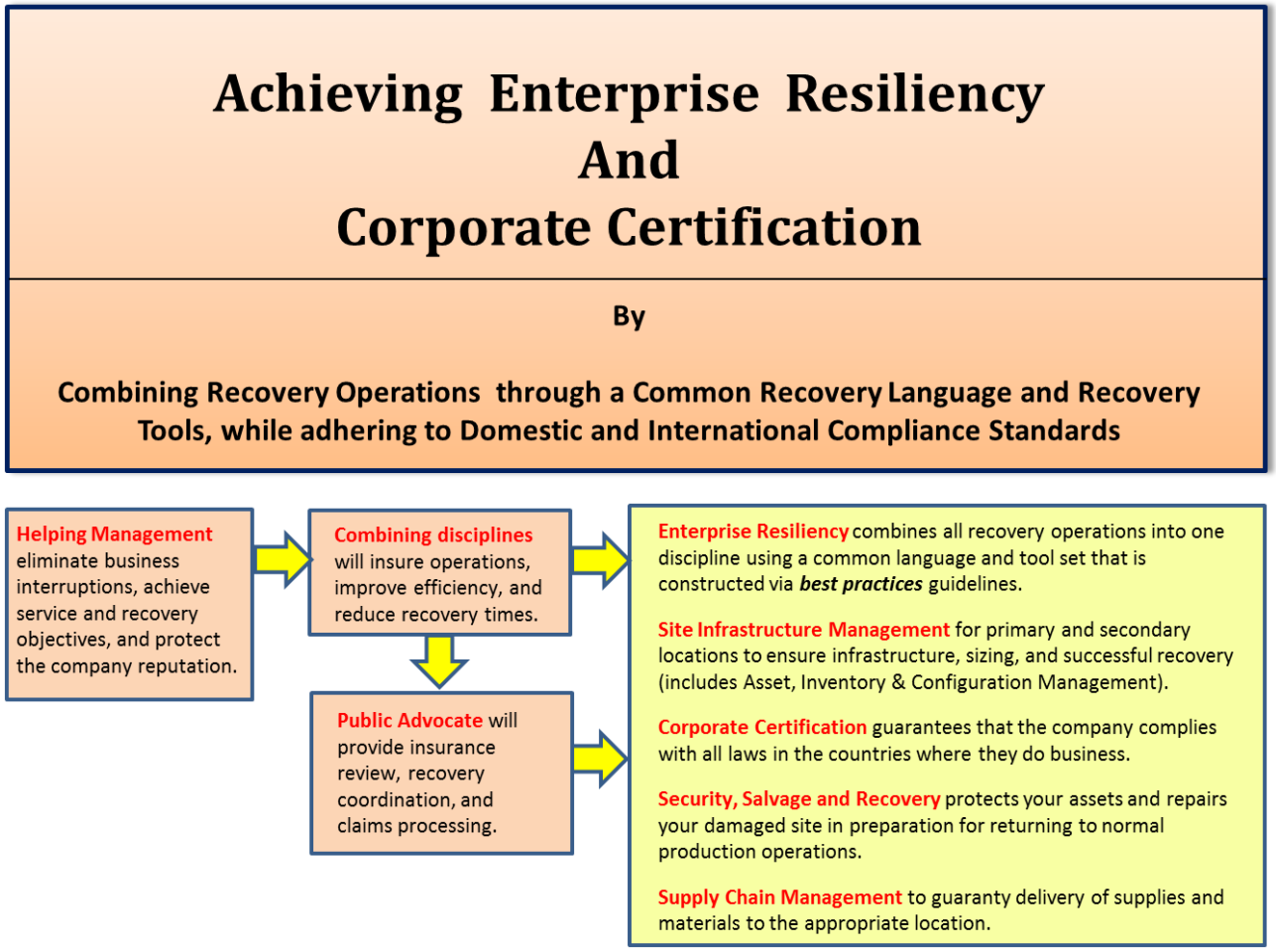
Introduction to "Achieving Enterprise Resiliency and Corporate Certification."

By Thomas Bronack, CBCP



Abstract

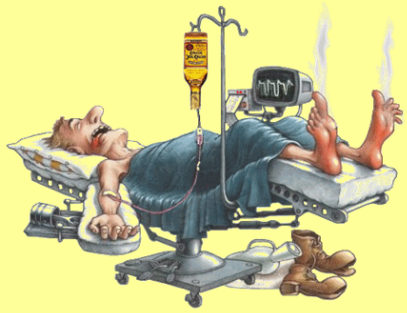
In today's Information Technology (IT) environment corporations are becoming global and facing new challenges in operational demands for the consistent delivery of services within required periods. Missing deadlines due to failures is becoming non-acceptable and can sometimes be easily detected by a wide audience of users and the media (such as the loss of a web-site, support center, or customer information), which may affect the company reputation and have an impact on the bottom line and customer loyalty.

Management is chartered to maintain the business in an uninterrupted manner and to constantly provide a safeguarded, compliant, and efficient environment that meets the demands of clients and business goals. A challenging task to achieve but one that is getting easier to meet because of innovative technologies and approaches to maintaining continued operations.

The demands of Recovery Management

Abstract – Recovery Management is hard and demanding on management

- Are you utilizing your recovery personnel to achieve **maximum protection**?
- Have you implemented a common recovery glossary of terms so that personnel speak the **same language** and can best communicate and respond to disaster events?
- Is your company utilizing a **common recovery management toolset**?
- Do you want to reduce disaster events, improve risk management, and insure fewer business interruptions through **automated tools and procedures**?



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

You can easily see why Enterprise Resiliency and Corporate Certification should be implemented at your company, but you may not have the staff or knowledge base to either continue normal business operations and convert your environment to be capable of achieving a safeguarded, efficient, and compliant enterprise, world-wide.

Management should seek assistance in defining the problems they face and agreeing on a path to follow that will lead to Enterprise Resiliency and Corporate Certification. These are not just buzzwords, but real technologies and procedures that have been developed by industry experts over a prolonged period. It would be wise to utilize that combined experience and knowledge base to help you determine the right path to follow for your firm. These concepts can be applied to large organizations or too Small to Medium Sized Businesses (SMB) and are scalable to match your growth and budget.

Although people think of Recovery Management as just the restoration of Information Technology, it is not. The most important part of Recovery Management is safeguarding your people, then company assets, services, and the company reputation. Do not forget to consider the loss of a location due to natural or human-caused circumstances. You can recover from a disaster event, recoup financial losses

over time, and even calm disgruntled customers, but the loss of a company's reputation is a hard thing to overcome – so make sure you are aware of your Risks and Exposures and take every step possible to safeguard your reputation and most valuable resources.

Objectives to be achieved.

Objectives to be achieved, include:

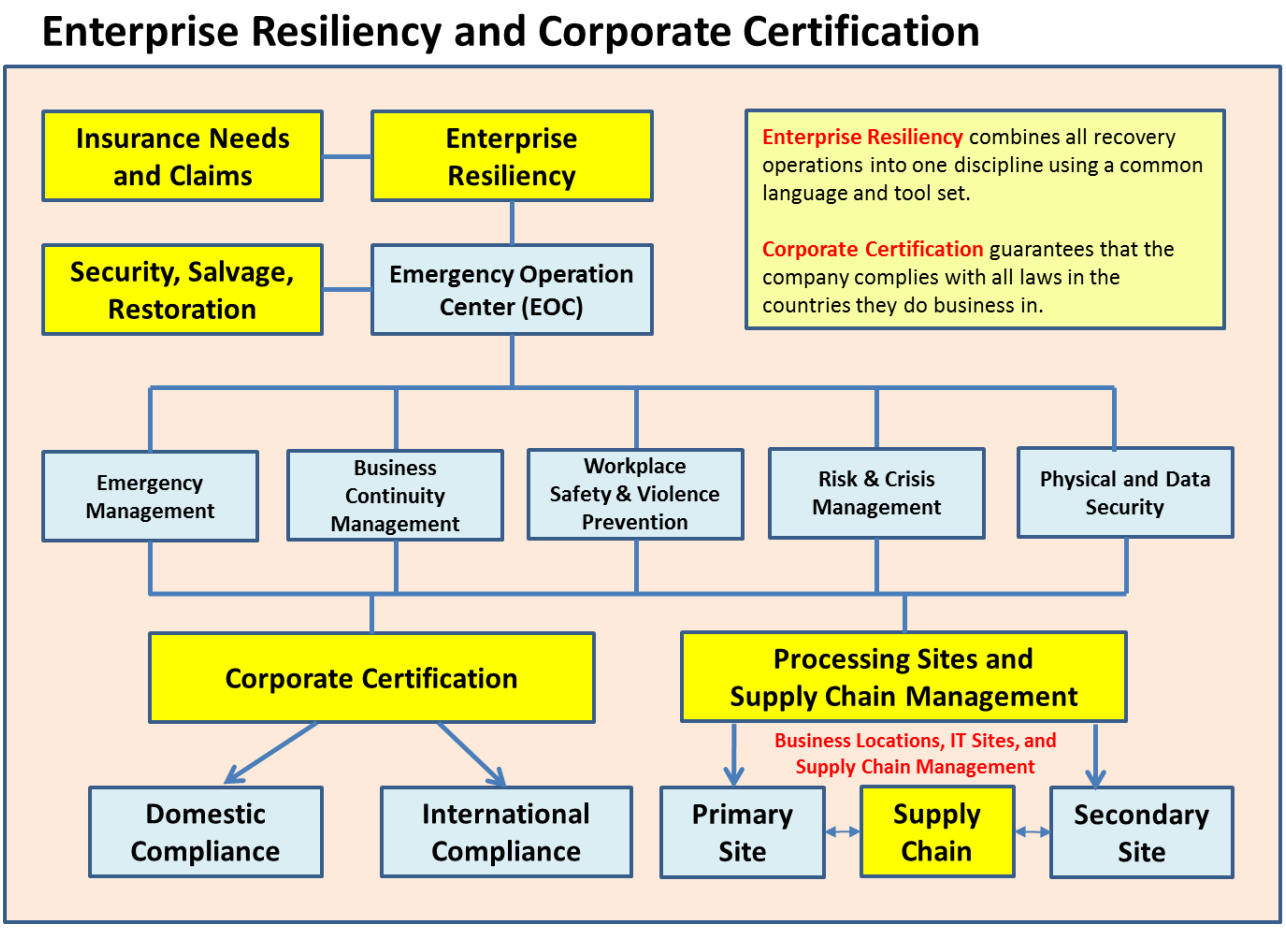
- **Safeguarded and Optimized Information Technology Environment that complies with all national and international laws and regulations, as required;**
- **Built upon "Best Practices" to insure best of breed standards;**
- **Integrated Systems Development Life Cycle (SDLC), Support and Maintenance procedures 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 are the goals of every company, and they can be achieved by following the concepts laid out in this paper.

Table of Contents

Contents

What is Enterprise Resiliency and Corporate Certification



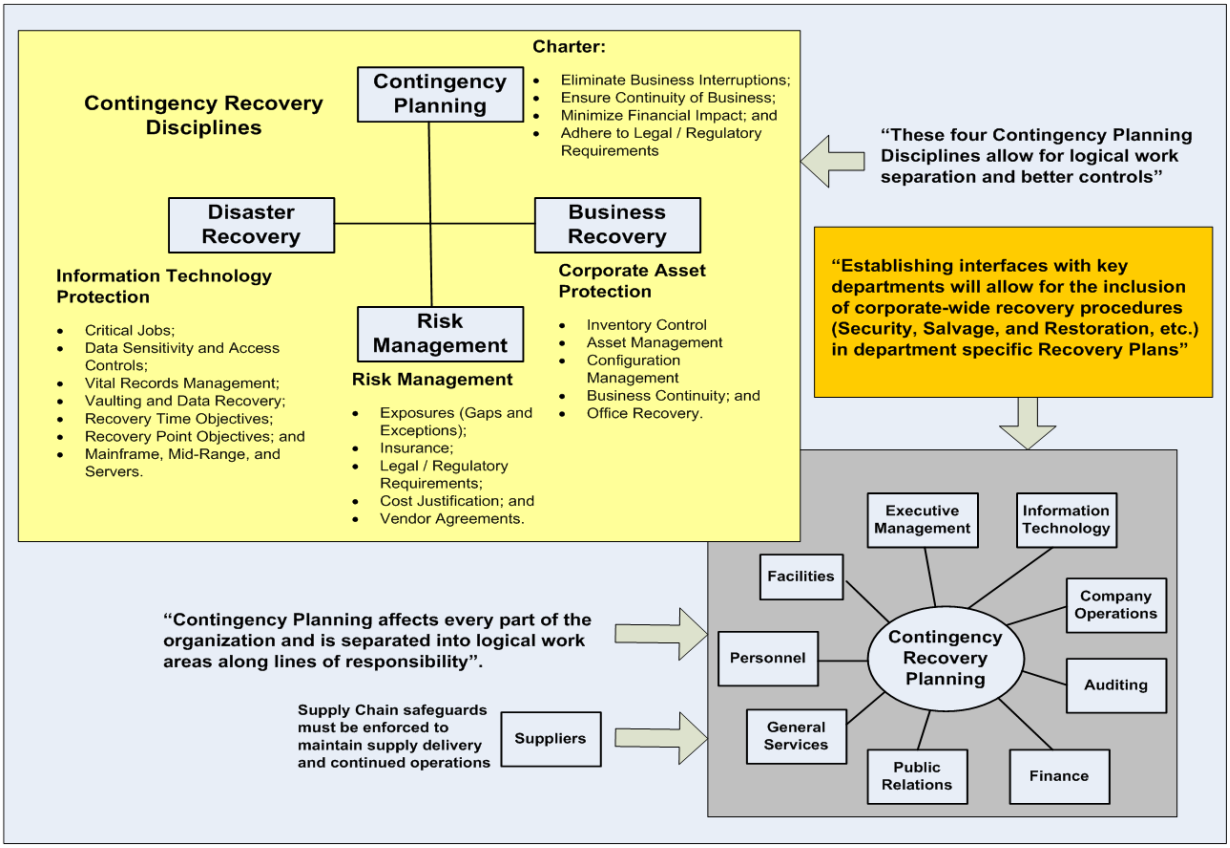
Enterprise Resiliency and Corporate Certification is a **Holistic Approach** to solving the problems facing Corporate Management today, specifically **protecting the Enterprise** from outages and safeguarding the environment by adhering to the laws and regulations of countries where you conduct business.

Based on **Industry Best Practices**, this approach can be integrated within the everyday functions performed by personnel so that new service developments, or enhancements to existing services can be achieved without interruption to production operations.

Should disaster events, either manufactured or natural, occur your enterprise will be able to quickly recover production operations at a recovery facility (IT or Business) within contracted recovery times, and sometimes instantaneously without the end user ever knowing there was an outage. It is our goal to achieve that objective by developing a safeguarded, efficient, recoverable, and compliant environment.

How management meets their functional responsibilities

Business Continuity Management Disciplines and Integration



After defining management requirements, a business plan or statement of work is issued to the staff announcing the importance of protecting the enterprise from prolonged outages and ensuring that the highest levels of company management require everybody's assistance and attention to achieving the goals of disaster recovery and compliance.

Problem Management

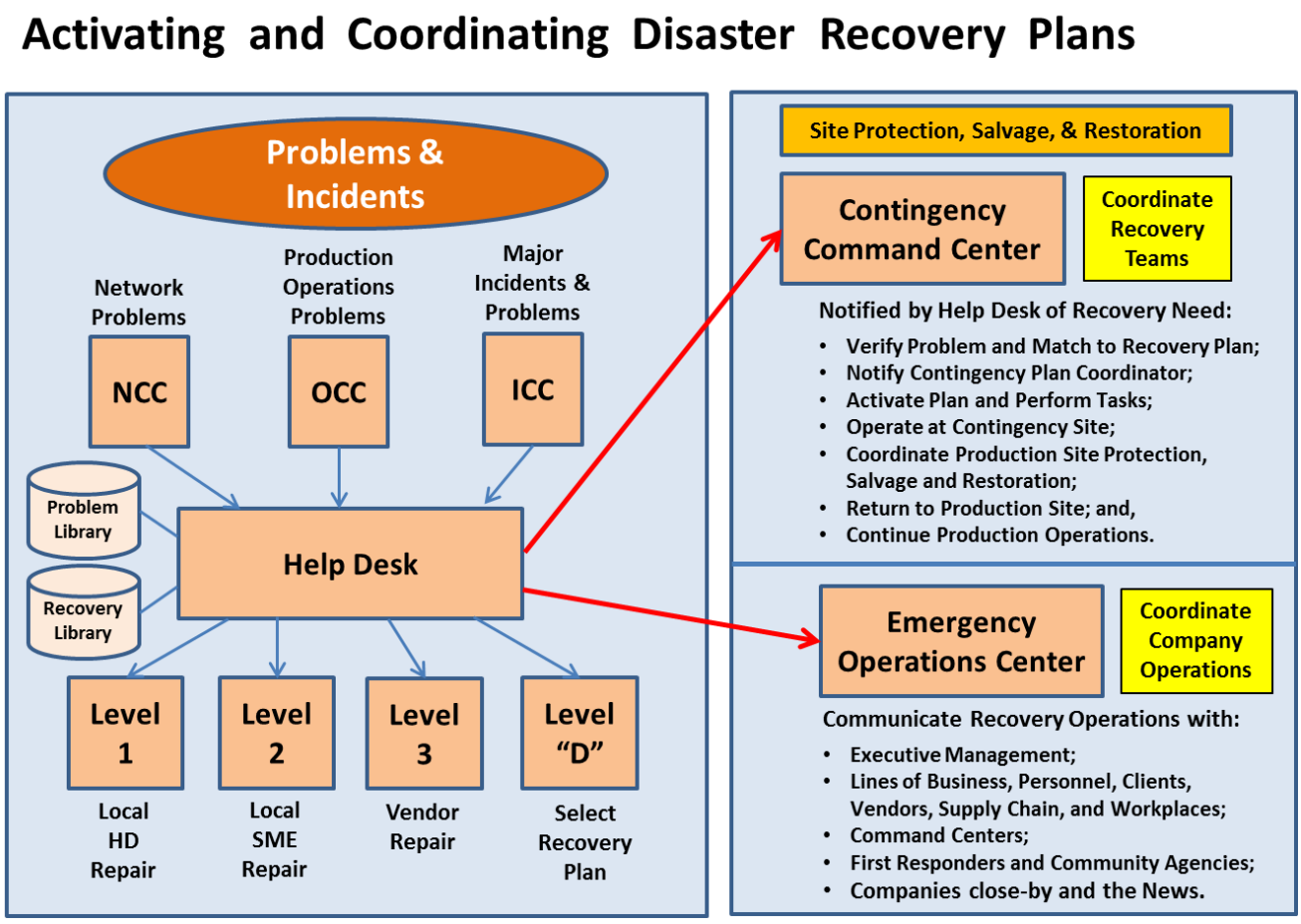
The first task in achieving business continuity is to be able to recognize a problem and take corrective actions that limit the impact of an encountered error. This task is performed by various personnel depending on the type of problem. Problem escalation procedures are employed to present the problem to the right person capable of resolving the issue.

The "Help Desk" (HD) is the central player in problem management and they maintain a data base of encountered problems and their resolutions. Unfamiliar problems are a repetition of a previously experienced incident (80% - 90%) and those repetitions are usually resolved by the Help Desk when reported (this is defined as Level I). If it is a new problem, then the Help Desk will escalate the problem

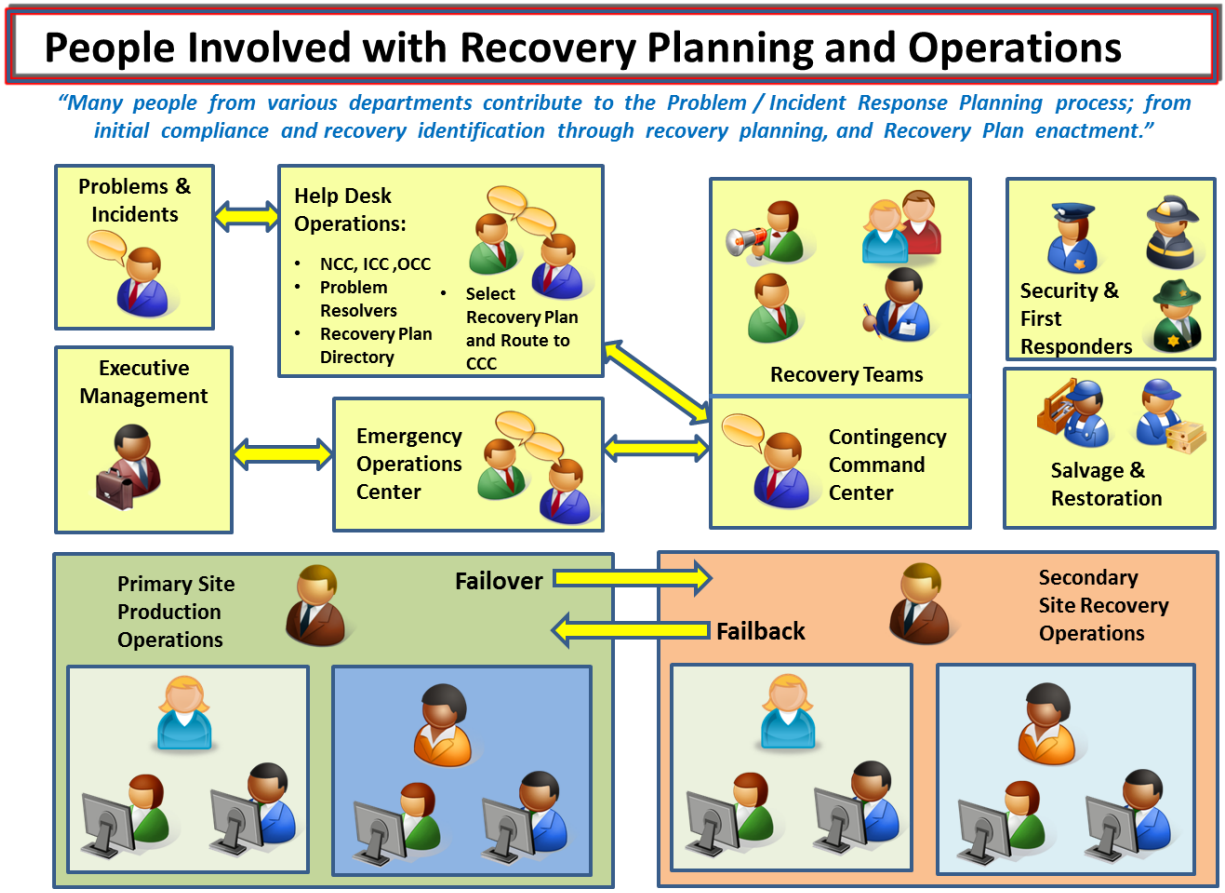
to the company Subject Matter Expert (SME) associated with the failing component (this is defined as Level II). Should the SME not be able to resolve then the problem it is then escalated to the Vendor responsible for supporting the failing component (this is defined as Level III), but should the vendor representative say the problem is unknown and will require extensive time to repair, then the problem is declared a disaster event and raised to Level 'D'. In that instance, the Help Desk relates the problem to the business, or Information Technology, area associated with the disaster event, the Disaster Recovery Manager (DRM) and the Contingency Command Center (CCC) manager alerted. At that point, the DRM calls the recovery team members and has them commence their recovery tasks.

Additional functional areas are activated to assist in Business Continuity operations. They include the Emergency Operations Center, which is responsible for making every attempt to restore business services and to coordinate with Executive Management and the CCC.

Activating and Coordinating Disaster Recovery Plans



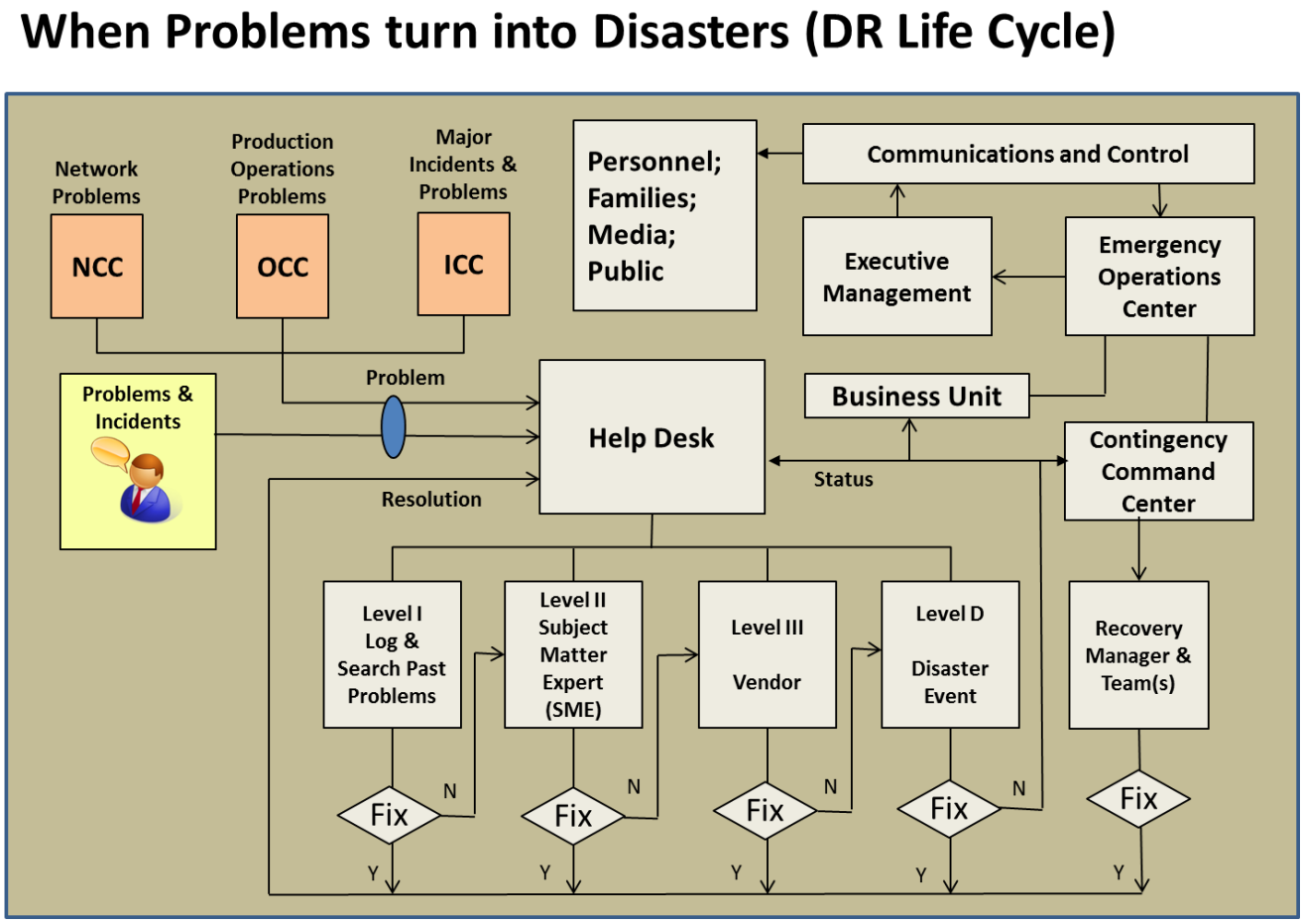
Managing Disaster Events and Coordinating Recovery Operations



Problems can be reported to the Help Desk by the Network Control Center (NCC), the Incident Command Center (ICC), the Operations Command Center (OCC), or by individuals. Problem resolvers are informed of the problem, and an escalation process is starting that could lead to the declaration of a disaster. If a disaster is declared, the help desk will relate the disaster event to a recovery plan and notify the Contingency Command Center and Disaster Recovery Manager of the event. They confirm the problem is indeed a disaster and that this recovery plan is the right one to execute. The Disaster Recovery Manager then notifies his DR team and commences recovery operations.

If a site is damaged and cannot be inhabited, then the personnel at the site are relocated to a business recovery site and the site is protected by company security (who coordinates security with the First Responders and Local Police Department). Salvage and Restoration operations commence when the First Responders turn the site back to the company. Once salvaged and restored, the company will verify that the site is ready for reoccupation and the staff will commence the process of returning to normal operations. This practice is defined as "Failover / Failback."

Problem Life Cycle



The entire Life Cycle of a Problem that has escalated into a Disaster Event is shown above. It starts when a Problem or Incident is reported to the Help Desk from a Command Center (NCC), Operations (OCC), or Incident (ICC)) or an individual. The Problem will go through Level I (Past Problems), Level II (Subject Matter Expert), Level III (Vendor), or Level 'D' (Disaster Event.

If the problem is escalated to a Disaster Event, the Help Desk will notify the Business Unit and the Contingency Command Center, who will in turn notify the Recovery Manager associated with the problem type (Business, information Technology, Application, etc.). The Contingency Command Center will coordinate recovery efforts with the Recovery Manager and the Emergency Operations Center. The EOC will make every attempt to continue business operation and coordinate recovery efforts with Executive Management, who in turn will coordinate recovery operations through communications and control with the EOC, Personnel, their Families, the Media, and the Public. At all times, the First Responders and appropriate government bodies will be kept in the loop until the disaster event is over.

Corporate Certification and Compliance

Adhering to Compliance Laws

- **Gramm Leach Bliley** – Safeguard Act (was Bank Holding Act);
- **Dodd – Frank** – Wall Street Reform and Consumer Protection Act;
- **HIPAA** – Healthcare regulations (including ePHI, HITECH, and Final Ombudsman Rule);
- **Sarbanes – Oxley Act** (sections 302, 404, and 409) on financial assessment and reporting by authorized "Signing Officer";
- **EPA and Superfund** (how it applies to Dumping and Asset Management Disposal);
- **Supply Chain Management "**Laws and Guidelines" included in ***ISO 24762*** (SSAE 16 for Domestic compliance and SSAE 3402 for International Compliance, and NIST 800-34);
- **Supply Chain Management "**Technical Guidelines" described in ***ISO 27031***;
- **Patriots Act** (Know Your Customer, Money Laundering, etc.);
- **Workplace Safety and Violence Prevention** via OSHA, OEM, DHS, and governmental regulations (State Workplace Guidelines and Building Requirements);
- **Income Tax and Financial Information protection** via ***Office of the Comptroller of the Currency*** (OCC) regulations (***Foreign Corrupt Practices Act***, **OCC-177** Contingency Recovery Plan, **OCC-187** Identifying Financial Records, **OCC-229** Access Controls, and **OCC-226** End User Computing).

Corporate Certification includes Adhering to the laws and regulations of the countries where you do business. This refers to Compliance and any deviation from compliance is defined as a GAP, EXCEPTION, or OBSTACLE, where:

1. Gaps are a non-adherence to a specific law or regulation or any required part of that law or regulation.
2. Exceptions are errors in complying with an entire law or regulation and can be caused by ignorance or simply not applying a proper safeguard.
3. Obstacles are barriers that interfere with the achievement of compliance to a specific law or regulation and can be caused by lack of awareness, equipment failures related to growth or the introduction of new technologies, non-adherence to maintaining equipment code levels in

production and recovery at the same levels, or simply not having matching equipment at the production and recovery site.

It is important that there are laws on books that may affect your enterprise and that the laws of countries differ greatly. Make sure you utilize the Audit and Legal departments to assist you determine which laws must be adhered to and which ones do not apply. Perform periodic reviews of the laws and regulations to maintain compliance.

Data Protection

How do we protect data

Laws and Regulations concentrate on the VALIDITY of PROVIDED DATA, so we start with a review of how sensitive data is described, created, protected, and used, including:

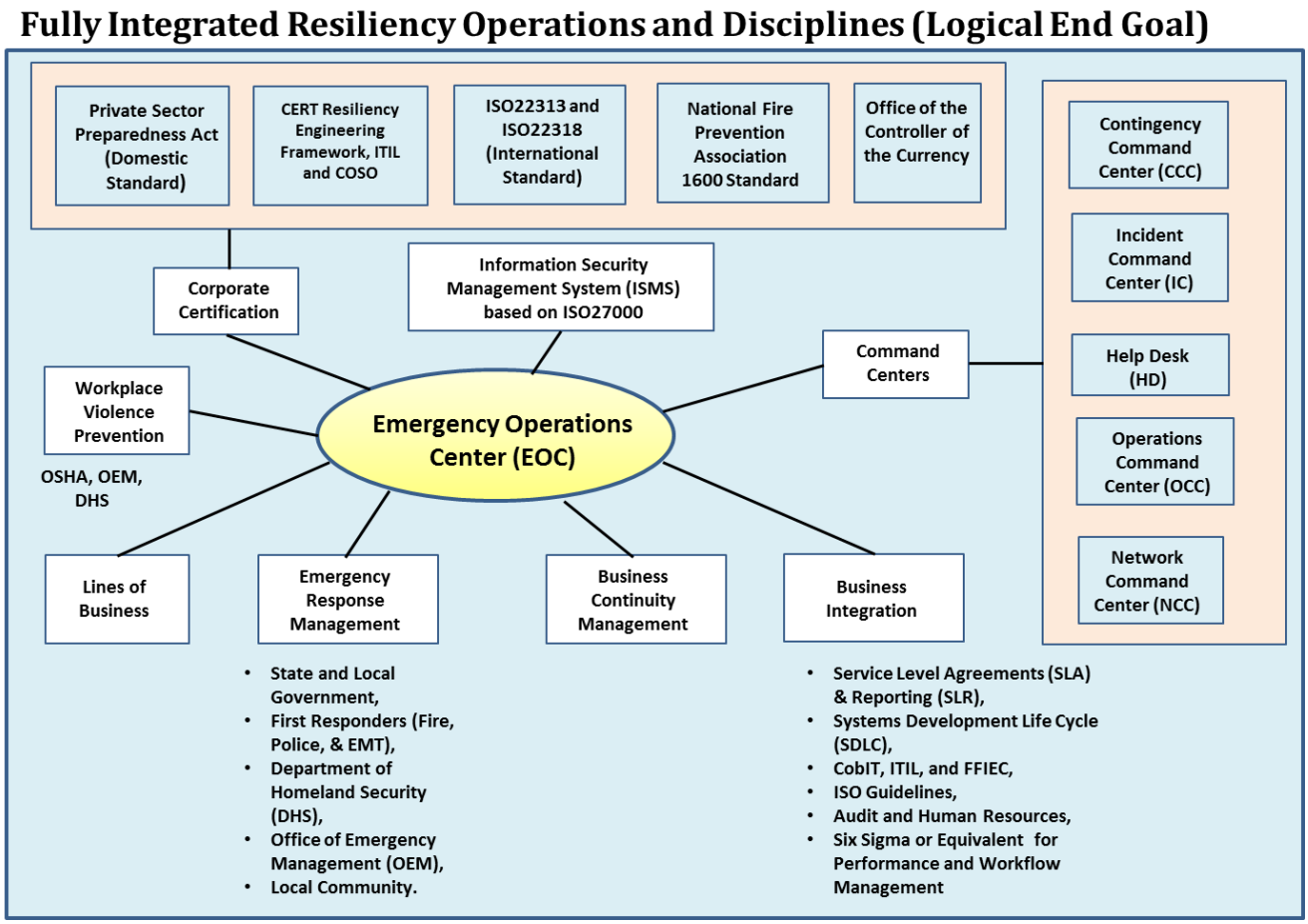
- **Identify the lifecycle of data used in financial reporting and compliance;**
  - **Where does it come from and who owns it?**
  - **What form is it in (Excel, Database, manual, fax, email, etc.),**
  - **Who has access to the data and how can they impact data (*CRUD* - create, read, update, and delete).**
- **Review current Data Sensitivity and IT Security procedures;**
- **Examine Library Management, Backup, Recovery, and Vaulting procedures associated with sensitive data;**
- **Review Business Continuity Planning and Disaster Recovery procedures used to protect and safeguard critical Information Technology and Business facilities;**
- **Utilize existing Standards and Procedures to duplicate process and identify errors; and,**
- **Examine the available Employee Awareness and Education programs.**

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

In today's world of Virtual Machines and High-Speed Transmission Bandwidths, it is possible to safeguard data and recover operations instantly without loss of information. Firewalls and security programs are used to allow data access to only authorized users, whose access is limited to their functional responsibility (end users cannot create, modify, or delete date unless specifically part of their job function).

Vital Records Management has been achieved by performing periodic back-ups of critical information and placing that information into on-site and off-site vaults, but in today's world these processes are sped up through Snapshots (periodic or continuous pictures that can be restored at a recovery or maintenance site) and the use of data Deduplication and Virtual Tape Libraries (eliminating redundant backups and the amount of data transmitted over the Wide Area Network (WAN).

The End Goal of EOC and Business Continuation



A fully integrated EOC will appear as shown above and will be capable of controlling disaster events, communicating within the company, and minimizing business interruptions. It is a goal every company strives to achieve.

If you would like to know how we can help you achieve this goal, please contact Tom Bronack at (917) 673-6992 or via email at bronackt@dcag.com. Thank you.

