Continuous, clean, and uninterrupted power and cooling is the lifeblood of any data center, especially one that operates 24 hours a day, 7 days a week. Critical enterprise power is the power without which an organization would quickly be unable to achieve its business objectives. Today, more than ever, enterprises of all types and sizes are demanding 24-hour system availability. This means enterprises must have 24-hour power and cooling day after day, year after year. One such example is the banking and financial services industry. Businesses demand immediate continuous uptime for all computer and network equipment to facilitate around-the-clock trading and banking activities anywhere and everywhere in the world. Banking and financial services firms are completely intolerant of unscheduled down-time, given the guaranteed loss of business that invariably results. However, providing the best equipment is not enough to ensure 24-hour operation throughout the year. The goal is to achieve reliable 24-hour power and cooling at all times, regardless of the technological sophistication of the equipment or the demands placed upon that equipment by the end user, be it a business or a municipality.

Today, all industries are constantly expanding to meet the needs of the growing global digital economy. Industry as a whole has been innovative in the design and use of the latest technologies, driving its businesses to become increasingly digitized in...
their highly competitive, business environment. Industry is progressively more dependent on continuous operation of its data centers in reaction to the competitive realities of a global economy. To achieve optimum reliability when the supply and availability of power are becoming less certain is challenging to say the least. The data center of the past required only the installation of relatively simple protective electrical and mechanical equipment, mainly for computer rooms. Data centers today operate on a much larger scale. The proliferation of distributed systems using networks of desktop PCs and workstations connected through LANs and WANs, simultaneously using millions of end-user business applications and supporting hundreds, thousands each building a computer room. As we add the total number of Terabytes of data held by each bank; all over the world utilizing the Internet, we now realize the necessity of a critical infrastructure and the associated benefits of options and availability.

The loss of corporate America was recently caused by a number of historically significant events: the collapse of the dot-com bubble and the high-profile corporate scandals. These events have taken a significant toll on financial markets and have caused to deflate the faith and confidence of investors. In response, governments and other groups have taken over new or revised existing laws, standards, and regulations. In addition, the Sarbanes-Oxley Act of 2002 (SOX), similar acts in Europe such as the New Market Order Act of 2002 (NMS), and the USA PATRIOT Act were enacted. In addition to management accountability, another essential component of SOX mandates it imperative for companies to have clear, well-developing plans and continuity of operations. This will not only result in ensuring the infrastructure that would support the company, but also maintaining the company's physical location that would continuously execute transactions in a timely fashion. These laws can actually improve business productivity and processes.

Many companies thoughtlessly fail to consider installing backup equipment or the proper redundancy based on their risk profile. When the lights go out due to a major power outage, these same companies quickly wake up, with the outcome of taking a huge hit operationally and financially. During the winter following the Northeast blackout of 2003, there was a marked increase in the installation of unacceptable power supply (UPS) systems and standby generation. Small and large businesses alike learned how susceptible they are to power outages and the associated costs of not being prepared. Storms businesses that were not typically considered mission critical learned that they could not afford to be unprepared during a power outage. The Northeast blackout of 2003 emphasized the importance of ensuring the critical infrastructure and the cascading effects that occur when one component fails. Most associated critical machines (ATMs, etc.) in the affected area stopped working; although several back up systems failed, the number of failures is significant for all critical systems. The result was a loss of revenue, reputations, and almost the loss of confidence in our financial system. More prudent planning and the proper level of investment in resilient critical infrastructures for electric, water, and telecommunications utilities, coupled with proactive building infrastructure preservation and operations, could have saved the banking and financial services industry millions of dollars.

At the present time, the risks associated with cascading power supply interruptions from the public electrical grid in the United States have increased due to the existen-
existing challenges in computer and related technologies. Today, there are close to one billion desktop computers and over one billion people connected to the Worldwide Web. As the number of computers and related technologies continues to multiply in this increasingly digital world, the demand for reliable quality power increases as well. Businesses and not only computers, in the marketplace to deliver whatever goods and services are purchased for consumption, but now they must compete to hire the best engineers from a diminishing pool of talent who can design the best infrastructure needed to obtain and deliver reliable power and cooling. This requires a much more critical understanding and technology exists now and coming with the ability to provide the very power that services that sustain them. The idea that businesses today must compete for the best talent to obtain reliable power is not new, and neither are the consequences of failing to meet this challenge. Without reliable power, there are no products and services for sale, no customers, and no profits—only losses. Mining and keeping the best trained engineers complicate the very best analysts, making the best strategic choices, and following the best operational plans to keep ahead of the power supply curve is essential for any technologically sophisticated business to thrive and prosper. A key to success is to provide proper training and educational resources to employees so they may increase their knowledge and keep current with the latest mission critical technologies available all over the world, which is one of the purposes of this book. In addition, all companies need to develop an educational system and certification programs for young mission critical engineers to help address the growing worldwide necessity to sustain the growing mission critical industry.

It is also essential for critical industries to consistently use systematically evaluate their mission critical systems, assess and measure their level of risk tolerance versus the cost of downtime, and plan for future upgrades in equipment and services that are designed to meet current needs and ensure maintenance of power and cooling systems for the years ahead. Simply put, minimizing unplanned downtime reduces risk. Unfortunately, the most common approach in existence, that is, selecting time and resources to repair a faulty piece of equipment, often results in a process of identifying when the equipment is likely to fail and repairing it without replacement. If the utility goes down, install a generator. If a ground fault trips critical loads, redesign the distribution system. If a lightning strike burns power supplies, install a new lightning protection system. Such measures certainly make sense, as they address real risks associated with the critical infrastructure; however, they are often performed after the damage has occurred. Strategic planning can identify internal risks and provide a prioritized plan for reliability improvements that identify the most causes of failure before they occur.

In the world of high-powered businesses, owners of critical assets have come to learn that they, too, must meet the demands for reliable power supply to their businesses. As more and more buildings are required to deliver service guarantees, management must decide what performance is required from each facility in the building. Availability levels of 99.9999% (5.2 minutes of downtime per year) allow virtually no facility downtime for maintenance or other planned or unplanned events. Meeting increased high reliability is imperative. Moreover, avoiding the problems that can cause outages and unscheduled downtime never ends. Even planning and impact assessments are tasks that are never completely fixed; they should be reviewed at least once every budget cycle.
The evolution of data center design and function has been driven by the need for unforeseen operational prowess. Data centers now employ many unique designs developed specifically to achieve the goals of uninterrupted power within defined project constraints based on technological needs, budgetary limitations, and the specific loads each center must maintain to function efficiently and continuously. Preventing continuous operation under all foreseeable risks of failure, such as power outages, equipment breakdowns, internal fires, and so on, requires an evolved design and modeling techniques to enhance reliability. These include redundant systems and components, standby power generation, dual systems, automatic transfer and restart mechanisms, power quality, UPS systems, cooling systems, load and power density, and fire protection, as well as the use of probabilistic risk analysis modeling practices (which will be discussed in detail later) on virtually potential failure scenarios, developing maintenance, and improving system plans for all major systems.

Also vital is the fulfillment of life cycle in two-way communication between equipment and facilities management. Only when both sides fully understand the share principles of infrastructure reliability design, maintenance, and operation of critical environments (including the potential risk of downtime and recovery time), can they and implement an effective plan. Because the costs associated with reliability enhancements are significant, sound decisions can only be made by quantifying performance benefits against downtime cost estimates for each upgrade option to determine the best course of action. Planning and careful implementation will maintain efficiency while making the business case to fund necessary capital improvements and implement comprehensive maintenance strategies. When the business case for additional redundancy, specialized workstations, communications, and computing capacity reaches the boardroom, the entire organization can be prevented from imminent catastrophic data losses, damages to critical equipment, and dangerous site life and limb.

1.2. RISK ASSESSMENT

Critical industries require an extraordinary degree of planning and assessing. It is important to identify the best strategies to reach the targeted level of reliability. In order to design a critical building with the appropriate level of reliability, the cost of decommissioning and the associated risks need to be assessed. It is important to understand that decommissioning, costs due to more than one type of failure: design failures, catastrophic failures, equipment failures, or failures due to human errors. Each type of failure will require a different approach for prevention. A rational and realistic approach to business resilience must be a priority, especially because the present critical infrastructure is inherently challenged with all the above factors in one bundle.

Within the banking and financial services industries, planning the critical area places considerable emphasis on designing an infrastructure that evolves into an option to support continuous business growth. Robust maintenance and upgrading of equipment allows users and consumers continued availability. The 24/7 operation of such services requires an absence of scheduled interruptions for any reason, including maintenance, modifications, and upgrades. The main question is how and why infrastructure failures occur. Employing new methods of distributing critical power, under-
standing, capital expenditures, and developing processes that minimize human error and scenario-based metrics in measuring recovery time in the event critical systems are impacted by base-founding failures.

The infrastructure reliability can be enhanced by conducting a formal risk assessment (BEMA), gap analysis, and by following the guidelines of the critical asset program (CAP). The BEMA and the CAP are used in other industries and customized specifically for power utility system components. The BEMA is an exercise that produces a system of detailed, documented processes, procedures, and checklists designed to minimize operator and service provider errors. The CAP ensures that only trained and qualified people are associated with and authorized to have access to critical units. These programs coupled with probabilistic risk assessment (PSA) address the hazards of data center outages. The PSA looks at the probability of failure of each type of electrical power equipment. Performing a PSA can be used to predict availability, number of failures per year, and annual degradation. The PSA, BEMA, and CAP are facilitating steps when assessing each step listed below:

- Engineering and design
- Project management
- Testing and commissioning
- Documentation
- Education and training
- Operations and maintenance
- Administrative certification
- Real-time indications related to improving facility life cycle processes
- Standard and benchmarking

Regulatory regulations and policies are more stringent than ever. They are heavily influenced by Baseline III, the Mathematics and Energy (MEE), NERC 2010, and the U.S. Federal and Energy Storage Commission (FSC). Baseline III recommends “three pillars” for improving and ensuring supervision of assets, and monitoring of financial markets to bring stability to the financial system and other critical industries. Baseline III implementation involves identifying operational risks, thereby allowing appropriate capital to cover potential losses. As a response to company scandals in the past decade, NERC came into force in 2002 and contains the following sanctions:

The financial statement published by issuers is required to be accurate (Sec. 401)
Issuers are required to publish information in their annual reports (Sec. 404)
Issuers are required to disclose to the public, on an ongoing basis, information on material changes in their financial condition or operations (Sec. 409)
Penalties of fines and/or imprisonment are imposed for not complying (Sec. 402)

The purpose of the NERC 2010 Standard is to help the disaster management, emergency management, and business continuity communities to cope with critical events.
Keeping up with the rapid changes in technology has been a longstanding priority. The constant dilemma of meeting the required changes within an already constrained budget can become a limiting factor in achieving optimum reliability.

1.2.1 Levels of Risk

Risk can be described as the worst possible scenario that might occur while performing a task within a facility. Risk assesses how much we know or can predict about unforeseen circumstances. As we review risk, it is essential that the facility IT team has the proper change management processes and procedures in place for planned events, so that downtime can be minimized. Reducing the frequency of these events and understanding their impact is the key to proper critical environment management. Table 1.1 shows the three typical levels of impact—high, medium, and low—that result from event occurrence.

1.3 CAPITAL COSTS VERSUS OPERATION COSTS

Businesses are at the mercy of the mission critical facilities sustaining them. Each year, billions of capital dollars are spent on the electrical and mechanical infrastruc-

<table>
<thead>
<tr>
<th>Risk impact</th>
<th>Effects of system failure</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>It will cause an immediate interruption to the clients’ critical operations such as:</td>
</tr>
<tr>
<td></td>
<td>• Activity requiring a planned major utility service outage, or temporary elimination of system redundancy in the critical environment</td>
</tr>
<tr>
<td></td>
<td>• Activity that would disrupt critical production operations</td>
</tr>
<tr>
<td></td>
<td>• Activity that would likely result in an unplanned outage or disruption of operations if unsuccessful</td>
</tr>
<tr>
<td>Medium</td>
<td>There is time to recover without impacting the clients’ critical operations, including any:</td>
</tr>
<tr>
<td></td>
<td>• Activity requiring a planned service outage that does not affect systems but may impact noncritical operations</td>
</tr>
<tr>
<td></td>
<td>• Activity that involves a significant reduction in system redundancy</td>
</tr>
<tr>
<td></td>
<td>• Activity that is not likely to result in an unplanned outage in the critical environment or disruption of operations if unsuccessful</td>
</tr>
<tr>
<td>Low</td>
<td>It will not interrupt operations and will have minimum potential of affecting the clients’ critical operations including:</td>
</tr>
<tr>
<td></td>
<td>• Activity involving systems directly supporting operations but the execution of which will be transparent to operations</td>
</tr>
<tr>
<td></td>
<td>• Activity that cannot result in an unplanned outage of the critical environment or impact operations if unsuccessful</td>
</tr>
<tr>
<td>None</td>
<td>Activity not associated with the critical environment</td>
</tr>
</tbody>
</table>
time that supports IT around the globe. It is important to keep in mind that downturns can cost companies millions of dollars per hour or more. An estimated 98% of all businesses that suffer a large data loss go out of business within two years, regardless of the size of the business. The daily operations of our economic system and manner way of life depend on critical infrastructure being available 100% of the time with no exceptions.

Critical industries are operating continuously, 365 days a year. Because continuity relies on the daily operations and maintenance of power, water, and sewers are being packed into a single week. The growing number of services operating 24/7 increases the need for power, cooling, and storage. When a disaster occurs the facility is required to experience lengthy downtimes, a prepared organization is able to quickly resume normal business operations by using a preplanned recovery strategy. Strategy selection involves focusing on key risk areas and selecting a strategy for each area. Among the key risks to ensure reliability and security, the potential impact and probability of these risks, as well as the costs to prevent or mitigate damages and the time needed to recover, should be established.

Many organizations associate disaster recovery and business continuity only with IT and communication functions and until other critical areas that can seriously impact their businesses. Within these areas may be a multitude of critical systems that require maintenance, data recovery, and appropriate documentation. Some of these systems are listed later in Table 1.3.

One major area that necessitates strategy development is the banking and financial services industry. The success of strategy that guarantees recovery has an impact on employees, facilities, power, customer service, and employee and public relations. All areas require a clear, well-thought-out strategy based on recovery time objectives, cost, profitability impact, and reliability. The strategic decision is based on several of the following factors:

- The maximum allowable delay time prior to the initiation of the recovery process
- The time frame required to execute the recovery process once it begins
- The minimum computer configurations required to process critical applications
- The minimum communication devices and hardware circuits required for critical applications
- The minimum space requirements for essential staff members and equipment
- The total cost involved in the recovery process and the total loss as a result of downtime

Developing strategies with implementation stages means no time is wasted in revising a recovery scenario. The focus is to implement the plan quickly and successfully, and in order to accomplish this people must be properly trained. Is the person you hired 3 months ago up to this task? The right strategies implemented will effectively mitigate disruptions, minimize disruptions, reduce the cost of disruptions, and ensure the threat to life and safety.
1.4 CRITICAL ENVIRONMENT WORKFLOW AND CHANGE MANAGEMENT

To ensure reliable operations, a critical environment workflow and change management process must be established and followed. Communication lines and responsibilities of the engineering, technology, and security groups must be developed, implemented, and followed to ensure an effective plan for planned and unplanned events and associated risks.

The critical environment (CE) is defined as the physical space and the systems within a facility that are uniquely configured, sized, and designed to support specific critical business operations as defined by the users. These are many specific elements and areas within facilities in today's ever-changing environment. Systems are located within the building's structure whereas others are located outside. Depending on where a CE may be located, these locations have immediate impact on the client's reliability in maintaining business operations and continuity. Examples of some of these CE areas can be seen in Table 1.2:

<table>
<thead>
<tr>
<th>Table 1.2: Critical Areas</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data centers</td>
</tr>
<tr>
<td>Operational servers</td>
</tr>
<tr>
<td>Mechanical and electrical systems</td>
</tr>
<tr>
<td>Telecommunications systems</td>
</tr>
<tr>
<td>Power distribution systems (PDS)</td>
</tr>
<tr>
<td>Backup distribution systems (BDS)</td>
</tr>
<tr>
<td>Backup equipment systems (BES)</td>
</tr>
<tr>
<td>Telecommunications systems</td>
</tr>
<tr>
<td>Networking and control systems</td>
</tr>
<tr>
<td>Voice telephony and data channels</td>
</tr>
<tr>
<td>Security systems</td>
</tr>
<tr>
<td>Business continuity and technology recovery services</td>
</tr>
<tr>
<td>Telecommunications services</td>
</tr>
<tr>
<td>Local area networks (LAN) services</td>
</tr>
<tr>
<td>Business operations control services</td>
</tr>
<tr>
<td>Uninterruptible power supply (UPS) services</td>
</tr>
<tr>
<td>Commercial systems</td>
</tr>
<tr>
<td>Critical emergency and disaster recovery services</td>
</tr>
<tr>
<td>Building management, monitoring, and automation centers</td>
</tr>
<tr>
<td>Fire protection equipment systems</td>
</tr>
<tr>
<td>Standby emergency power (SEP) generation and standby power systems</td>
</tr>
</tbody>
</table>
Critical infrastructure systems are prevalent throughout a facility. Depending on the facility size, these could be many and varied systems supporting the same critical environment. Knowing which systems would impact the critical functions and operations is paramount. Some of these systems are listed in Table 1.3.

1.4.1 Change Management

Change management is a process for managing and communicating change across relevant facilities and business units to ensure an effective integration of procedures and processes. Note that during contingency situations, established contingency response plans and escalation procedures must be followed.

While some is must be done within the critical environment, some cannot. Simple procedures for minor changes to existing IT systems and maintenance activities to very complex and critical procedures involving entire systems, it is essential that any changes made during change management approaches to work planning and execution be validated. In any instance where work is planned or conducted in the critical environment, all departments must ensure that the risk for contingency operations is thoroughly assessed and that appropriate risk mitigation is in place while the work is performed.

The level of detail required in a standard of procedures (SOP) must be balanced in the complexity of the event and magnitude of the potential risk. Minimum/complex or high risk work must be meticulously detailed in the SOP. The standard required for these complex events would need to be necessary for an event. The bottom line is that a program

<table>
<thead>
<tr>
<th>Table 1.3: Critical Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consultation and support systems</td>
</tr>
<tr>
<td>Utility power delivery systems</td>
</tr>
<tr>
<td>Electrical emergency systems</td>
</tr>
<tr>
<td>Fire and life safety systems</td>
</tr>
<tr>
<td>Natural gas supply systems</td>
</tr>
<tr>
<td>Hydraulic distribution supply systems</td>
</tr>
<tr>
<td>Communication voice systems</td>
</tr>
<tr>
<td>Telecommunication and data supply communication systems</td>
</tr>
<tr>
<td>Information computer systems</td>
</tr>
<tr>
<td>Electrical systems</td>
</tr>
<tr>
<td>Environmental control systems (HVAC, CRACs, etc.)</td>
</tr>
<tr>
<td>Building automation systems (BAS) systems</td>
</tr>
<tr>
<td>Building systems</td>
</tr>
<tr>
<td>Uninterruptible power supplies (UPS) systems</td>
</tr>
</tbody>
</table>
by developed, reviewed, and approved MCRs will result in reduced risk to business operations. Required changes request information includes:

- Who is doing the review?
- What areas will be reviewed?
- Which areas of the building will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that are already in use?
- Do systems need to be repaired or replaced?
- Are there mechanical systems that will be affected?
- How long will the building be affected?
- How long will the building be affected?
- Will systems be damaged or destroyed?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
- Are there mechanical systems that will be affected?
The definition of commissioning can be found in ASHRAE's Guideline 0. The Guideline 0.2005 is a recognised model and provides guidance that explains commissioning as a quality control process in detail and can be applied to critical facilities with some embellishment when it comes to verifying critical systems performance. The quality control process given by ASHRAE is in phases, starting with the pre-design phase and continuing through the commissioning and operations phases.

A summary of the phases given in the ASHRAE Guideline are given below, which are additional commissioning critical facilities, and these phases should be included in all mission critical facility projects:

- Design phase:
  - Commissioning team/design review
  - Specification writing

- Construction phase:
  - Functional acceptance testing (FAT)
  - Construction check listing
  - Start-up (precommissioning) testing

- Acceptance phase:
  - Site acceptance (functional)
  - Acceptance testing to verify performance of critical equipment
  - Integration testing
  - O&M document review
  - Staff training/overseas
  - Develop and prove out BODA, BDMA, and BDMA

- Commissioning and operations phase:
  - Commission review and documenting of contracts
  - Commission training of O&M staff
  - Reliability assessment training (commission certification)

A quality control process would never be overlooked in any valuable production project. Why would we neglect quality control for critical facility projects? In the case of critical facility projects, quality control on commissioning means at the pre-design phase we can ensure that the commissioning requirements (CRPs) are fully documented and used as reference documents such as the basis of design (BOD). We also ensure that during design engineering, we can evaluate any impact on the CRPs and CPs, and if the proposed change does not meet the documented requirements, then that change must be offset on it. It should also clear that these documents are the foundation of any
project and part of the quality control process required for the commissioning of a critical facility.

In the design phase, we have a commissioning-focused design review that should not be confused with a peer review. In a commissioning-focused design review, the commissioning authority (CxA) should provide input on making the building and systems easier to commission and comment on equipment layout as it pertains to operational symmetry to help prevent operational staff from making errors during crisis situations. The CxA should also verify that bid documents adequately specify building commissioning as this will help reduce vendor change orders. It may be better to have the CxA provide commissioning specifications and have them included in the pre-purchase and other bid sets. The focused review also needs to verify that there are adequate monitoring and control points specified to facilitate commissioning and O&M (trending capabilities, test points, control points, gages, and thermometers). A review needs to include a review of design as it pertains to the reliability and redundancy standards of the owner and industry standards and verify that building O&M plan and documentation requirements specified are adequate.

During the construction phase, much of the rudimentary testing is accomplished. During this time, the factory acceptance testing is being conducted and it is important to have the CxA involved to verify that the controls and interlocks will work with the complete system. During this time, equipment is being delivered and installed. During this installation, the vendors and GC should be verifying the installation using construction checklists provided by the CxA. These checklists basically track the construction process and verify that the vendor delivered what was paid for in good condition, and that it was installed properly and has the proper clearance. The vendor start-up will follow and, if performed in accordance with the agreed procedures, all the functions including all the alarms will be verified. It is important to track all these documents and have them signed off by the vendors as proof of proper start-up. In some cases, the vendors will sign off the documents and not perform all the requirements, and that will slow down the acceptance and integrated testing. In this case of improper start-up, the delays can be back charged to the responsible vendor.

In the acceptance phase, the CxA will first operate all the equipment in all configurations and verify proper start-up by the vendors. Once this is completed, the CxA should verify performance of certain equipment without using vendor-provided test gear. This is done to keep the quality control process in the hands of the CxA and make sure that only calibrated equipment is used and the calculations are performed without bias. The equipment listed below is recommended to be subjected to this extra acceptance test phase:

1. Emergency power systems and controls
2. Uninterruptible power supply (UPS) systems and batteries
3. Flywheel energy storage systems
4. Static transfer switches (STS) and all associated controls

If the acceptance testing is done properly, it as a minimum will verify that the equipment is worthy of critical load. In some cases, deficiencies found during this
process have forced the vendors to meet their own specifications and improve product quality.

We are now ready for integrated testing, and the intent of this test is to verify that the building and all the systems work together to meet the client's design requirements. Some limits for having a successful integrated test that proves proper operation and no unexpected system interaction exist:

1. Perform a full data center load-level test, including anyredundant cooling systems.
2. Perform integrated testing at 25%, 50%, 75%, and 100% of the design load.
3. Use data loggers on the data center floor to verify measured data and HVAC commands.
4. Check all operating modes, including maintenance configurations.

Staff training and operations documents need to be provided before we can start operations. Proper training must be given to the staff for systems and integrated operations. It would suggest that the vendors provide system training, and the CxA provide overall operations documents. The operations documents should include maintenance operation procedures (MOPs), emergency operation procedures (EOPs), standard operation procedures (SOPs), and alarm response procedures (ARP). With properly trained staff and proper operations documents, the human error factor can be minimized.

As we entered each phase, the commissioning process continues into the occupancy phase to maintain operational readiness. A yearly review and update of training as required due to system upgrades or operational requirements maintains staff and procedural quality. This maintains operational efficiency, a yearly verification of performance for electrical systems prevents loss of productivity due to system degradation, this is referred to as reliability assurance testing. These tests should be similar to those performed for the acceptance test parameters used during the acceptance phase and should use the original data for trending any changes in the system. The reliability assurance testing should be performed after the vendor has provided preventive maintenance (PM). The reason we perform these tests after the vendor preventive maintenance (PM) is that the vendor will have interacted with a commissioned system and de-rated the system's performance. In some cases, they provide updated equipment or enhanced hardware. This review may result in the updated through reliability assurance testing to be worthy of critical load. Remember that the vendor-provided PM does not replace preventive maintenance on back-of-system degradation, so without a reliability assurance testing program the quality control process will have been compromised.

Before the facility goes online, it is essential to resolve all potential equipment problems (technology, operation, etc.). This is the commissioning team's sole opportunity to integrate and commission all the systems, as in the facility's 24/7 mission-critical status. At this point in the project, all systems installed have been tested at the factory and witnessed by a competent commissioning authority (CxA) familiar with the equipment guarantees and warranties.

Once the equipment is delivered, set in place, and wired, it is time for the second phase of equipment testing and integration. The importance of this phase is to verify each
validate that all components work together and in fine tune, calibrate, and integrate the system. This is a tremendous amount of programming for this phase. The facilities engineers work with the: designer, field engineers, and independent test consultants to coordinate testing and calibration. Critical circuit boards must be tested and calibrated prior to placing any critical electrical load on them. When all the tests are complete, the facilities engineers must compile the certified test reports, which will establish a benchmark for all future testing. The test phase is important in each major piece of equipment and prepares for the transition to operations.

Many decisions regarding how and where it services a facility's mission critical electrical and mechanical equipment are going to be made. The objective is easy: a high level of safety and reliability from the equipment, components, and systems. But discovering the correct and effective and practical methods required to accomplish this can be challenging. Network with colleagues, consult knowledgeable sources, and review industry and professional standards and best practices before choosing the approach best suited to your requirements going forward. Also, keep in mind that the individuals performing the testing and service should have the best training and experience available. You depend on their knowledge, expertise, and consultation ability to avoid potential problems with packages the most critical equipment in your building. Beyond your experience, be aware of what others have learned. Maintenance programs should be continuously improved. If a standardized procedure has not previously identified a problem, consider adjusting the schedule, respectively. Continue your maintenance programs on a regular basis and make appropriate adjustments as constantly improves.

Acceptance and commissioning testing are worthless unless the test results are evaluated and compared to standards and to previous test reports that have been established beforehand. It is imperative to recognize failing equipment and to take appropriate action as soon as possible. Common problems in this industry is the hesitation to perform maintenance without reviewing prior work orders and reports. This approach delays the value of benchmarking and tracking and must be improved. The mission critical facility engineers can then have objectives in perspective and depend upon their opinions when faced with a real controversy.

The importance of having every opportunity to perform preventive maintenance thoroughly and completely, especially in mission critical facilities, cannot be stressed enough. If not, the next opportunity will come at a much higher price: downtime, lost business, and lost potential clients, not to mention the liability issues that arise when technicians react to the same maintenance problem. So do it correctly—before it is too late and avoid дороже because it will be very difficult to do it again.

1.6 SPECIFICATIONS AND THE HUMAN FACTOR

The mission-critical industry's drive on physical infrastructure: enhancement demands from the early stages of the basic, where all clients were dedicated solely toward design and construction techniques to enhance mission critical equipment.

Twenty-five years ago, the technology supporting mission critical loads was simple. There were little sophistication in the electrical load possible; at that time the indus-
During the infancy of computer systems, the capabilities were focused on a few mainframe computers supporting minimal software applications like payrolls and tax systems that can occupy 100,000 ft² or more, with computer times being prime examples.

As work processes grew and required to sustain our global economy, the electrical and mechanical systems supporting the critical load became increasingly complex. With businesses relying on these infrastructures, more capital dollars were invested to increase the uptime of the business's lives. Today, billions of dollars are invested at the enterprise level in the infrastructure that supports the business 24/7 applications; the major investments are normally in design, equipment procurement, and project management. Few capital dollars are invested in documentation, change management, education and training, or operations and maintenance. The initial capital investment was just the tip of the iceberg (Figure 1.1).

Years ago, most organizations relied heavily on their workforce to maintain much of the infrastructure supporting the mission critical systems. A large body of personnel had a similar level of expertise. They remained with the company for decades. Therefore, little emphasis was placed on maintaining a living document for a critical infrastructure. Tables 1.4 to 1.6 identify questions and regard to managing loss of personnel, documentation, and training during a critical event.

The mission critical industry can no longer manage critical systems as they did 25 years ago. The requirements are very different today in that the sophisticated nature of the data center infrastructure requires the constant refreshing and updating of documentation. One way to achieve this is to include a living document system that provides the level of granularity necessary to operate a mission critical infrastructure on a critical project. This will assist in keeping the living document current each time a project is completed or a milestone is reached. Accurate information in the first level of
support that provides front line responders the intelligence they need to make informed decisions during critical events. It also helps leaders understand how their employees interact with other employees and leaders, thus reducing risk and improving their learning curve. The number that greater than 50% of all accidents can be traced to human error.

Human error as a cause of hazardous scenarios must be identified and the factors that influence human error must be considered. Human error is a given and will arise in all stages of the process. It is what the factors influencing the likelihood of errors be identified and assessed in determining if improvements inem the human factors design of a process are needed. Surprisingly, human factors are perhaps the most poorly understood aspect of process safety and reliability management.

Balancing system design and training operating staff in a cost-effective manner is essential to critical infrastructure planning. When designing a new critical facility, the level of complexity and cost of maintainability in a major concern (Figures 1.2 and 1.3). When there is a problem, the facility manager (1.4) is under tremendous pressure to isolate the facility system while maintaining data center loads and other critical loads.
Figure 1.2 Typical screenshot of mission critical access. (Courtesy of Power Management Concepts, LLC.)

Figure 1.3 Mission critical access screenshot. (Courtesy of Power Management Concepts, LLC.)
The field does not have the time to go through complex, time-consuming procedures during a critical event. A design for human disasters whose systems are complex, especially if key system operations and telecommunications of emergency action procedures (TAPE) and standard operating procedures (SOP) are not immediately available or have not been maintained or updated periodically. A rather simplistic mechanical system design will allow far quicker and easier troubleshooting during this critical time.

To further complicate the problem, equipment manufacturers and service providers are challenged to find solutions that are really effective within their own company. As TAPE operations become more prevalent, the demand for available equipment will continue to diminish. This would indicate that response times could increase from the current standard off-the-shelf times to much higher and less tolerable times. This would, for a simplification, easily accessible, well-documented design is already further substantiated by the growing imbalance of supply and demand of highly qualified mission critical technicians.

When designing a mission critical facility, a budgeting and training plan should be established. Each year, substantial amounts of money are spent on building improvements, but inadequate capital is allocated to maintain that critical environment through the use of proper documentation, education, and training.

**Chapter 4**

**Education and Training**

Technology has been progressing faster than Moore’s Law. It is expected that technology standards in the mission critical industry, now oft today’s critical missions system standards, are being met. As a result, new medical, educational, and engineering personnel, and continued research and development, unfortunately, little attention is given to the human resources involved. For example, reliability increases, a bigger percentage of downtime results from actions by personnel who were not properly trained or did not have access to accurate data during crisis events. The diversity among mission critical systems severely hinders people’s ability to fully understand and master all necessary equipment and relevant information.

In the past, a greater percentage of people would handle a job, and it was assumed for many facilities to make their own teams and ascend without much of a standard. In closing, there became a mushroom style, untrained, and ad hoc understanding of these systems operators. This experience prove a number of today’s mission critical professionals a test of skills to build upon.

Today’s “Nineteen generations” is gaining a slightly different set of skills through computer, software, and video games. They are gaining valuable experiences with IT systems, and will have a solid foundation to continue to enhance more advanced IT skills. The next step is to create a strategy for succession planning that bridges the information infrastructure gap and continues the already established IT knowledge to engineering. These existing professionals can share their base to apply that knowledge in this field.

The local strategy may be to shift training resources as early as possible and, upon retirement of current staff, ensure in training with the necessary experience to take on organizational responsibilities. Since training may have unused (Figure 4-6). These collocate programs that include internships should be developed and made attractive for young
1.3.2 Operation and Maintenance

What can facility managers do to ensure that their critical systems are as reliable as possible? The seven steps to improved reliability and maintainability are:

1. Planning and impact assessment
2. Engineering and design
3. Project management
4. Testing and commissioning
5. Documentation
6. Containing education and training programs
7. Operations and maintenance

The concept of professionals in each step of the way. When building a data processing center in an existing building, you must have the luxury of designing the electrical and mechanical systems from scratch. A competent engineer will design a system that satisfies the needs of the existing building design. However, before investing precious capital in new systems, you must understand your business requirements for the next 3-5 years, as well as the reliability levels you must sustain. The contractor who has experienced in data processing installations or has experience in the installation of air-conditioning units can assist you in selecting and using the right equipment to ensure that your capital is not wasted due to high maintenance or low reliability equipment. Finally, you should plan for routine shutdowns of your facility so that you can perform preventive maintenance on critical equipment. Facility managers as well as senior management must not underestimate the cost-effectiveness of a thorough preventive maintenance program. Maintenance is not a luxury; it is a necessity. Do you want scheduled outages to be scheduled in advance? Or better yet, can you afford to deal with the consequences of an unscheduled outage?

Understanding the ideal infrastructure is just about impossible. In fact, the best possible infrastructure is one that solves your problems. Competent engineers will have the knowledge, tools, testing equipment, training, and experience necessary to understand the risk of equipment failure, as well as the importance of implementing proper and new preventive maintenance. While there is no one-size-fits-all solution, always select the best system design, testing procedures, and outcomes. Your decision will determine the system's ultimate reliability, as well as the ease of system maintenance. Each experienced professional from within your own company as well as outside professionals: information systems, property and operations managers, space planners, and the best consultants in the industry for all engineering disciplines. The bottom line is to leave proven organizations working on your project.

1.9 EMPLOYEE CERTIFICATION

Empowering employees to function effectively and efficiently can be achieved through an well-planned certification program. Employees have a vested interest in working with management to reduce risk. Empowering employees to take charge in times of crisis creates valuable communication allies who not only maintain core messages internally, but also carry them into daily experiences. The national crisis communication should be conducted using established communication channels and events in addition to those that may have been developed to manage specific crisis scenarios.
Technology is changing itself faster than ever. Large investments are made in new technologies to keep up to date with advances in computer technology, yet industries are still faced with operational challenges. One possible solution to this is to implement technology provided to employees to keep up with advanced technology, but also to promote quick emergency response and situational awareness. Over the last few years, technologies have been developed to solve the technical problems of linkage and interaction of equipment without skilled technical personnel. How can we ensure that these employees meet the complex requirements of the facility at their highest levels of reliability?

1.10 Standards and Benchmarking:

The past decade has seen an increasing change in many organizations. As firms and institutions have realized the ways in which to survive and remain profitable, a simple fact has become more evident. The underlying rationale for the benchmarking process is to learn by example and from best practices, hence the need for effective means of understanding the principles and the specifics of effective practices. Recovery and resiliency together cannot provide sufficient resiliency if they can be disrupted by an uncontrolled event. A minimum critical datacenter must be able to endure hundreds of minutes, such as earthquakes, hurricanes, floods, and other natural disasters, as well as human-made events. Critical data centers should be designed to ensure these critical functions that will minimize downtime. Systems should be established with guidelines and mandatory requirements for the continuity of business applications. Procedures should also be developed for the systematic sharing of safety and performance related material, best practices, and standards.

The key to benchmarking the facility on a routine basis with the goal of identifying performance differences from the original design specifications. More properly, this will provide an early warning mechanism to allow a potential failure to be addressed and corrected before it occurs. Once deficiencies are identified, and before any corrective action can be taken, a method of operation (MOP) must be selected. The MOP will clearly outline step-by-step procedures and conditions, including what is to be present, the documentation required, planning of works, and the status in which the system is to be placed after the work is completed. The MOP will greatly minimize common and potential system failures by identifying responsibility of personnel, equipment, the resource, the location, policy, and common errors also involved. In addition, a program of ongoing
operational resilience training, and procedures is important to deal with emergencies outside of the regular maintenance programs.

The most important aspect of bench-marking is that it is a process driven by the participants who seek to improve their organizations. It is a process through which participants learn about successful practices in other organizations and then choose and embrace those practices to develop solutions most suitable for their own organizations. These processes bench-marking identifies the best and sets the performance gaps and helps organizations learn and understand how to perform with higher standards of practice. Keep in mind that you cannot implement if you do not measure and benchmark.

1.11 CONCLUSION

Today's industries are becoming increasingly dependent on continuous business operations. As a result, companies need to understand the level of reliability that they can supply to their customers and evaluate how this can either be improved or maintained. The following chapters will reinforce the concept that reliability and resiliency is dependent on a number of variables such as communication and training, operation and maintenance, documentation, and testing and exercising. It is the responsibility of employees at all levels of an organization to communicate and develop best practices that will strengthen their business.

1.12 RISK ANALYSIS AND IMPROVEMENT

Below is a list of questions that you may want to ask yourself about the needs analysis and risk assessment of the mission critical infrastructure. You are supporting with regards to reliability and resiliency. Your answers to these questions should help to shed some light on areas where you can improve your operations.

1. How much does each minute, hour, or day of operational downtime cost your company if a specific facility is lost?
2. Have you determined your recovery time objectives for each of your business processes?
3. Does your financial institution conduct comprehensive business impact analyses (BIA's) and risk assessments?
4. Have your calculated disruption scenarios and the likelihood of disruption affecting information resources, technology, personnel, facilities, and service providers in your risk assessments?
5. Have your disruption scenarios included both internal and external sources, such as natural events (e.g., fires, floods, severe weather), technical events (e.g., communication failures, power outages, equipment and infrastructure failures), and malicious activity (e.g., network security attacks, fraud, terrorism)?
6. Does this BIA identify and prioritize business functions and define the maximum allowable downtime for critical business functions?

7. Does the BIA estimate data loss and transaction backlog that may result from critical business function downtime?

8. Have you prepared a list of "critical facilities" to include any locations where a critical operation is performed, including all work areas, environments such as branch, branch operations facilities, headquarters, or data centers?

9. Have you classified each critical facility using a critical facility ranking/impact system such as the Tier 1, II, III, and IV rating categories?

10. Has a cumulative assessment been performed on each critical facility?

11. Has a facility risk assessment been conducted for each of your key critical facilities?

12. Do you know the critical, essential, and discretionary loads in each critical facility?

13. Have your comply with the regulatory requirements and guidelines discussed in this chapter?

14. Are any internal corporate risk and compliance policies applicable?

15. Have you identified business continuity requirements and expectations?

16. Has a gap analysis been performed between the capabilities of each company facility and the corresponding business processes recovery time objectives resulting in that facility?

17. Based on the gap analysis, have you determined the infrastructure needs for your critical facilities?

18. Have you considered fault tolerance and maintainability in your facility infrastructure requirements?

19. Given your new design requirements, have you applied redundancy modeling to optimize cost-effective solutions?

20. Have you planned for rapid recovery and timely resumption of critical operations following a wide-scale disruption?

21. Ensuring the least possible disablement of staff in at least one major operating location, how will you respond in a timely manner and resume critical operations?

22. Are you highly confident, through ongoing use or robust testing, that critical internal and external continuity arrangements are effective and compatible?

23. Have you identified clearing and settlement activities in support of critical financial transactions?

24. Do you employ and maintain sufficient geographically dispersed resources to meet recovery and resumption activities?

25. Is your organization such that there is diversity in the labor pool of the headquarters and headquarters, such that a wide scale event would not simultaneously affect the labor pool of both sites?
26. Do you routinely use in-house recovery and resumption arrangements?

27. Are you familiar with National Fire Protection Association (NFPA) 1600 -- Standard on Disaster/Emergency Management and Business Continuity Programs, which provides a standardized basis for disaster/emergency management planning and business continuity programs for private and public sectors by providing common program elements, techniques, and processes?