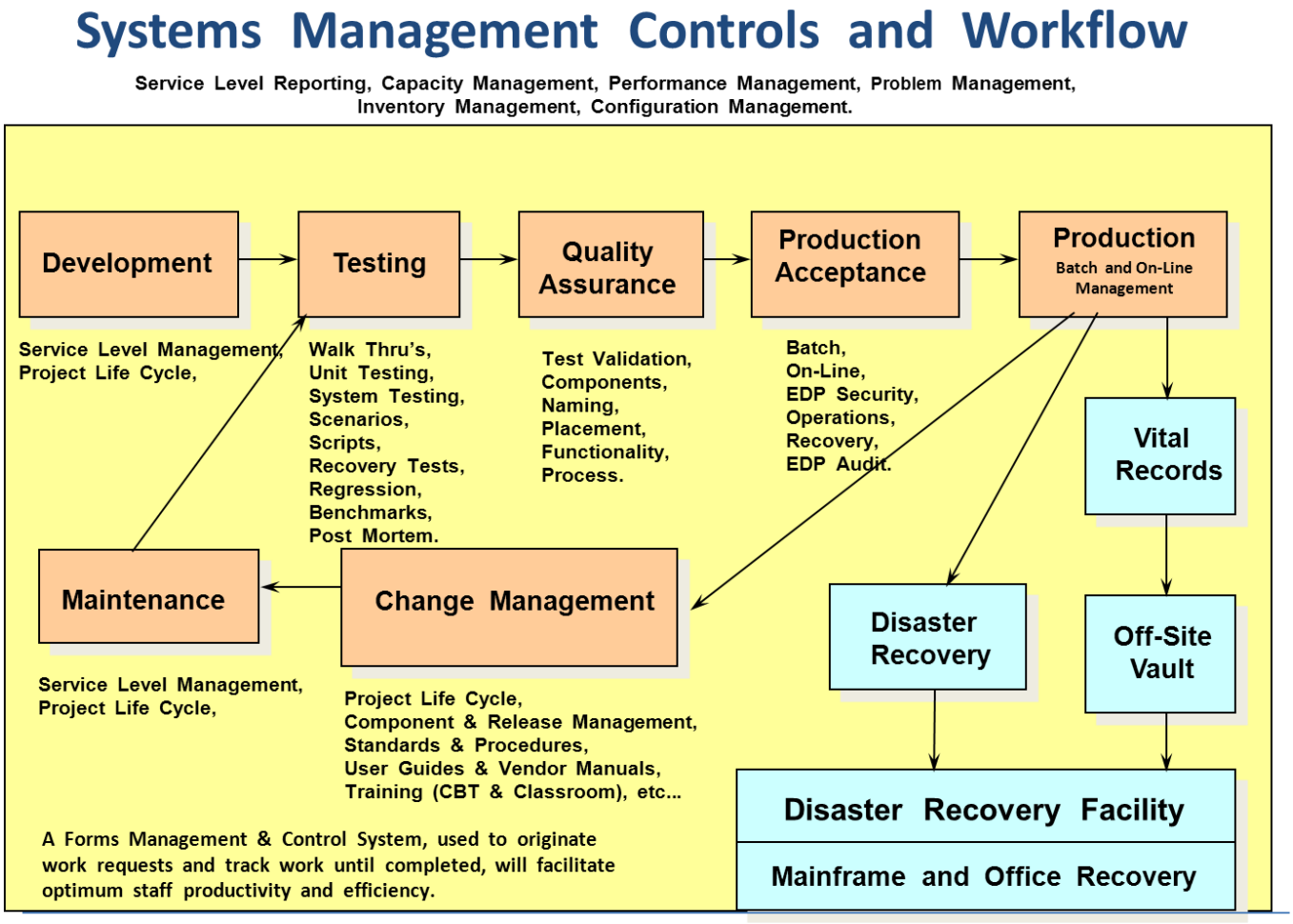
Initially, the end user makes a development request that is approved and scheduled for creation. The development group produces test data that is used to verify proper operations for both normal and error processing. When testing is successful, the Quality Assurance Group reviews the documentation and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

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

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

Systems Management and Controls

Figure 26: Systems Management and Control Overview

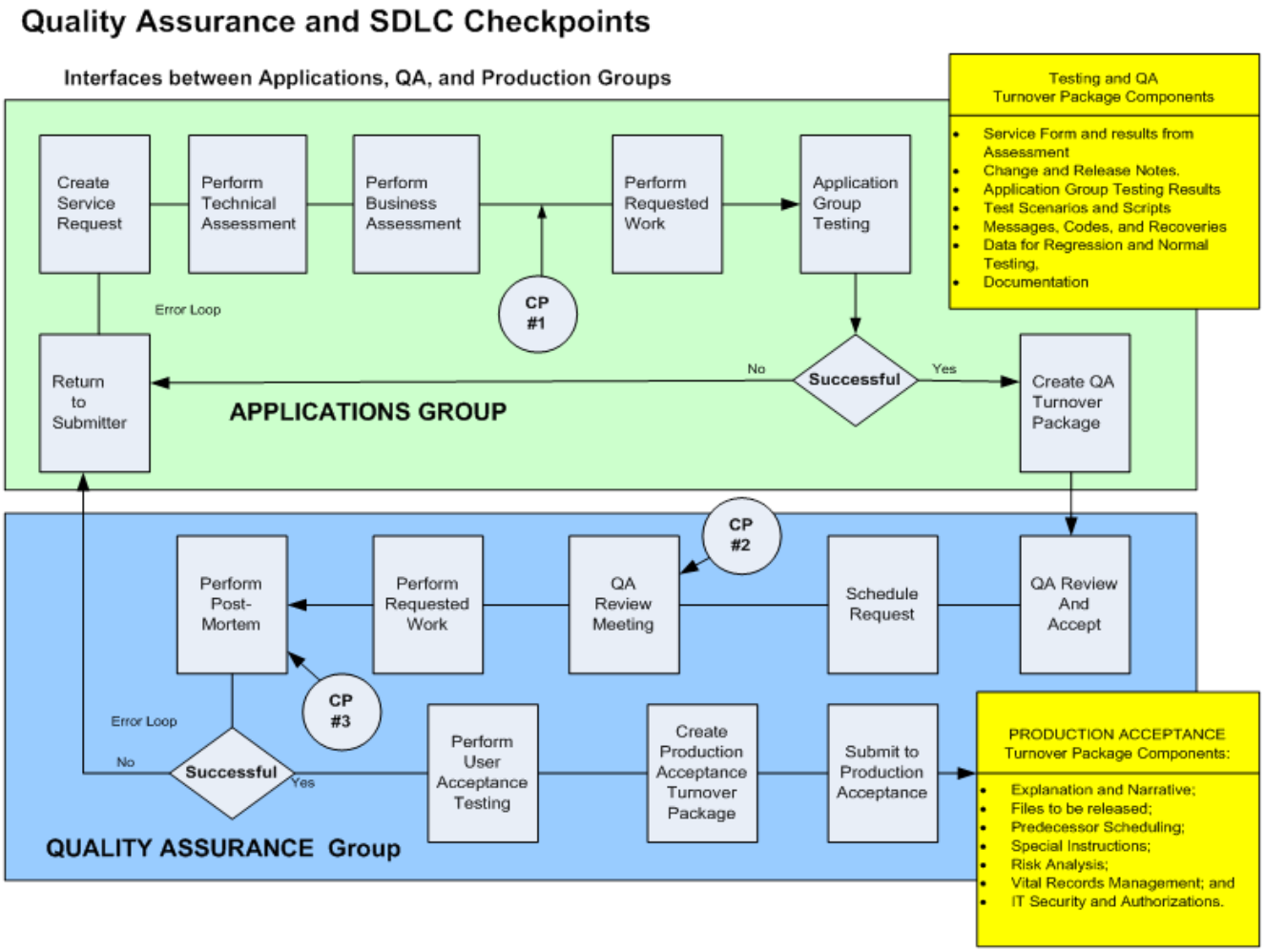


The tasks performed to support the SDLC are shown above. Development initially creates the application, but then all further changes to the application are performed via the Maintenance process. Testing is performed in phases and must guaranty that normal and abnormal conditions are recognized and reported on in a manner documented within the Operator's Job Run Book and the Applications Messages and Codes ("Problem

Identification and Definition", "Probable Causes", and "Actions to be Taken" in response to problems). The QA Group assures that all testing was successfully performed and that accompanying documentation adheres to Version and Release Management guidelines. Production Acceptance sets the application up to run in Production and Production is responsible for Vital Records Management, Back-up, Vaulting, and Recovery Operations. Support recognizes and responds to problems, and Change Management is responsible for validating that a problem resolutions or enhancement can be adequately performed and scheduled. This cycle is repeated and on-going.

Migrating Applications to the Production Environment

Figure 27: Migrating Applications to the Production Environment Overview



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

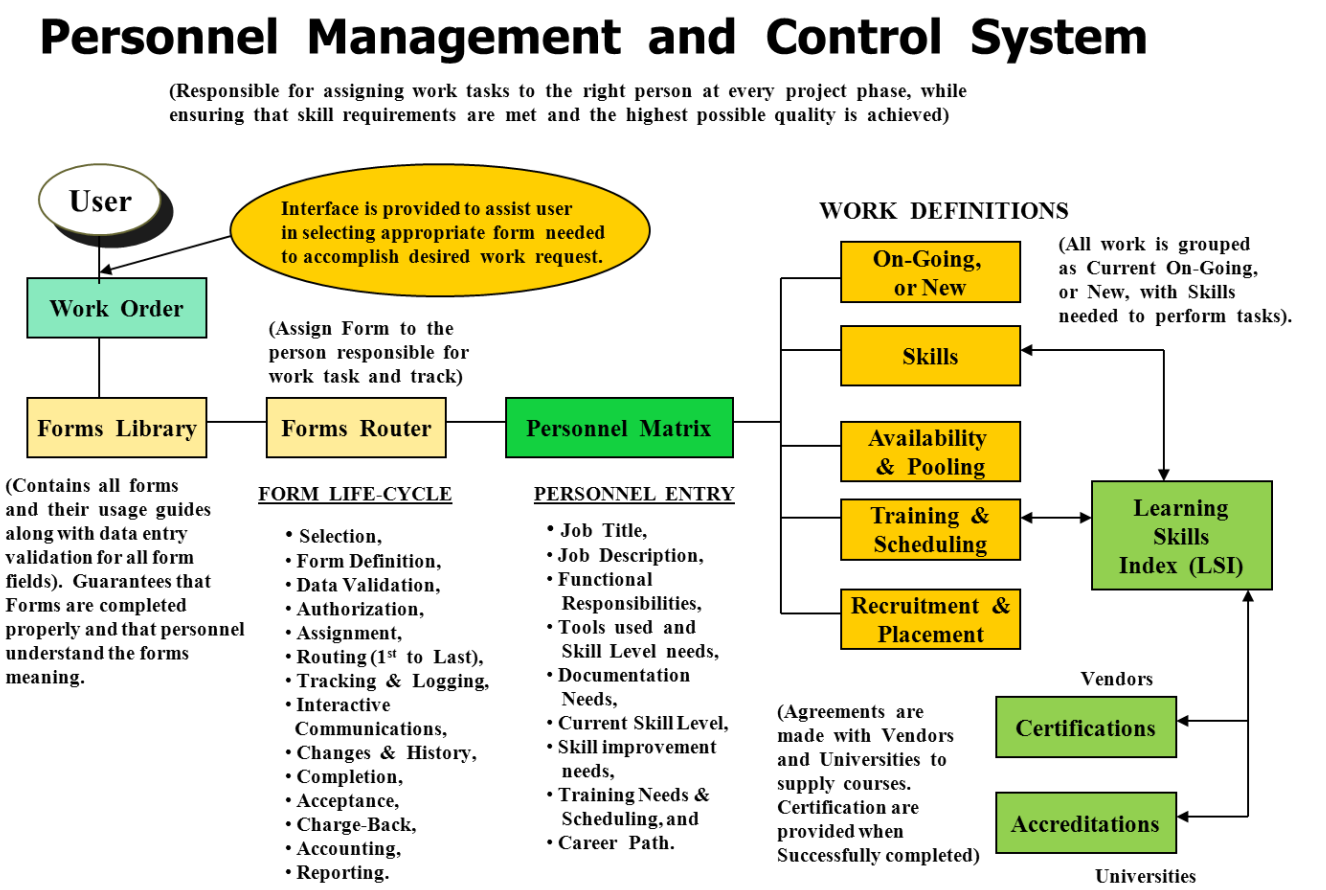
Information requirements can be accumulated via a Relational Database System (RDBS) used for forms completion and movement. This information can be accessed through structured query language instructions

(SQL) that pick information from various forms and generate specific reports for management and technical analysis.

Personnel Management and Control System

It is important to manage your staff by ensuring that they are prepared to perform their assigned duties and are supported by training and workload balancing.

Figure 28: Personnel Management and Control System



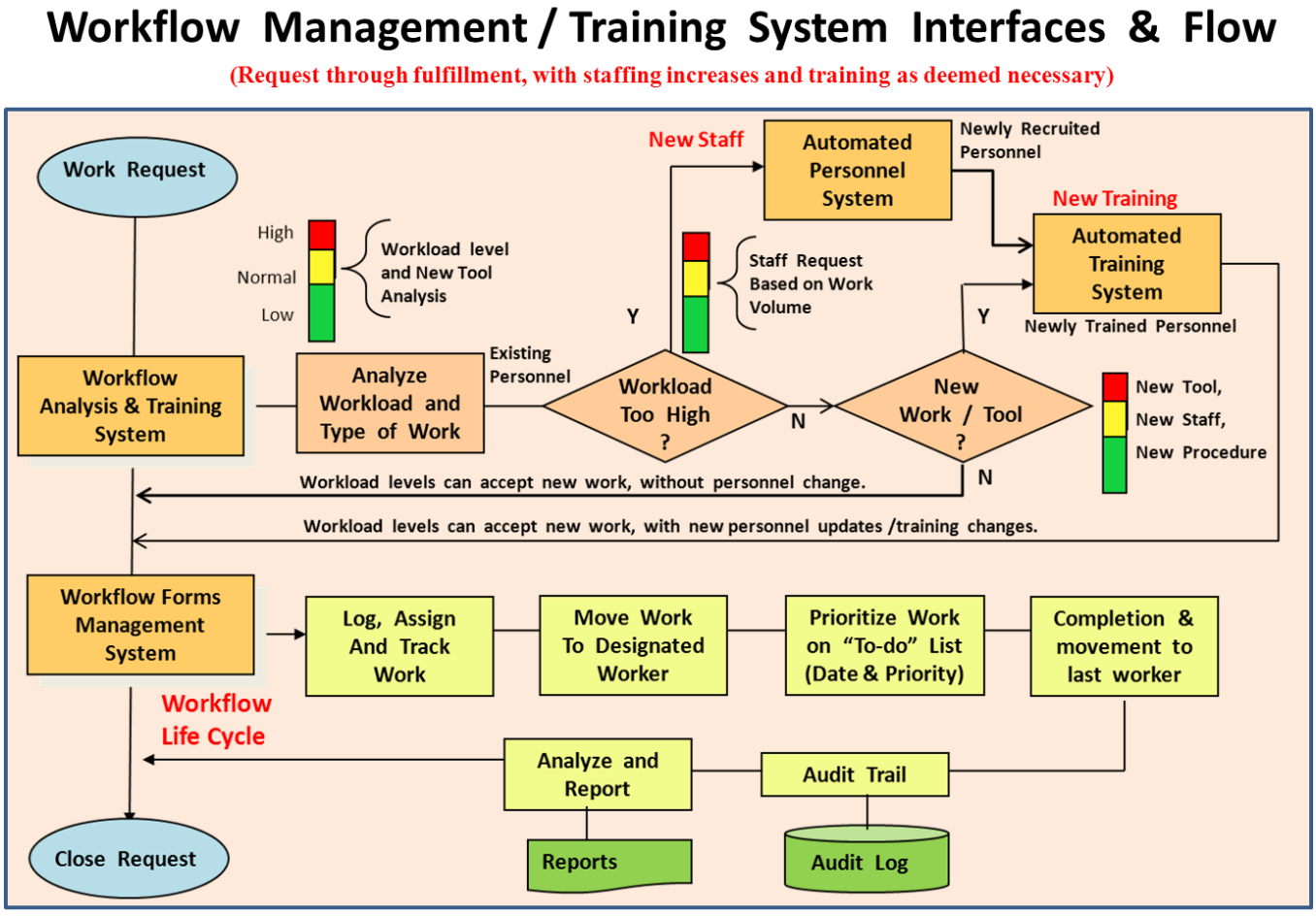
People have a job to do and a company has standards and procedures to ensure that their staff does what is requested of them in an efficient manner. In order to achieve this goal, it is first necessary to define the functions and responsibilities of the organization. Then people must create a profile of their present skills and career path desires. The company then provides training on the existing functions and responsibilities assigned to personnel and monitor the workload assigned to people. Along with workloads are the new technologies entering the environment and which ones people must be trained on. When personnel are attending training, they are away from their assigned everyday functions, so the other staff must assume their responsibilities –

making it doubly hard to maintain workflow. Because of this, workflow must be monitored and new technology training provided.

Training can be provided by universities, professional organizations, or internally by the company. When training has been successfully completed, a certification should be issued and placed into the employees' record.

Monitoring personnel workloads and providing training and hiring services

Figure 29: Workflow management / training system interfaces & flow



People normally spend their time at work in the following manner:

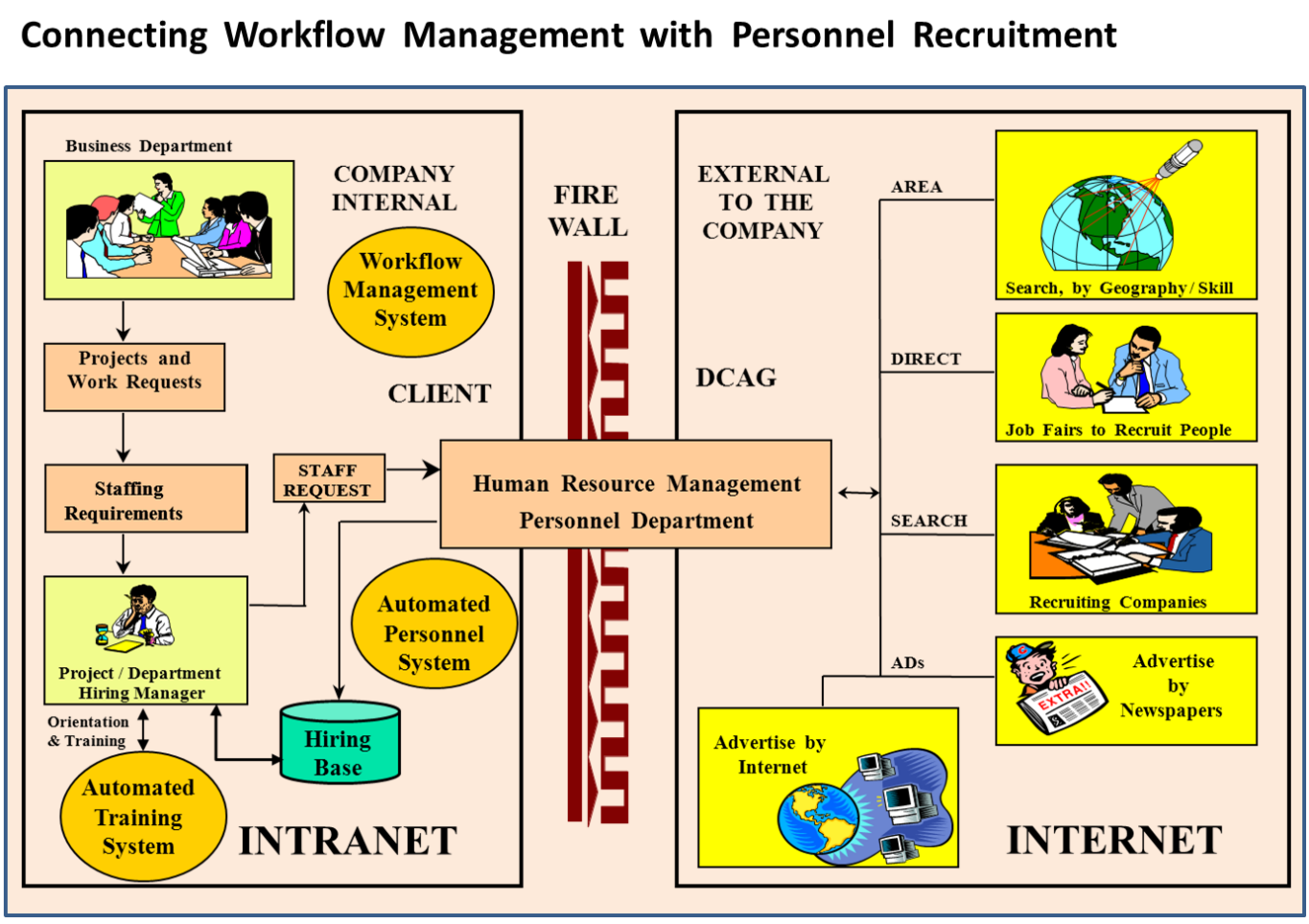
- 60% of their time is devoted to performing their functional responsibilities as defined in their job description;
- 20% of their time is spent attending meetings;
- 10% of their time is devoted to education; and,
- 10% of their time is spent performing special projects.

A method for monitoring workflow throughout the organization is shown above. Whenever workloads rise above a threshold actions are taken to rectify the problem, either through training, adding staff, or new technologies.

Following this method will allow you to better load balance work assignments and service client needs, while ensuring that your staff is well trained on their job functions and the technologies they use. This will produce a trained and happy staff with high morale, which assists in retaining staff and clients and enhances the company reputation.

Connecting Workflow Management with the Hiring Process

Figure 30: Connecting Workflow Management with the Hiring Process



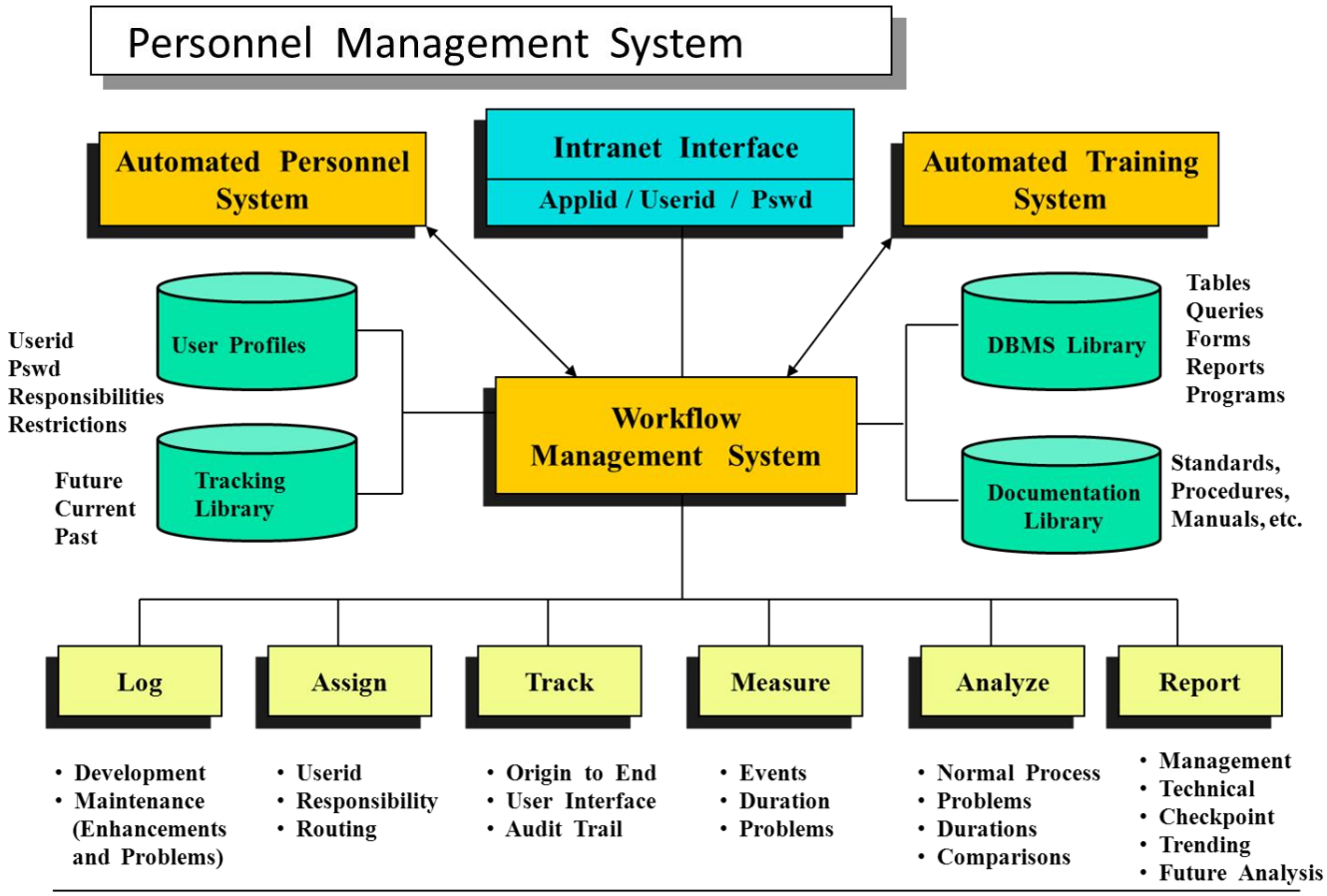
Whenever workflow levels or new technologies dictate the need for additional staff an electronic interface is utilize to solicit personnel. The process includes:

- Planning session results in new work utilizing new technologies and needing additional staff.
- All of the projects and work requests that require additional staff are translated into job descriptions and forwarded to HR.

- Human Resources would then review the new assignments and job descriptions with the Hiring Managers to gain a solid understanding of what type of person they are looking for.
- HR then submits hiring requests through various methods, from Internet, through News Papers.
- Resumes are solicited, validated, screened, and forwarded to HR for review.
- Resumes passing scrutiny by HR are placed on a queue for the Hiring Manager to review.
- The Hiring Manager selects personnel he wants to interview, or rejects resumes and speaks with HR to better recruit personnel that better meet the Hiring Manager needs.
- Once ideal personnel are located, they are interviewed, hired, orientated, and trained to meet the requirements associated with the position.

Fully implemented Personnel Management System

Figure 31: Fully implemented Personnel Management System



An example of a fully implemented Personnel Management system is shown above. It is responsible for providing workflow monitoring, personnel hiring, and training – all accessible through a Computer Graphics Interface equipped with Help and Data Entry Validation.

Requests flowing through this system are logged, tracked, and reported on so that problems can be located and corrected as they arise, eventually resulting in a fully debugged and tailored system capable of best satisfying work levels assigned to personnel.

Creating Business Recovery Plans

To protect a business from interruptions and prolonged outages it is necessary to create Business Recovery Plans. These Plans can be grouped into a discipline called "Recovery Management" or "Enterprise Resiliency", because they represent recovery plans from the various disciplines contained with the organization.

Recovery Planning includes:

- Emergency Management;
- Disaster Recovery;
- Business Recovery;
- Application Recovery;
- Site Recovery (Data Center or Business Location);
- Workplace Safety and Violence Prevention;
- Risk Management;
- Crisis Management; and,
- Crisis Recovery Planning (includes Pandemic, transportation, active shooter, etc.).

Other considerations associated with Recovery Management include:

- Site Protection when disaster events occur;
- Salvage Operations to recover a site damaged because of a disaster event; and,
- Restoration Operations to facilitate a return to the primary site after the disaster event is over (includes facilities, office equipment, supplies, phone, communications, and Information Technology).

The DRII Ten Step Process for Recovery Management

The Disaster Recovery Institute International uses a "Ten Step Process" to achieve Recovery management. The Ten Step DRII Process includes:

1. Project Initiation and Management

Establish the need for a Business Continuity Management (BCM) Process or Function, including resilience strategies, recovery objectives, business continuity and crisis management plans and including obtaining management support and organizing and managing the formulation of the function or process either in collaboration with, or as a key component of, an integrated risk management initiative.

2. Risk Evaluation and Control

Determine the events and external surroundings that can adversely affect the organization and its resources (facilities, technologies, etc.) with disruption as well as disaster, the damage such events can cause, and the controls needed to prevent or minimize the effects of potential loss. Provide cost-benefit analysis to justify investment in controls to mitigate risks.

3. Business Impact Analysis

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. Identify time-critical functions, their recovery priorities, and inter-dependencies so that recovery time objectives can be set.

4. Developing Business Continuity Management Strategies

Determine and guide the selection of possible business operating strategies for continuation of business within the recovery point objective and recovery time objective, while maintaining the organization's critical functions.

5. Emergency Response and Operations

Develop and implement procedures for response and stabilizing the situation following an incident or event, including establishing and managing an Emergency Operations Center to be used as a command center during the emergency.

6. Developing and Implementing Business Continuity Plans

Design, develop, and implement Business Continuity Plans that provide continuity within the recovery time and recovery point objectives.

7. Awareness and Training Programs

Prepare a program to create and maintain corporate awareness and enhance the skills required to develop and implement the Business Continuity Management Program or process and its supporting activities.

8. Exercising and Maintaining Business Continuity Plans

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

9. Crisis Communications

Develop, coordinate, evaluate, and exercise plans to communicate with internal stakeholders (employees, corporate management, etc.), external stakeholders (customers, shareholders, vendors, suppliers, etc.) and the media (print, radio, television, Internet, etc.).

10. Coordination with External Agencies

Establish applicable procedures and policies for coordinating continuity and restoration activities with external agencies (local, state, national, emergency responders, defense, etc.) while ensuring compliance with applicable statutes or regulations.

The Risk Assessment process was explained earlier, so I will continue with the Business Impact Analysis.

Business Impact Analysis (BIA) report components

The Business Impact Analysis is responsible for analyzing Business Locations, or Business Units, to determine the criticality of services or products supported by the group. The Business Impact Analysis (BIA) documents:

Section I – BIA Impact Indicators:

(Indicators are rated as Significantly High (S), High (H), Medium (M), or Low (L)

- Business Unit / Work Area Name;
- Midrange computing usage;
- Distributed Processing / Client Server usage; and,
- Suppliers and Vendors used to support operations and their criticality.

Section II – Impact Scoring:

(Scoring is H = 4 Points, H = 3 Points, M = 2 Points, and L = 1 point)

- Service Delivery;
- Enterprise Support; and,
- Operational Support.

Section III - Business Scope:

(**Business Scope is rated as: H = 71-80 Points, H = 50-70 Points, M = 29 – 49 Points, L = 20-28 Points)**

- Organization Location (3 Dot organization Structure used – Division, Business Function, Business Unit);
- Business Unit, By Location;
- Number of Associates;
- Production Locations;
- Criticality of Operations; and,
- Contact Name and Phone Number.

Section IV – Supplier Scope:

(Complete for each Function)

- Function Name;
- Application;
- Supplier (What is Provided by Supplier, Criticality, and RTO);
- Comments; and,
- Work Around in Place?

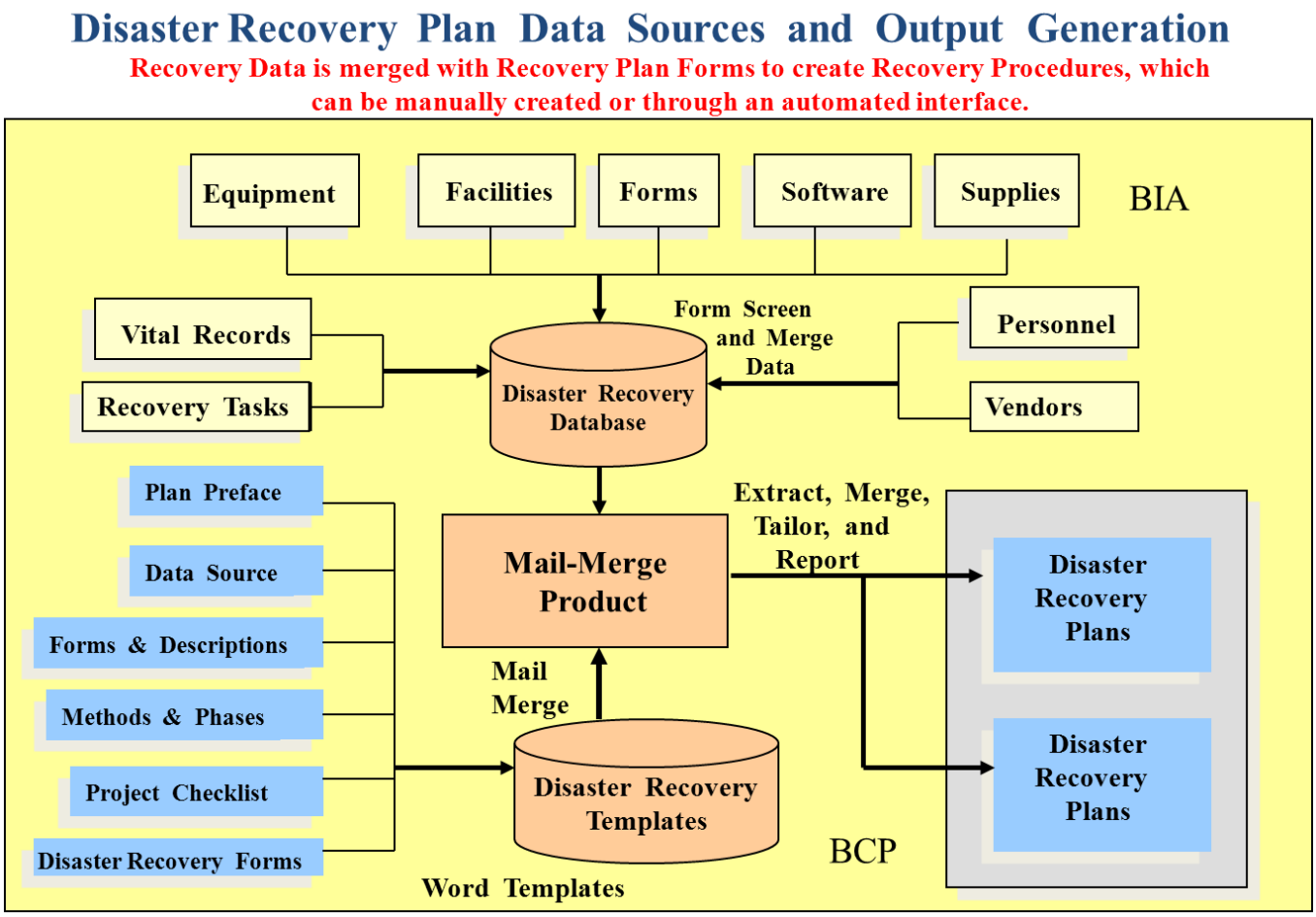
Section V – Recovery Guidelines:

(Repeated for each component)

- Component;
- Attribute;
- Recovery Level (S, H, M, L);
- Midrange Recovery Definitions;
- Distributed Computing / Client Server Recovery Definitions; and,
- Recovery Definitions.

Generating a BIA (Overview)

Figure 32: Generating Business Impact Analysis (BIA)



The above illustration shows the information used to populate a BIA and how that information is used to help generate Business Continuity Plans.

BIA's are created for every Business Unit or Business Location and are used to define Recovery Time Objectives for recovery operations, along with defining the number of people at the location who have to be evacuated and included in recovery planning.

Normal evacuation planning includes leaving the building under the supervision of company Fire Marshals and Recovery Assistance Leaders. The Employees then go to an assembly point si that a head count can be created to validate the safety of the staff. Any people not present will have to be located or their absence defined (not at work, on business trip, etc.). The list of safely evacuated personnel will be used to inform family members of their safety. Assembly sites should be defined and more than one available should the primary assembly site be inaccessible. Pictures and directions should be provided to evacuees and included in recovery plans.

Personnel will then be directed to go to their recovery location, which could be going home and reclogging on to continue work or travel to a remote site. If travel is required, it should be supplied by the company along with living and other conditions needed to support the staff at a remote site.

Integrating BIA Plan with BCP Plans and the organization

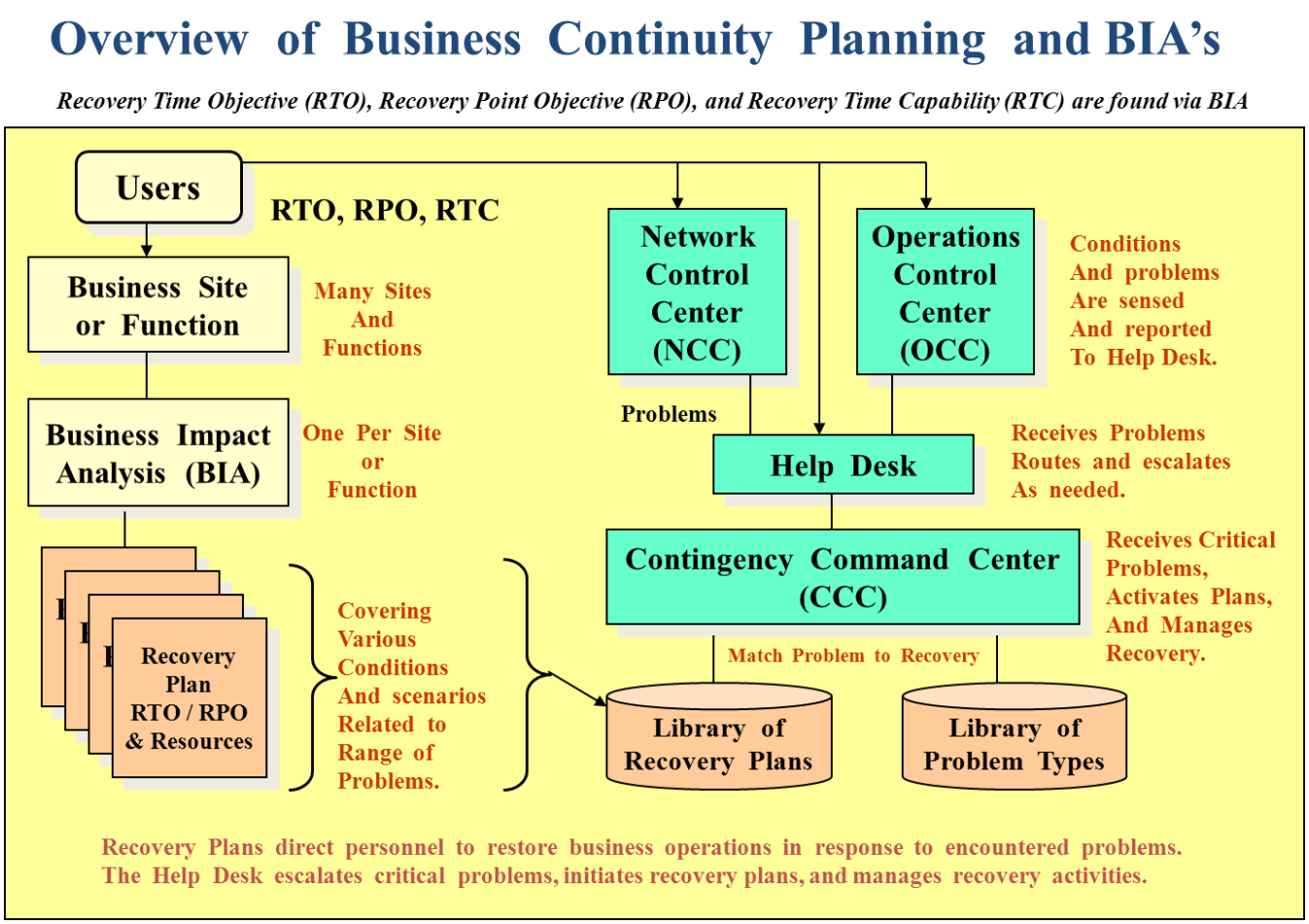
The information contained in a BIA is used to help populate the Business Recovery Plan and other company departments and functions as shown below.

When problems are reported to the Help Desk they go through an escalations process including:

- Level I – Help Desk Resolved (simple problems, or repeat problems that have been resolved earlier);
- Level II – Company Subject Matter Expert responsible for the failing component;
- Level III – Vendor support resolves problem, or replaces component; and,
- Level D – Disaster Recovery Plan pulled and Contingency Coordinator notified to activate recovery plan.

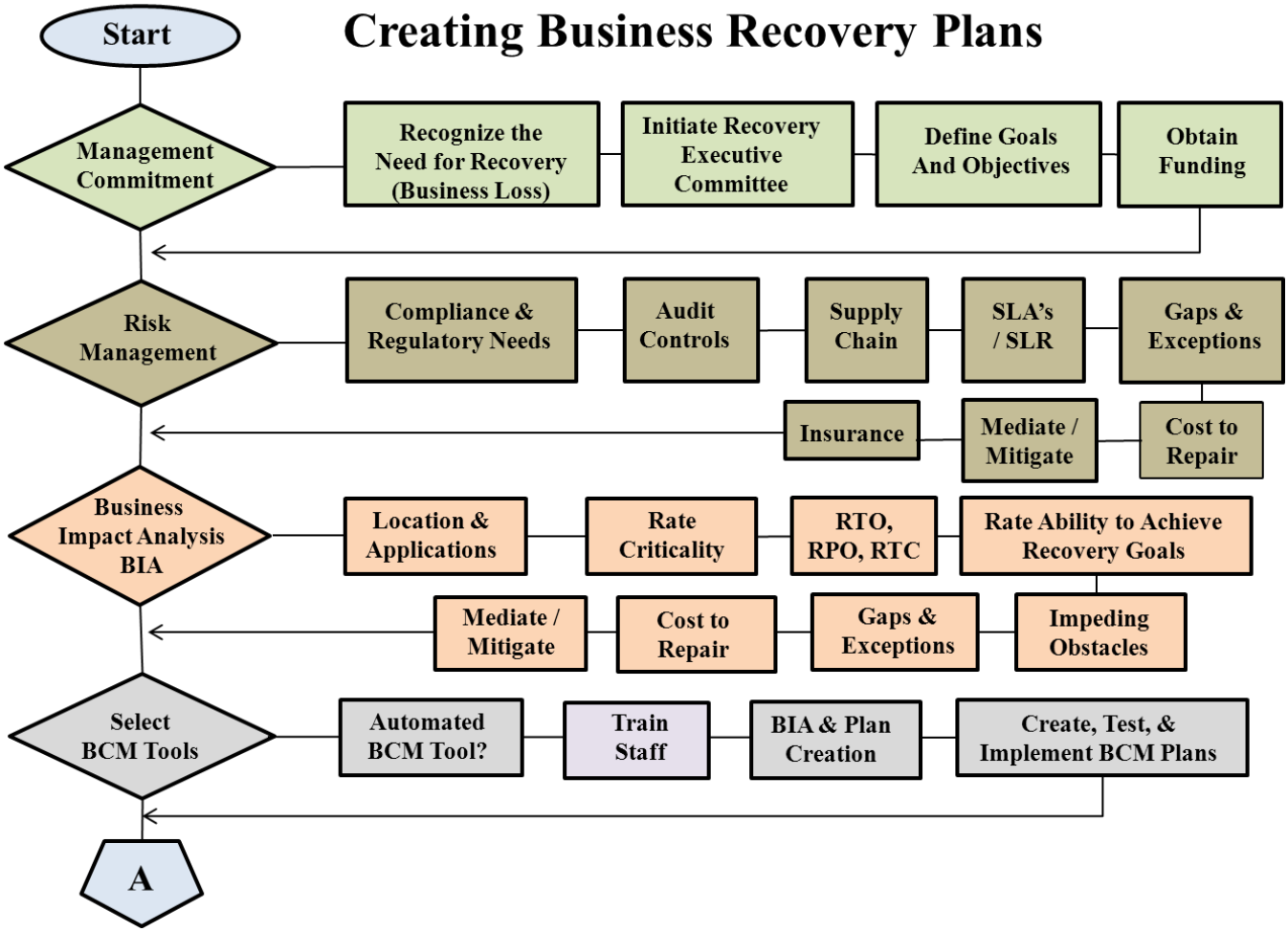
BIAs are placed into repository and associated with the site or business unit, by functional name. Business Continuity Plans are created and stored in a Recovery Plan repository. Disasters are related to recovery plans and passed onto the Contingency Coordinator to activate the plan by calling recovery team and directing them to perform their assigned recovery functions. Staff is directed to recovery facility, or Information Technology function is switched to a secondary site to continue business operations.

Figure 33: Overview of BIA and BCP integration



Creating Recovery Plans (Flowchart)

Figure 34: Creating Recovery Plsn (Flowchart)

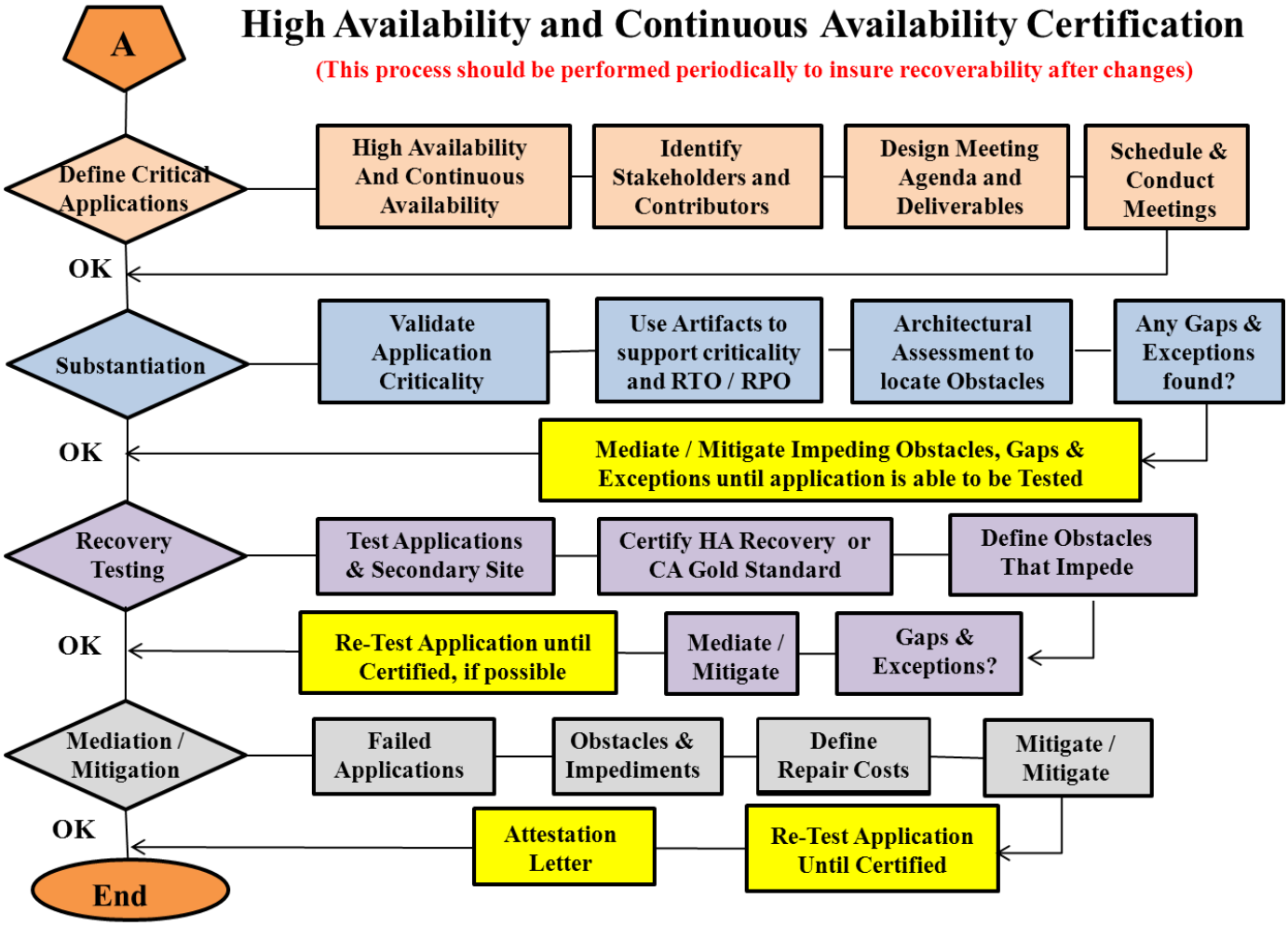


The process of creating recovery plans is illustrated in the above flowchart. It includes:

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)

Figure 35: 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.

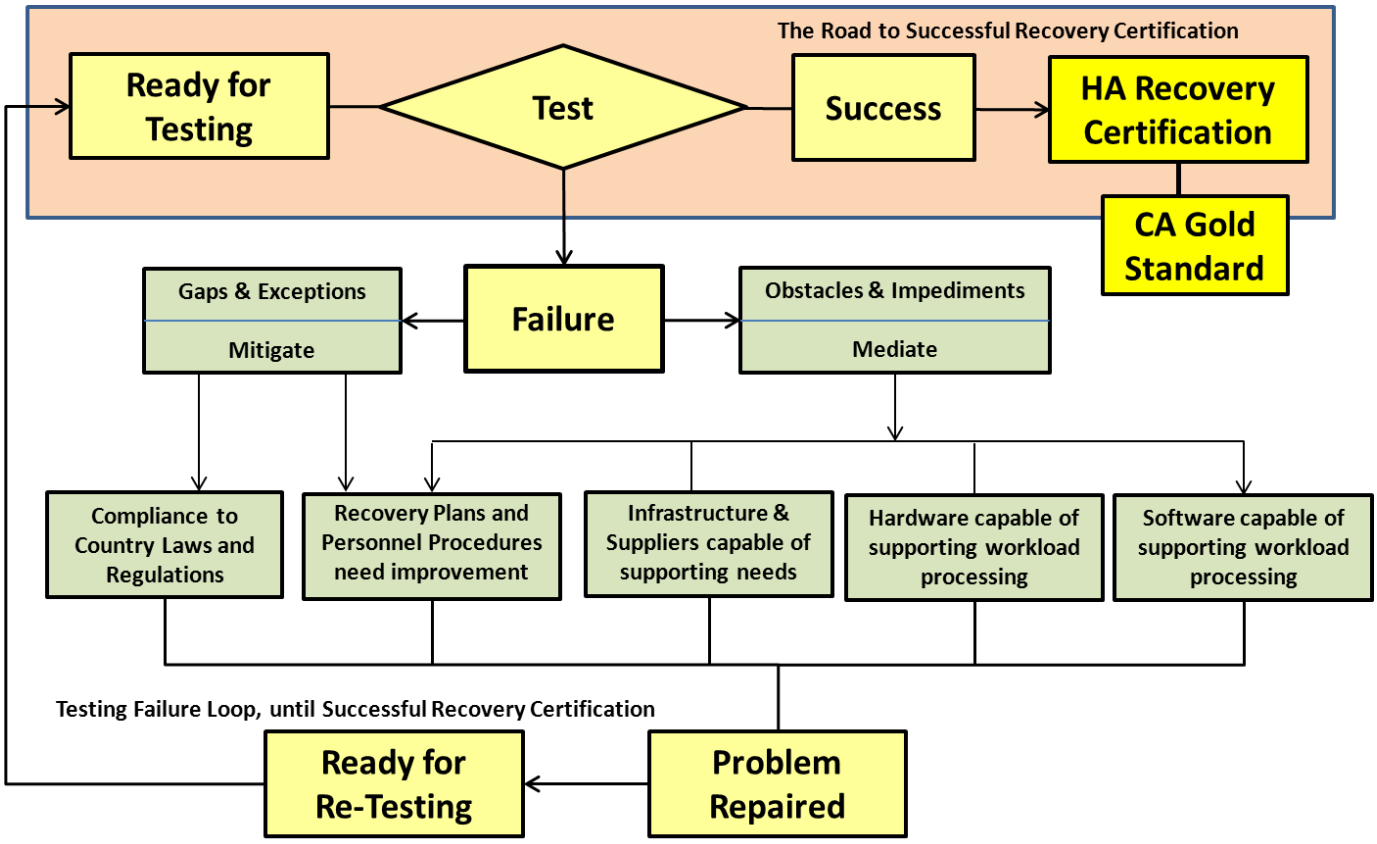
4. Testing is finally conducted in a scheduled manner with a ramp up from Tier-1 through Tier-n. Any uncovered Gaps, Exceptions, or Obstacles are detected and repaired. After repairing problems, the application is re-tested until certification is achieved.

Testing 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.

Figure 36: Testing recovery ability of applications



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 at 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.

Applications that fail recovery certification are reported and their problems repaired. They are then re-tested until certification is achieved. Application Recovery Certification is acceptable for High Availability (HA) applications (Failover / Failback), but a Gold Standard Recovery Certification is required for Continuously Available (CA) applications (Flip / Flop) that must always be available. This process is shown above.

Certifying Application Recovery

Applications are certified depending upon their Availability Requirements, which are:

- **Continuously Available (CA)** applications that can not have any down-time, like Demand Deposit in Banks where customers demand access to their funds 24 hours a day, 7 days a week. Recovery for CA applications is performed in a **Flip / Flop** manner, in which the CA application can flip operations to a secondary site when a disaster event occurs and Flop back to the primary site when the disaster event is completed. CA applications periodically switch production operations from the primary to the secondary site and run operations there for a period of time to insure that both sites are always capable of supporting the most critical applications of the company Other financial applications that would be rated as CA include:
    - SWIFT – Systems for World-Wide Funds Transfer;
    - Web Based applications that are accessed 24 / 7 world-wide and are critical to the business;
    - Payroll System the day before or on Payday; and,
    - Recovery Certified Applications must meet the "**Gold Standard**" of "**Zero Downtime**".

- **High Availability (HA)** applications are very important but can sustain a short outage without violating their recovery time contract clauses (usually recovery must be accomplished within 2 – 72 hours of the disaster event). HA application recovery is conducted using a **Failover / Failback** approach, where the HA application would Failover to a secondary site when a disaster event occurred and then Failback to the primary site when the disaster event is over. HA applications that pass recovery testing are considered "**Recovery Certified**".

The Recovery Certification process is comprised of the following steps:

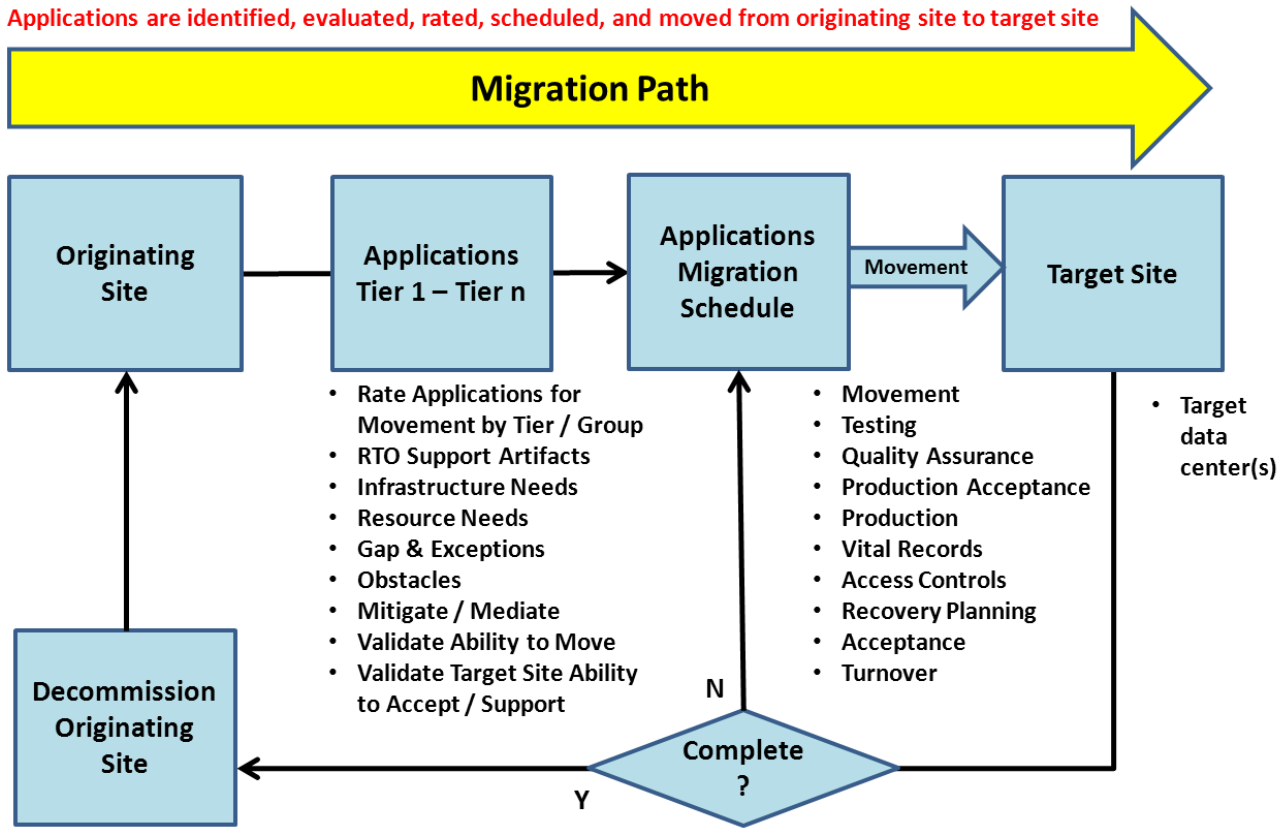
- Validating that an applications claimed Recovery Time Objective is correct and supported by accepted artifacts (i.e., SLA, Client Contract, Key Performance Indicators, BIA, etc.);
- Insuring that Infrastructure and Resources needed to support recovery operations are at the recovery site (as validated by Engineering and Infrastructure groups); and,
- Testing is performed as planned to validate successful recovery (Certify if passed, or reject to fix uncovered problem);
- Repair any uncovered gaps, exceptions, or obstacles that impede successful Recovery Certification;
- Re-Test application for Recovery Certification (repeat this and previous step until Recovery Certification is achieved)

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, in support of mergers, 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.

Figure 37: Migrating applications between locations



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.

Job Documentation process

Jobs must be documented at every step of their life cycle, including:

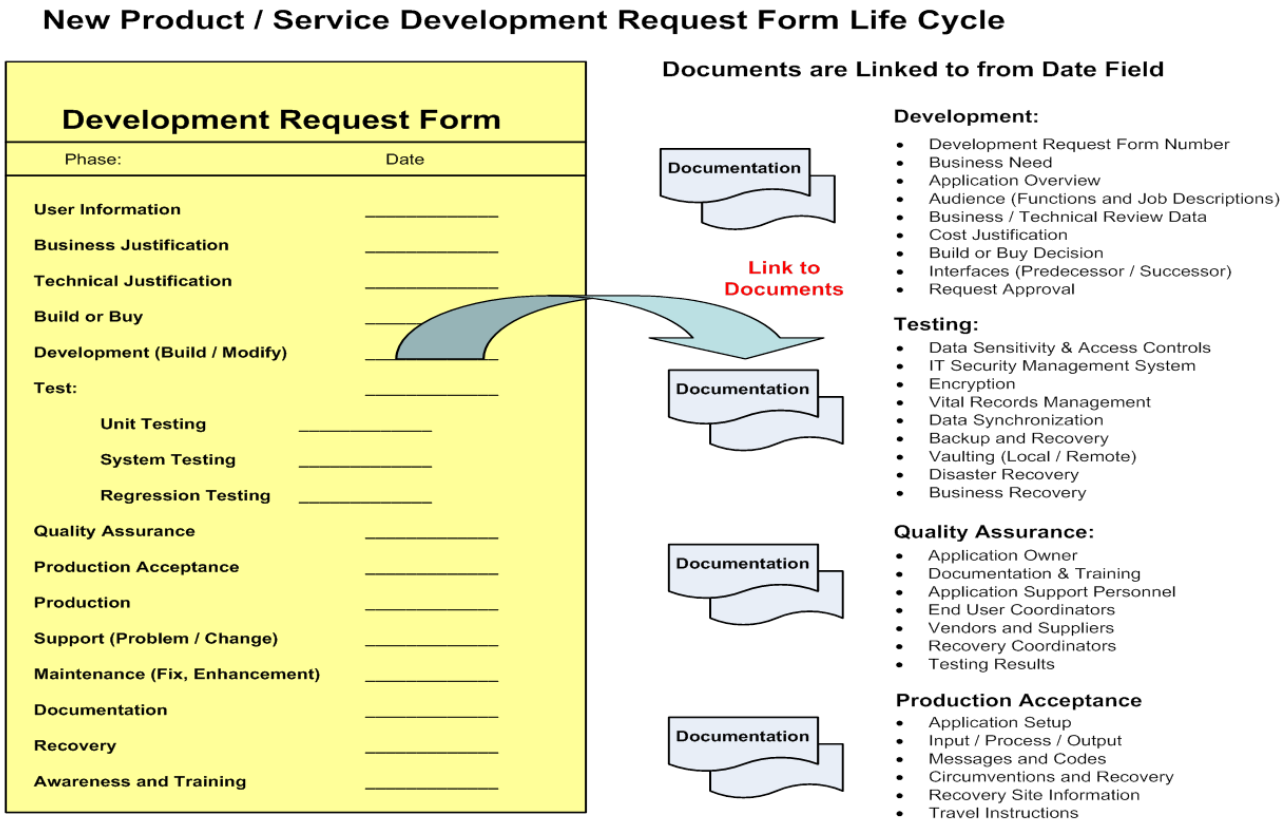
- **Development** – forms include critical information about goal of the job and the programs included in the job,
- **Testing** – modular testing through full system testing to run test data and produce all messages,
- **Quality Assurance** – inclusion of all required documentation and successful test results,
- **Production Acceptance** – instruction for populating the production environment and safeguard information,
- **Production Processing** – processing instructions for normal and disaster situations,
- **Support** – personnel who are responsible for isolating and repairing problems from Help Desk personnel through internal Subject Matter Experts and external Vendor Support,
- **Maintenance** (Enhancements, problem repairs, new technologies, etc.) – taking a copy of existing production environment and implementing changes as dictated,
- **Version and Release Management** – raising the Version and Release number to be one higher than the current production copy so that they can be identified and all components grouped together,
- *Re-Testing*, Quality Assurance, Production Acceptance, Production Processing.

The originator provides information on:

- Reason for Job and its Criticality;
- Ownership and Contacts;
- Vital Records Management (Data Sensitivity, Access Controls, Recovery Time Expectations, Data Back-up cycle and techniques, Data Recovery cycle and techniques)
- Recovery Management (Disaster Recovery facility requirements for Information Technology, Business Recovery requirements for business locations, Application Categorization into High Availability (HA) or Continuously Available (CA) status and importance, etc.);
- The people responsible for development and maintenance of this job use the Systems Development Life Cycle to achieve their goals;
- The people responsible for support and maintenance of this job use the Systems Management and Control System to perform their job; and,
- Recovery Management personnel use the customer supplied information to perform their recovery management rating and testing to insure job recovery support meets the needs of the company , end users, and owner.

Development and Maintenance Forms

Figure 38: Job Documentation Requirements



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

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

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

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

Job Run Books

Jobs require information inputs, in a specific sequence and format, to process through their programs and produce the desired output. To insure that this process is accomplished, Job Run Books are included with new or upgraded jobs entering the production environment. Job Run Books specify:

- What the purpose of the job is,
- The jobs required Inputs and Job Scheduler processing position (predecessor / successor),
- Required Input Tapes and files (file requirements are sensed by the scheduler and used to trigger and activate jobs when all required predecessor files are available),
- Operator messages and Replies during normal processing,
- Error Messages and Codes Manual entries (what problem is, possible causes, actions to be taken),
- Job Recovery Procedures (if job fails during processing, then input files must be reset and used from the recovery point of failure going forward),
- Error Circumvention Techniques,
- Normal Job conclusion message or condition (notify successor jobs that appropriate inputs are ready),
- Job output procedures for; breakdown, validation, and distribution to clients.

Job Messages and Codes Manual

The operator must know if an error condition occurs during job processing, which is displayed in either a message (Write to Operator, or Write to Operator with Reply) or code (Condition Code associated with end of job step (usually anything above zero is an error code, but low codes may not be significant but rather warning alerts that exceptions occurred and should be examined).

A Messages and Codes Manual will:

- **List** all of the Messages and Codes that a job can generate,
- Explain the "**Possible Causes**" associated with this Message or Code; and
- Provide "**Actions to be Taken**" instructions that should be followed when this condition occurs, including:
    - Circumvention techniques to be followed,
    - Contacting Supervisor for instructions,
    - Contacting the job owner for instructions,
    - Writing a Trouble Report,
    - Activating a recovery plan if the problem can cause a disaster or prolonged outage.

Successful Job Output Processing

Validate Output,
Break-Down output into deliverable packets of information, and
Distribute output to clients as instructed.

Information Accounting and Charge-Back System concept

Figure 39: Charge-Back system

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

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

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

Total Cost: $ _____

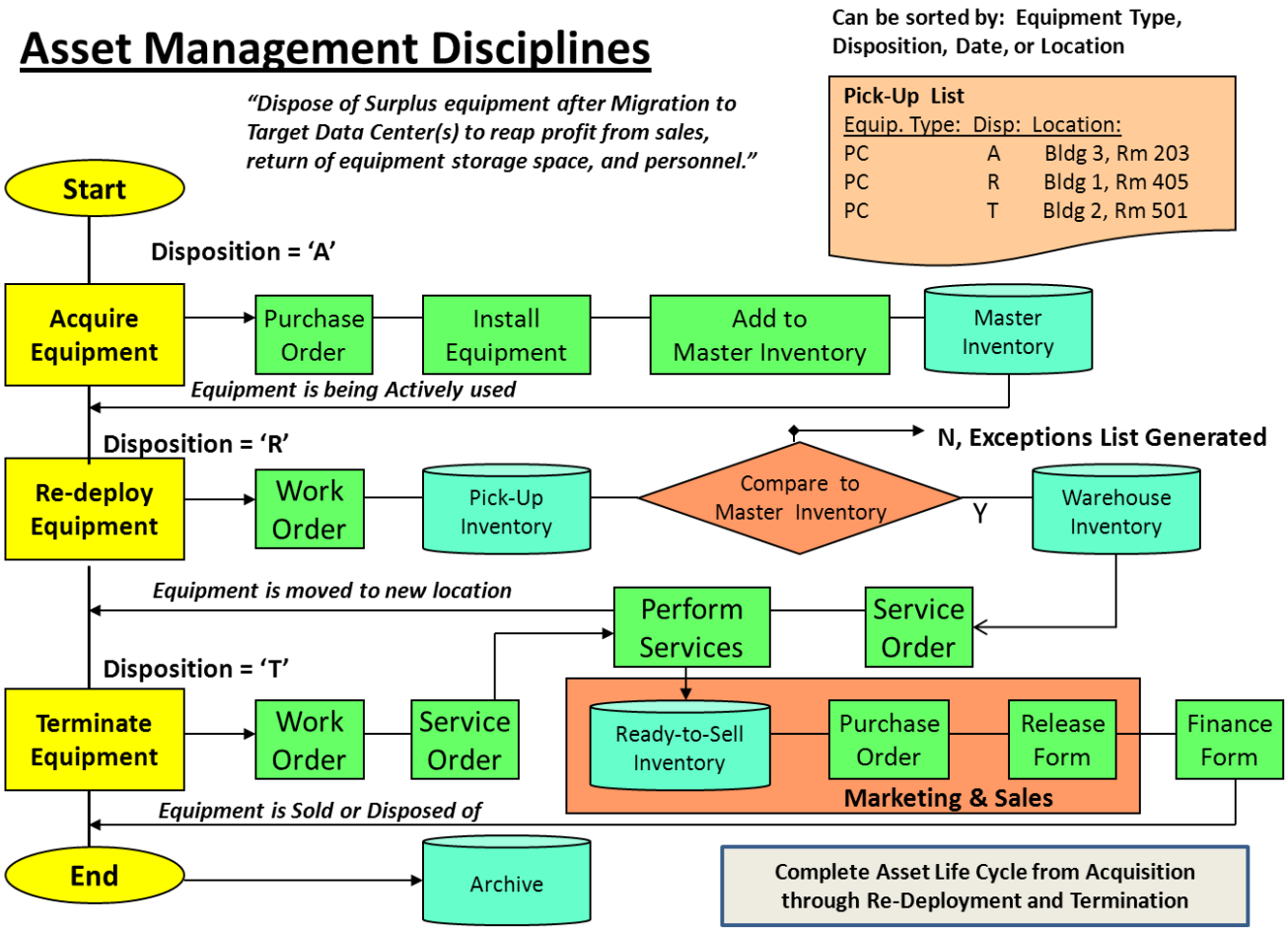
Bill can be generated via Forms Management, Time Accounting, or Flat Cost for Services. This system can be used to predict costs for future projects and help control expenses and personnel time management.

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

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

Asset Management (Asset Acquisition, Redeployment, and Termination)

Figure 40: 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.).

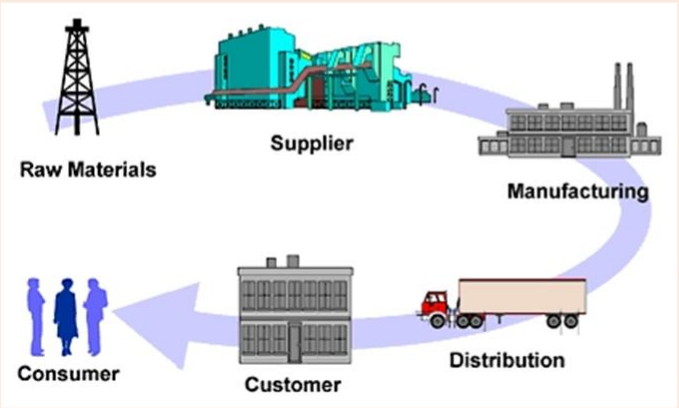
When the asset is updated due to repairs or enhancements, the asset status is updated to reflect the change. Should an asset be redeployed, because the user left the firm or the product is moving to a new location, then data must be erased from the private drive and updates made to the asset profile. 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.

Supply Chain Management

Figure 41: 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. This could interrupt your revenue stream and lead to the close of a business.

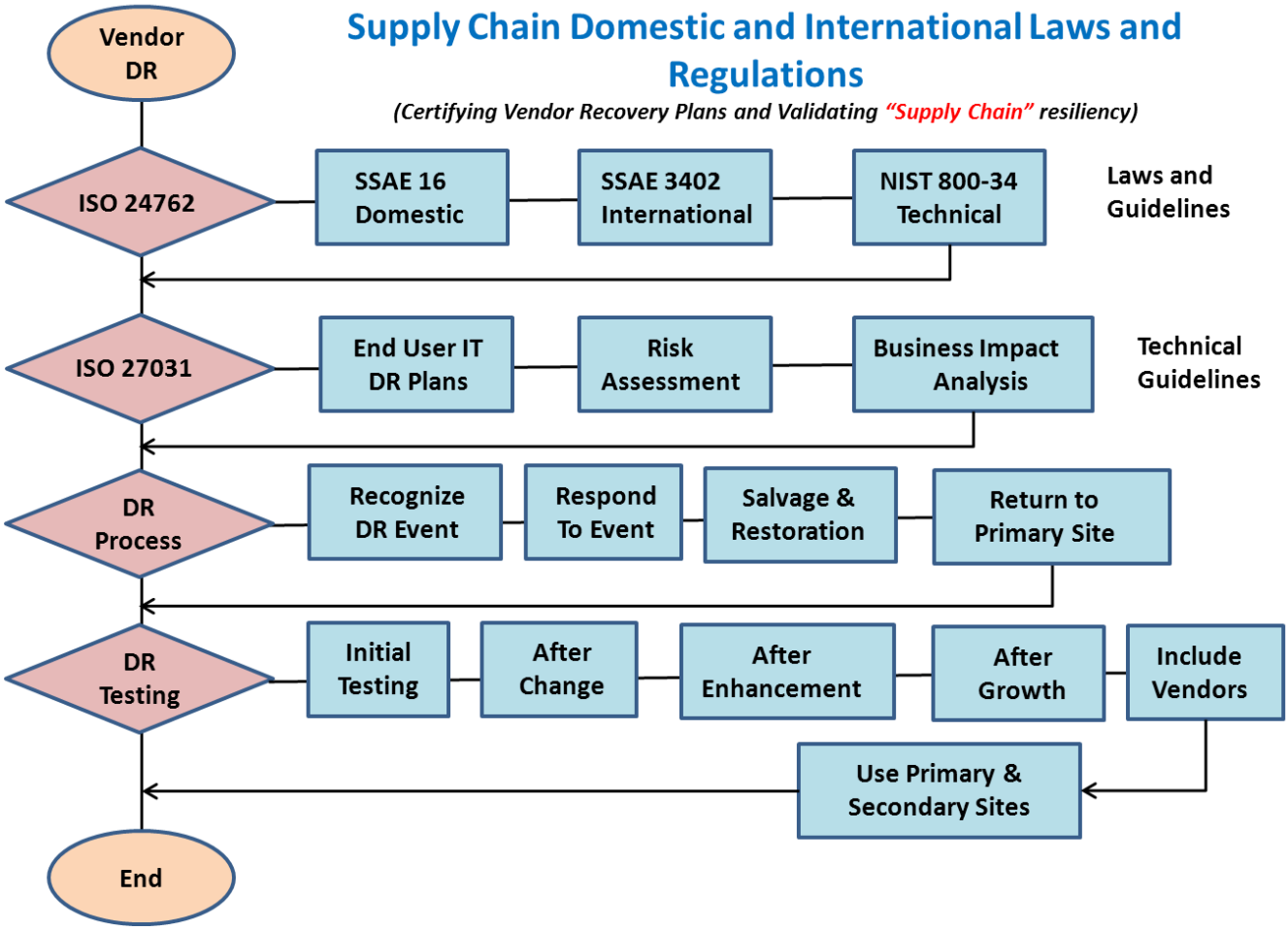
For the reasons mentioned above, it is important that you pay attention to supply chain management so that you can quickly become aware of any failures and take appropriate actions to protect your business operations and continue to provide products and services to your clients.

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

The illustration below lists the Laws and Regulations associated with Supply Chain Management that were created by industry experts to help organizations validate the supply chains ability to provide supplies and goods even when a disaster event occurs for you or them.

Figure 42: Supply Chain Management (Flowchart)



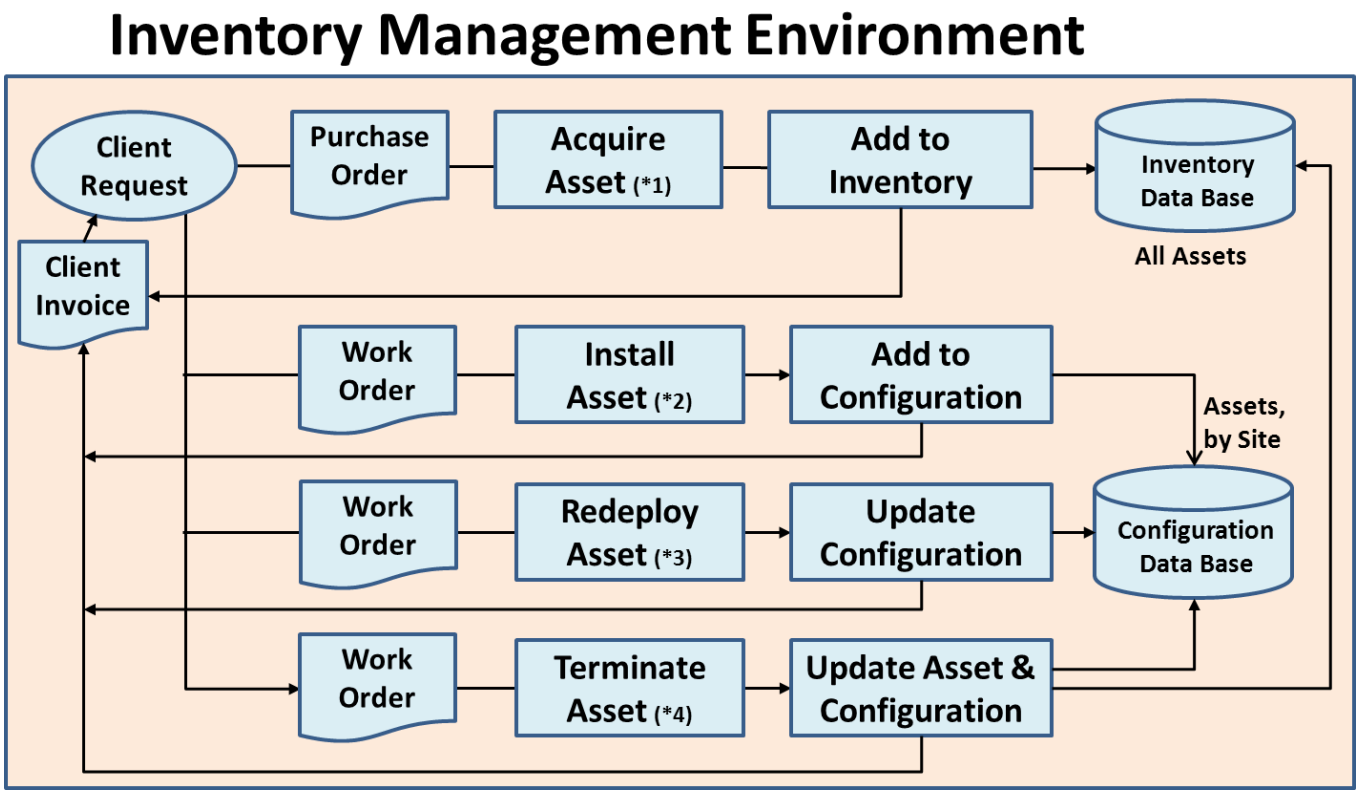
Laws and Guidelines associated with Supply Chain Management include ISO 24762, SSAE 16 (Domestic Supply Chain Management) and SSAE 3402 (also known as ISAE 3402 – International Supply Chain Management) and NIST 800-34 (National Institute of Standards, ISO stands for International Standards Organization).

Technical Guidelines on how to achieve adherence to the Laws and Regulations are provided in ISO 37031 and the DR Process should include adherence to these Supply Chain Management requirements so that needed supplies can be received at either the normal or recovery site.

Employee awareness regarding Supply Chain Management should be made available and validated periodically when DR testing is performed.

Inventory Management System Overview

Figure 43: Inventory Management System review



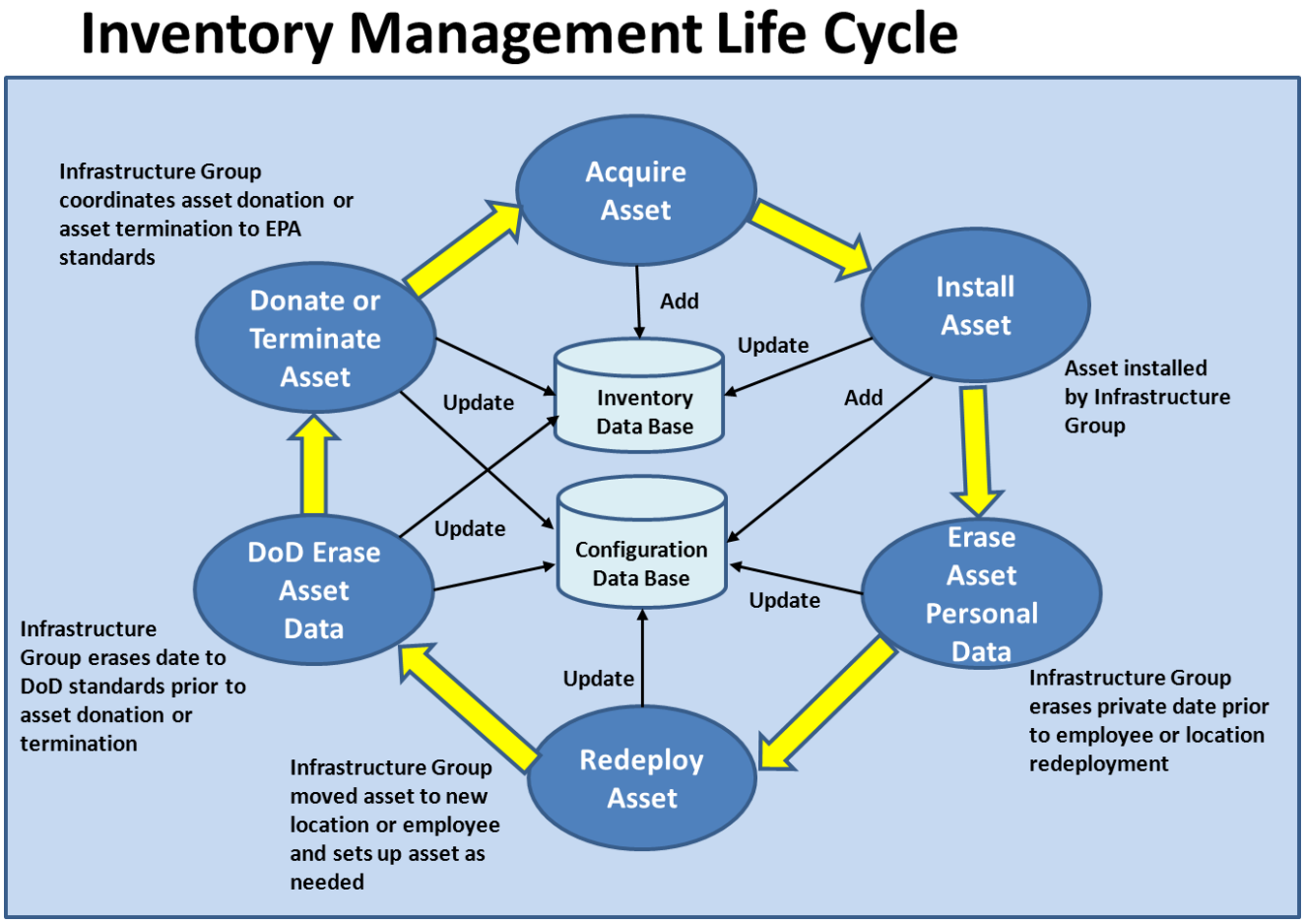
*1 – Purchased Equipment as per guidelines (Leased, Owned, Rented, Type, and Vendor).
*2 – Infrastructure Group schedules and installed Asset.
*3 – Assets are moved from one location to another or reassigned to staff with work performed by the Infrastructure Group.
*4 – Asset are terminated and data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

Inventory Management is the process of tracking inventory that has been received by vendors and stored at a location until its use is needed. A warehouse or physical location at a company site can be used to store inventory when not in use, but if a device is being used than where the device is and its identifying characteristics (Part Number, Serial Number, RFID Identifier, or simply a company identification sticker) should be recorded in the Inventory Management System

The Inventory Management System can provide valuable cost and evaluation information that can be used by management and facilities to calculate the best components to use or eliminate. For example, if you wanted to reduce data centers by combining operations from multiple sites through the use of new technologies whose capacity and performance is greater than the present inventory, then it would easy to evaluate the current inventory by costs (Rented, Owned, Leased) or horsepower (Memory, Age, Technology, etc.). Without an Inventory Management System this would be a very difficult task.

Inventory Management System Life Cycle

Figure 44: Inventory Management Life Cycle



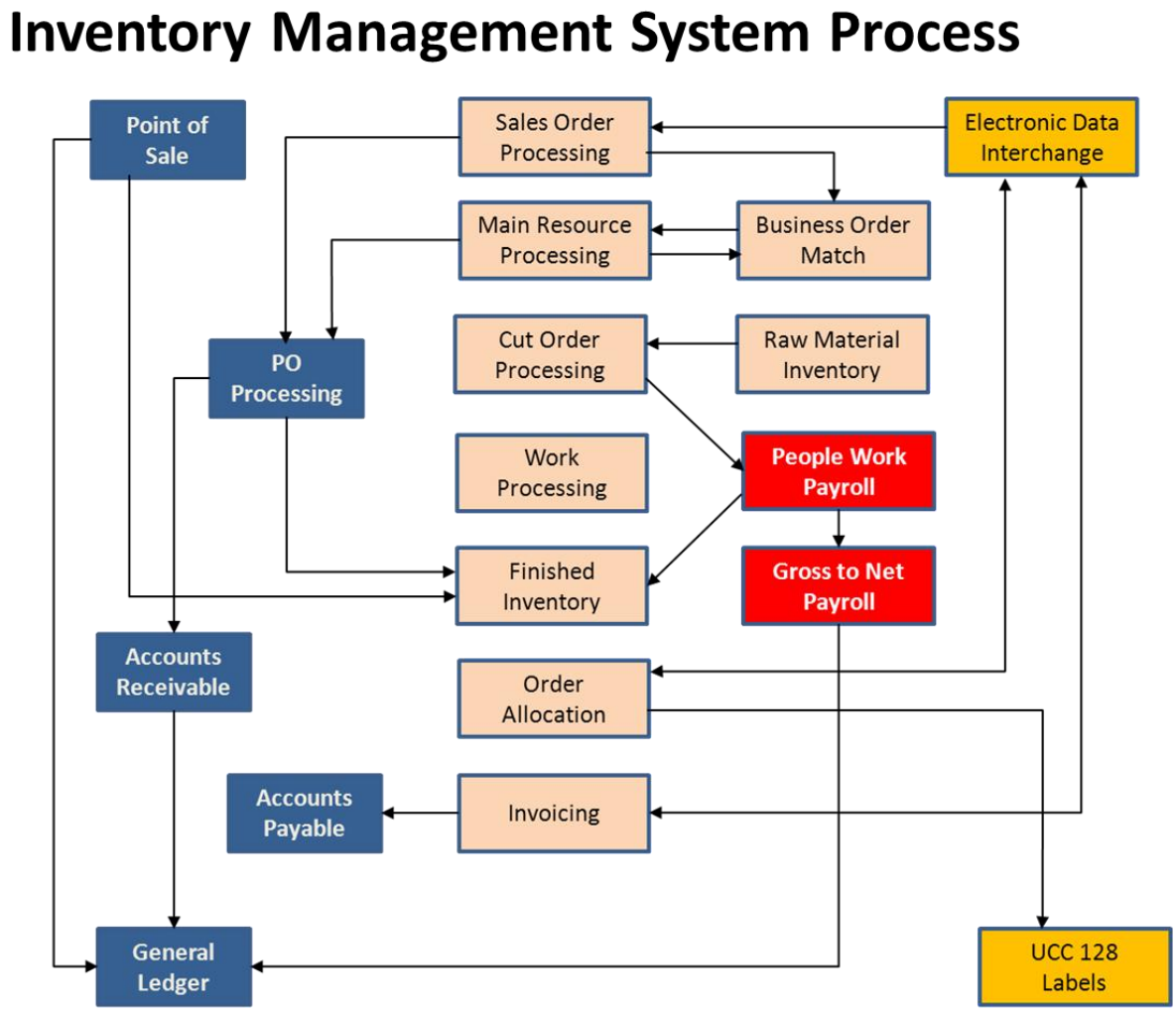
Inventory goes through a Life Cycle similar to the Systems Development Life Cycle. It is illustrated above, but basically inventory is either "Acquired", "Deployed / Re-Deployed", or "Donated / Terminated". Each of these cycles has a manpower part to it, in that equipment is delivered, inventoried, shipped, installed, tested, turned over and supported via the "Acquisition" process.

When equipment has to be moved because an employee left or the device is being shipped to a new location, then personnel become involved by: erasing any personal data that should not reside on the device, packing, scheduling, and moving the device, unpacking, set-up, testing, and turning the device over to the end user.

When a device reaches the end of its life cycle (usually devices are replaced every four years), they can be donated to a charity where the company receives a tax break, or terminated and disposed of. In either case critical data should be erased following the DoD (Department of Defense seven step erasure process) regulations for data erasure. When terminating a device for disposal, EPA rules and regulations governing land fill and hazardous materials and superfund clauses should be followed or you may expose the company to large fines and a bad reputation as a polluter.

Inventory / Warehouse Management and System Process Flow

Figure 45: Inventory / Warehouse Management and System Flow



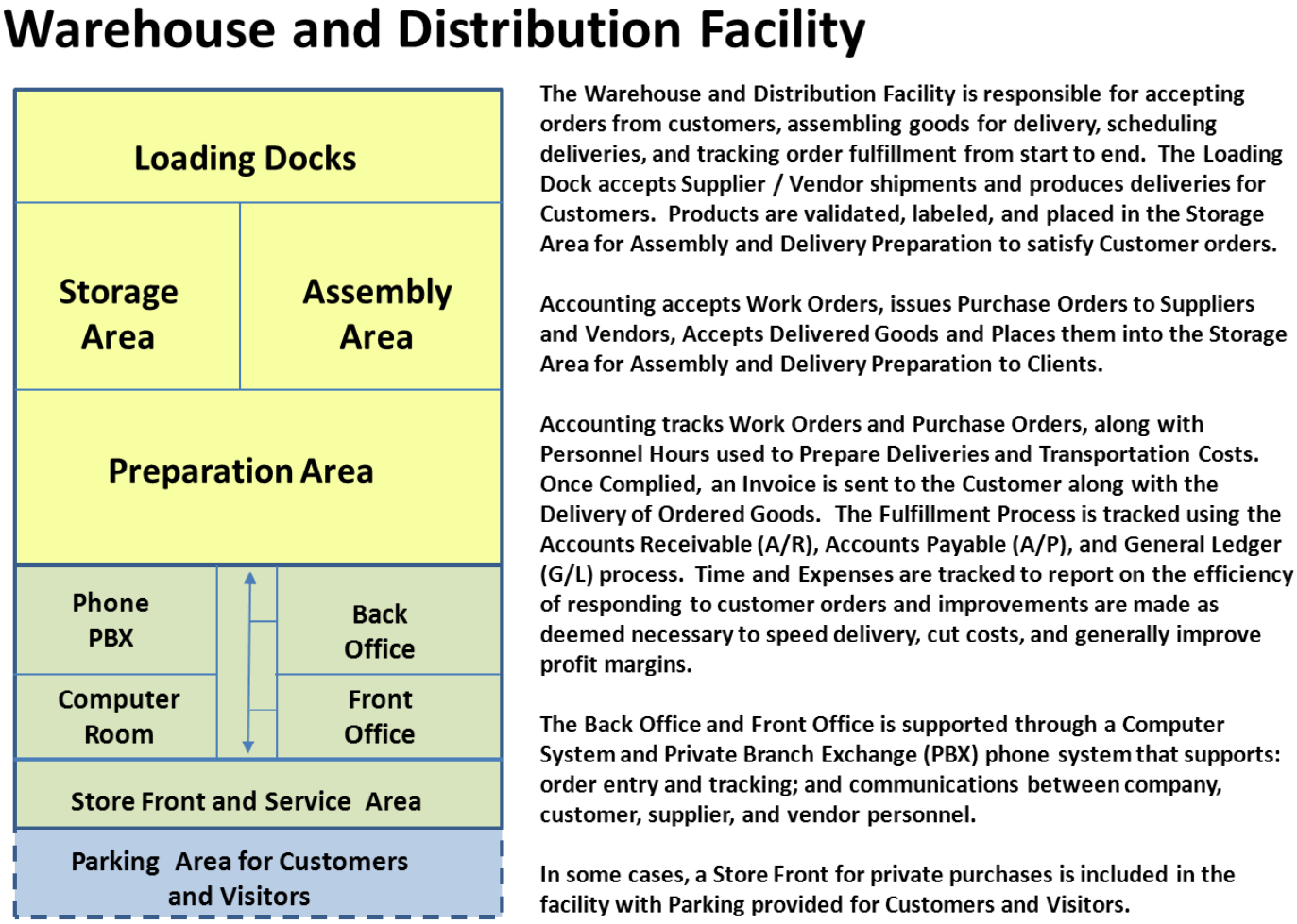
A fully implemented Inventory Management System is shown above. It shows how inventory is ordered, processed through the organization from loading dock, to warehouse shelf or storage location, and through the payment process and accounting. Items can be ordered via Electronic Data Interchange, the web, a phone call, or through a sales representative.

Supplies are accounted for within the normal accounting system components of Accounts Receivable (A/R), Accounts Payable (A/P), and General Ledger (GL). Supply costs are maintained in a reporting system using accounting system information to determine the costs, delivery times, install times, and general life cycle of supplies.

Equipment and Supplies are labeled for tracking and inventory purposes. These labels can be simple stickers, or RFID (Radio Frequency Identification) tags.

Warehouse, Distribution, Facility and Wholesale Storefront example

Figure 46: Warehouse, Distribution, and Storefront Facility example



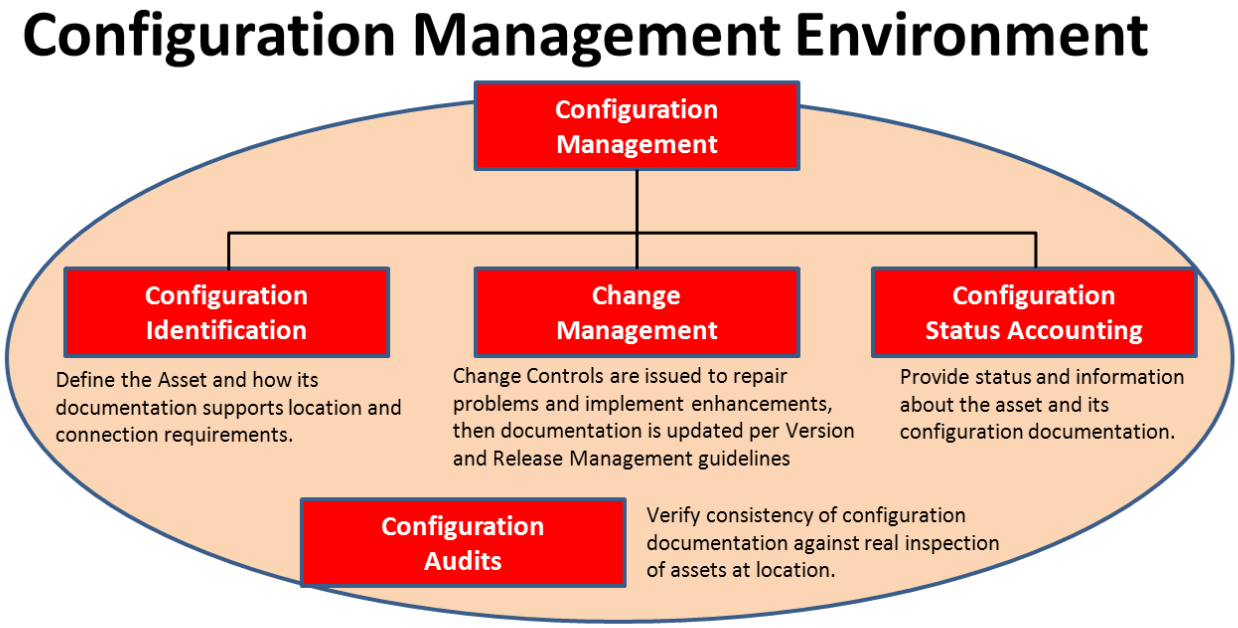
Orders are received via computer facilities, customer phone calls, or walk-in customers. The orders are:

- Pulled from the Storage Area;
- Their Label Scanned to update Inventory;
- Provided to the Assembly Area for order validation and identification;
- Sent to the Preparation Area for packing and packaging (Mailing Labels are used for deliveries);
- Accounted for via A/P, A/R, and G/L;
- Order is delivered and revenue collected then accounted for to accomplish fulfillment;
- Order could be picked up and paid for by customer at front desk; and,
- All Accounting and Inventory Records are updated and actions taken as deemed necessary to maintain stock and collect receivables, or make payments to suppliers and vendors.

This example is widely used for Small to Medium Sized firms, as well as large corporations and is considered an industry standard for “Best Practices”.

Configuration Management System Environment

Figure 47: Configuration Management Environment



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

Enterprise Computing Environment and its Evolution

Initially computing was performed on Tape Operating Systems (TOC), then Disk Operating Systems (DOS), Operating Systems (OS), and Virtual Storage Systems (VS, VS1, MVS, zOS, etc.), which is an evolution based on how memory is used to support a single or multiple applications. When the Personal Computer (PC) was introduced, everybody could take advantage of computing power to support their everyday needs. In the business environment, the use of PCs became rampant (three stage growth cycle associated with new technologies is – Acquisition, Rampant Growth, Control). In order to gain control over this rampant growth, reduce costs, and improve security, Servers and Thin Clients were introduced to separate resources into compartments that where cheaper and could be better secured. For example:

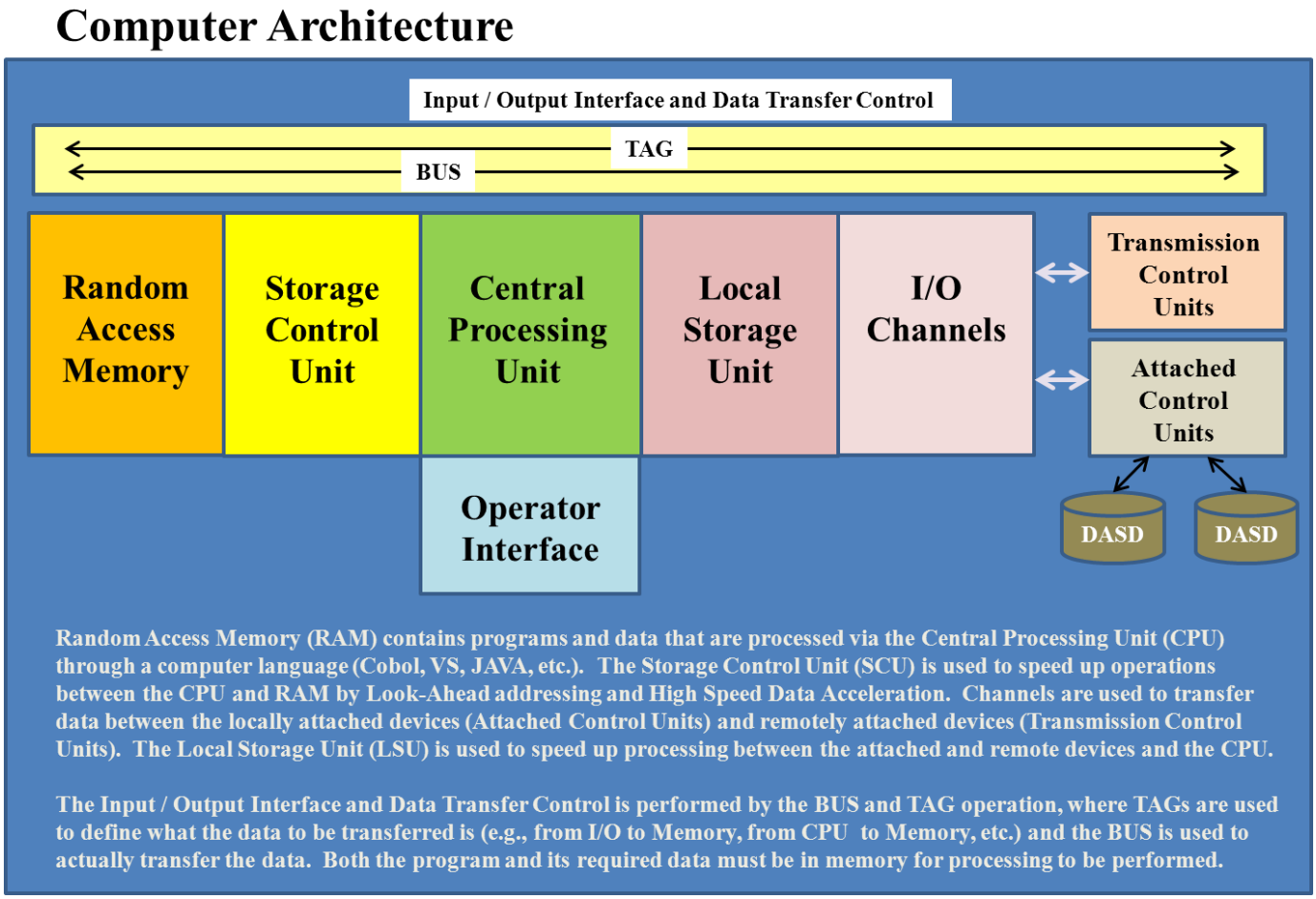
- Printers were pooled off of a server and authorized personnel could print documents on the printer best suited for their needs (locally, or remotely);
- Data Storage devices were limited to the server, with the exception of a local disk to support personal / private processing, but removing of data via Thumb Drives or other media was eliminated;
- Data Encryption was also utilized to further safeguard data;
- Personnel could access the system from any accessible location if the need arose (i.e., presentations in conference rooms there their own PC was not available);
- The Server Administrator would provide programs that the user needed to perform their job function, but would place restrictions on what the user could access (no outside locations that were not authorized by the enterprise, but perhaps sites like Google were allowed to support research);
- Eventually, mainframe systems provided access to PCs through Servers so that distributed processing could be better performed;
- Then a multitude of Web Enabled applications were created to make it easier to support end-user and client demands;
- A separate Internet (outside users) and Intranet (inside users and company personnel) were created to better distribute information and support operations;
- The evolution of Enterprise Computing has grown into a diverse and complex configuration, where access controls are used to compartmentalize the enterprise to restricted zones that can only be accessed by authorized personnel;
- Because of the importance of corporate data and its user base, the need for security has never been higher and today's technologies must be constantly upgraded to better safeguard the Information Technology infrastructure without degrading performance;
- Finally, Regulators became involved with Enterprise Computing because a company may be "too big to fail" or provide information services that are essential to supporting a community of users and government organizations;
- The following illustrations and narratives try to show how this goal of a Safeguarded and Efficient Enterprise Information Technology Environment can be achieved that is in Compliance with all of the Laws and Regulations of the countries where the Enterprise does business.

Enterprise computing has matured from hard metal mainframes devoted to a single user to virtual environments used to support many users. We even utilize Cloud Computing (its real but based on IP addressing and Web access, hence the term Cloud) to support production and recovery operations.

This section will try to provide information regarding Enterprise Computing and its end goal.

Computer Architecture Overview

Figure 48: Computer Architecture Overview

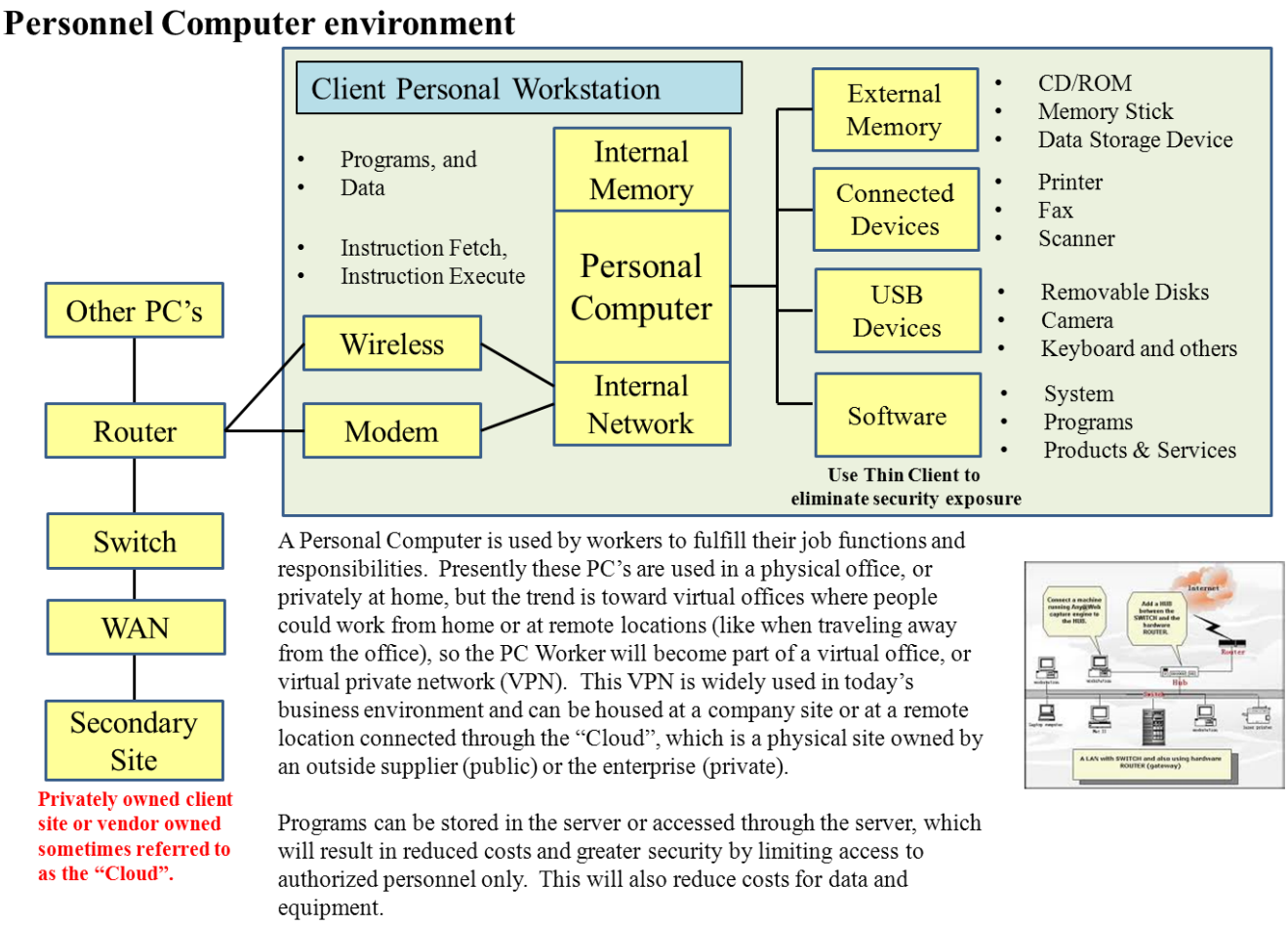


The above illustration shows how a computer's architecture is designed to allow programs and data to be moved from external devices to Random Access Memory (RAM) where processing can be accomplished by the Central Processing Unit (CPU) using a computer language that has been complied into machine language. The CPU can process three types of operations, which are: Computer Memory to External Device or Memory to Memory operations (1 ½ words long), CPU to Memory (1 word long), and CPU Register to Register (1/2 word long) operations. The Local Storage Unit (LSU) and Storage Control Unit (SCU) are used to accomplish speed matching between the CPU (the fastest component of a computer) and Memory or Devices (slower components of the Computer). This architecture applies to all computers, from mainframe to Personal Computers.

Communications between computer programs and the operator are accomplished via Write to Operator (WTO) and Write to Operator with Reply (WTOR) messages. The operator can control program initiation, class, and priority settings that allocate computer resources used by processing applications. He resides in the Operations Control Center (OCC) and reports encountered problem to the Help Desk. The Network Control Center (NCC) monitors Transmission Control Units (TCU) and remote communications, reporting encountered problems to the Help Desk.

Personnel Computer Environment

Figure 49: Personal Computer Environment



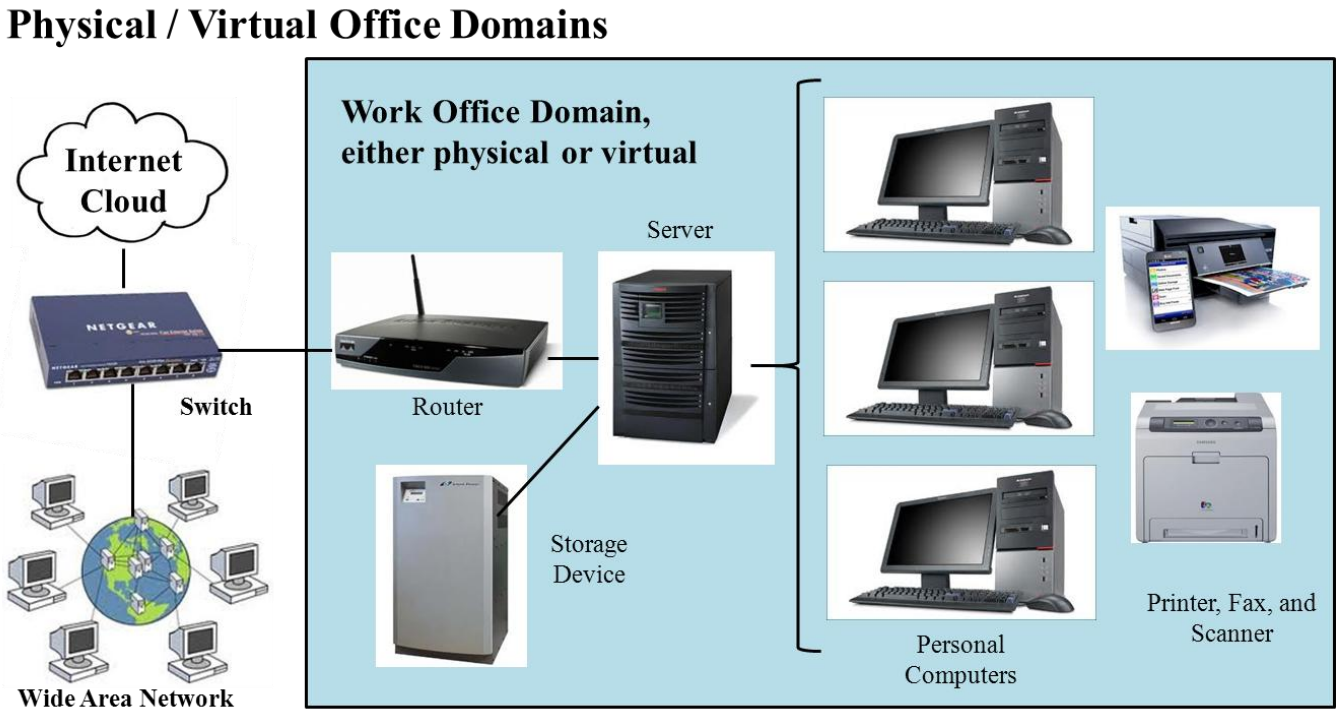
Personnel Computers have grown over the years from a simple Disk Based Operating System (DOS – Disk Operating System) where programs and data had to be loaded into memory via floppy disk drives using a basis 80-80 processing system (computer card based) to a VMware based system using Virtual Memory Partitions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

As time went by, the devices connected to a 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 50: Physical / Virtual Office Domains



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.

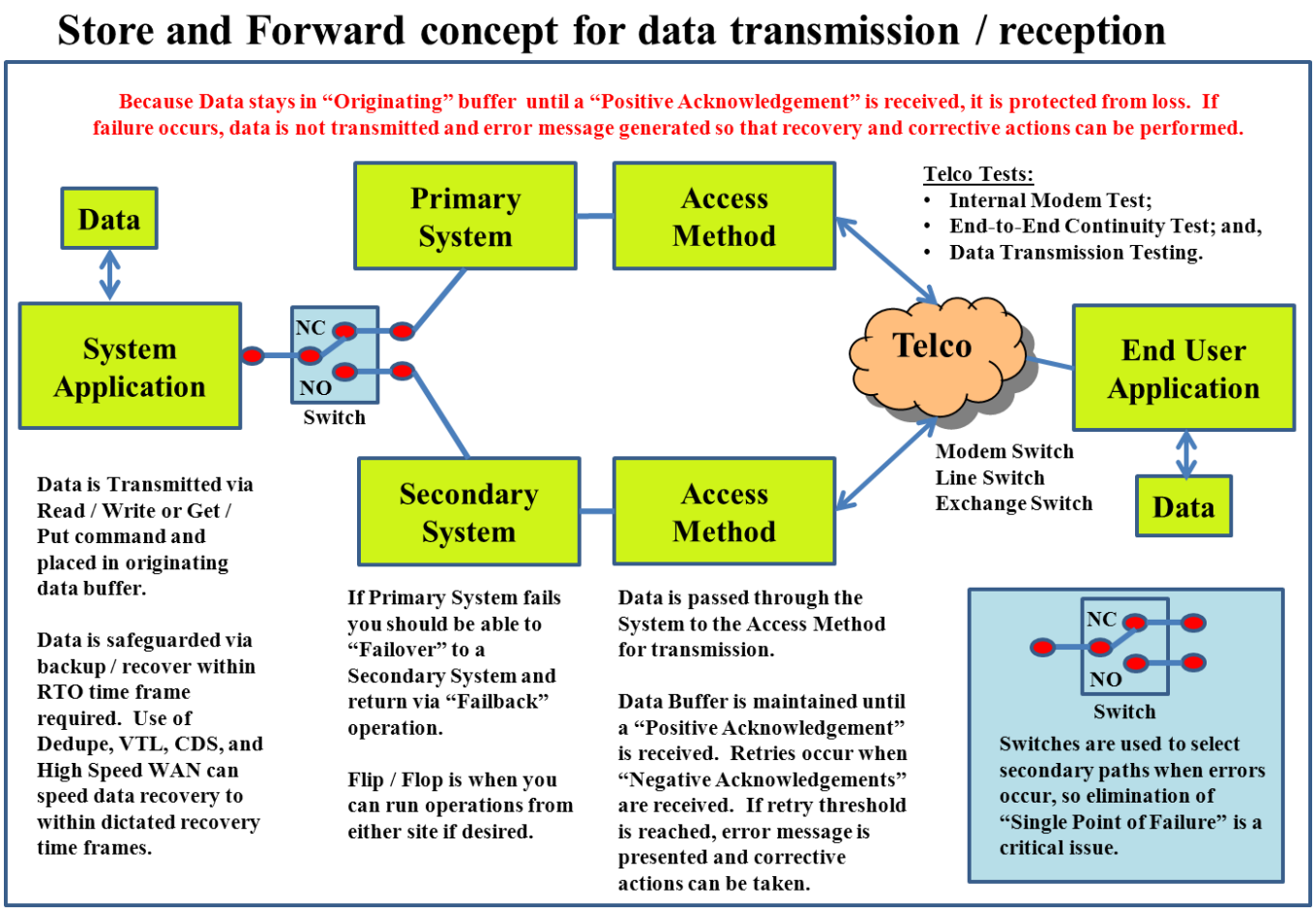
Utilizing this approach eliminates the possibility of personnel downloading data onto transportable media that can be taken off-site and used to expose company secrets or sensitive information. Also, taking personal data away from a protected company environment may result in Identity Theft and large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

The Thin Client environment protects 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 provides 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 51: Data Transmission between programs and devices



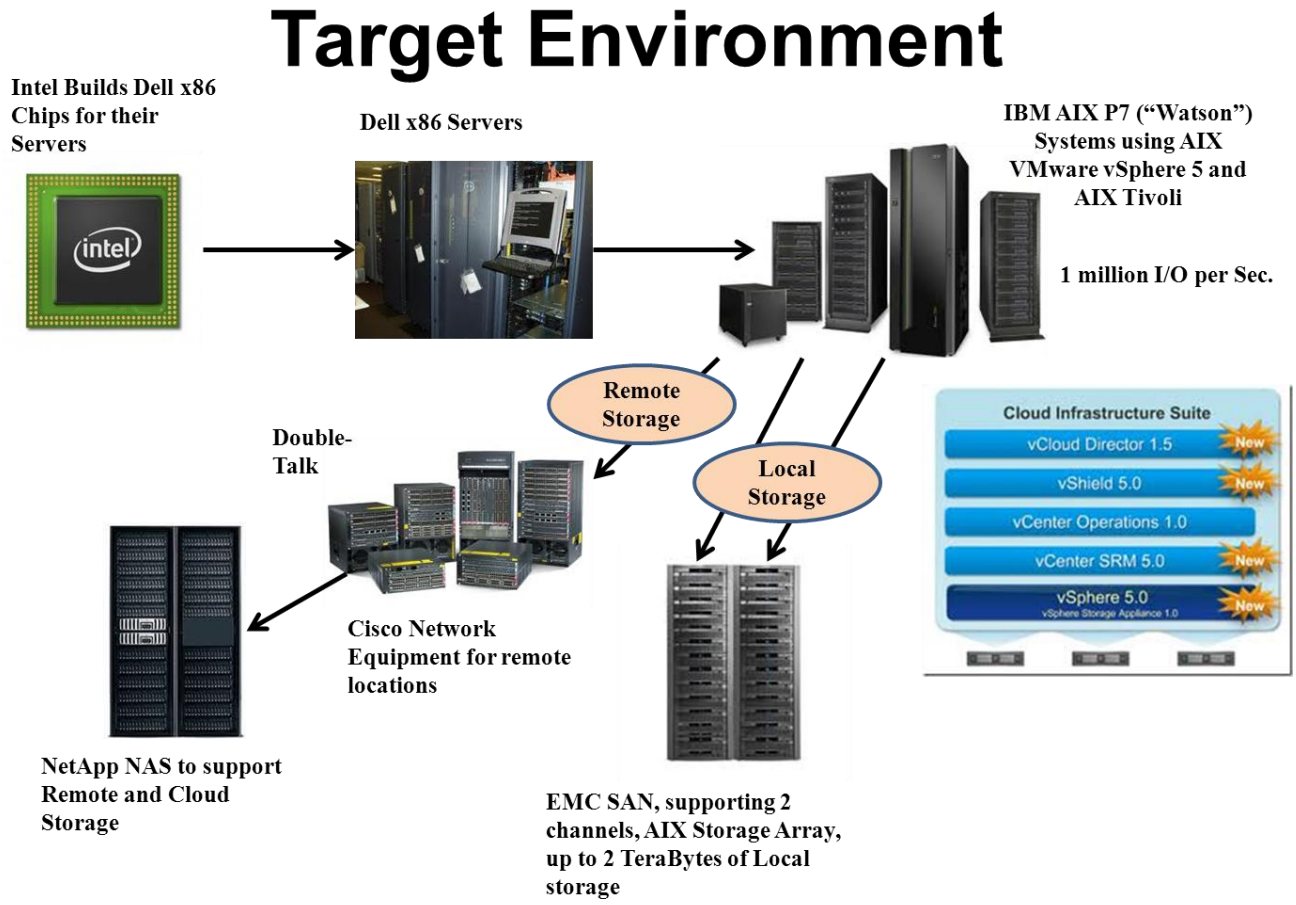
The "Store and Forward" method used to transfer data between programs and devices is shown above and used to ensure the safe arrival of transmitted information.

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 System Target Environment

Figure 52: Sample IT Target 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 provide business operations.

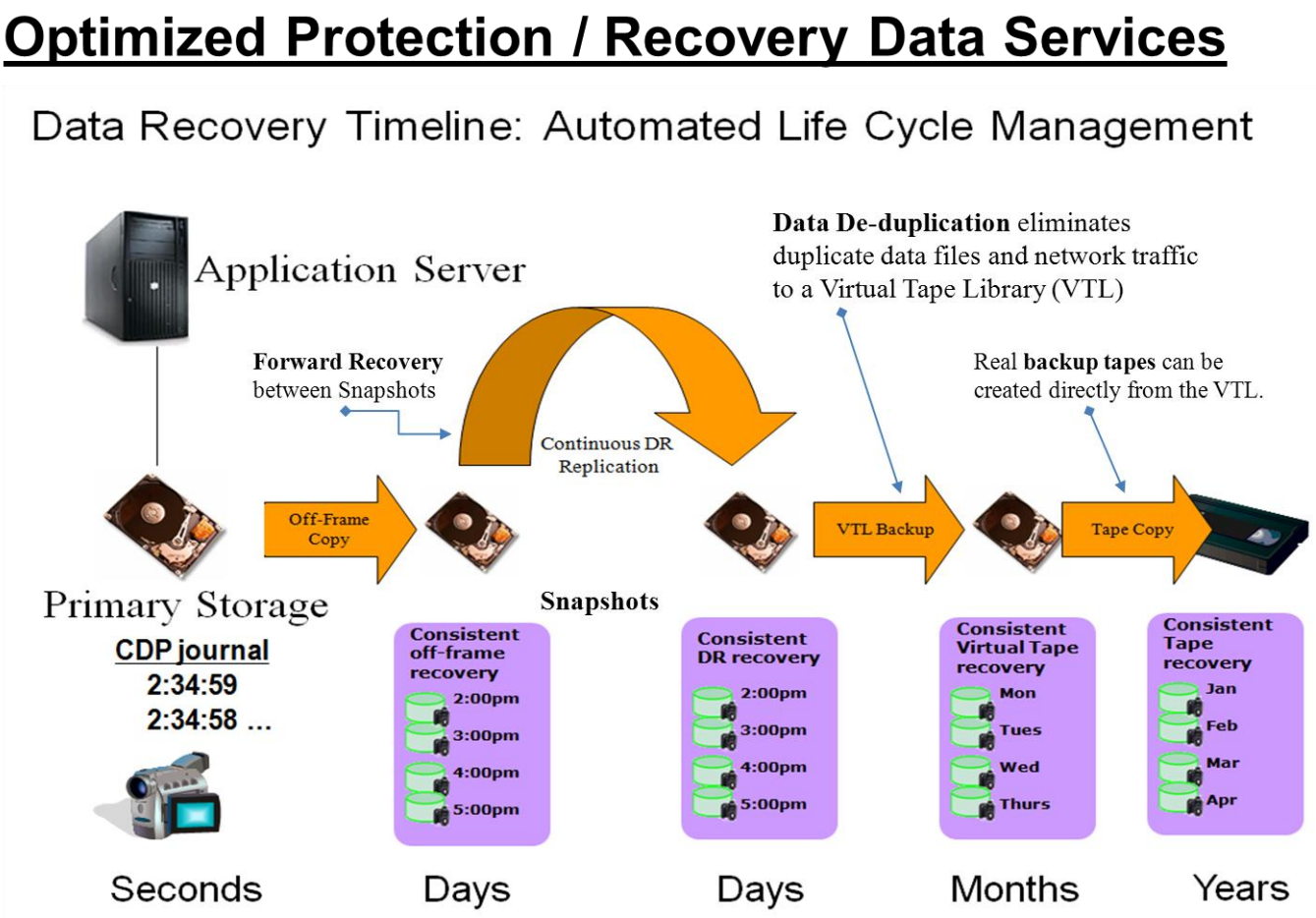
By incorporating the vSphere 5.0 environment the client can host multiple virtual server environments within a single physical server, or server cabinet. The vSphers 5.0 system product directs traffic to the appropriate VMware system, vShield is used to provide security protections, vCenter Operations 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 53: Optimizing Data Storage and Recovery



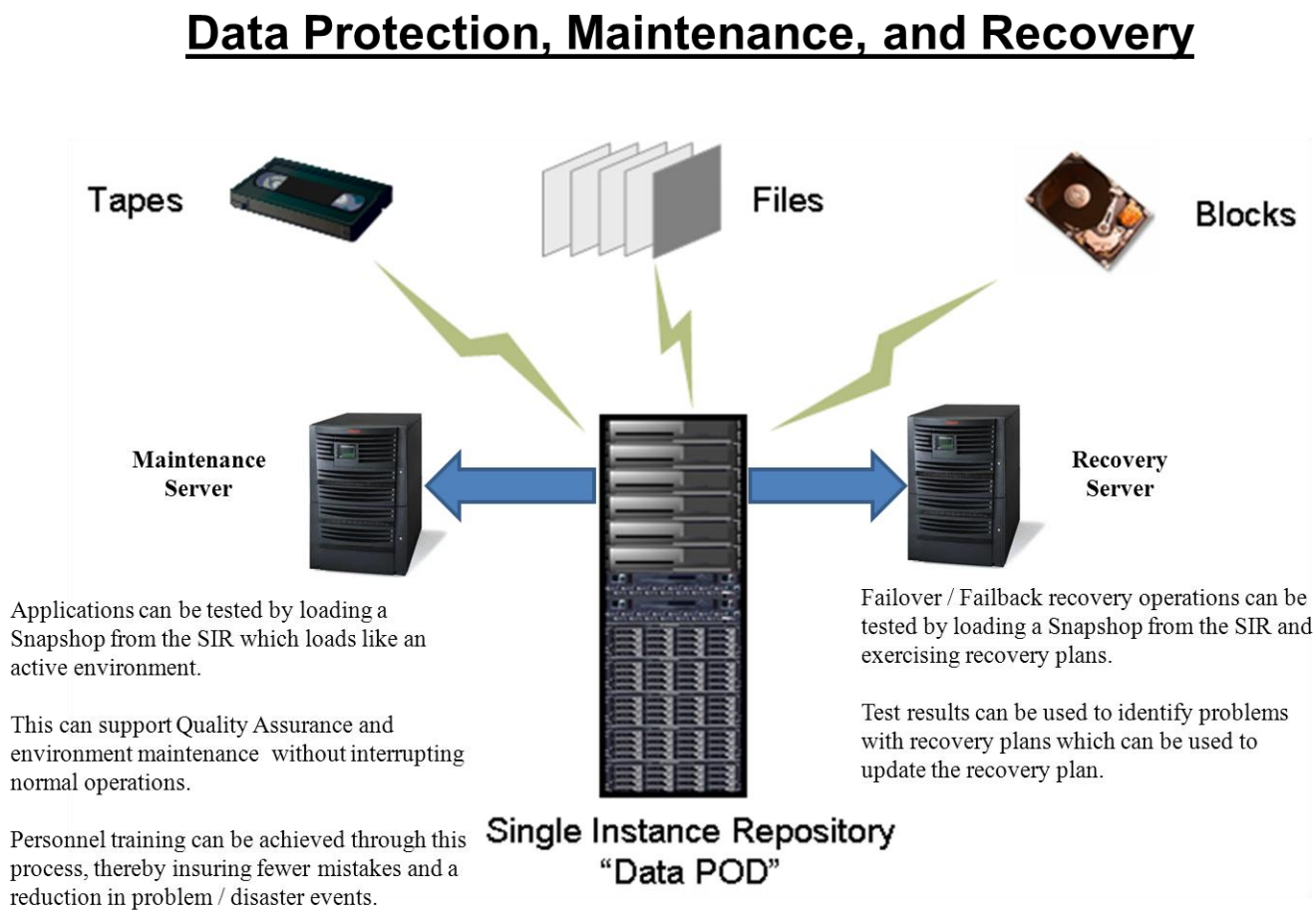
As systems become more important to the business, protecting and restoring data becomes crucial. Today's technology is shown in the above illustrations and includes:

- 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 54: Recovering Data and Restoring the Operating Environment



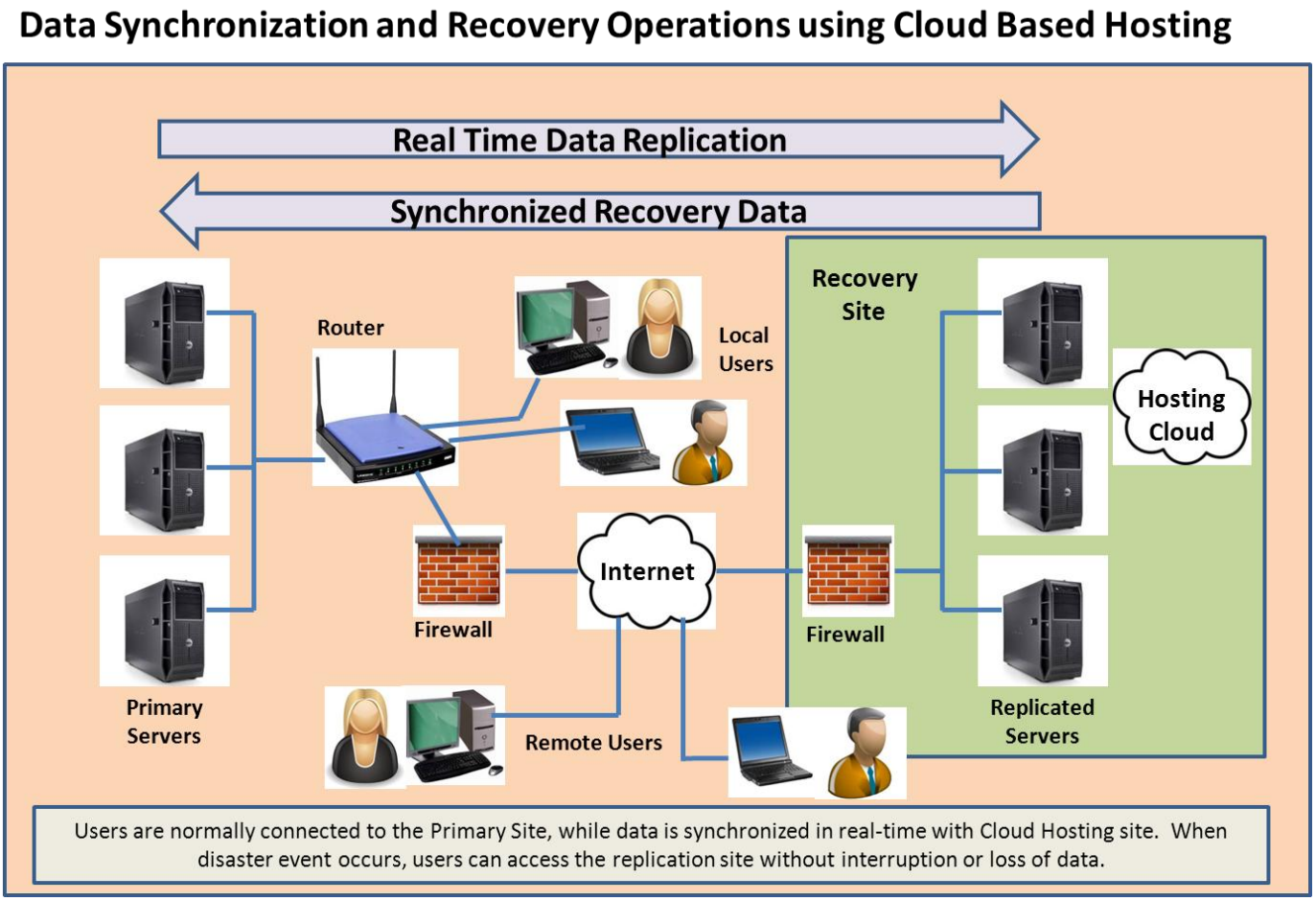
The use of a "Single Instance Repository (SIR)" will allow a company to go back in time to perform a recovery operation. This may prove essential when a virus is detected, because the only way to completely eliminate a virus is to go back in time just prior to the virus being introduced and then performing a "Forward Recovery" from that time after eliminating the virus.

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.

Data Synchronization and recovery through a Hosted Cloud based environment

Figure 55: Data Synchronization and Recovery via Cloud Hosted Facilities



Many companies are now utilizing Cloud Hosting facilities (Private or Public) to support recovery operations. This method is gaining popularity as problems and fears about Cloud Computing are being resolved. A number of organizations provide this service today (Google Chrome, Microsoft Office 365, DropBox, etc.) that are transparent to users. It allows you to log-on and gain access to your data anywhere you are located and will probably be used by more organizations in the future.

In the illustration above, external and internal users can access the primary and secondary sites through their normal logon procedure and data is maintained in synchronization at both sites to support continuous business operations. This is an example of how a Cloud Hosted Facility can support business operations within recovery time expectations and should be examined to see if it can fit your continuity of operations requirements.

Some existing Cloud Applications allow for storing of your information in the Cloud along with maintaining it on your PC (like SkyBox and Chrome). This automated recovery approach has been running successfully for years and has allowed some vendors to provide its customers with a high level of protection against damage or loss of equipment. Additionally, the data stored in a cloud can be translated into any format used by your present or future devices, thereby guarantying that you will not lose data or have to perform the laborious work associated with translating information from one vendor format to another.

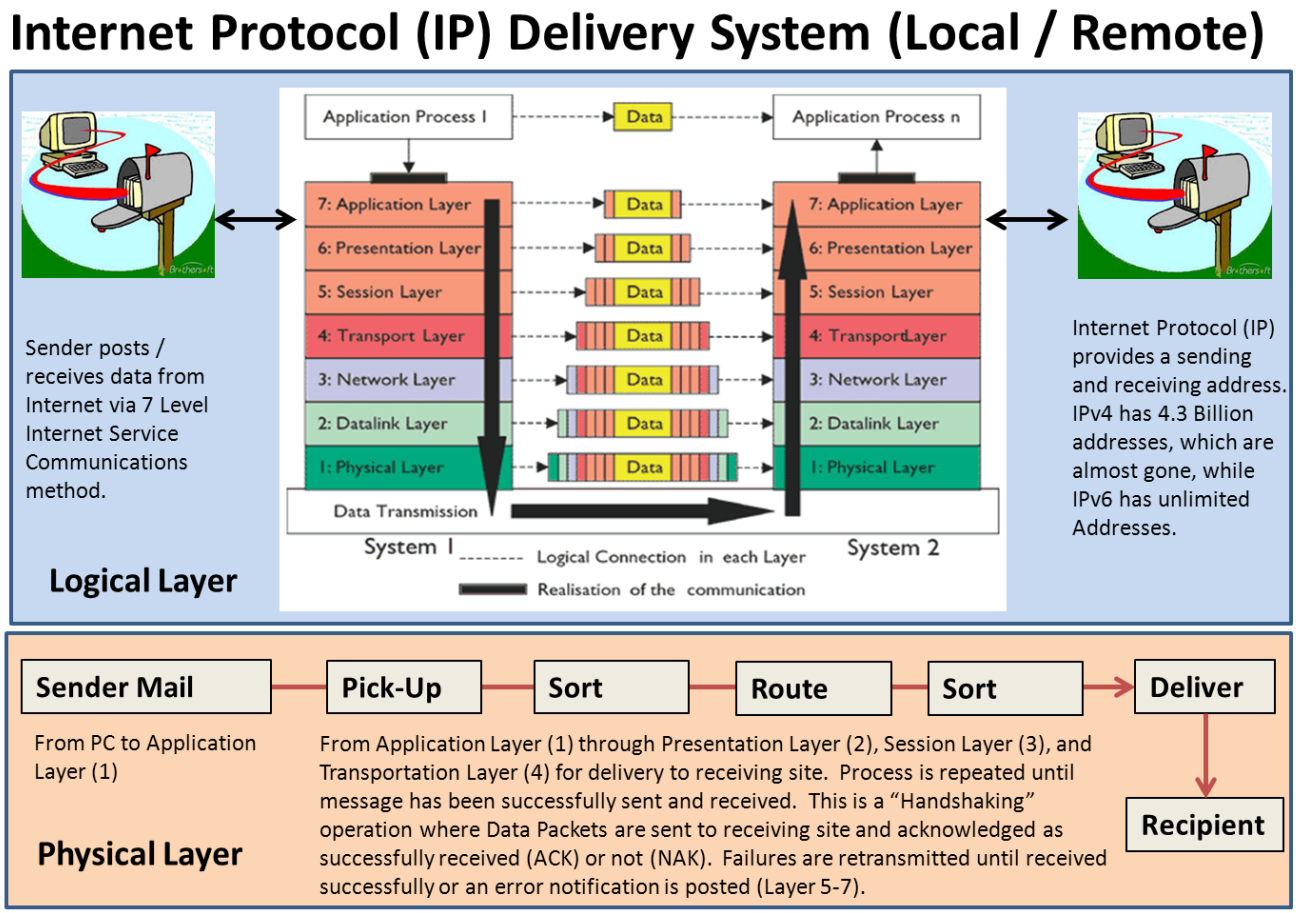
If you do not already use Cloud Computing and Virtualization then it is an option that should addressed. Cloud Computing uses IP (Internet Protocol) addresses to access their site and equipment rather than channels and I/O addresses used in data centers. This supports use of the Web to access and utilize your programs from any Web accessible location.

Virtualization allows you to take a single real server and divide its applications into parts, each assigned to a section of the virtual server. In this case a relationship is established between real resources and the virtual applications (in essence a resource management scheme). For example, if you have three applications that all reside on different real servers, you can combine them into a single virtual server (could be one of the existing real servers that has been reconfigured via a product like VMware) by relating the real servers' resources (memory, processing power, I/O configuration, etc.) through real control blocks and virtual control blocks (like sub-diving a real disk into virtual parts, etc.). Security is maintained by assigning a real control register to each of the virtual environment so that paging can be accomplished without interference from any of the other users. The memory Page Segment Table is pointed to by the hardware Control Register and pages are then pointed to by segments. This separation of hardware and software provides a boundary that cannot be crossed by other virtual users. It is a concept that has been in existence since Virtual Systems were introduced by IBM.

Using Virtualization can reduce resource requirements, reduce energy bills, and allow for the same or greater performance as previously received. It is an exceptionally good method for dividing applications that are time dependent (like an application that is scheduled to process during normal business hours with applications that process after close of business) that will allow for a single server to replace two servers immediately.

Internet Protocol and Data Transmission / Delivery Operations

Figure 56: Internet Protocol and Data Transmission / Delivery



Data is transmitted through the World Wide Web (WWW) like letters are delivered by the Post Office because they both have a receiving address and a return address (Header and Footer), but the WWW supports Internet Protocols requiring an Internet Address (IP Address) contained within a Domain (like a building where residents live). Each post box is like an IP address in a Domain and delivery validation is confirmed by an ACK (Positive Acknowledgement) or rejected by a NAK (Negative Acknowledgement).

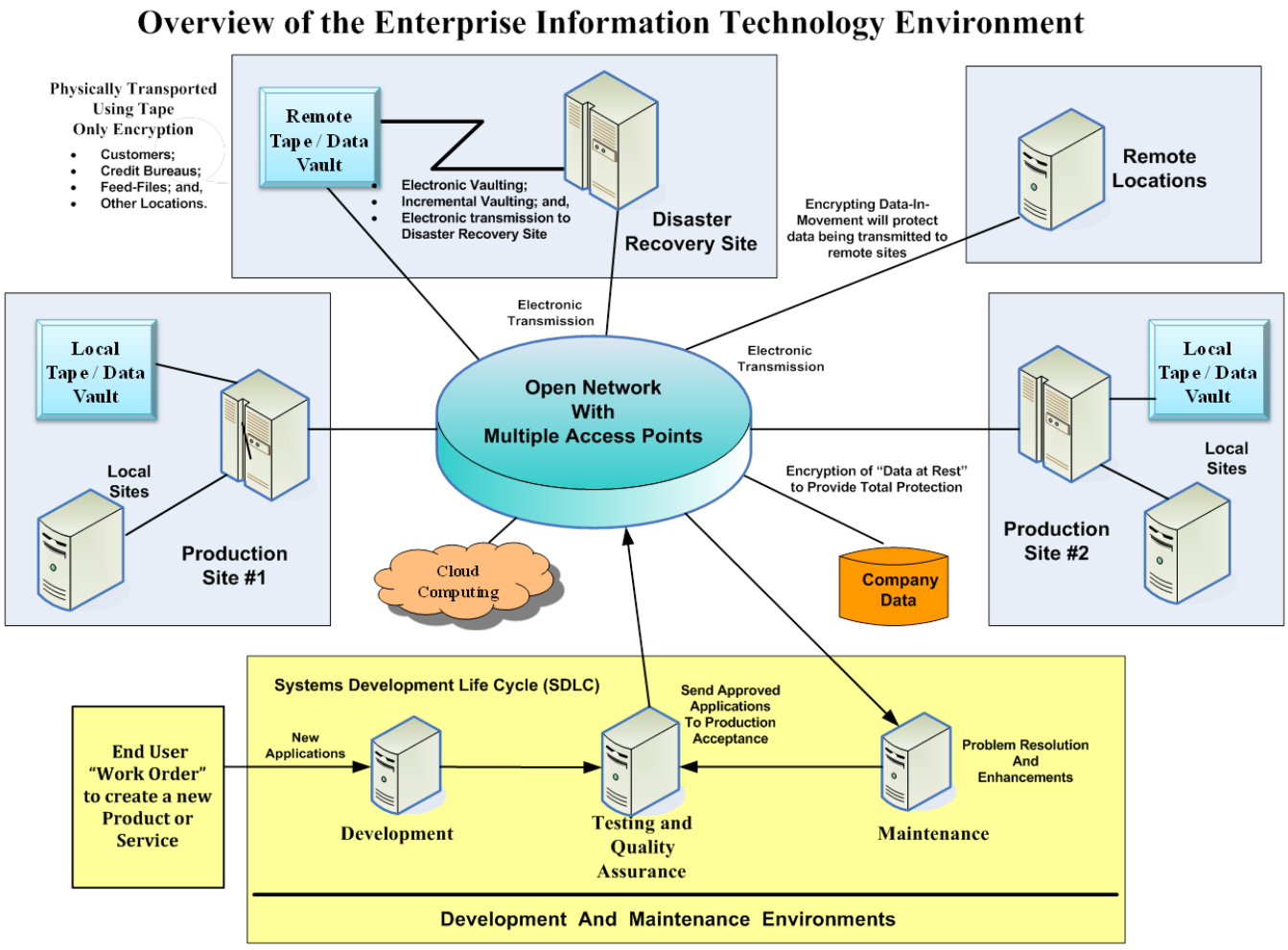
The Physical and Logical Layers of data transmission are shown above and related to how Web Based IP Domains are similar to normal Post Office mail delivery.

The growth of the Internet has made it necessary to increase the number of available IP Address, so we are migrating from an "Internet of Things" to an "Internet of Everything". Be prepared to have conversations with your appliances in the future because of this growth. Machines will identify problems and make service calls, and homes and physical facilities may be able to sense problems and notify the appropriate person as well. This may improve facility and personnel protection, while shortening downtimes and improving production.

The Enterprise Information Technology Environment

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

Figure 57: Overview of an Enterprise IT Environment



New development requests, enhancements, and problem resolutions are presented to the Development and Maintenance departments and follow the Systems Development Life Cycle (SDLC) described earlier. An enterprise must be able to recover production operations to a secondary site in accordance to SLA / RTO

requirements and be able to return to the production site when a disaster event is over. This environment is shown above.

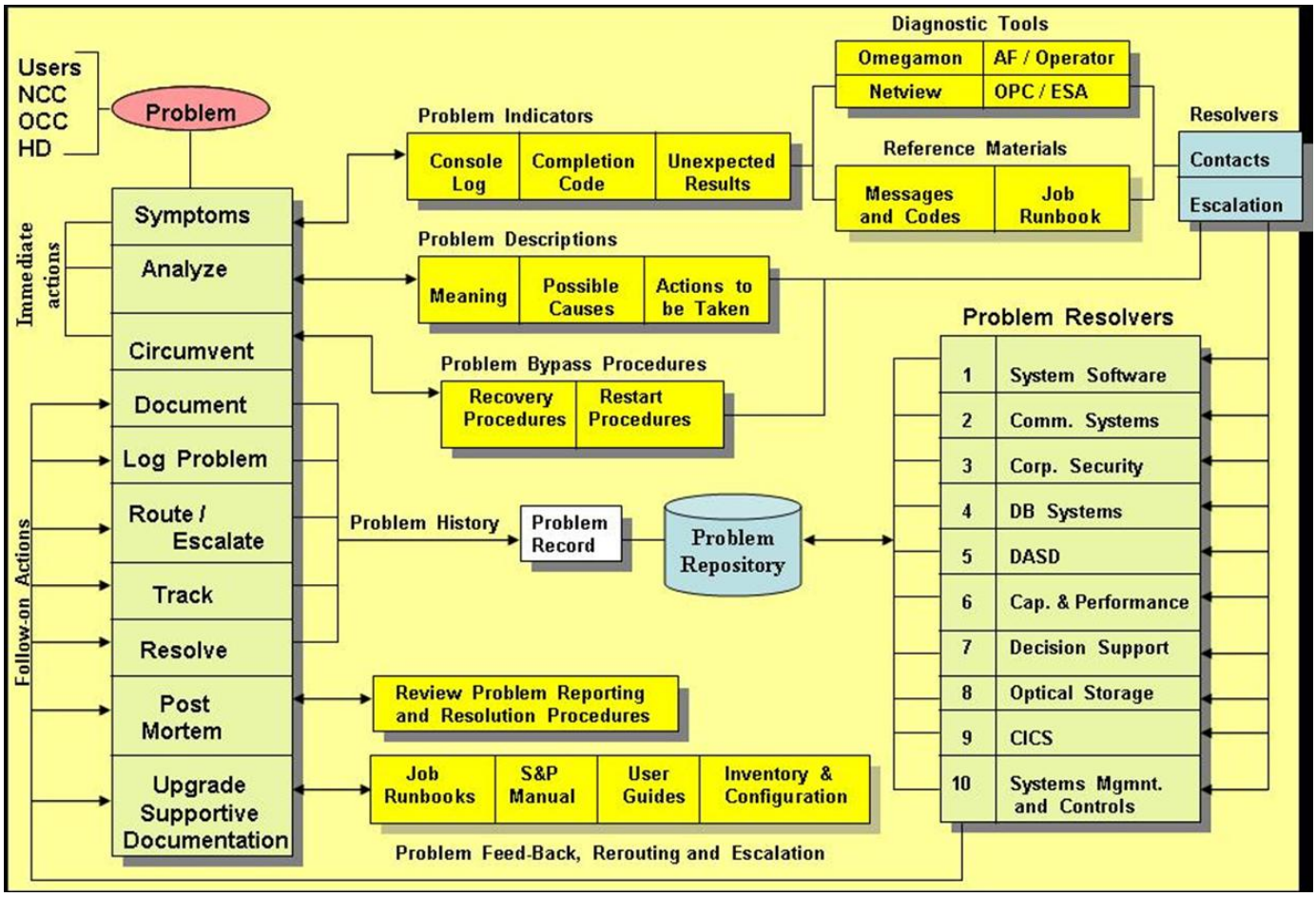
To support this responsibility, Recovery Plans are developed, tested, and implemented. There are many types of recovery plans that must be developed, each with sections that must comply with company standards.

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

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

Problem Recognition and Circumvention Techniques

Figure 58: Problem Recognition and Management Environment and Flow

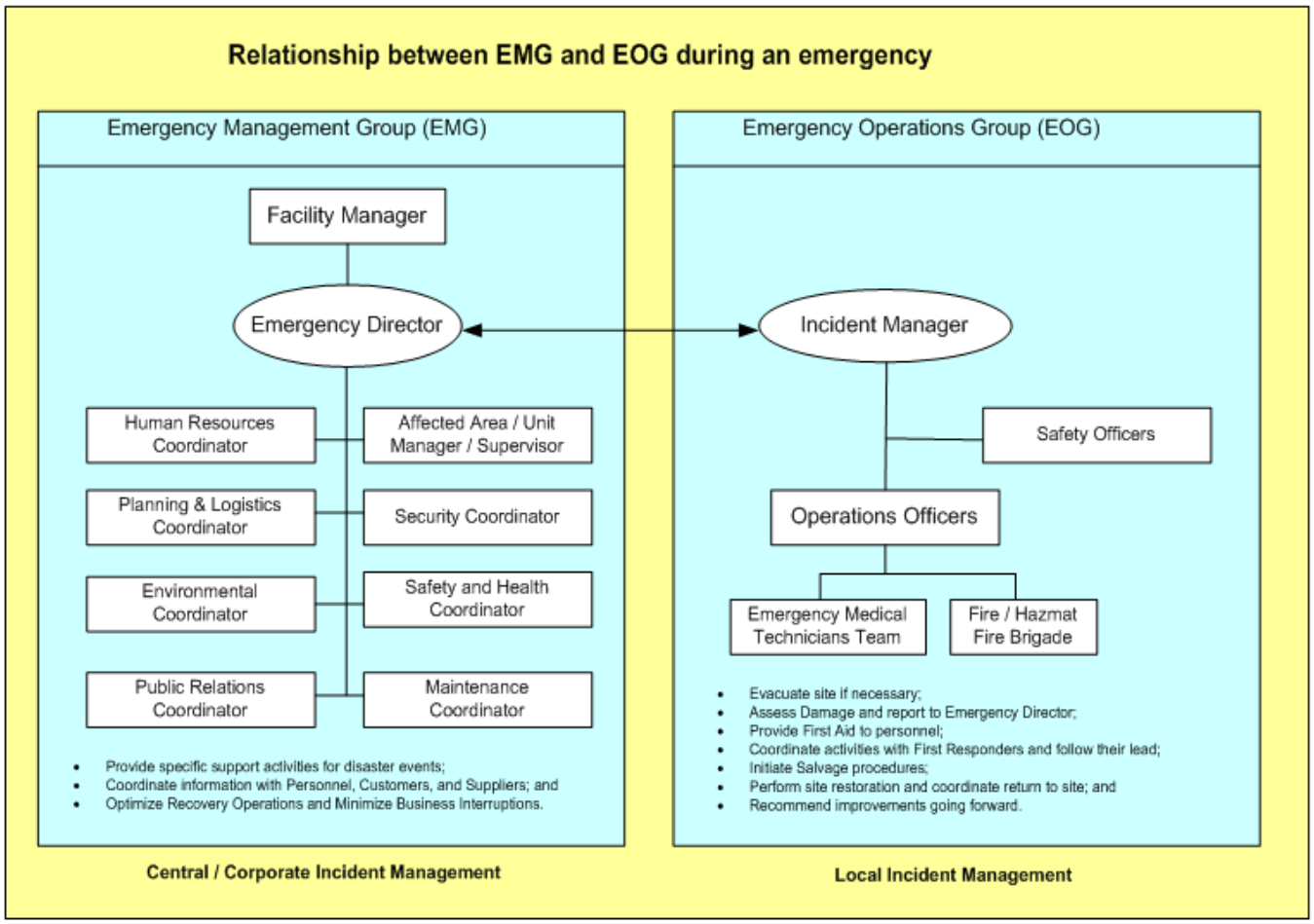


How problems are recognized, circumvented and reported is shown above. Some problems are repeats or easy to repair (Level 1). These problems are repaired by Help Desk personnel. Other problems may require that the Subject Matter Expert become involved in resolving the problem (Level 2), while even harder problems will require the vendor to repair the problem (Level 3). On rare occasions the problem results in a disaster event (Level D) and the initiation of a recovery plan. These problems are routed to the Contingeny Coordinator associated with the problem type and they enact a Contingency Command Center / Emergency Operations Center environment to react to the disaster event.

The above illustration shows every step associated with problem identification, circumvention, reporting, escalation, completion, reporting, and review.

Incident Management Organizational Structure

Figure 59: Incident Management Environment



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

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

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

Workplace Violence Prevention Act

June 7, 2008 – Article 27-6 of Labor Law

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

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

1. Comprehensive Policy for Workplace Safety and Violence Prevention;
2. Building and Perimeter security as dictated by OSHA and supported by First Responders;
3. Training employees on Workplace Violence and its impact; and,
4. Use "Best Practices" for physical security and access controls (card key, recorders, guards, etc.).

Why Workplace Violence occurs and most likely reasons for offence:

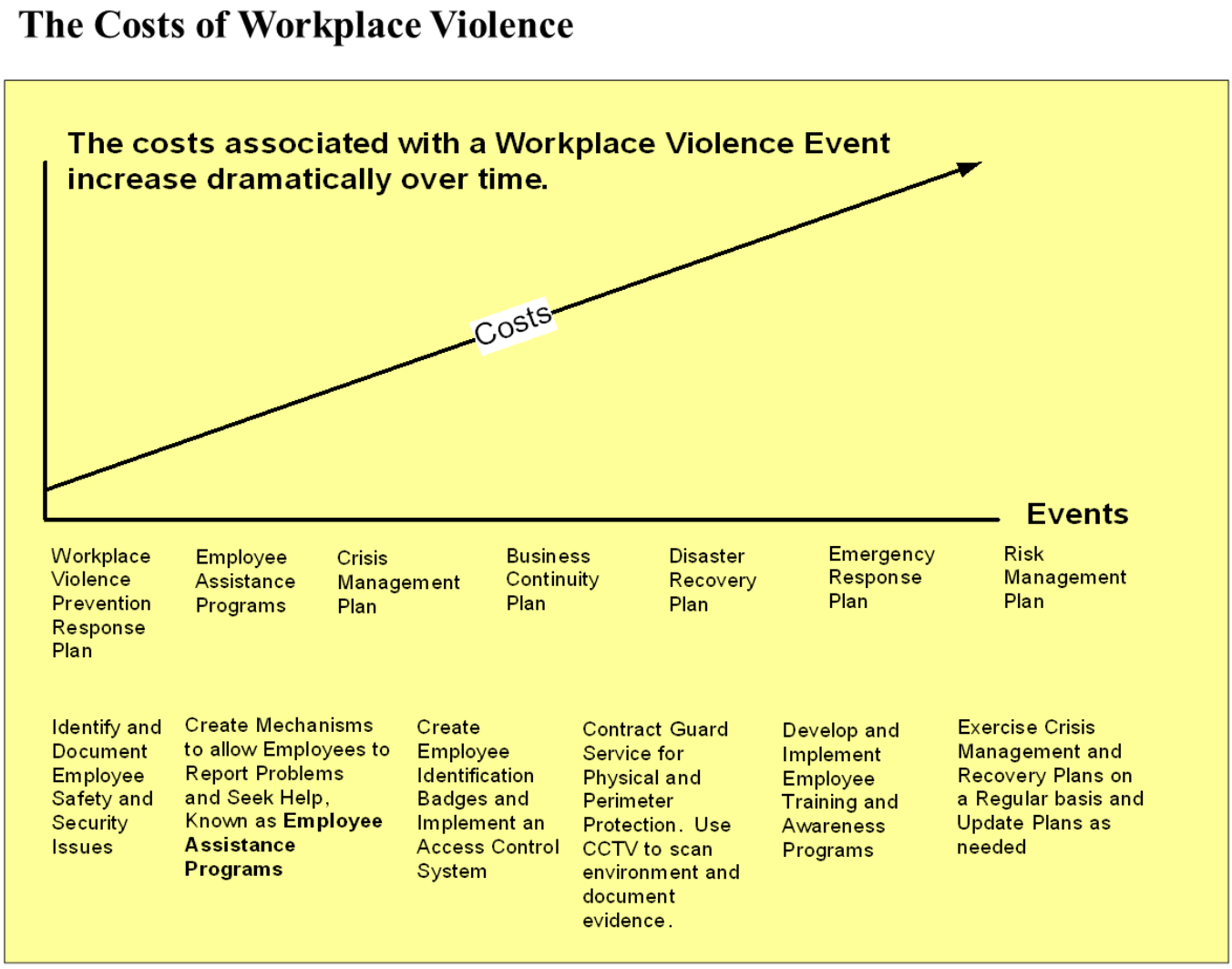
- Number one cause is the loss of a job or perceived pending loss of job.
- Presently being addressed REACTIVELY, but should be addressed PROACTIVELY.
- Corporate culture must first accept importance of having a Workplace Safety and Violence Prevention policy that is embraced and backed by Executive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

- Employee Assistance Programs can be developed to help cope with personal life crisis and avoid Workplace Violence situation – a range of these programs should be developed and made available to the staff and their family.

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

Costs associated with Workplace Violence

Figure 60: The costs associated with Workplace Acts of Violence



As was mentioned earlier, the costs associated with a Workplace Act of Violence are great indeed (even great enough to force a company and its owners into bankruptcy), but some simple and inexpensive steps can be taken to reduce or eliminate the possibility of an act of violence occurring at one of your work sites.

To begin with, physical security and perimeter protection are essential. Protecting access to the facility by insuring that access points are secured and open access points protected by guards. Beyond access controls, it is essential to be able to collect enough evidence when attacks occur to identify and prosecute the offender, which can be accomplished by Closed Cable TV (CCTV) located at strategic locations and monitored by the guards.

Physical security would compartmentalize the location and allow access to restricted areas to authorized personnel in possession of card keys that guaranty that the card and person are related (i.e., eye scanners, id checked by a guard, etc.).

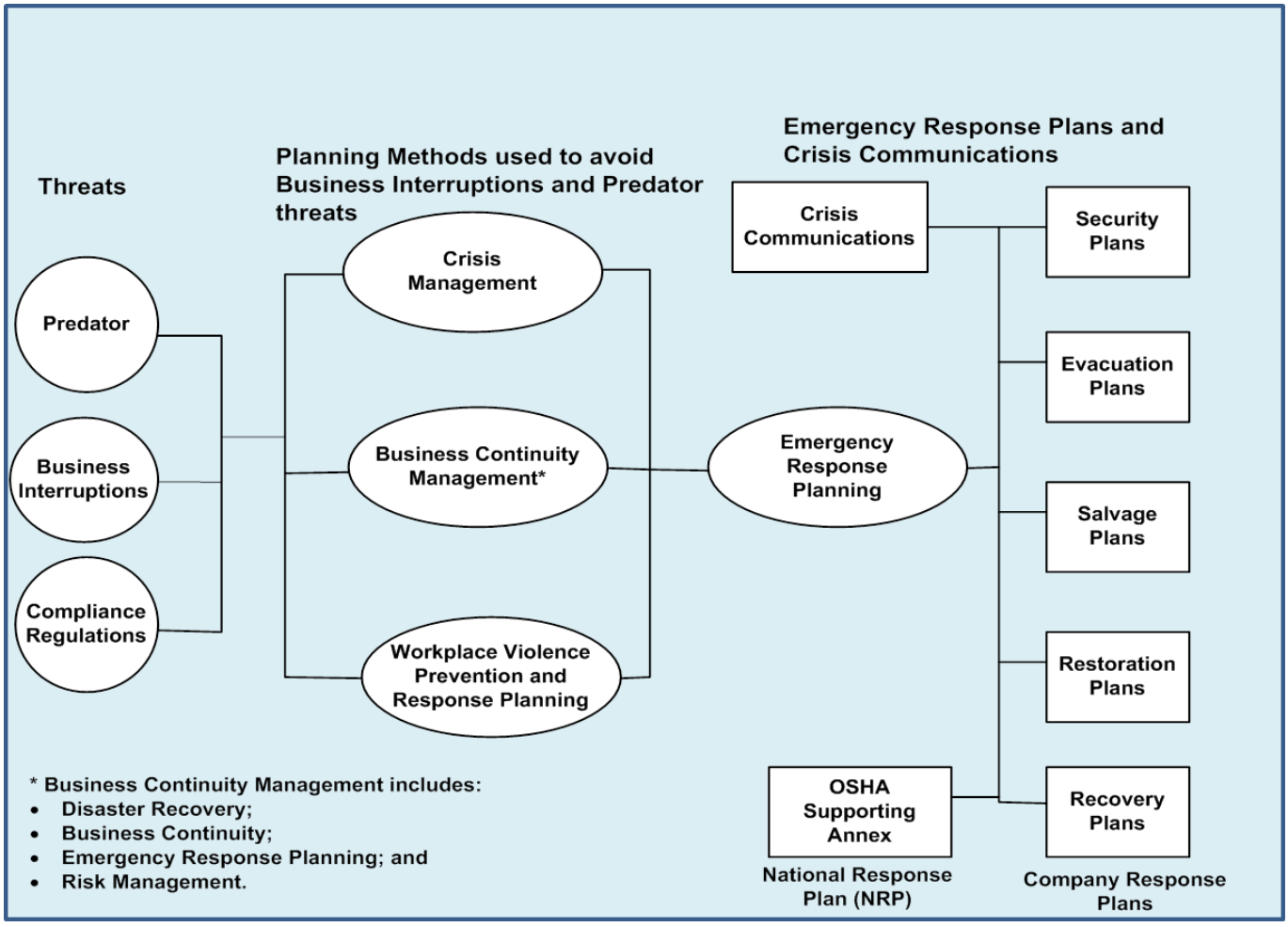
Employee Assistance Programs (EAPs) can be used to allow employees to notify personnel that a problem has arisen in their life that the company should know about (e.g., wife works for the company and after recent divorce she obtained a court issued Restraining Order restricting her ex-husband from being within 100 feet of her, but he told her he wouldn't let some piece of paper stop him from getting even with her). These programs can activate additional protective services that can help employees overcome potential threats to themselves and other company personnel (e.g., notify guards, post picture, notify other staff and management to be on the look-out, etc.).

The plans that should be implemented to protect environments are shown in the above illustration, but it is OSHA, Building Management Laws developed by the city and the department of Housing and Urban Development (HUD), Homeland Security, the Office of Emergency Management, and First Responders (Police, Fire Department, Emergency Medical Technicians) who should be responded to and notified about workplace protections. They will be happy to assist you by reviewing your plans and making any suggestions for improvement that would better protect your personnel and adhere to the required laws.

Risk Management assessments and Crisis Management Plans should be created to identify specific problem areas where having an exercised and well know Crisis Management Plan can result in saving lives and safeguarding the company reputation. This is a very important issue and every enterprise should make every effort possible to promote Workplace Safety and Violence Prevention. After all, your most valuable asset is your staff and they deserve the best protection possible. It will improve morale and help retain your staff and clients.

Workplace Safety and Violence Prevention

Figure 61: Workplace Safety and Violence Prevention Environment



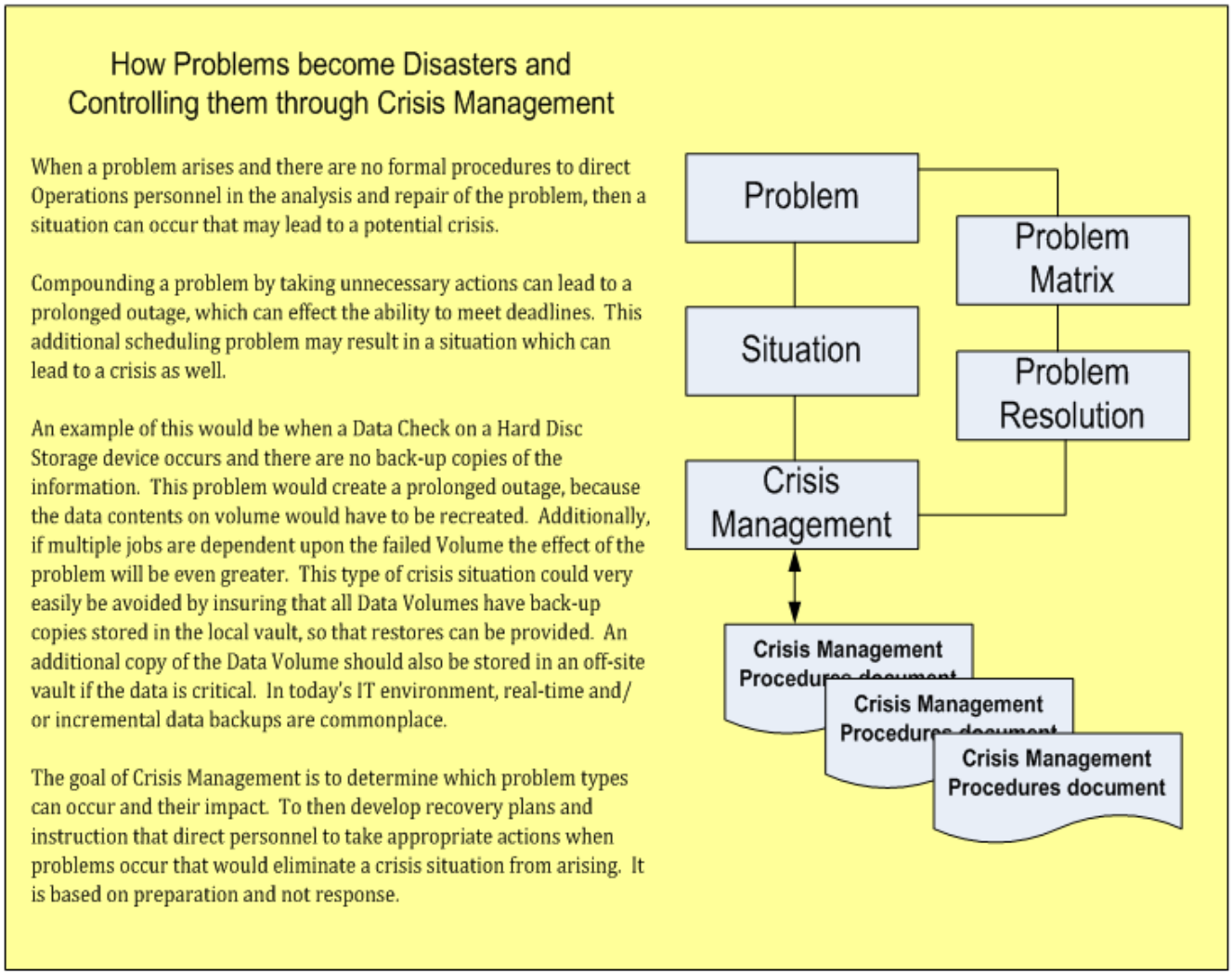
A fully implemented Workplace Safety and Violence Prevention environment is shown above. It is designed to be aware of threats and intrusions that may result in harm to the staff and company. Once identified, threats can be addressed through Crisis Management Plans, or via a simple call to a First Responder.

Starting from left to right, all threats are identified by Round Circles, while Actions to protect people and the company are shown in Ovals. All plans and written materials are shown in Boxes to the right. It is very important that a company understand this process, because should a workplace event occur and First Responders are called you should be aware that recovery plans should be activated for any application that has a recovery time objective of less than four hours. This is because First Responders usually secure and rope off areas until the reported problem is resolved, and we all know how long that can take from watching local news events. Additionally, the First Responders must be made aware of any existing chemical or hazardous condition which is listed in the OSHA Appendix document.

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

Crisis Management and responding to events

Figure 62: Crisis Management and Responding to Events



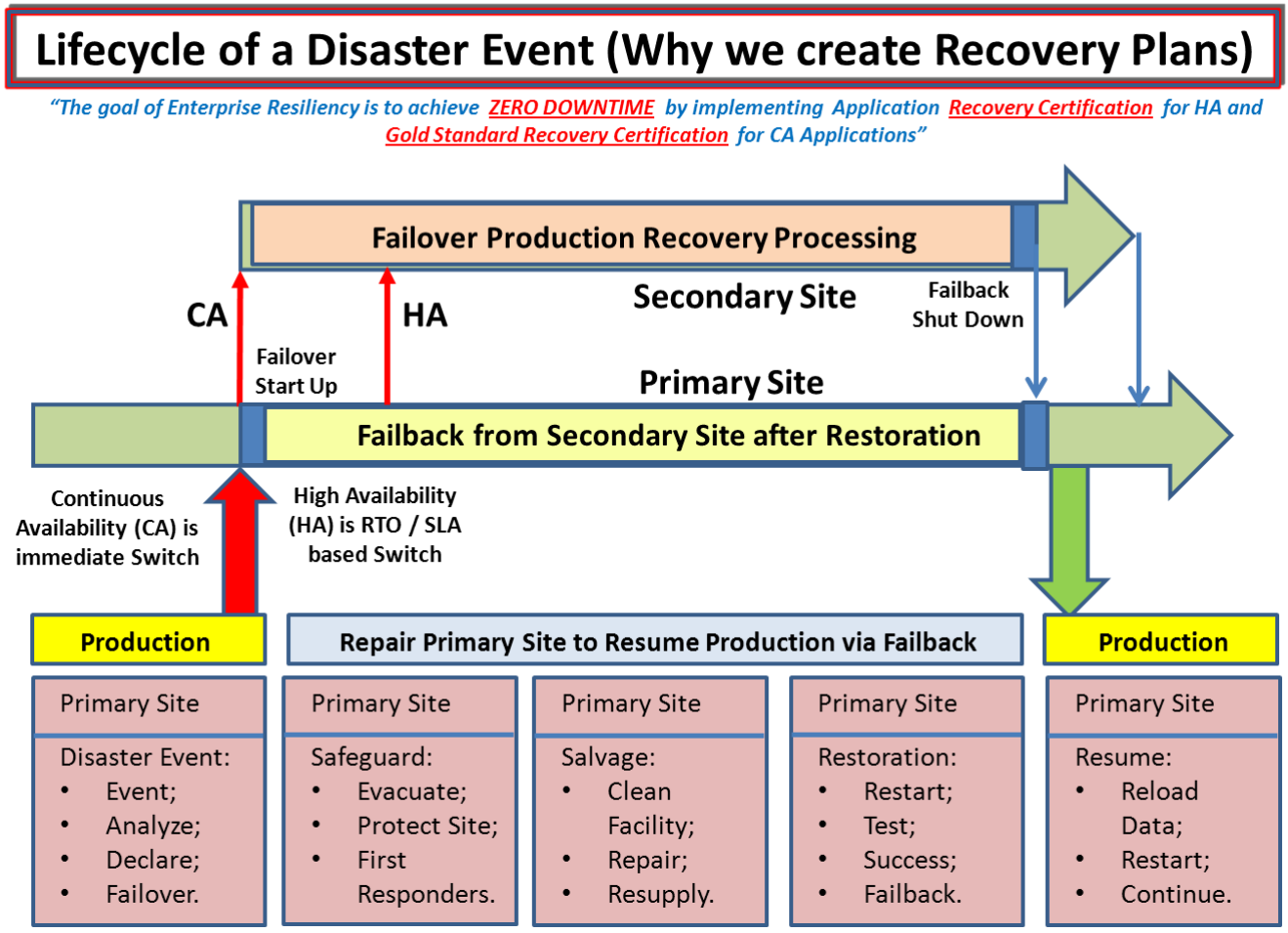
Problems sometimes grow into crisis situations when response plans are not created and followed as illustrated above. It is therefore imperative that Risk Management uncovers potential problems and Crisis Management plans created to respond to these potential problems.

Remember, Problems are deviations from standards, so it is imperative to have solid standards and procedures in place so that the likelihood of a problem turning into a crisis is reduced or eliminated.

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

The Disaster Life Cycle revisited

Figure 63: Disaster Recovery Life Cycle review

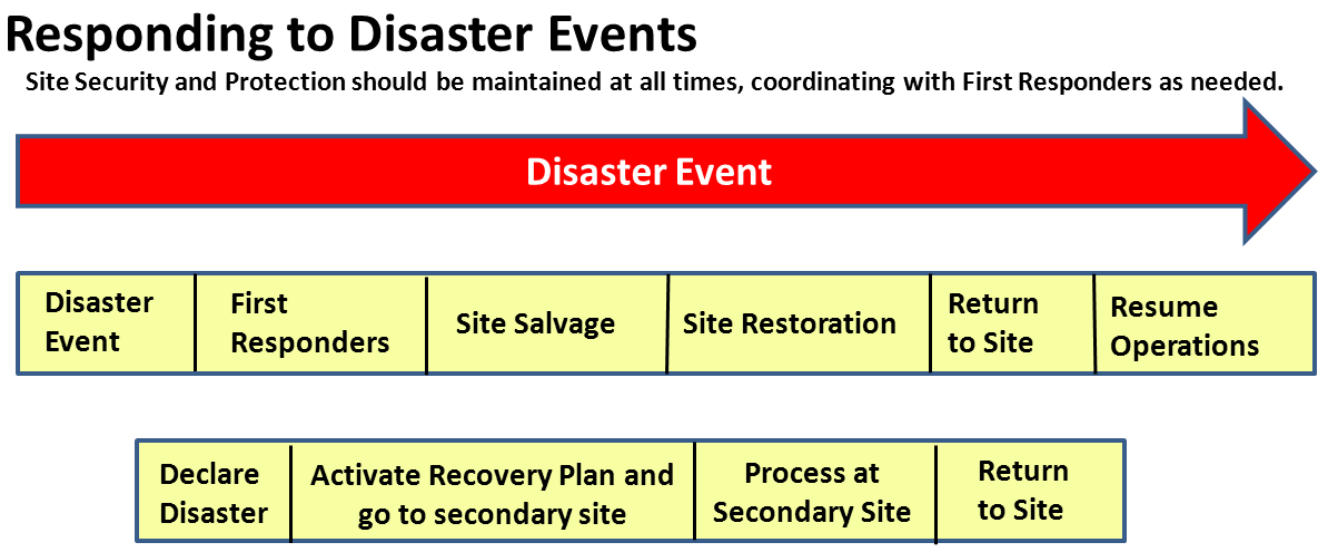


Disasters have a Life Cycle that is shown below. When a disaster event occurs, it must be recognized and acted upon appropriately. This initial action is included in a recovery plans initial problem analysis section. Once recognized, the problem is reported to management and the Help Desk. Management 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 64: Responding to Disaster Events



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.

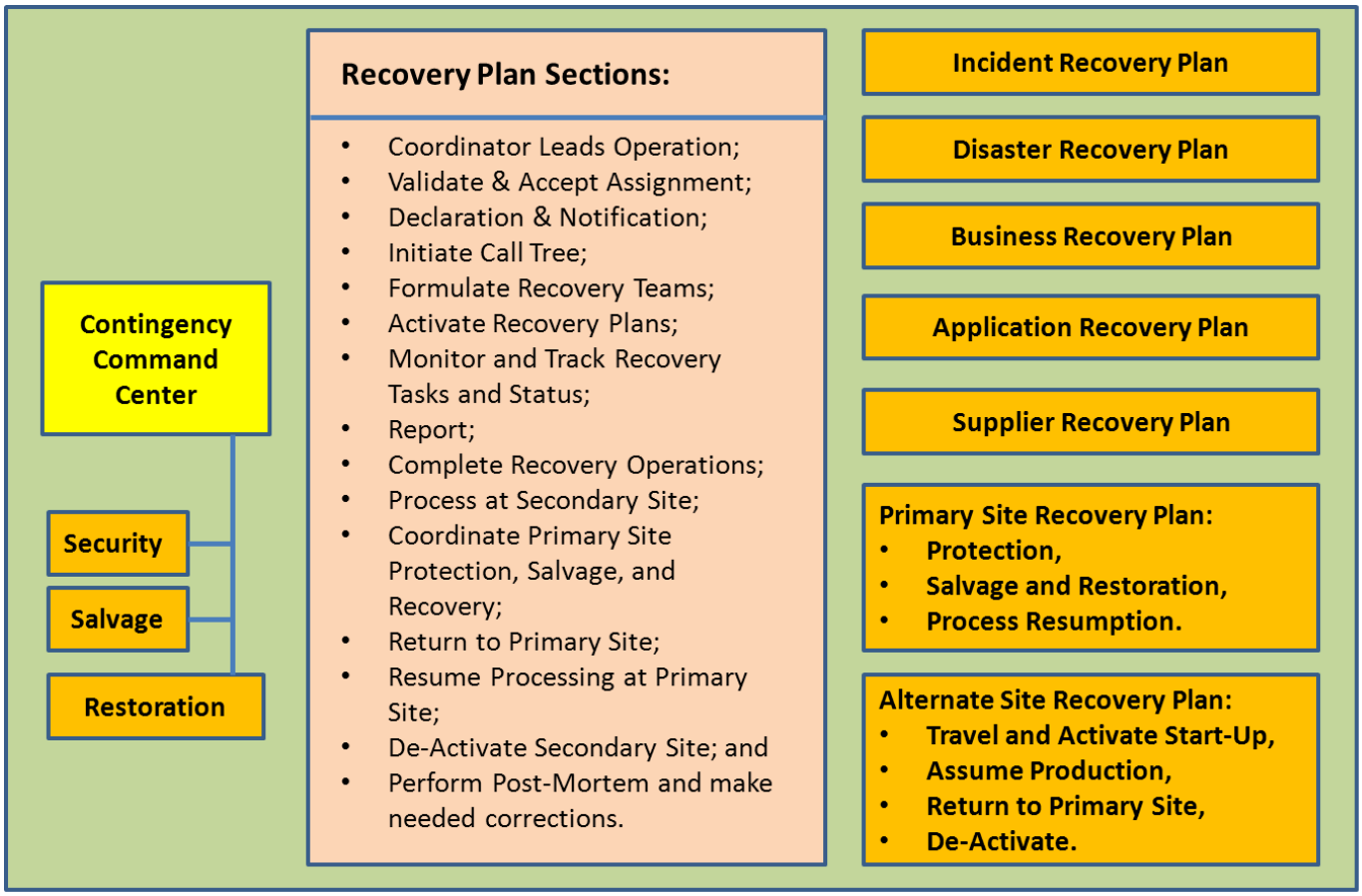
First Responders (consisting of the police, fire department, and emergency medical technicians) will perform their tasks immediately upon arrival on the scene. In some cases the building or affected area will be cordoned off which would interfere with normal business operations. You can usually be assured 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 65: Types of Recovery Plans and their components



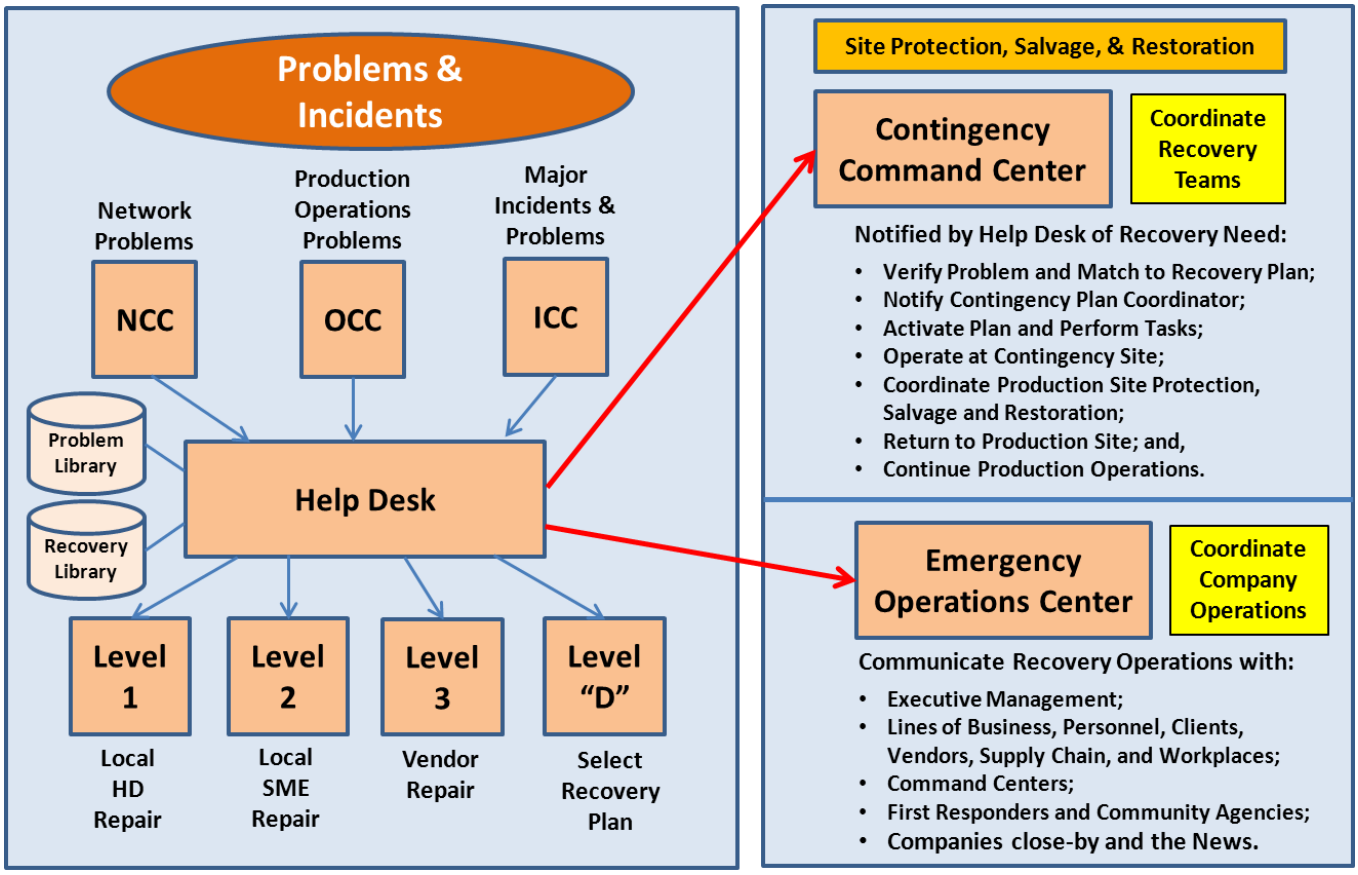
Once recovery plans are created, they must be identified, declared, and acted upon which requires interactions between end-users, command centers, and management.

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 66: Activating and Coordinating Disaster 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.

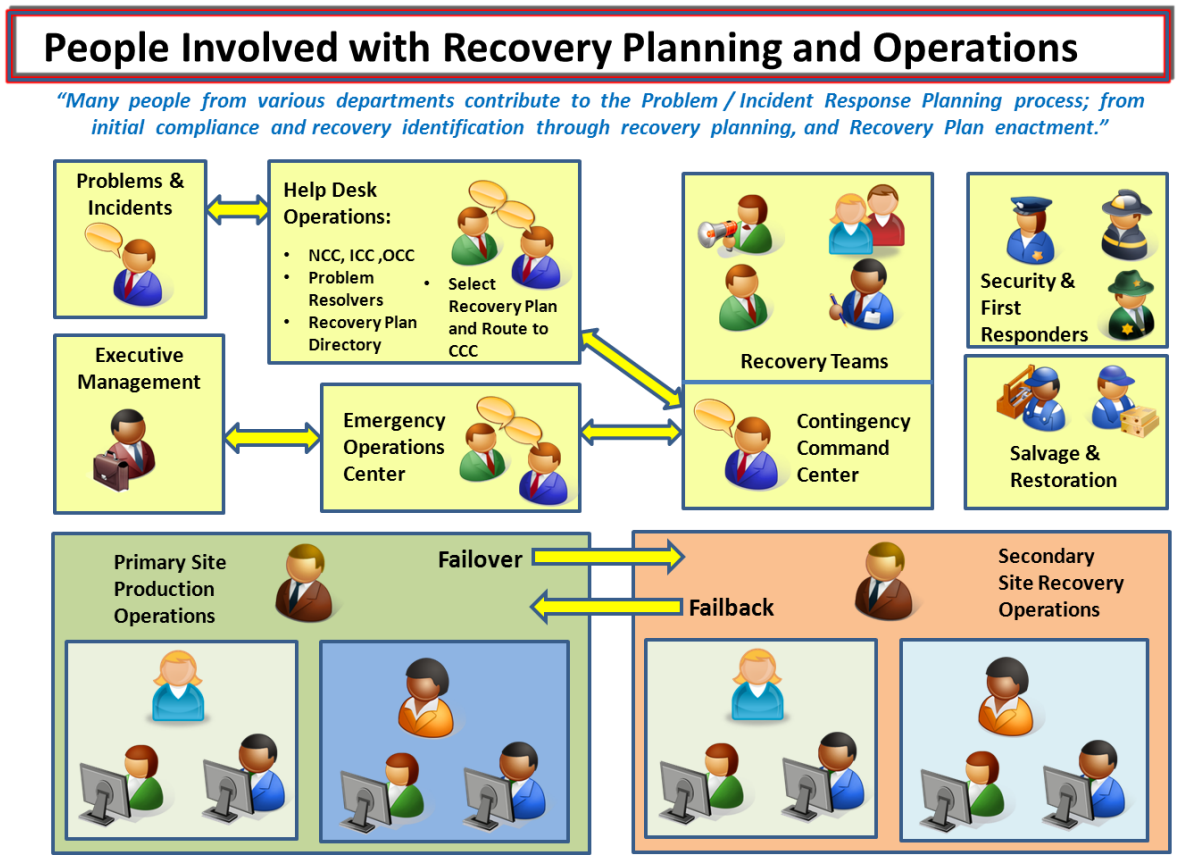
The Emergency Operation Center (EOC) coordinates business operations to minimize the impact of the disaster and communicates with Executive Management on the status of the disaster event, while Executive

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 67: People involved with Recovery Planning and Operations

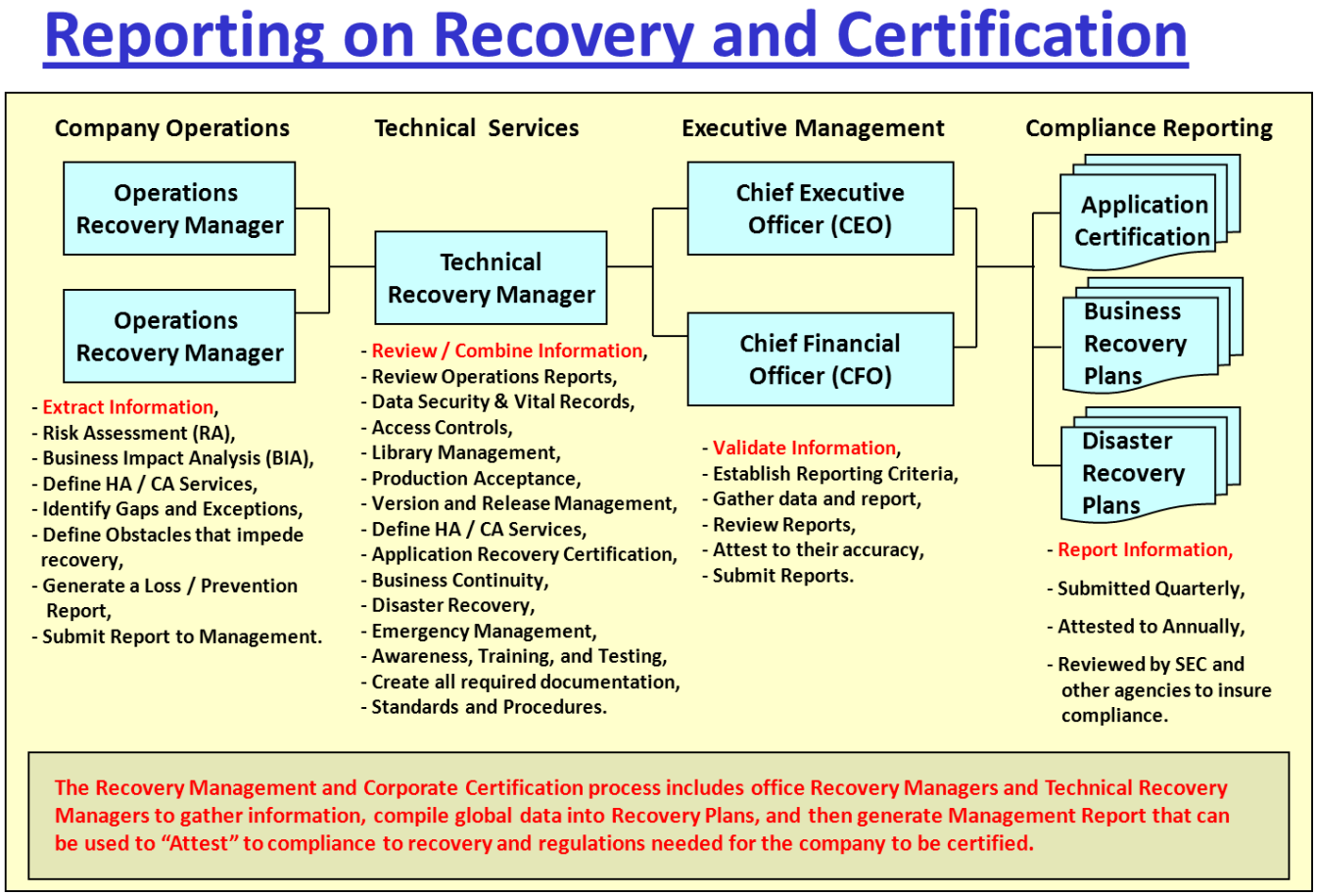


The above illustration demonstrates the many people involved in recovery operations and support the logistic, documentation, and training problems associated with recovery management

Reporting on Recovery and Certification

Once you have implemented Recovery Management, Corporate Certification, Personnel Training, Support and Maintenance procedures, they must be validated and reported to management so they can sign a "Letter of Attestation" on their ability to recover from a business interruption. This process is shown below.

Figure 68: Reporting on Recovery and gaining Certification

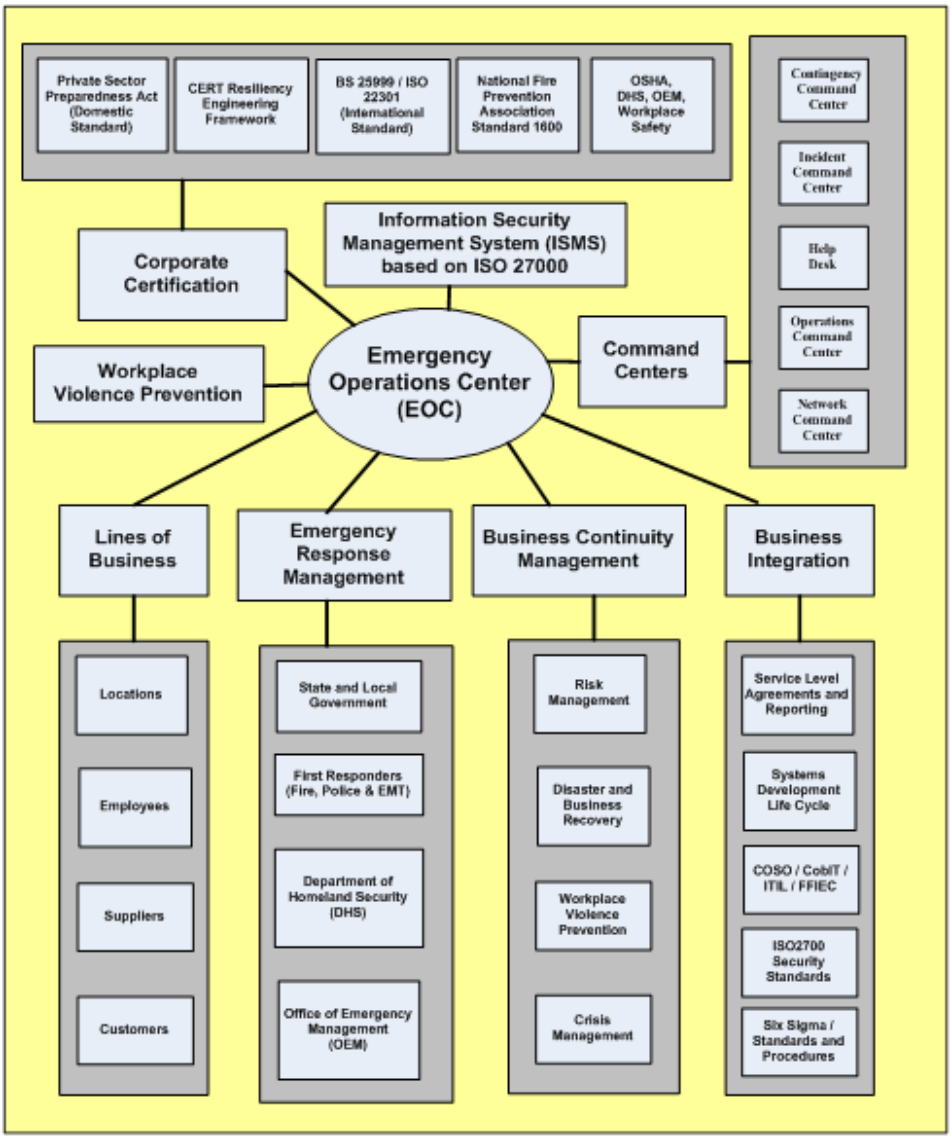


Operations Recovery Managers are associated with Business Units and they complete and maintain Recovery Requirements and Testing Results for their unit. The Technical Recovery Manager compiles all reports from the Operations Recovery Managers into an Enterprise Recovery Report and presents it to management for their review and approval. Once approved by management, a "Letter of Attestation" is completed and signed. This letter is presented to the Regulators to validate the enterprises ability to continue business operations, even when a disaster event occurs.

This process is repeated on a periodic basis, depending upon your enterprises requirements, so that continued recovery operations can be maintained even when growth or technology changes.

Fully Integrated Recovery Operations and Disciplines (Physical End Goal)

Figure 69: Fully Integrated Recovery Operations and Disciplines (Physical End Goal)



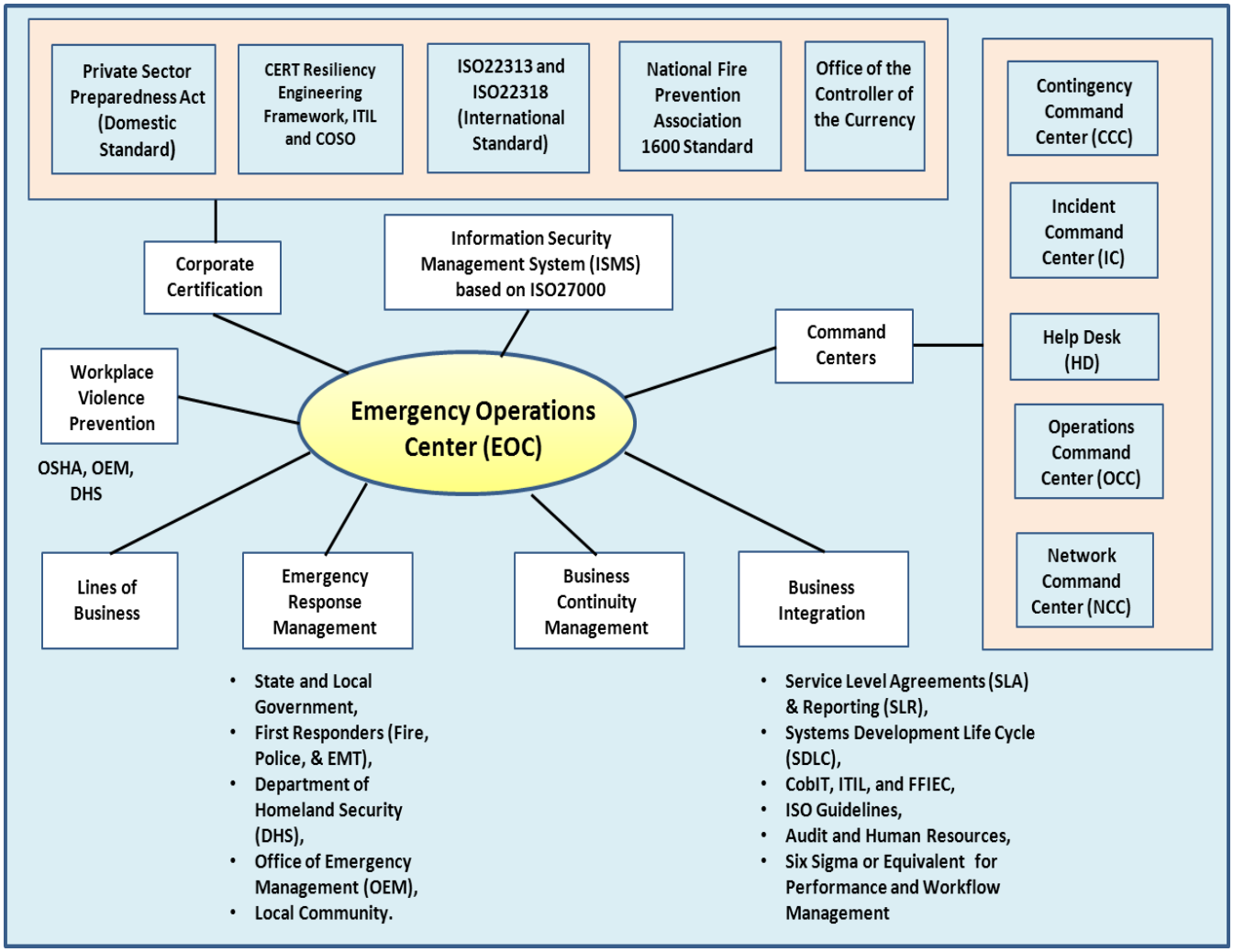
The EOC is activated when a disaster event occurs. It communicates with the Help Desk, Contingency Command Center, Business Units, and Executive Management in order to coordinate recovery operations and maintain business requirements associated with Corporate Certification and Enterprise Resiliency.

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 70: Fully Integrated Resiliency Operations and Disciplines (Logical End 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 in a professional manner.

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.

Conclusions

Figure 71: Conclusions

What you will achieve by implementing Enterprise Resiliency and Corporate Certification

- Use of "**Best Practices**" to implement Enterprise Resiliency and Corporate Certification, which will raise the standards used by the company to support business and Information Technology services;
- **Improved business recovery** organization that combines all recovery disciplines and utilizes a common language and common set of tools, resulting in a better educated recovery staff, better recovery plans and shorter business interruptions when disaster events occur;
- **Zero Downtime** through testing and recovery certifying all applications, while utilizing Flip / Flop support for Continuously Available applications (Gold Standard), Failover / Failback for High Availability applications (Recovery Certification), and all other applications used by the company (Normal Recovery Certification);
- **World-Wide compliance** to all necessary laws and regulations of the countries where you do business;
- A **Recovery Management and Support Services** structure best suited to maintain business operations;
- **Fully documented** standards and procedures, usage manuals, messages and codes, and training materials needed to educate your staff and leading to an efficient business environment;
- Use of **automated tools** to support business operations, Systems Development Life Cycle, Workflow Management and Controls, Forms Management and Controls, and personnel recruitment, orientation, training, and awareness;
- **Implemented Management Disciplines** including: Supply Chain Management, Asset Management, Inventory Management, Configuration Management, Version and Release Management, and Infrastructure Management procedures;
- **Integrated** procedures supporting personnel functional defined in their job description that will insure that compliance and recovery requirements are maintained in a current and accurate status at all times;
- Creation of and **adherence to customer service contracts**, SLA/SLR, or Key Performance Indicators through capacity and performance management and reporting;
- Use of the latest **Data Management techniques** to insure adherence to business recovery time objectives (RTO), Data Security, Access Controls, and Vital Records Management;
- Integrated **Charge-Back System** to account for Work Orders and Purchase Orders, associated with the development, support, and maintenance of business services and products;

- **Command Center integrations**, including: Emergency Operations Center (EOC), Contingency Command Center (CCC), Incident Command Center (ICC), Operations Control Center (OCC), Network Control Center (NOC), and Help Desk that identify and respond to encountered problems;
- **A well trains and loyal staff** that will best support retention of personnel and customers, while enhancing the company character and reputation and attracting new business; and,
- **Optimized business operations** resulting in an efficient and safeguarded enterprise that can best respond to customer demands during normal and disaster processing, thereby enhancing the company reputation in the eyes of the community and its customer base (both current and prospective).

How to get started implementing Enterprise Resiliency and Corporate Certification

Figure 72: How to get started implementing this project

The following tasks are recommended when considering implementation of Enterprise Resiliency and Corporate Certification:

- Make a presentation to key management and technical personnel on what Enterprise Resiliency and Corporate Certification is and what can be accomplished by its implementation;
- Agree that you want to implement Enterprise Resiliency and Corporate Certification, while making any suggestions for improvement to the discussed process, or eliminating sections that the company does not deem necessary;
- Create a Business Plan and general Project Plan associated with achieving Enterprise Resiliency and Corporate Certification;
- Obtain Management and Technical Approval, a Budget, and strong Management Support for the project and its goals from implementation through support and maintenance going forward;
- Issue a Management Letter regarding the projects importance and the necessity to support project personnel in the achievement of their goals and deliverables;
- Identify Stakeholders and Participants, Formulate Teams, and provide Project Orientation training;
- Create a Detailed Project Plan, identify resources, training requirements, and time schedule for deliverables;
- Perform a Risk Assessment to uncover problems and poor controls that need to be mitigated (Gaps and Exceptions) or mediated (Obstacles impeding project deliverables) and report findings to management for decisions regarding mitigation / mediation costs and efforts or available insurance to protect against the conditions;
- Perform a Business Impact Analysis (BIA) for locations and Business Units;
- Decide on utilizing an automated tool to support Risk Assessments, Audits, BIA and Recovery Plan creation, support, and maintenance going forward. Have personnel assist in the tool selection and provide product training to Stakeholders and Participants;
- Create a “Proof of Concept” recovery plan and present it to management for approval, making any updates deemed necessary;
- Create, Test, Implement, Support, and Maintain recovery plans going forward.
- Integrate recovery management, risk management, audit, and reporting into the everyday functions by personnel; and,

- Integrate training and awareness for recovery management, risk assessment, BIA, Audit, and Reporting with the everyday functions performed by company personnel.

The process of deciding on moving forward with implementing Enterprise Resiliency and Corporate Certification must include management and technical decision makers who best understand your business, its direction, your client base, the budget, and the staff. They know the people and culture better than anyone else and will have a knowledge that may help identify alternatives to some of the steps mentioned in this paper, or see how the process can cure a multitude of problems or directions that you want to achieve already. Combining those goals within the process may help you achieve many more goals than are mentioned in this paper and can reduce overall costs associated with repeating goals through multiple projects that can all be achieved within one project.

Appendix A – Links to Helpful Documents

The following links will provide additional information that can help you achieve Enterprise Resiliency and Corporate Certification. They can also be found on my web site at www.dcag.com.

IT Organization Maturity Model

http://www.dcag.com/images/IT_Org_Maturity_Model.pdf

Technology Risk Management and Audit Document Template

http://www.dcag.com/images/Balnk_Detailed_Work_Program.pdf

Crisis and Emergency Management Review Document

http://www.dcag.com/images/Emergency_-_Crisis_Mgmt01.pdf

Compliance Laws and Regulations – Review Document

http://www.dcag.com/images/Compliance_Laws_and_Regulations_Review.pdf

Migrating Applications to a Target Environment

http://www.dcag.com/images/Application_Migration_Guideline_Document.pdf

Tape Vaulting and Encryption Document

http://www.dcag.com/images/Tape_Vaulting_Audit_and_Encryption_Usage_Analysis.pdf

Creating a Business Contingency Plan document

http://www.dcag.com/images/DRPROJ01.pdf

Sample Business Continuity Plan with all components explained

http://www.dcag.com/images/Business_Continuity_Plan_Overview.pdf

About the Article and the Author

Achieving Enterprise Resiliency and Corporate Certification

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

As an end result, you will achieve a safeguarded and optimized business environment that complies with the laws and regulation of countries you do business in, and is capable of recovering from a wide range of disaster events. Personnel morale and client satisfaction will be raised and the company reputation will exceed industry standards.

Thomas Bronack Bio.

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

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