"Achieving Enterprise Resiliency and Corporate Certification"
By Thomas Bronack, CBCP

Introduction

Do all of your recovery personnel understand the full range of recovery disciplines used by your firm? Do you have a recovery organization chart defining functions, naming people to positions, and showing work flow? Is your recovery operation as efficient as you would like it to be? Can people function across recovery disciplines should the need arise due to personnel shortages or unplanned for disaster events? Have you utilized industry best practices to create and support recovery operations? Is gaining a corporate certification for recovery operations a goal of the company? Are you afraid your company's reputation could be affected by a disaster event? Any of these problems can hurt your company and its clients. This document will help you develop a direction to address these issues.

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

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

The steps followed to "Achieving Enterprise Resiliency and Corporate Certification" include:

1. **Problem Definition –** what your organization must do to improve recovery operations by implementing a common recovery language and toolset that will optimize recovery communications and efficiency. The goal of this phase is to define where you are today and identify any gaps and exceptions that need to be mitigated through better controls.

2. **Solution Formulation –** define the best solution to achieve Enterprise Resiliency for your company. The goal of this phase is to determine how to best mitigate uncovered gaps and exceptions, while establishing a foundation upon which Enterprise Resiliency and Corporate Certification can be achieved.

3. **Implement Enterprise Resiliency –** will combine recovery operations into a common recovery discipline and develop a common language and toolset for recovery operations. It is not designed to eliminate the current recovery disciplines, but rather to help them communicate better. Common tools will allow for the gathering of information needed to support recovery operations and better respond to disaster events.

4. **Utilize Best Practices –** by using industry accepted Best Practices you will be assured that whatever recovery process is developed it will have a solid foundation upon which recovery operations can be optimized. This will both protect the company better and allow for corporate certification should you choose to go in that direction. An illustration of how Enterprise Resiliency is constructed on a solid foundation is provided in this document.

5. **Integrate Enterprise Resiliency –** will provide for new and changed components to be included in recovery operations without personnel having to perform additional steps that are outside of their everyday functions and company standards. Adherence to System Development Life Cycles and Version and Release Management will insure that the recovery environment is constantly maintained in a current state. Documentation, awareness activities, and educational services must be provided to employees and other personnel affected by recovery operations.

6. **Emergency Response Structure –** a recovery environment that protects against threats, business interruptions, and adheres to compliance requirements will be constructed by following the direction of this document. The Emergency Response environment will feed Emergency Management Operations via Crisis Management, Business Continuity, and Workplace Violence Prevention processes, which will result in the production of all required recovery operations and better Crisis Communications. An illustration of how this environment might be constructed is provided in this document.

7. **Gaining Corporate Certification –** will be a company decision that management will have to make, but following the guidelines included in this document will allow you to create a solid recovery operation that can support corporate certification through best practices, integration, and audit ability. Adherence to certification guidelines described in this document will lead to gaining a corporate certification

8. **Enterprise Resiliency Environment –** once completed recovery operations will have a specific structure that interfaces with all aspects of the organization. An illustration of what that organization should look like is provided.

The Problem

Using different recovery disciplines with various languages and tools will affect your ability to:

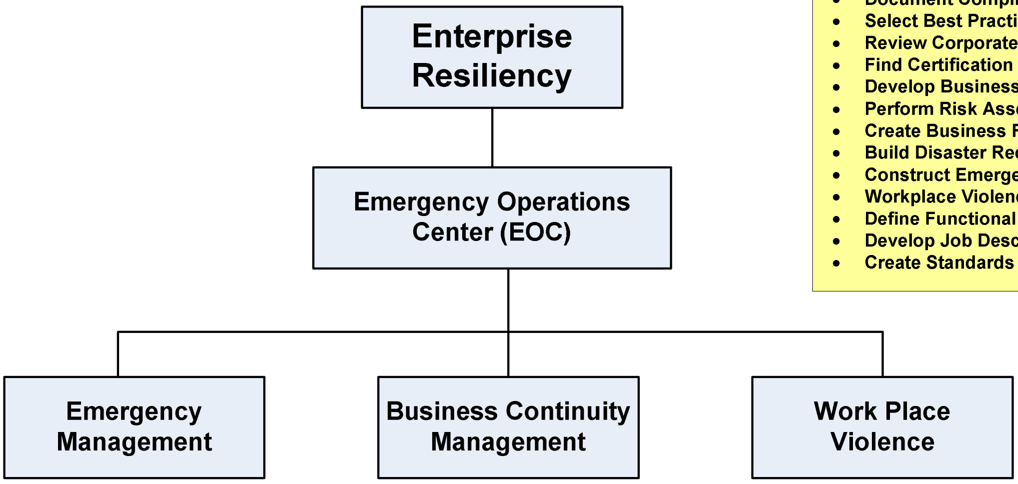
- Coordinate recovery operations (common tools, common language, common procedures, etc.);
- Protect personnel, clients, suppliers, and business operations;
- Efficiently respond to problems and disasters;
- Adhere to compliance and regulatory requirements;
- Comply with domestic and international recovery guidelines and best practices;
- Achieve corporate certification for recovery operations; and
- Ensure clients and suppliers that your recovery operations are at their highest efficiency.

A Risk Assessment and Business Impact Analysis (BIA) will uncover gaps and exceptions in your organization's existing recovery operations. Once detected, mitigations and controls to eliminate the gaps and exceptions should be analyzed to determine if the cost to fix is greater than the cost of the problem. This information should be reported to management so that a direction can be selected to move the project forward.

What is Enterprise Resiliency

The Road to Enterprise Resiliency Includes:

- **Define Risks (Natural, Man-Made);**
- **Document Compliance Requirements;**
- **Select Best Practices tools and processes;**
- **Review Corporate Certification Guidelines;**
- **Find Certification Firms / Organizations;**
- **Develop Business Plan;**
- **Perform Risk Assessment / BIA;**
- **Create Business Recovery Plans;**
- **Build Disaster Recovery Plans;**
- **Construct Emergency Recovery Plans;**
- **Workplace Violence Prevention Plans;**
- **Define Functional Responsibilities;**
- **Develop Job Descriptions; and**
- **Create Standards and Procedures.**


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

The goal of Enterprise Resiliency is to combine the three recovery disciplines of Emergency Management, Business Continuity Management, and Workplace Violence Prevention into a cohesive discipline with a common language and common tools. By following this path, all Recovery Personnel will learn about Emergency Management, Business Continuity Management, and Workplace Violence. This will make Recovery Personnel better able to respond to disaster events by utilizing existing tools, disciplines, a common language, and a common set of Standards and Procedures.

The Solution

Before you can combine the recovery disciplines into an enterprise resiliency organization you must perform the following tasks. Analysis of collected information will allow your company to determine the best direction to follow when creating an Enterprise Resiliency environment.

- **Review** existing recovery operations including Emergency Management Preparedness, Business Continuity Management, Workplace Violence Prevention, and Enterprise Security Operations (physical and data).

- **Evaluate** Command Centers and how they interact with recovery operations. The command centers that should be evaluated include: Emergency Operations Center (EOC); Incident Command Center (ICC); Help Desk (HD); Network Control Center (NCC); and the Operations Control Center (OCC).

- **Define** company Lines of Business (LOBs), including: business functions, products, and services provided; locations and personnel; customers and suppliers; applications and business processes; and existing evacuation, crisis management, and recovery management operations.

- **Document** integration requirements, including Service Level Agreements (SLA) and Service Level Reporting (SLR) requirements; Systems Development Life Cycle (SDLC); Best Practices tools and procedures; the recovery organization, personnel assigned to positions, functional responsibilities, job descriptions, and standards and procedures.

- **Create** a Business Plan including: Mission Statement; Goals and Objectives; Assumptions; Scope and Deliverables; Detailed Project Plan with phases and tasks included; gain management acceptance and approval through a report and presentation; assign personnel and resources; define functional responsibilities; job descriptions; and standards and procedures; monitor, report, improve, validate, roll-out, train, and implement Enterprise Resiliency.

Implementing Enterprise Resiliency will combine the recovery disciplines of:

- **Business Continuity Management**, consisting of:
  - **Business Recovery** for office facilities;
  - **Disaster Recovery** for information technology facilities;
  - **Risk Management** for compliance and insurance; and
  - **Crisis Management** for evacuations and personal safety.

- **Emergency Management**, having the ability to respond to:
  - **Malicious Activities** (fraud, theft, blackmail, sabotage, and terrorism);
  - **Natural Disasters** (fire, floods and other water damage, severe weather, avian flu, swine flu, epidemics, pandemics, air contaminants, and hazardous chemical spills);
  - **Technical Disasters** (communications, power failures, data failures, backup and storage management systems, equipment and software failure, and transportation system failures);
  - **External Threats** (suppliers down, business partner down, and neighboring business down); and
  - **Facilities** (HVAC – heating ventilation, and air conditioning, emergency power or uninterrupted power, and recovery site unavailable).

- **Workplace Violence Prevention**, including:
    - Compliance with the **Workplace Violence Prevention Act** which directs every employer to perform a Workplace Evaluation and Risk Assessment to develop and implement programs to prevent and minimize workplace violence events;
    - Adherence to "**Standard of Care**" and OSHA "**General Duty Law**" consisting of:
        - Comprehensive policy for workplace violence;
        - Trained employees on Workplace Violence and its impact;
        - Adherence to "**Duty to Warn**" precautions that require a threat to be reported and background checks for potential hires performed; and
        - Use of best practices for physical security and access controls.
    - Physical security perimeters utilizing guards and surveillance cameras;
    - Card keys and access controls; with physical accompanying or some guests;
    - Employee Assistance Programs to help personnel cope with a personal life crisis and avoid workplace violence situations – a range of these programs should be made available to employees and their family.

- **Enterprise Security Operations**, including physical and data security to ensure access to physical locations and data assets is only provided to authorized personnel and that safeguards are in place to identify, record, analyze, and respond to security violations in a timely and accurate manner.

Utilizing Best Practices to implement Enterprise Resiliency, including:

- **COSO –** Committee of Sponsoring Organizations - to develop Risk Management and Mitigation guidelines that will help identify areas where improvement must be sought. The use of COSO guidelines will protect stakeholders from uncertainty and associated risks that could erode value. COSO Risk Assessments include:

    - Internal environment reviews;
    - Objective setting;
    - Event identification guidelines and definitions;
    - Risk Assessment standards and procedures;
    - Risk response guidelines and objectives;
    - Mitigation and Control Activities;
    - Information and communication requirements; and
    - Monitoring and reporting requirements.

The Human Resource Management component of COSO includes:

- Creation of an Organizational Structure, with personnel assigned to functions;
- Definition of Functional Responsibilities and Job Descriptions;
- Work Flow definitions;
- Personnel Evaluations and guidelines;
- Defining Personnel Career Paths and providing training; and
- Creation of required supportive documentation, including Standards and Procedures, User Guides, Job Run books (setup, processing, breakdown, and delivery), and Messages and Codes Manuals (Error definitions and Circumventions).

- **CobIT –** Control Objectives for Information Technology, is designed to extend COSO controls over the Information Technology environment by:

  - Providing guidelines for planning and integrating new, or changed, products and services into the IT organization;
  - Integrating new acquisitions and mergers;
  - Delivering new acquisitions and mergers, then supporting and maintaining them going forward;
  - Monitoring IT activity, capacity, and performance so that management can meet business objectives while protecting information and IT resources.

- **ITIL –** Information Technology Infrastructure Library, is responsible for Service Delivery and Service Support in the IT environment consisting of:

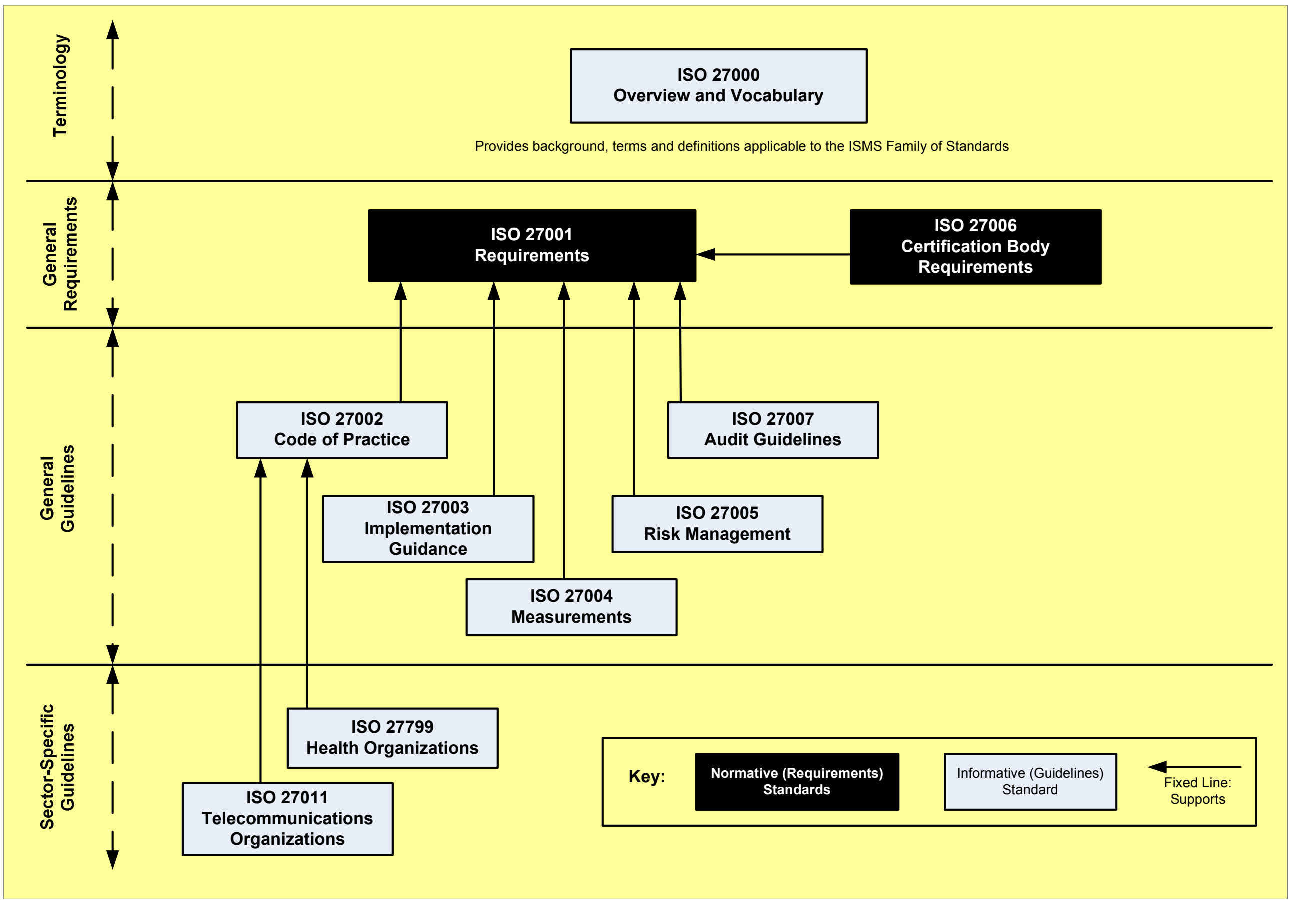
  - **Service Delivery** is comprised of Service Level Management, Availability Management, Capacity Management, IT Service Continuity Management, and Financial Management for IT Services.
  - **Service Support** is comprised of Incident Management, Problem Management, Change Management, Configuration Management, and Version and Release Management.
  - **ISO27000 Information Security Management System**

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

    1. ISO 27000 – Overview and Vocabulary;
    2. ISO 27001 – Requirements definitions and guidelines;
    3. ISO 27002 – Code of Practices document and guidelines;

4. ISO 27003 – Implementation Guidelines;
5. ISO 27004 - Measurements guidelines and practices;
6. ISO 27005 – Risk Management guidelines and practices;
7. ISO 27006 – Audit Guidelines;
8. ISO 27799 – Health Organization guidelines and practices; and,
9. ISO 27011 – Telecommunications Organizations guidelines and procedures.

ISO 2700 Overview and Sections



- **Six Sigma** – Methodology to optimize operations through review and change. Its goal is reduce errors to only 4 per million or less.

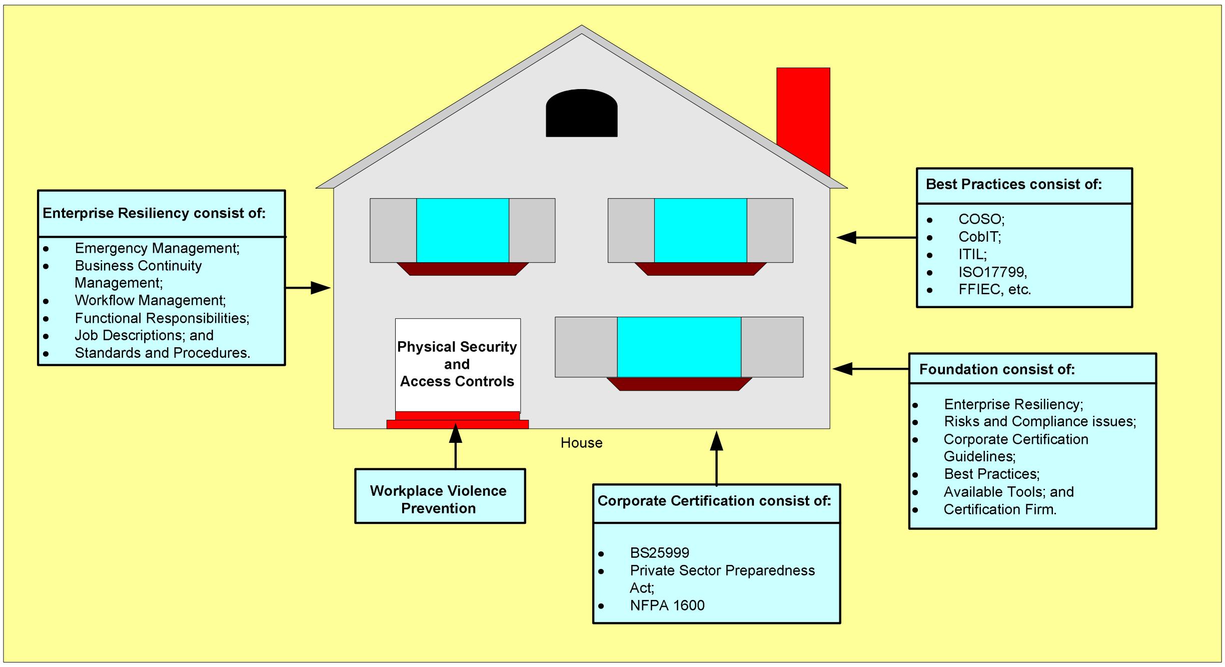
- **FFIEC** – Federal Financial Institutions Examination Council Business Continuity Handbook – Set of recovery guidelines that is widely accepted as the most robust and accurate in the financial services sector, and other sectors. The guidelines contained within FFIEC will help you develop an excellent recovery operation environment.

Even if you choose not to go forward with a corporate certification, using best practices will insure that your recovery operations are based on industry accepted guidelines and practices. Using best practices is a win-win situation that allows your company to gain a corporate certification or just build a strong foundation for further recovery operations and efficiency improvements.

Integrate Enterprise Resiliency throughout the corporation, including:

- Business Operations, Client Support, Supplier Support, and Community Outreach;
- Systems Development Life Cycle, Systems Management, and Functional Responsibilities;
- Documentation, Awareness, and Training;
- Job Descriptions and a Standards and Procedures Manual; and
- Corporate-Wide Recovery Operations.

Enterprise Resiliency must be built upon a Solid Foundation


Enterprise Resiliency consist of:
• Emergency Management;
• Business Continuity Management;
• Workflow Management;
• Functional Responsibilities;
• Job Descriptions; and
• Standards and Procedures.
Physical Security and Access Controls
House
Workplace Violence Prevention
Corporate Certification consist of:
• BS25999
• Private Sector Preparedness Act;
• NFPA 1600
Best Practices consist of:
• COSO;
• CobIT;
• ITIL;
• ISO17799,
• FFIEC, etc.
Foundation consist of:
• Enterprise Resiliency;
• Risks and Compliance issues;
• Corporate Certification Guidelines;
• Best Practices;
• Available Tools; and
• Certification Firm.

Just like when building a house, it is essential to establish a solid foundation upon which you can establish the Enterprise Resiliency operation. For this reason, it is imperative that you plan the process and use Best Practices guidelines and tools to better coordinate the delivery of recovery operations and procedures. Emergency Management should respond to natural disasters, Business Management is responsible for responding to Technology and Business Interruptions, and Workplace Violence Prevention should block unauthorized entrance to facilities and offer Employee Assistance Programs to help personnel through life problems that may lead to violent acts. Integrating these disciplines within the corporate work-flow, documenting procedures, providing training, and implementing a Standards and Procedures Manual will assist in achieving the Enterprise Resiliency environment.

The integration of Enterprise Resiliency with the everyday functions performed by personnel will insure that recovery operations are always maintained in a current and accurate manner. Updating supportive documentation and providing awareness and education classes will provide personnel with a better understanding of recovery operations and result in more efficient recovery operations through better protection for the company and its clients.

Identifying and including Audit Checkpoints within the Enterprise Resiliency environment will provide auditors and regulators with the information they need to insure that your environment is safeguarded and in compliance. Utilizing these checkpoints internally will allow your auditing department to better provide management with warnings that operations are exposed to threats and interruptions, thereby allowing for the improvement of recovery operations to respond to these gaps and exceptions through better controls and mitigations. This direction adheres to Best Practices, Corporate Certification guidelines and just makes great business sense.

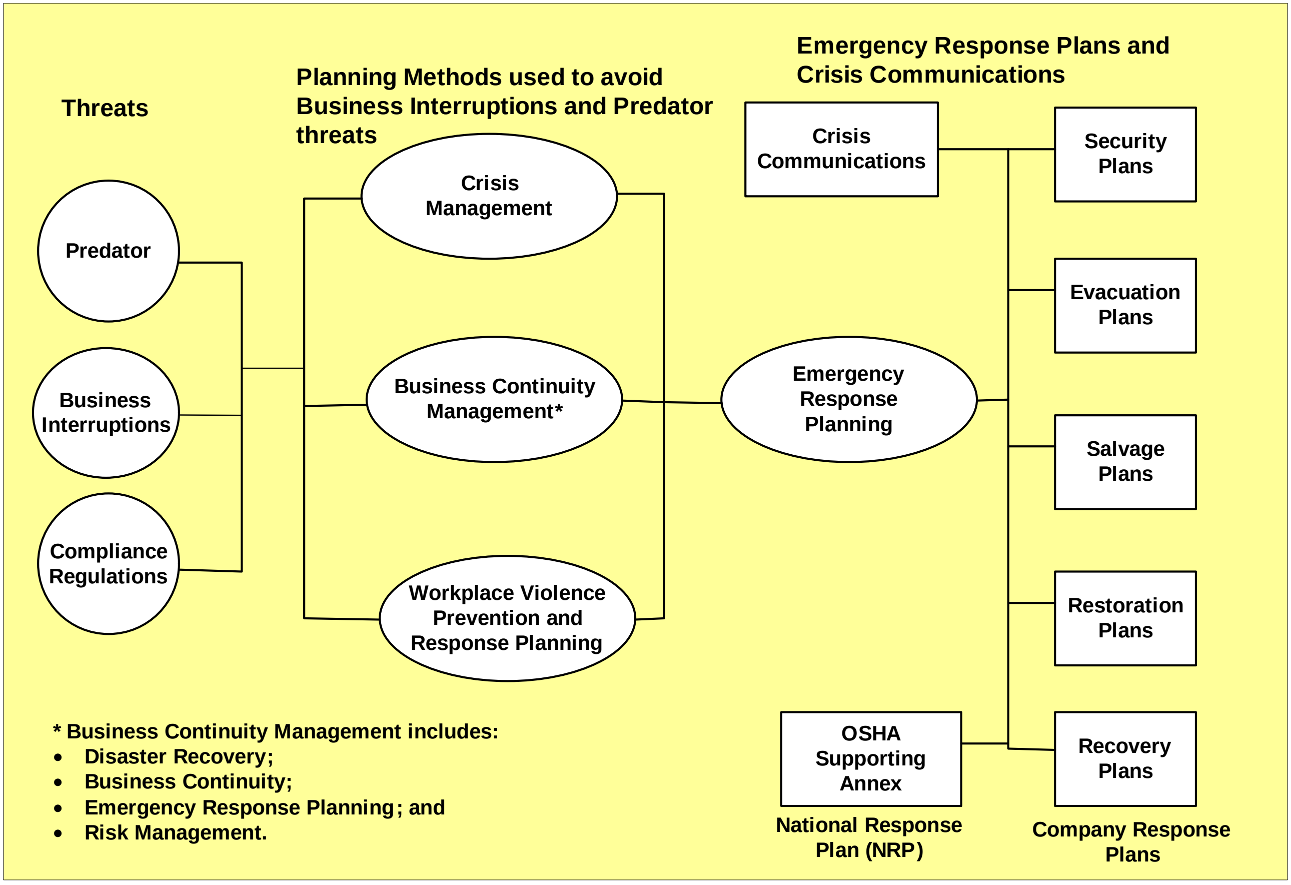
BS25999 is a Business Continuity Management (BCM) standard consisting of two parts. The first part, “BS25999-1:2006 Business Continuity Management Code of Practice”, takes the form of general guidance and seeks to establish processes, principles, and terminology for Business Continuity Management. The second part, “BS25999-2:2007 Specification for Business Continuity Management”, specifies requirements for implementing, operating, and improving a documented Business Continuity Management System (BCMS), describing only requirements that can be objectively and independently audited. A useful means of understanding the difference between the two parts is that Part 1 is a guidance document and uses the term “should”, while Part 2 is an independently verifiable specification that uses the word “shall”. BS25999-2 uses the “**Plan-Do-Check-Act**” model of continuous improvement so that recovery operations will be constantly improved over time. You may want to review the BS25999 documents to better understand their recommendations.

Emergency Response Structure

The structure of a recovery operation should provide for the identification of all threats, reduction or avoidance of business interruptions, and compliance with all regulatory requirements. The recovery operations environment should be able to use planning disciplines like Crisis Management, Business Continuity Management, and Workplace Violence Prevention and Response Planning to support Emergency Response Planning operations.

Reducing threats and business interruptions, while adhering to compliance requirements, is the goal of Enterprise Resiliency. Achieving this goal requires the full cooperation of all existing recovery disciplines and ensuring that all national and local regulations are adhered to. Refer to Homeland Security and the Office of Emergency Management to learn about National Response Plans, while First Responders (Fire / Police) can provide essential local assistance in developing recovery plans that will best protect people, customers, suppliers, and business operations.

Emergency Response Planning environment


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

Achieving a recovery structure that supports Emergency Response Planning through Crisis Management, Business Continuity Management, and Workplace Violence Prevention will allow an organization to protect against Predators, Business Interruptions, and allow for the adherence to Compliance Regulations.

Emergency Response Plans can be constructed to provide Crisis Communications, OSHA compliance through National Response Plans (Hazardous Materials, etc.), Security Plans to protect assets and personnel, Evacuation Plans, Salvage Plans, Restoration Plans, and Recovery Plans.

Gaining Corporate Certification

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

Corporate Certification must be validated by an outside firm who is qualified to review recovery operations and declare a firm in compliance to certification requirements.

Corporate Certification is based on:

- Private Sector Preparedness Act (PL 110-53, Title IX, Section 524);
- National Fire Prevention Association standard 1600; and
- BS25999 International Standard.

Procedures and guidelines included in the Corporate Certification guidelines will provide a direction to follow, including:

- Defining Risk (Natural and Man-Made);
- Researching and documenting Compliance Requirements;
- Obtaining Best practices tools and guidelines;
- Locating Certification Firms and Organizations;
- Defining Certification Requirements and Adherence Guidelines;
- Creating a Business Plan and Project Plan to implement Corporate Certification;
- Performing a Risk Assessment and Business Impact Analysis;
- Defining Audit Requirements and Checkpoints;
- Elimination of any identified Gaps and Exceptions through Mitigations and Controls;
- Defining the Recovery Organization, Functional Responsibilities, Job Description, and Standards and Procedures for developing and maintaining recovery operations;
- Providing Awareness and Educational Courses; and
- Developing Recovery Plans for Business Recovery Management, Emergency Management Preparedness, and Workplace Violence Prevention.

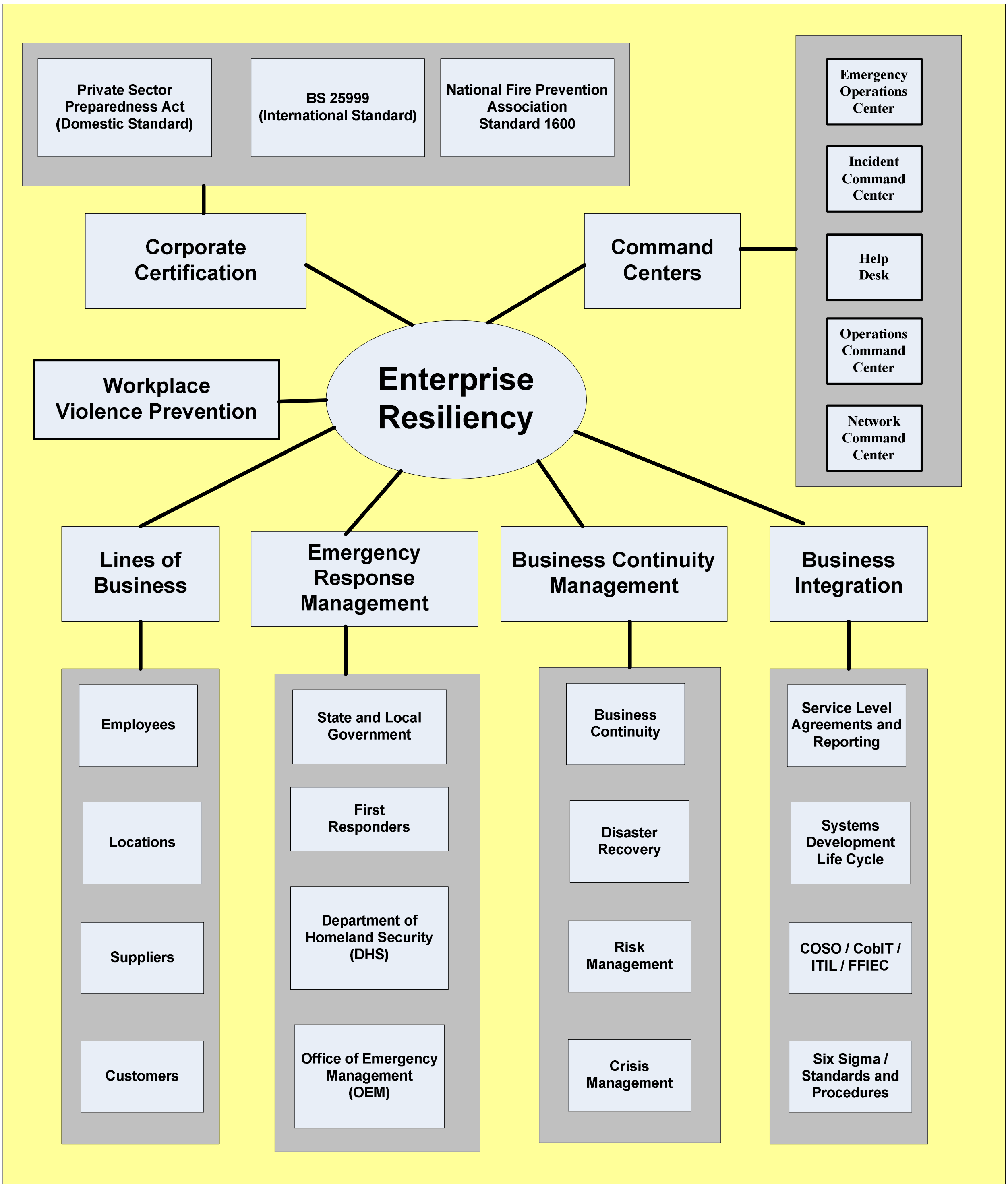
The Enterprise Resiliency Environment

The final step in implementing an Enterprise Resiliency environment is to integrate the recovery operations throughout the organization, including Command Centers, Lines of Business, Emergency Response Management, Business Continuity Management, Workplace Violence Prevention, and Business Integration. Achieving Corporate Certification will require integrating the Private Sector Preparedness Act; BS25999 international standards, and the National Fire Prevention Association standard 1600.

An illustration of the final Enterprise Resiliency Organizational Structure is provided as a guideline for you to follow. You may not complete all sections shown, but any improvement will result in better recovery operations and more protection for you people and business. It can be considered as a foundation that will allow for the inclusion of the various recovery disciplines, a common language, and a common set of recovery tools.

Fully integrated Enterprise Resiliency Environment

Integrating Recovery Operations and Disciplines


Private Sector Preparedness Act (Domestic Standard)
BS 25999 (International Standard)
National Fire Prevention Association Standard 1600
Corporate Certification
Command Centers
Emergency Operations Center
Incident Command Center
Help Desk
Operations Command Center
Network Command Center
Workplace Violence Prevention
Enterprise Resiliency
Lines of Business
Emergency Response Management
Business Continuity Management
Business Integration
Employees
Locations
Suppliers
Customers
State and Local Government
First Responders
Department of Homeland Security (DHS)
Office of Emergency Management (OEM)
Business Continuity
Disaster Recovery
Risk Management
Crisis Management
Service Level Agreements and Reporting
Systems Development Life Cycle
COSO / CobIT / ITIL / FFIEC
Six Sigma / Standards and Procedures

Conclusion

By following the direction and recommendations contained in this article, your company will establish recovery operations that meet or exceed industry standards, while preparing the corporation for international and domestic certification of recovery operations.

Even if you choose not to go forward with certification, your recovery organization will certainly be improved through a common language and set of tools that enhances communications throughout all recovery disciplines, while reducing the time needed to identify, analyze, respond to, and recover from encountered disaster events.

Command center operations will be improved through recovery standards that support a dialog between the Emergency Operations Center (EOC) and the command centers that identify, analyze, and report problem events and incidents that could escalate to a disaster event if not addressed in a timely and appropriate manner.

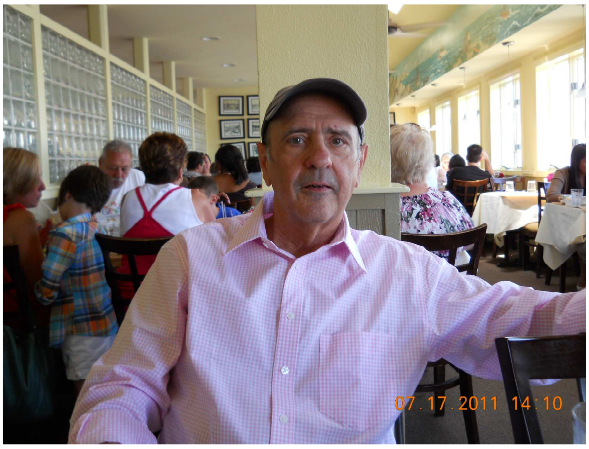
Lines of Business (LOBs) will be better supported through recovery operations that protect people, clients, suppliers, and locations by executing Business Impact Analysis (BIA), Risk Assessments, leading to the creation of: Business Recovery Plans for business processes; Emergency Recovery Plans to protect facilities; and Workplace Violence Preventions Plans to protect personnel and assets from intrusion and violent acts.

By integrating recovery operations within the company and using best practices to create and implement the recovery organization, you will know that recovery plans adhere to company standards and are included in the systems development life cycle (SDLC), support, change, and maintenance processes. Also the creation and support of recovery operations is accomplished through the everyday functions performed by personnel and not through additional tasks that will certainly not always be accomplished.

The improvements in recovery operations gained through using a common language and tool set will result in more efficient communications, reduced recovery times, better support of clients and suppliers, improved community outreach, and a better reputation for the firm. Recovery personnel will have an expanded knowledge base allowing them to better understand potential disaster events and communicate their concerns to management, resulting in improved recovery operations.

Better plans, a more knowledgeable staff, better recovery coordination, improved reputation, and the opportunity to gain corporate certification all add up to a great direction to follow. Consistently improving recovery operations built on a solid foundation and adhering to industry best practices will insure that recovery operations are at the highest level of efficiency. Including audit check points by following the recommendations included in BS25999-2 will lead to fewer gaps and exceptions that would require mitigations or controls to be established. All this leads to a safer environment that is in full compliance and offers the best protection for personnel and the business. Sounds like a good plan to me, I hope you agree.

Bio.



Tom 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, and procedures documentation. Tom has also presented materials and conducted workshops to IFSA, ISACA, ISSA and CPE User Groups. Tom career included: IBM (NY Banking Office as CE / PSR); MHT Bank (started the Computer Risk Management department, then became the Technical Support Manager for the Trust Data Center); Chemical Bank (Mainframe Capacity and Performance Manager); Storage Technology Corporation (NE Regional SE Manager supporting 135 field personnel and 45 salesmen); SIAC (Systems Programming Manager supporting the NYSE and AMEX); and then Tom created the Data Center Assistance Group (DCAG) in January, 1980 to provide consulting, personnel placement, and sales services to client base. Tom is presently on the Board of Directors of the NYC Metro Chapter of the Association of Contingency Planners and the Director of Vendor Relations.