

BITS

FINANCIAL SERVICES
R O U N D T A B L E

BITS GUIDE TO BUSINESS-CRITICAL POWER

BITS
1001 PENNSYLVANIA AVENUE, NW
SUITE 500 SOUTH
WASHINGTON, DC 20004
202-289-4322
WWW.BITSINFO.ORG

CRITICAL POWER COALITION
SECURITY + CONTINUITY + QUALITY



TABLE OF CONTENTS

I. **Executive Summary**3

II. **The Grid**6

III. **Needs Analysis/Risk Assessment**.....14

IV. **Installation**.....23

V. **Maintenance and Testing**29

VI. **Training and Documentation**33

VII. **Conclusion**37

Appendices:

- Appendix A: Acknowledgements and References39
- Appendix B: Glossary.....41
- Appendix C: Case Study – Blackout August 2003.....45
- Appendix D: Cause and Effect of Recent Power Outages48
- Appendix E: Consolidated List of Key Questions49

I – EXECUTIVE SUMMARY

The *BITS Guide to Business-Critical Power* (the *Guide*) provides financial institutions with industry business practices for understanding, evaluating, and managing risks associated when the predicted reliability and availability of the electrical system is disrupted. Further, it outlines ways financial institutions can enhance reliability and ensure uninterrupted back-up power. The *Guide* is written for interested parties—from CEOs to business managers, risk managers to business continuity professionals, procurement experts to facilities managers—as they analyze risks, conduct due diligence for critical power, and integrate evolving regulatory and building code requirements into business continuity plans.¹

Business practices for the financial services industry mandate continuous uptime for computer and network equipment to facilitate around-the-clock trading and banking activities anywhere and everywhere in the world. Financial services institutions are appropriately and understandably intolerant of unscheduled downtime. Business-critical power is the power that an organization absolutely requires to achieve its business objectives. Today, more than ever, financial institutions are demanding continuous 24-hour system availability.

The risks to the financial services industry associated with cascading power supply interruptions from the public electrical grid in the United States have increased due to the industry's ever-increasing reliance on computer and related technologies. As the number of computers and related technologies continues to multiply in this increasingly digital world, demand for reliable quality power increases as well. Without reliable power, there are no goods and services for sale, no revenues, and no profits.

The financial services industry has been innovative in the design and use of the latest technologies, driving its businesses to increased digitization in this highly competitive business environment. Achieving optimum reliability is very challenging since the supply and availability of uninterrupted, conditioned power is becoming more and more critical to the industry. For example, data centers of the past usually required the installation of standalone protective electrical and mechanical equipment only for computer rooms. Data centers today operate on a much larger scale 24/7. The proliferation of distributed systems using hundreds of desktop PCs and workstations connected through LANs and WANs that simultaneously use dozens of software business applications and reporting tools makes each building a “computer room.” The uninterrupted power needs for any single institution are formidable, but the power requirements are truly staggering when the entire interconnected financial services industry is considered.

To provide continuous operation under all foreseeable risks of failure is a nontrivial matter and requires a holistic, enterprise approach. Communication between managers of business lines, business continuity and facilities is vital. Only when all parties fully understand the three pillars of power reliability—design, maintenance and operation—can an effective plan be funded and implemented. The costs associated with reliability enhancements are significant and sound decisions can only be made by quantifying performance benefits against downtime cost estimates.

¹ This document is intended only to provide suggestions on business objectives, not to provide legal advice. An appropriate legal professional should be engaged to provide such advice on a case-by-case basis.

Financial institutions cannot develop a plan to protect against threats they do not envision. This *Guide* assumes the following:

- There will be power failures that affect your financial institution.
- Financial institutions may be exposed to regulatory or fiscal penalties (monetary or customer loss) as a result of these outages.
- The only way to ensure that your financial institution will be protected is to buy and install standby power generation and/or power protection systems (hereinafter referred to as critical power) so as to make the facility independent of the public power “grid” when needed.²
- Reliability and facility infrastructure health are not guaranteed simply by investing in and installing new equipment. Unexpected failures can compromise even the most robust facility infrastructure if appropriate testing, maintenance and due diligence techniques are not employed.
- Financial institution personnel need to be trained and records kept.

The sections that follow address each of these assumptions in more detail and endeavor to address applicability from a variety of perspectives. Each financial institution will have its own organizational structure, so it will be up to each financial institution to interpret the terms in this document according its respective structure.

In general, the provision of critical power will often fall under the purview of the business continuity professional working in concert with business managers, risk managers and practitioners. The following definitions can be used as guidelines:

- Business Continuity Professional refers to the individual responsible for preparing and coordinating the business continuity process. Potential titles: business continuity manager; disaster recovery coordinator; business recovery coordinator.
- Business Manager refers to the individual responsible for lines of business and ensuring that the financial institution is profitable. This individual is the ultimate decision maker and the level of executive can run the gamut from the most senior executive to a line manager. Potential titles: chief executive officer; executive vice president; senior vice president; vice president; chief technology officer; chief information officer.
- Risk Manager refers to the individual responsible for evaluating exposures, and controlling exposures through such means as avoidance or transference. There are various types of risk, including operational, credit and market risk. This *Guide* deals with operational risk. Potential titles: corporate risk officer; risk management officer; chief risk officer.
- Practitioner refers to the individual who will be responsible for the implementation and maintenance of critical power. Potential titles: facilities manager; chief engineer; event manager.

A list of questions is included at the end of each section. A consolidation of all the questions is included in Appendix E and items are cross referenced to their respective section. The questions are presented in a “worksheet” format providing space so that financial institutions can indicate whether the question is applicable and record comments germane to the question.

² For a discussion of the range of options for standby power generation and/or power protection systems, please see section III, Needs Analysis/Risk Assessment and section IV, Installation, of this Guide.

These questions are a starting point for a rigorous examination of a financial institution's business continuity strategy for critical power needs. They may also serve as considerations in procuring adequate levels of critical power.

II – THE GRID

Electricity occupies a uniquely important role in all operations of financial institutions. The loss of power takes out data and communications capabilities, and virtually all of the new systems and technologies being deployed for physical and operational security.

The public electric grid is inherently vulnerable. Relatively small numbers of huge power plants are linked to millions of locations by hundreds of thousands of miles of exposed wires. Nearly all high-voltage lines run above ground and traverse open country. A handful of high-voltage lines serve entire metropolitan regions. Serious problems may propagate rapidly through the grid itself.

Most accidental grid interruptions last barely a second or two, and many “power quality” issues involve problems that persist for only tens of milliseconds (one or two cycles). In most areas of the country, grid outages of an hour or two occur, on average, no more than once or twice a year, and longer outages are even rarer. Accidental outages tend to be geographically confined as well; the most common involve blown circuits in a single building (typically caused by human error, much of it maintenance related), or interruptions confined to the area served by a single utility substation.

There is normally very little risk that several high-voltage lines feeding a metropolitan area from several different points on the compass will fail simultaneously, and when just one such line fails, all the resources at hand can be mobilized to repair it. Deliberate assaults, by contrast, are much more likely to disable multiple points on the network simultaneously. A 2002 National Academy of Sciences report drove this reality home, observing starkly: “[A] coordinated attack on a selected set of key points in the [electrical] system could result in a long-term, multi-state blackout. While power might be restored in parts of the region within a matter of days or weeks, acute shortages could mandate rolling blackouts for as long as several years.”³ Operations that can afford simply to shut down and wait out short blackouts may not be able to take that approach in response to the mounting threats of longer outages.

UNDERSTANDING THE GRID

The national electric grid is a vast, sprawling, multi-tiered structure that reaches everywhere, and is used by everyone. Measured by route miles and physical footprint, the North American grid is by far the largest network on the planet.

Architecturally similar arrays of generators, wires, switches, and transformers appear within each of the grid’s principal tiers. The generation and transmission tiers at the top have stadium-sized, gigawatt-scale power plants and commensurately high-voltage wires, building-sized transformers, truck-sized capacitors, and arrays of mechanical, electromechanical, and electronic relays and switches. The distribution tiers in the middle have tennis-court-sized, megawatt-scale substations, van-sized transformers, and barrel-sized transformers mounted ubiquitously on poles and in underground vaults. The bottom tiers transform, condition, and distribute power within factories, commercial buildings, and homes via power-distribution units, lower-voltage on-premise grids, and dispersed switches, batteries, and backup systems further downstream.

³ *Making the Nation Safer: The Role of Science & Technology in Countering Terrorism*, National Academy of Sciences, National Research Council (2002).

The top tier of the grid is typically fueled by coal, uranium, water, or gas; each lower tier is typically “fueled” initially by the electric power delivered from the tier above. Generating stations in the top tier dispatch electrical power through some 680,000 miles of high-voltage, long-haul transmission lines, which feed power into 100,000 substations. The substations dispatch power, in turn, through 2.5 million miles of local distribution wires. At the same time, a couple of large power plants can provide all the power required by a city of a half-million. Many communities are served by just a handful of smaller power plants, or fractional shares of a few bigger power plants.

In the most primitive architecture, the grid includes only a power plant and wires. Power is generated at the top tier, consumed at the bottom, and transported from end to end by a passive, unswitched, trunk-and-branch network. This was the structure of the very first grid, from Edison’s Pearl Street station in New York, in 1882. The higher up things fail, the more widely the failure is felt.

The modern grid is, of course, much more robust. Many different power plants operate in tandem to maintain power flows over regions spanning thousands of miles. In principle, segments of the grid can be cut off when transformers fail or lines go down, so that failures can be isolated before they propagate to disrupt power supplies over much larger regions. The effectiveness of such failure isolation depends on the level of spending on the public grid, which has been in decline for years. Identical strategies of isolation and redundancy are used on private premises to make the supplies of power to critical loads absolutely assured, insulating those loads from problems that may affect the grid.

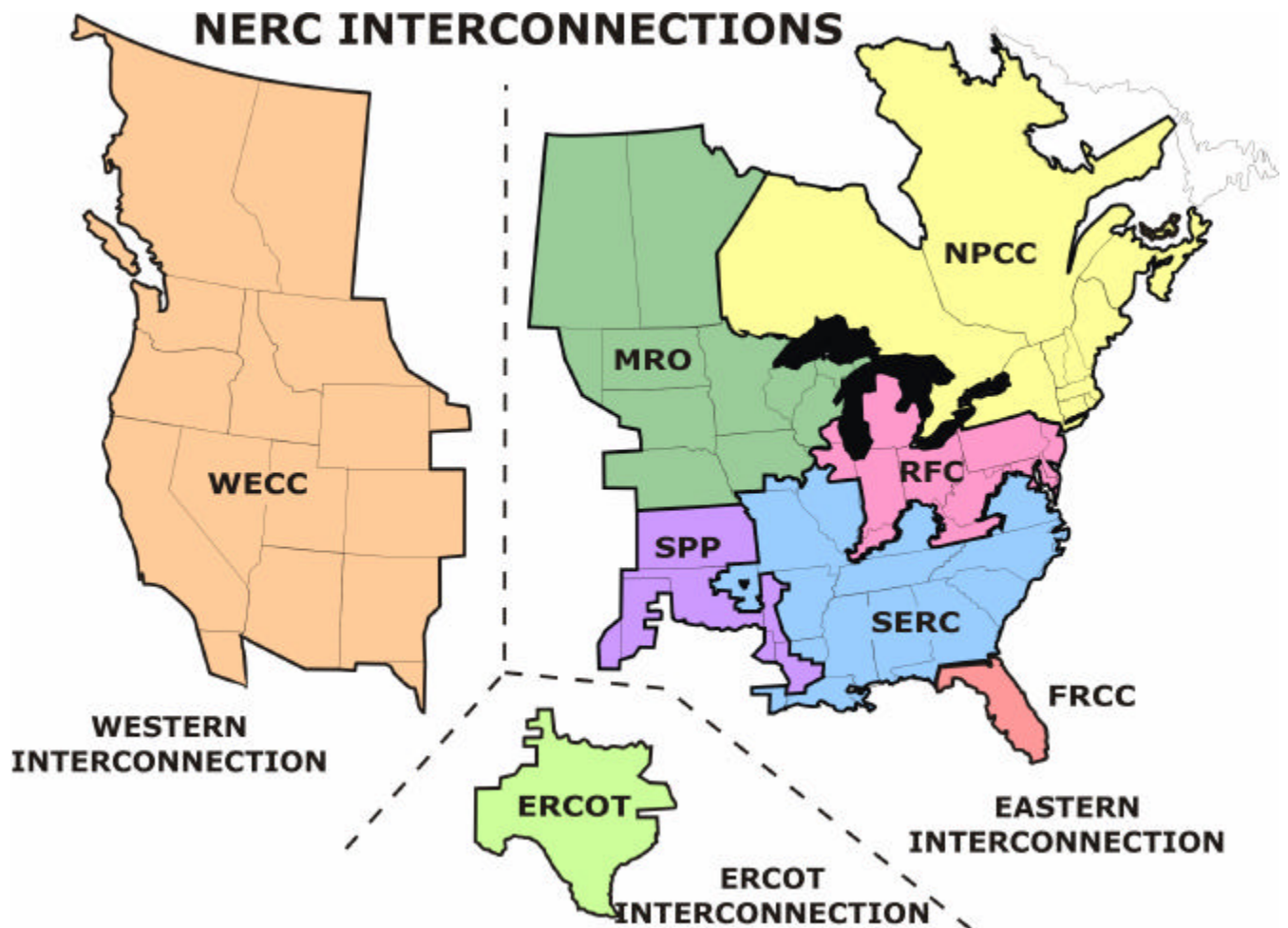
Switches control the flow of power throughout the grid, from power plant down to the final load. “Interties” between high-voltage transmission lines in the top tiers allow even the very largest plants to supplement and back each other up. Distributed generation facilities in the middle tiers can power smaller segments of the grid and keep them lit even when power is interrupted in the highest tiers. When power stops flowing through the bottom tiers of the public grid, critical-power circuits on private premises are isolated and private, on-premises generators kick in.

Much of the critical-infrastructure literature refers to the grid as a single structure, and thus implicitly treats it as “critical” from end to end. But utilities themselves necessarily prioritize and rank the customers and loads they are expected to serve. Large power plants and high voltage underground cables that serve densely populated urban areas obviously require more protection before they fail, and more urgent attention after, than small plants and rural distribution lines. In defining priorities and deploying new facilities, collaboration between utilities and critical power customers is becoming increasingly important. Most notably, power is critical for the continued provision of other critical services—those provided by E911, air traffic control, wireline and wireless carriers, emergency response crews, and hospitals, among others.

Hardening of the grid begins at the top tier, in generation and transmission facilities. Much of the modern grid’s resilience is attributable to the simple fact that “interties” knit local or regional grids into a highly interconnected whole, so that any individual end user may receive power from many independent power plants, often located hundreds (or even thousands) of miles apart. Promoting development of this resilient architecture is the primary mission of the North American Electric Reliability Council (NERC).

It is important to note that there is no "national power grid" in the United States. In fact, the continental United States is divided into three main power grids:⁴

- The Eastern Interconnected System, or the Eastern Interconnect
- The Western Interconnected System, or the Western Interconnect
- The Texas Interconnected System, or the Texas Interconnect.



The main interconnections of the U.S. electric power grid and the 10 [North American Electric Reliability Council](#) (NERC) regions. (Source: North American Electric Reliability Council)

- ERCOT — Electric Reliability Council of Texas
- FRCC — Florida Reliability Coordinating Council
- MRO — Midwest Reliability Organization

⁴Reprinted from the Department of Energy's website. http://www.eere.energy.gov/de/us_power_grids.html

- NPCC — Northeast Power Coordinating Council
- RFC – ReliabilityFirst Corporation
- SERC — Southeastern Electric Reliability Council
- SPP — Southwest Power Pool
- WECC — Western Electricity Coordinating Council

The Eastern and Western Interconnects have limited direct current interconnections with each other. The Texas Interconnect is also linked with the Eastern Interconnect via direct current lines. Both the Western and Texas Interconnects are linked with Mexico, and the Eastern and Western Interconnects are strongly interconnected with Canada. All electric utilities in the mainland United States are connected with at least one other utility via these power grids.

The grid systems in Hawaii and Alaska are much different than those on the U.S. mainland. Alaska has an interconnected grid system, but it connects only Anchorage, Fairbanks, and the Kenai Peninsula. Much of the rest of the state depends on small diesel generators, although there are a few minigrids in the state as well. Hawaii also depends on minigrids to serve each island's inhabitants.

New interties provide an effective way to boost overall reliability and create capacity margins without building new plants; new interties also facilitated the wholesale trading that regulators authorized in the 1990s. So long as there is sufficient margin in the generating capacity and redundancy in wires, and sufficiently fast and accurate control of the key switches that isolate faults, the failure of any one power plant or line in the top tiers of the grid should not be discernible by end users at the bottom.

After September 11, 2001, NERC expanded their recently created Critical Infrastructure Protection Advisory Group (currently the Critical Infrastructure Protection Committee [CIPC]) to bring together the public utilities responsible for securing the thousands of miles of long-haul, high-voltage wires and the 7,000 transmission-level substations. Among other initiatives, CIPC has formed a working group to inventory and develop a database of “critical spare equipment.” Given the customization required in the high-voltage transmission system (which often uses custom-built, high-power hardware such as massive substation transformers), maintenance of spare equipment can be challenging. CIPC’s database helps to assure overall continuity of operation through the intelligent sharing of stand-by assets.

Complementary discussions are addressing the possibility of creating a critical-equipment warehousing system, with geographically dispersed warehousing of spares, and cost-sharing by the potential beneficiaries of such planning. This solution has already been implemented for power line (“telephone”) poles, and is now being applied to fleets of substation-scale generators-on-wheels.

Very large end users rely on similar intertie strategies one tier lower down in the grid to help secure their specific critical power needs. In such configurations, the key “switch” controlling the dual feeds will often be a dedicated utility substation located on the doorstep of a factory, office park, or data center. By deploying additional substations in close collaboration with major critical-load customers, utilities shrink the footprint (i.e., reduce the number of customers affected) by failures that occur elsewhere. More substations create more points at which to interconnect independent parts of the grid so that distant transmission lines and power plants effectively back each other up.

Substations can also serve as sites for utility deployment of distributed generation. With the addition of its own generating capacity, the substation is “sub” no longer—it becomes a full-fledged “mini-station.” Opportunities for deploying new generating capacity at this level of the grid, either permanently or when emergencies arise, are expanding as large electromechanical switches and related components are being replaced by new solid-state technologies that have much smaller footprints.

By such means, much can be, and is being, done to lower the likelihood of a loss of grid power needed by the most critical loads. Closer collaboration between utilities and their largest customers is now needed to advance such initiatives in the distribution tiers of the grid. Nevertheless, the grid is inherently subject to external factors that can cause outages, and there is only so much that feasibly can be done to secure it against these possible problems. Guaranteeing supplies of critical power at high-demand, high-reliability locations, such as data centers and communications hubs, ultimately means adding increasingly sophisticated on-site generating capacity and storage to back up whatever is being done to improve reliability higher in the grid.

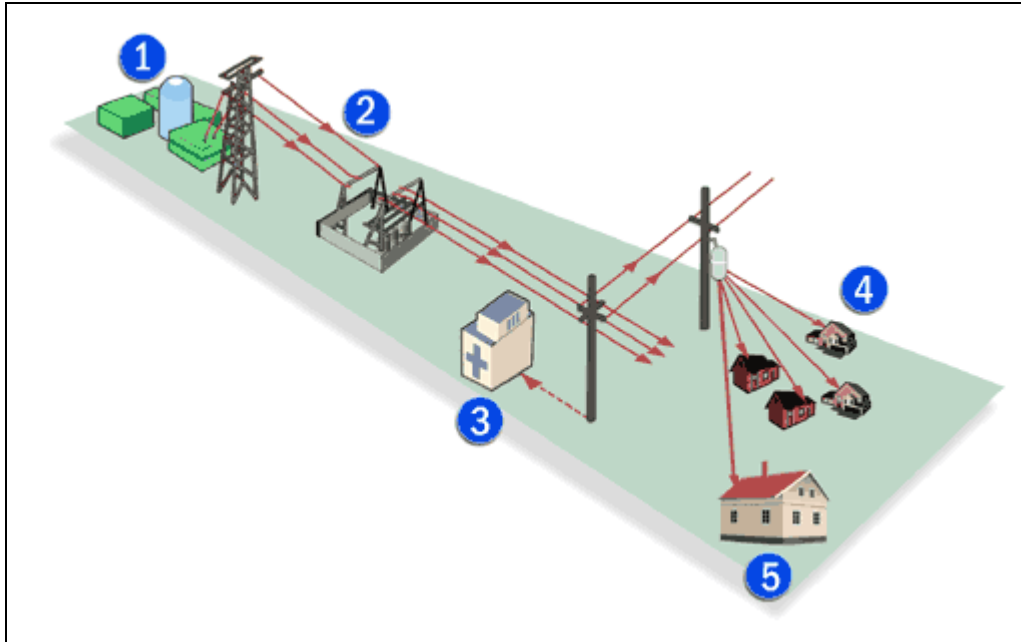
POWER RESTORATION

The first essential step in restoring power after a major outage is to isolate faults and carve up the grid into smaller, autonomous islands. From the perspective of the most critical loads, the restoration of power begins at the bottom, with on-site power instantly cutting in to maintain the functionality of command and control systems that are essential in coordinating the step-by-step restoration of the larger whole.

Major utilities establish electric service priority protocols to prioritize power restoration efforts after a major outage, typically targeting hospitals and other emergency services. Such programs acknowledge that certain users and uses are atypically dependent on supplies of electric power, and suffer unusually serious consequences when their power fails. Thus, they are given priority over business restoration. All such priorities are swept aside, however, when a high-level failure cuts off power to an entire region. Then, the focus is almost entirely on the systematic restoration of power from the top-down, beginning with the highest-power stations, trunks, and switching centers, in a process structured largely to minimize damage to the utility’s own, most essential equipment.⁵ It is thus likely in both cases of isolated and of widespread, extended outages, that financial facilities will remain relatively low in the restoration priority hierarchy. Ensuring the security and continuity of critical power will increasingly require facility-specific planning and systems, with relevant coordination with, and occasionally engineering help from, local utilities.

While each utility has its own restoration plan, there are elements that will likely be common. The following plan is duplicated here courtesy of JEA which owns, operates, and manages the electric system established by the City of Jacksonville in 1895. JEA is the largest community-owned utility in Florida and the eighth largest in the United States.

⁵ See for example: *Blackstart Regional Restoration Plan*, Southeastern Electric Reliability Council (March 14, 2003).



Power Restoration Process

1. The first step is damage assessment, which includes physical inspections of facilities and plants. Once damage assessments have been made, repairs begin.
2. Repairs begin at generating facilities and transmission lines from plants, and to water and wastewater treatment facilities.
3. Next, main line repairs begin on electric circuits, water and sewer systems that serve critical facilities such as hospitals, police and fire stations.
4. The goal is to restore services to the greatest number of customers as soon as possible.
5. Once the large impact areas have had power restored, restoring power begins to small pockets or individuals still without power.

NERC published Standard EOP-005-0⁶ to “ensure plans, procedures, and resources are available to restore the electric system to a normal condition in the event of a partial or total shut down of the system.” As mentioned earlier, each utility may have a pre-determined order in which it restores power. It is imperative that financial institutions understand “if” their utility has a prioritization order; “what” the prioritization order is; and “if and where” within that order the financial services industry falls. Specific questions are outlined in the section that immediately follows.

ELECTRIC POWER/UTILITY QUESTIONNAIRE⁷

Financial institutions should be in touch with their electric power utility to establish the working relationship needed to help through real or potential service interruptions. Check with facilities management and/or accounts payables offices as staff may already have contacts that can be used to establish a business continuity planning partnership. Communicate directly with the provider and

⁶ ftp://www.nerc.com/pub/sys/all_updl/standards/rs/EOP-005-0.pdf

⁷ This section is excerpted from and reprinted with the permission of the Securities Industry Association Business Continuity Planning Committee’s “Critical Infrastructure Guide” published in January 2005.

ask to speak with the person responsible for business continuity, crisis or emergency management. The following guidelines may help as you try to ascertain information:

- Explain that you need information to help in developing a plan.
- Refer to regulatory guidelines or business continuity requirements that necessitate planning with critical infrastructure providers.
- Seek to establish an on-going relationship with your counterpart. Such a relationship can be the difference between getting access to good information at the time of disaster and getting only that information available to the general public.
- Get involved in crisis management testing performed by the utility.
- Understand the utility's operating strategy and position within any larger regional or national infrastructure.

QUESTIONS

ITEM	DESCRIPTION
	General
1.	Do you have a working and ongoing relationship with your electric power utility?
2.	Do you know who in your financial institution currently has a relationship with your electric power utility, e.g., facilities management or accounts payable?
3.	Do you understand your electric power utility's electric service priority protocols?
4.	Do you understand your electric power utility's restoration plan?
5.	Are you involved with your electric power utility's crisis management/disaster recovery tests?
6.	Have you identified regulatory guidelines or business continuity requirements that necessitate planning with your electric power utility?
	Specifically for an Electric Power Utility
7.	What is the relationship between the regional source power grid and the local distribution systems?
8.	What are the redundancies and the related recovery capacity for both the source grid and local distribution networks?
9.	What is the process of restoration for source grid outages?
10.	What is the process of restoration for local network distribution outages?
11.	How many network areas are there in (specify city)?
12.	What are the inter-relationships between each network segment and the source feeds?
13.	Does your infrastructure meet basic standard contingency requirements for route grid design?
14.	What are the recovery time objectives for restoring impacted operations in any given area?
15.	What are recovery time objectives for restoring impacted operations in any given network?
16.	What are the restoration priorities to customers—both business and residential?
17.	What are the criteria for rating in terms of service restoration?
18.	Where does the financial services industry rank in the priority restoration scheme?

ITEM	DESCRIPTION
19.	How do you currently inform clients of a service interruption and the estimated time for restoration?
20.	What are the types of service disruptions, planned or unplanned, that (specify city) could possibly experience?
21.	Could you provide a list of outages, type of outage and length of disruption that have affected (specify city) during the last 12 months?
22.	What are the Reliability Indices and who uses them?
23.	During an outage, would you be willing to pass along information regarding the scope of interruptions to a central industry source, e.g. a financial services industry business continuity command center?
24.	Are the local and regional power utilities cooperating in terms of providing emergency service? If so, in what way? If not, what are the concerns surrounding the lack of cooperation?
25.	Would you be willing to provide schematics to select individuals and/or organizations on a non-disclosure basis?
26.	Could you share your lessons learned from the events of 9/11 and the regional outage of 8/14/03?
27.	Are you familiar with the “Critical Infrastructure Assurance Guidelines for Municipal Governments” document written by the Washington Military Department Emergency Management Division? Is so, would you describe where (specify city) stands in regard to the guidelines set forth in that document?
28.	Independent of the utility’s capability to restore power to its customers, can you summarize your internal business continuity plans, including preparedness for natural and manmade disasters (including but not limited to weather-related events, pandemics and terrorism)?

EVOLVING RISK LANDSCAPE

Planning rationally for infrequent but grave contingencies is inherently difficult. Financial institutions that have prepared properly for yesterday's risk profiles may be unprepared for tomorrow's. The risk-of-failure profiles of the past reflect the relatively benign threats of the past—routine equipment failures, lightning strikes on power lines, and such small-scale hazards as squirrels chewing through insulators or cars colliding with utility poles. Now, in addition to concerns about weather-related outages (hurricanes and ice storms in particular), as well as recent experiences underscoring the possibility of widespread operational outages, there is as well the possibility of deliberate attack on the grid. The latter changes the risk profile fundamentally—that possibility poses the risk of outages that last a long time and that extend over wide areas. The planning challenge now shifts from issues of power *quality* or *reliability* to issues of business *sustainability*. Planning must now take into account outages that last not for seconds, or for a single hour, but for days.

Events such as the terrorist attacks of September 11th, the Northeast Blackout of 2003 and the 2006 Hurricane season have emphasized our interdependencies with other critical infrastructures—most notably power and telecommunications⁸. There are numerous national strategies and sector specific plans, all of which highlight the responsibility of the private sector for “building in increased resiliency and redundancy into business processes and systems”⁹. These events have also prompted the promulgation and revision of laws, regulations, and policies governing reliability and resiliency of the power industry. Some of these measures also delineate controls required of some critical infrastructure sectors to maintain business-critical operations during a critical event. A financial institution's ability to comply with these legislative and regulatory measures is therefore impacted by its success in providing its key facilities with critical power. A more detailed discussion of the regulatory environment can be found later in this section.

The need to provide continuous operation under all foreseeable risks of failure, such as power outages, equipment breakdown, internal fires, natural phenomena, and terrorist attacks, requires use of many techniques to enhance reliability. These techniques include redundant systems and components, standby power generation and UPS systems, automatic transfer and static switches, and the use of probability risk analysis modeling software to predict potential future outages and develop maintenance and upgrade action plans for all major systems.

CRITICAL POWER OPTIONS

Financial institutions require highly sophisticated uninterruptible power systems, generators, HVAC systems, transfer switches, and other high-voltage electrical and mechanical systems to ensure fail safe power delivery and operation. The first step in the needs analysis process is to determine the level of criticality. Individual institutions establish their level of criticality based on their own criteria

⁸For a review of steps financial institutions can take to enhance resiliency and business continuity specific to telecommunications see the *BITS Guide to Business-Critical Telecommunications Services*, published in 2004.

⁹ National Infrastructure Protection Plan, Draft Version 6.0, January 2006.

and their customers' criteria. The primary criterion is availability. What is the impact if a specific facility is lost for a day, an hour, or three minutes? Is failure an option?

Traditionally, when discussing critical facilities, there is an assumption that those facilities are data centers. This *Guide* broadens the definition of "critical facility" to encompass any location where a critical operation is performed. So, a critical facility can include, but is not limited to, all work area environments such as branch backroom operations facilities, headquarters or data centers. The critical level of an operation dictates the reliability and the security of the facility in which the operation is performed. Because the cost of these facilities is driven by reliability requirements, it is critical to calculate the reliability of various design options and budget requirements. Developing innovative design strategies and, subsequently, state of the art critical facilities requires a deep understanding of both design and operational issues. Clearly, design impacts operation, and operation impacts design. Redundancy adds considerable cost to the construction and operation of a mission critical facility. It is critical to optimize engineering design for high reliability and performance versus cost.

Reliability is one of the major cost drivers associated with construction and operations. The availability metric is commonly used for measuring reliability of critical facilities and is usually expressed as a percentage. For modern critical facilities, the benchmark availability is in the range of 99.999% ("five nines") to 99.9999% ("six nines"). To achieve six nines availability, the engineered systems will have to incorporate designs that include system+system $[2(N+1)]$ redundancy. It is worth noting that engineered systems in a critical facility are often over-designed to include too much redundancy. That is, systems become more complex than they need to be, which leads to decreased reliability.

DEFINING THE FOUR TIERS OF FACILITIES

Material in this section was based, in part, on concepts developed and information provided by the Uptime Institute.¹⁰ Facilities can be generally classified by Tiers, with Tier I being the most basic, and Tier IV being the most reliable facility. The reason for having different tiers is due in large part to maintainability, i.e. can the facility be maintained without shutting it down. Tiers I and II need to be shut down; Tiers III and IV are deemed "concurrently maintainable." Critical functions of financial institutions will usually require a facility in the Tier III to Tier IV range or utilize other strategies such as co-location. Although rare, it is possible that critical business functions will be located in a Tier II or even a Tier I facility configuration, despite the fact that both lack full backup and redundancy support. This is not to be encouraged. The commercial/financial industry definitions and characteristics for the four tiers are as follows:

Tier I - Basic, Non-redundant. A Tier I facility has no redundancy and is susceptible to disruptions from both planned and unplanned activities. Typical equipment configurations for electrical and mechanical support of the facility are represented by a single 'N' path. 'N' in such configurations represents the minimum number of systems or components (also called paths) required to operate.

¹⁰ "Tier Classifications Define Site Infrastructure Performance," A White Paper by W. Pitt Turner, IV., John H. Seader and Kenneth G. Brill, © 2006 The Uptime Institute, Inc., www.uptimeinstitute.org <<http://uptimeinstitute.org/>>. Reprinted with permission.

A basic non-redundant facility is shut down completely on at least an annual basis in order to perform scheduled maintenance and repair work. Urgent situations may require shutdowns on a more frequent basis. Errors in operation or spontaneous failures of site infrastructure components or distribution paths will cause service disruptions.

Tier II - Basic, Redundant. This tier of facility has limited backup and redundancy support and is therefore still susceptible to disruptions from both planned and unplanned activity. This facility may contain functions with limited criticality which, if they are shut down correctly, will have no major impact on the business or only some of the functions in the building are considered critical and require backup and redundancy support. As a result, UPS modules or limited generator support to only part of the building may be provided. Although there is some backup and redundancy, it is not a fully redundant system and the facility will still be considered a single 'N' facility. Except for maintenance of uninterruptible power supply (UPS) modules and other redundant capacity delivery components, a basic redundant facility is usually scheduled for a complete shut down on an annual basis to perform maintenance and repair work to the distribution systems. Urgent situations may require shutdowns on a more frequent basis. Errors in operation or spontaneous failures of site infrastructure distribution paths may cause a facility disruption. Additionally, unexpected failures of capacity components may cause a facility disruption.

Tier III – Concurrently Maintainable. This tier has a full single system backup and redundancy support (N+1). Functions in this building are critical and the system provides for any planned activities to be conducted without disrupting building operations. However some unexpected disruption or downtime may occur and can be tolerated. Planned activities include preventative and programmable maintenance, repair and replacement of components at the end of their lives, addition or removal of capacity components, testing of components and systems, or reliability-centric maintenance (RCM). This means that planned activities must never remove from service more than the redundant component or distribution path. Every component must be able to be removed from service on a planned basis without disruption to the load. This requires sufficient capacity to carry the full load on one path while performing maintenance or testing on the other path. Unplanned activities such as errors in operation or spontaneous failures of facility infrastructure distribution paths may cause a facility disruption. Unexpected failures of components may cause a facility disruption.

Tier IV - Fault and Failure Tolerant. Functions in this tier facility cannot tolerate downtime or disruption. As a result the facility has no single points of failure with multiple system backup and automated redundancy support (N+2) and can withstand at least one unplanned capacity component failure, error, or event with no critical load impact. Fault-tolerant functionality also provides the ability to permit scheduled preventative maintenance and repair activity without disrupting the critical load in any way. With this level of capability, the site infrastructure maintains flexibility and redundancy. At this level, any component must be able to fail without disruption to the load.

LOAD CLASSIFICATIONS

Critical, Essential or Discretionary Load

The key to overall effectiveness is the ability to completely and accurately fulfill missions within the critical facility and within the network of facilities. The backup power system typically does not

provide power to all building systems. The first step in the design process is to identify risks, i.e., the impact that a power outage would have on the facility and the operations. A key component of this risk assessment is determining which loads need to be connected to the back up power system. The classifications of loads that support critical facilities are referred to as critical, essential or discretionary.

Critical Load - That portion of the load requiring one hundred percent continuity in power service. This equipment must have an uninterrupted power input to prevent damage or loss to a facility (including its information technology and infrastructure), to its specific business functions, or to prevent danger of injury to personnel.

Essential Load - That portion of the load that directly supports routine accomplishment of site operations. Generally, these are loads that can tolerate power outages without loss of data and without adversely affecting the vital mission.

Discretionary Load - That portion of the load that indirectly supports the operations at the facility. This generally means loads associated with administration and office functions. This load is often referred to as “sheddable” and can be curtailed without overall adverse impact on the facility or the business.

SYSTEMS REQUIREMENTS

There are further detailed requirements for each discipline (e.g., electrical, mechanical, architectural), subsystem (e.g., AC power, DC power, backup power, emergency power), and element of the subsystem. This detail is often manifest in checklists with which individual facility and IT engineers can assess their situation, measure the reality of their hardware and software against industry standards, and plan and budget for achieving compliance.

These requirements could also map into a compliance matrix of assessment checklists and tier rankings. Such a matrix would enable those at the highest levels to understand their institution’s level of preparedness without having to weed through reports that may or may not accurately state their readiness or vulnerabilities.

For electrical systems, a complete analysis must include on-site power generation, electrical distribution, service entrance (utility feed), uninterruptible power supplies (UPS) and batteries (for critical systems), generators (for essential systems), power distribution units (PDU), branch circuits, fire alarm systems, grounding systems, conduit and static transfer switches to switch between power sources in response to interrupted power. Although a totally critical system, the electrical system is not the only system that requires evaluation.

Mechanical system assessment must include the mechanical plant (e.g., control plant chillers, cooling towers, pumps, piping, fluid coolers, air compressors), strategies for air flow and rack cooling (including high density racks), fuel oil and other fluid storage and distribution, generator exhaust, air conditioning units, direct expansion system, and humidification. Potential failure modes for mechanical systems, such as floods, very low temperatures affecting outdoor mechanical equipment, and make up water for cooling towers must be addressed.

Architectural issues include space adjacencies, physical separation of systems, minimum seismic requirements (tailored locally and approved regionally), raised floor issues (bolted stringers, colored aisle tiles, field tile loading capacity, pedestal and base anchorage) natural disaster planning and avoidance, physical security, and managing vendor activities during service and maintenance events.

Reliability Modeling and Probabilistic Risk Assessment

Once these determinations are made, the process can begin to develop a complete facility assessment to determine needs and budget constraints. Recognizing that reliability is a major cost-driver for these facilities, there are some leading edge approaches that can be applied to optimize the ratio between reliability and budget requirements. These approaches should follow established guidelines for designing reliability and maintainability into the facility. This methodology needs to be included in the programming/conceptual phase of the design. Each design alternative needs to quantify performance (reliability and availability) using Probabilistic Risk Assessment Analysis against cost analysis, in order to optimize the main decisions in the initial phase of the project.

Probabilistic Risk Assessment is a decision tool that has been gaining utility in the design and construction industry, especially for facilities designed with various system redundancies and with millions of dollars of assets at risk. This technique incorporates reliability models and provides for quantitative assessment of decision making. Traditionally used extensively in the aviation, nuclear, and chemical industries, the analysis of these types of redundancies requires the use of probability simulations to calculate failure rate, reliability, availability, unreliability, and unavailability.

Reliability modeling quantifies the resilience of critical nodes in the facility using matrices such as probability of failure or availability. The reliability evaluation process includes the following steps:

- Analyze existing systems and calculate reliability of the present environment.
- Develop recommendations and solutions for improving system resiliency.
- Calculate reliability of the upgraded configuration.
- Estimate costs of the upgrades and improvements.

Reliability predictions are only as good as the ability to model the actual system. In past reliability studies, major insight was gained for various topologies of the electrical distribution system using standards from IEEE Standard 493-1997, Recommended Practice for the Design of Reliable Industrial and Commercial Power Systems. However, aspects of the electrical distribution system for a critical facility differ from other industrial and commercial facilities and reliability modeling should include other sources of information (e.g., from Telcordia, DOD military handbooks and technical manuals, and other real world data).

REGULATORY ENVIRONMENT

Following are some of the most notable laws and guidance affecting the financial services industry, compliance with which might be impacted by success in providing its key facilities with critical power.

Sound Practices to Strengthen the Resilience of the U.S. Financial System

The Federal Reserve, the Office of the Comptroller of the Currency, and the Securities and Exchange Commission issued the *Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S.*

Financial System in September 2002. The purpose of the paper was to advise financial institutions of steps essential to increase financial services resilience and business continuity. The paper identifies three new business continuity objectives that are applicable to all financial services institutions. These objectives aim to relieve immediate pressure placed on the financial system by a wide-scale disruption of critical financial markets.

These objectives are: the rapid recovery and timely resumption of critical operations following a wide-scale disruption; rapid recovery and timely resumption of critical operations following the loss of inaccessibility of staff in at least one major operating location; and a high level of confidence, through ongoing use or robust testing, that critical internal and external continuity arrangements are effective and compatible. These business continuity objectives should be pursued by all financial institutions because of the high degree of interdependency in the financial services sector.

In addition to these three new business continuity objectives, the paper details four broad sound practices. Unlike the business continuity objectives, the sound practices have been identified specifically for core clearing and settlement organizations and for firms that play significant roles in critical financial markets. The paper identifies timelines for the implementation of these sound practices by such organizations.

The first sound practice is to identify clearing and settlement activities in support of critical financial markets. Second, organizations should determine appropriate recovery and resumption objectives for clearing and settlement activities in support of critical markets. Here, the paper specifies that core clearing and settlement organizations should be able to recover and resume clearing and settlement on the business day of the disruption, with a two hour goal for recovery. Although firms that play significant roles in critical financial markets are also expected to recover in the same business day, their goal is to recover within four hours of the disruption.

The third sound practice is to maintain sufficient geographically dispersed resources to meet recovery and resumption activities. The paper advises careful examination of the geographic diversity between primary and backup sites, including diversity of transportation, telecommunications, and power infrastructures. In addition, organizations should be sure that there is diversity in the labor pool of the primary and backup sites, such that a wide-scale event would not simultaneously affect the labor pool of both sites. Appropriate diversity should be confirmed through testing. The fourth sound practice is to routinely use or test recovery and resumption arrangements. Here the paper stresses the importance of testing backup arrangements with third-party service providers, major counterparties, and even customers. Backup connectivity, capacity, and data integrity should be tested, and scenarios should include wide-scale disruptions.

FFIEC Information Technology Booklets

The Federal Financial Institutions Examination Council¹¹ (FFIEC) issued an Information Technology Booklet on Business Continuity Planning in May 2003. The booklet outlines broad expectations for financial institutions and includes the procedures by which federal examiners evaluate the adequacy of a financial institution's business continuity plan and information security

¹¹ The FFIEC is composed of the Board of Governors of the Federal Reserve System ([FRB](#)), the Federal Deposit Insurance Corporation ([FDIC](#)), the National Credit Union Administration ([NCUA](#)), the Office of the Comptroller of the Currency ([OCC](#)), and the Office of Thrift Supervision ([OTS](#)).

program. The booklet includes references to power issues including, for example, the expectation that financial institutions conduct comprehensive business impact analyses (BIA) and risk assessments. The BIA should identify and prioritize business functions and it should state the maximum allowable downtime for critical business functions. It should also estimate data loss and transaction backlog that may result from critical business function downtime. Examiners review, among other things, a financial institution's risk assessment to ensure that it includes disruption scenarios and the likelihood of disruption affecting information services, technology, personnel, facilities, and service providers. Such disruption scenarios should include both internal and external sources, such as natural events (e.g., fires, floods, severe weather), technical events (e.g., communication failure, power outages, equipment and software failure), and malicious activity (e.g., network security attacks, fraud, terrorism).

Basel II Accord

With the globalization of financial services firms and rise of sophisticated information technology, banking has become more diverse and complex. The Basel Capital Accord was first introduced in 1988 by the Bank for International Settlements (BIS) and was then updated in 2004 as the Basel II Accord. Basel II provides a regulatory framework that requires all internationally-active banks to adopt similar or consistent risk-management practices for tracking and publicly reporting their operational, credit, and market risks. Basel II's risk management guidelines implicate the collection, storage, and processing of data. Financial organizations also must implement operational controls such as power protection strategies to ensure reliability, availability, and security of their data and business systems, to minimize operational risk.

National Fire Protection Association (NFPA) 1600 – Standard on Disaster/Emergency Management and Business Continuity Programs - 2004 Edition¹²

NFPA 1600 provides a standardized basis for disaster/emergency management planning and business continuity programs in private and public sectors by providing common program elements, techniques, and processes.

Other noteworthy laws and/or guidance with less specific applicability to financial services are:

- **U.S.A. PATRIOT Act of 2001** – The Act was designed to support counter-terrorism activities, threat assessment, and risk mitigation; to support critical infrastructure protection and continuity; to enhance law enforcement investigative tools; and to promote partnerships between government and industry.
- **Sarbanes-Oxley Act of 2002 (SOX)** – SOX was enacted in response to major instances of corporate fraud, abuse of power, and mismanagement. SOX required major changes in securities law, and reviews of policies and procedures with attention to data standards and IT processes. A key part of the review process is how vital corporate data is stored, managed and protected. From a power protection standpoint, the focus is on availability, integrity, and

¹² NFPA 1600 Standard on Disaster/Emergency Management and Business Continuity Programs - 2004 Edition, Copyright © 2004, National Fire Protection Association, All Rights Reserved.

accountability. Critical data must not be lost or corrupted, tampered with, or rendered unavailable.

- **High Level Principles for Business Continuity** – The Joint Forum¹³ released High Level Principles for business continuity in December 2005. The paper proposes to set out a framework for international standard setting organizations and national financial authorities. These organizations identified seven high-level business continuity principles to increase resiliency to a major operational disruption. The principles are
 - Assigning responsibility for business continuity to an institution’s board of directors and senior management.
 - Planning for the occurrence of and recovery from major operational disruptions.
 - Establishing recovery objectives proportionate to the risk posed by a major operational disruption.
 - Including organizational and external communications in business continuity plans.
 - Including cross-border communication components in business continuity plans.
 - Testing of business continuity plans. Evaluation and, if necessary, updating should follow continuity testing.
 - Reviewing of institutional business continuity plans by financial authorities.

- **ANSI Homeland Security Standards Panel** – The Panel is near completion of a report that captures in one place all relevant standards and guidance documents in the marketplace on the subject of enterprise power security and continuity, as well as makes recommendations for addressing gap areas. For more information, contact the ANSI-HSSP Secretary and go to www.ansi.org/hssp.

QUESTIONS

ITEM	DESCRIPTION
29.	How much does each minute, hour or day of operational downtime cost your company if a specific facility is lost?
30.	Have you determined your recovery time objectives for each of your business processes?
31.	Does your financial institution conduct comprehensive business impact analyses (BIA) and risk assessments?
32.	Have you considered disruption scenarios and the likelihood of disruption affecting information services, technology, personnel, facilities, and service providers in your risk assessments?
33.	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 failure, power outages, equipment and software failure), and malicious activity (e.g., network security attacks, fraud, terrorism)?
34.	Does this BIA identify and prioritize business functions and state the maximum allowable downtime for critical business functions?
35.	Does the BIA estimate data loss and transaction backlog that may result from critical business function downtime?

¹³ The Joint Forum is composed of the Basel Committee on Banking Supervision, the International Organization of Securities Commissions and the International Association of Insurance Supervisors.

ITEM	DESCRIPTION
36.	Have you prepared a list of “critical facilities” to include any location where a critical operation is performed including all work area environments such as branch backroom operations facilities, headquarters or data centers?
37.	Have you classified each critical facility using a critical facility ranking/rating system such as the Tier I, II, III, IV rating categories?
38.	Has a condition assessment been performed on each critical facility?
39.	Has a facility risk assessment been conducted for each of your key critical facilities?
40.	Do you know the critical, essential and discretionary loads in each critical facility?
41.	Must you comply with the regulatory requirements and guidelines discussed in this chapter?
42.	Are any internal corporate risk and compliance policies applicable?
43.	Have you identified business continuity requirements and expectations?
44.	Has a gap analysis been performed between the capabilities of each company facility and the corresponding business process recovery time objectives residing in that facility?
45.	Based on the gap analysis, have you determined the infrastructure needs for your critical facilities?
46.	Have you considered fault tolerance and maintainability in your facility infrastructure requirements?
47.	Given your new design requirements, have you applied reliability modeling to optimize a cost effective solution?
48.	Have you planned for rapid recovery and timely resumption of critical operations following a wide-scale disruption?
49.	Following the loss of accessibility of staff in at least one major operating location, how will you recover and timely resume critical operations?
50.	Are you highly confident, through ongoing use or robust testing, that critical internal and external continuity arrangements are effective and compatible?
51.	Have you identified clearing and settlement activities in support of critical financial markets?
52.	Do you employ and maintain sufficient geographically dispersed resources to meet recovery and resumption activities?
53.	Is your organization sure that there is diversity in the labor pool of the primary and backup sites, such that a wide-scale event would not simultaneously affect the labor pool of both sites?
54.	Do you routinely use or test recovery and resumption arrangements?
55.	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 in private and public sectors by providing common program elements, techniques, and processes?

IV – INSTALLATION

Critical power is protected and secured by deployment of specialized infrastructure equipment designed to provide a continuous facility power stream and immunity from public power “grid” disturbances.

Based on the results of the Needs Analysis and Risk Assessment process, decisions will result in authorizing projects to install or upgrade critical power facility infrastructure at your financial institution.

Depending on the size and scope of the project, a range of electrical, mechanical, security, and fire protection infrastructure will be impacted even though the project purpose is improvement of the critical power. The range of infrastructure typically included in a project scope can include:

Electrical Systems

- Transformers
- UPS systems
- Emergency generators and controls
- Utility switchboards
- Automatic transfer switchgear
- Auto-Static transfer switches
- Power Distribution Units
- Transient Voltage Protection

Mechanical Systems

- Computer Room Air Handling Units (CRAH)
- Water chillers, Pumps
- Cooling towers
- Water storage tanks (chilled, makeup)
- Automatic controls (BMS, BAS)
- Fuel oil systems for Diesel Generators
- Fire protection
- Security

The five typical phases of a project to provide critical power are design, procurement, construction, commissioning/acceptance testing, and transition to operations.

Design

The design phase of the project involves a comprehensive review and identification of the project purpose resulting in issuance of detailed plans and specifications that will be used by the contractors to install and by the operations staff to understand the project intent. The design phase should include a qualified architect, engineering, and design firms, and the design team members should include representation from the end user, facility management, and IT staff. It is during the design phase that environmental issues should be considered. These issues can range from avoiding placement of equipment in flood prone areas to ensuring compliance with local ordinances regarding noise abatement.

Procurement

The resulting design documents can be sent to qualified contractors for bidding or pricing. Depending on the institution, the procurement staff may be facilities, project, or dedicated purchasing/procurement staff. Appropriate contractors and equipment vendors are then chosen.

Construction

Entering the construction phase, the work flow should shift to construction and to project management professionals who are experienced in this type of mission critical infrastructure. The construction team should include financial institution facilities operations staff who will gain invaluable exposure to the project and have a vested interest in project success because of their operational role once the infrastructure is in service.

Commissioning/Acceptance Testing

Before a new facility or new infrastructure in an existing building goes on-line, it is crucial to resolve all potential equipment problems during a commissioning and acceptance phase. Commissioning is a systematic process of ensuring, through documented verification, that all building systems perform according to the documented design intent, and to the owner's operational needs. The goal is to provide the owner with a safe, reliable installation. Commissioning specifications should be written and included in bid documents

Acceptance testing will be the construction team's sole opportunity to integrate and commission all the systems, given the facility's 24/7 mission critical status. There is no "one size fits all" formula and the commissioning agent facilitates a highly interactive process through coordination with the owner, design team, construction team, and vendors during the various phases of the project. Prior to installation at the site, all systems should be tested at the factory and witnessed by an independent test engineer familiar with the equipment. However, reliance on the factory testing and competence of independent test engineers is insufficient.

Once the equipment is delivered, placed, and wired, the second phase of certified testing and integration begins. The goal of this phase is to verify and certify all components work together while fine tuning, calibrating, and integrating all systems. A tremendous amount of coordination is required during this phase. The facilities engineer and commissioning team work with the factory, field engineers, and independent test consultants to coordinate testing and calibration. Critical circuit breakers must be tested and calibrated prior to placing any critical electrical load on them. After all tests are completed, results must be compiled and the certified test reports prepared, which will establish a benchmark for all future testing. Steps to educate staff regarding each major system and piece of equipment should be included in the construction process. This training phase is an ongoing process that begins during construction and continues over the life of the facility.

Transition to Operations

Transition to operations is the final phase of the project. This phase ensures that the design and construction team smoothly hands off the new infrastructure or facility to a confident, fully trained operations team that is charged with its reliable and safe operation. Plans for this transition should be discussed during the design concept phase. Steps should be included to ensure that accurate documentation, detailed tracking/resolution of open items and maximization of training opportunities are incorporated into all project phases

Security Considerations

It is important to address physical and cyber security needs of critical infrastructure since it includes systems, facilities, and assets so vital that, if they are destroyed or incapacitated, could disrupt the safety and the economic condition of the financial institution. Operation of these systems typically utilizes environmentally-hazardous diesel fuel oil and lead acid batteries which require special accommodations. Security requirements may include capabilities to prevent and protect against intrusion, hazards, threats, and incidents, and to expeditiously recover and reconstitute critical services.

A sensible and cost effective security approach can provide a protection level achieved through design, construction, and operation that mitigates adverse impact to systems, facilities, and assets. This can include vulnerability and risk assessment methodologies which determine prevention, protection, monitoring, detection, and sensor systems to be deployed in the design. It is essential to include representation from the financial institution security department and from the engineering/design firm from the onset of the initial design.

The increased use of and advances in information technology, coupled with the prevalence of hacking of and unauthorized access to electronic networks, requires physical security to be complemented by cyber security considerations. Before enabling remote access for monitoring and /or control of critical infrastructure systems, cyber security protection must be assured.

ITEM	DESCRIPTION
	Design
56.	Has the owner, working with an engineering professional, developed a Design Intent Document to clearly identify quantifiable requirements?
57.	Have you prepared a Basis of Design document that memorializes, in a narrative form, the project intent, future expansion options, types of infrastructure systems to be utilized, applicable codes and standards to be followed, design assumptions, and project team decisions and understandings?
58.	Will you provide the opportunity to update the Basis of Design to reflect changes made during the construction and commissioning process?
59.	Are the criteria for testing all systems and outlines of the commissioning process identified and incorporated into the design documents?
60.	Have you identified a qualified engineering and design firm to conduct a peer project design review?
61.	Have you considered directly hiring the commissioning agent to provide true independence?
62.	Have you discussed and agreed to a division of responsibilities between the construction manager and the commissioning agent?
63.	Do you plan to hire the ultimate operating staff ahead of the actual turnover to operations so they will benefit from participation in the design, construction and commissioning of the facility?
64.	Have you made a decision on the commissioning agent early enough in the process to allow participation and input on commissioning issues and design review by the selected agent?
65.	Is the proper level of fire protection in place?
66.	Is the equipment (UPS or generator) being placed in a location prone to flooding or other

ITEM	DESCRIPTION
	water damage?
67.	Do the generator day tanks or underground fuel cells meet local environmental rules?
68.	Does the battery room have proper ventilation?
69.	Has adequate cooling or heating been specified for the UPS, switchgear or generator room?
70.	Are the heating and cooling for the mechanical rooms on the power protection system?
71.	Have local noise ordinances been reviewed and does all the equipment comply with the ordinances?
72.	Are the posting and enforcement of no-smoking bans adequate, specifying, for example, no smoking within 100 feet?
73.	Are water detection devices used to alert building management of flooding issues?
	Procurement
74.	Is there a benefit to using an existing vendor or supplier for standardization of process, common spare parts, or confidence in service response?
75.	Have the commissioning, factory, and site testing requirement specifications been included in the bid documentation?
76.	If the project is bid, have you conducted a technical compliance review which identifies exceptions, alternatives, substitutions, or non-compliance to the specifications?
77.	Are the procurement team members versed in the technical nuances and terminology of the job?
78.	If delivery time is critical to the project, have you considered adding late penalty clauses to the installation or equipment contracts?
79.	Have you included a bonus for early completion of project?
80.	Have you obtained unit rates for potential change orders?
81.	Have you obtained a GMP (Guaranteed Maximum Price) from contractors?
82.	Have you discussed preferential pricing discounts that may be available if your institution or your engineer and contractors have other similar large purchases occurring?
	Construction
83.	Do you intend to create and maintain a list of observations and concerns that will serve as a check list during the acceptance process to ensure that these items are not overlooked?
84.	Will members of the design, construction, commissioning agent, and operations team attend the factory acceptance tests for major components and systems such as UPS, generators, batteries, switchgear and chillers?
85.	During the construction phase, do you expect to develop and circulate for comment the start up plans, documentation formats and pre-functional checklists that will be used during startup and acceptance testing?
86.	Since interaction between the construction manager and the commissioning agent is key, will you encourage attendance at the weekly construction status meetings by the commissioning team?
87.	Will an independent commissioning and acceptance meeting be run by the commissioning agent ensuring that everything needed for that process is on target?
88.	Will you encourage the construction, commissioning, and operations staff to walk the job site regularly to identify access and maintainability issues?
89.	If the job site is an operating critical site, do you have a risk assessment and change control

ITEM	DESCRIPTION
	mechanism in place to ensure reliability?
90.	Have you established a process to have independent verification that labeling on equipment and power circuits is correct?
	Commissioning and Acceptance
91.	Do testing data result sheets identify expected acceptable result ranges?
92.	Are control sequences, check lists, and procedures written in plain language, not technical jargon that is easily misunderstood?
93.	Have all instrumentation, test equipment, actuators and sensing devices been checked and calibrated?
94.	Is system acceptance testing scheduled after balancing of mechanical systems and electrical cable/breaker testing are complete?
95.	Have you listed the systems and components to be commissioned?
96.	Has a detailed script sequencing all activities been developed?
97.	Are all participants aware of their responsibilities and the protocols to be followed?
98.	Does a Team Directory with all contact information exist and is it available to all involved parties?
99.	Have you planned an “all hands on deck” meeting to walk through and finalize the commissioning schedule and scripted activities?
100.	Have the format and content of the final report been determined in advance to ensure that all needed data is recorded and activities are scheduled?
101.	Have you arranged for the future facility operations staff to witness and participate in the commissioning and testing efforts?
102.	Who is responsible for ensuring that all appropriate safety methods and procedures are deployed during the testing process?
103.	Is there a process in place that ensures training records are maintained and are updated?
104.	Who is coordinating training and ensuring that all prescribed training takes place?
105.	Will you videotape training sessions to capture key points and for use as refresh training?
106.	Is the training you provide both general systems training as well as specifically targeted to types of infrastructure within the facility?
107.	Have all vendors performed component level verification and completed pre-functional check lists prior to system level testing?
108.	Has all system level acceptance testing been completed prior to commencing the full system integration testing and “pull the plug” power failure scenario?
109.	Is a process developed to capture all changes made and to ensure that these changes are captured on the appropriate built drawings, procedures, and design documents?
110.	Do you plan to re-perform acceptance testing if a failure or anomalies occur during commissioning and testing?
111.	Who will maintain the running punch list of incomplete items and track resolution status?
	Transition to Operations
112.	Have you established specific Operations Planning meetings to discuss logistics of transferring newly constructed systems to the facility operations staff?
113.	Is all as-built documentation, such as drawings, specifications, and technical manuals, complete and has it been turned over to operations staff?

ITEM	DESCRIPTION
114.	Have position descriptions been prepared that clearly define roles and responsibilities of the facility staff?
115.	Are Standard Operating Procedures (SOP), Emergency Action Procedures (EAP), updated policies, and change control processes in place to govern the newly installed systems?
116.	Has the facility operations staff been provided with warranty, maintenance, repair, and supplier contact information?
117.	Have spare parts lists, setpoint schedules after Cx is complete, TAB report and re-commissioning manuals been given to operations staff?
118.	Are the warranty start and expiration dates identified?
119.	Have maintenance and repair contracts been executed and put into place for the equipment?
120.	Have minimum response times for service, distance to travel, and emergency 24/7 spare stock locations been identified?
	Security Considerations
121.	Have you addressed physical security concerns?
122.	Have all infrastructures been evaluated for type of security protection needed (e.g., card control, camera recording, key control)?
123.	Are the diesel oil tank and oil fill pipe in a secure location?
124.	If remote dial in or Internet access is provided to any infrastructure system, have you safeguarded against hacking or do you permit read-only functionality?
125.	How frequently do you review and update access permission authorization lists?
126.	Are critical locations included in security inspection rounds?

Electrical maintenance is a necessity, not a luxury. Understanding the risk and sensitivity of mission critical sites affords a financial institution mitigation of downtime with regard to a range of mission critical engineering services.

An effective maintenance and testing program for a mission critical electrical load is key to protecting the investment by safeguarding against power failures. Maintenance procedures and schedules must be developed, staff properly trained, spare parts provisioned, and mission critical electrical equipment performance tested and evaluated regularly.

There are various approaches to establish a maintenance program. In most cases, a program will include a blend of the strategies listed below:

- Preventive Maintenance (PM) is the completion of tasks performed on defined schedule. The purpose of PM is to extend the life of equipment and detect wear as an indicator of pending failure. Tasks describing the maintenance procedures are fundamental to a PM program. They instruct the technician on what to do, what tools and equipment to use, what to look for, how to do it, and when to do it. Tasks can be created for routine maintenance items or for breakdown repairs.
- Predictive Maintenance uses instrumentation to detect the condition of equipment and to identify pending failures. A predictive maintenance program uses these equipment condition indices for the purpose of scheduling maintenance tasks.
- Reliability Centered Maintenance (RCM) is the analytical approach to optimize reliability and maintenance tasks with respect to the operational requirements of the business. Reliability, as it relates to business goals, is the fundamental objective of the RCM process. RCM is not equipment centric, but business centric. RCM analyzes each system and how it can functionally fail. The effects of each failure are analyzed and ranked according to their impact on safety, mission, and cost. Those failures which are deemed to have a significant impact are further explored to determine the root causes. Finally, maintenance is assigned based on effectiveness, with a focus on condition-based tasks.

The objective of a maintenance program is to use a blend of predictive, preventative and RCM techniques to reach the optimum point at which the benefits of reliability are maximized while the cost of maintenance is minimized.

The appropriate frequency of electrical maintenance should be driven in part by the level of reliability an institution requires. Specifically, risk tolerance expectations and uptime goals must be weighed. An institution satisfied with 99% reliability, or 87.6 hours of downtime per year, will run a maintenance program every three to five years. However, if 99.999% reliability, or 5.25 minutes of downtime per year, is mandatory, then an institution must perform an aggressive preventive maintenance program every six months. The cost of this hard-line maintenance program could range between \$300 and \$400 annually per kilowatt (kW), not including the staff to manage the program. The human resources cost will vary depending on the location and complexity of the facility.

The other factor affecting maintenance frequency is the state of industry-accepted guidelines. There are several excellent resources available for developing the basis of an electrical testing and maintenance program. For example, the InterNational Electric Testing Association (NETA)

publishes the *Maintenance Testing Specifications* that recommend appropriate maintenance test frequencies based on equipment condition and reliability requirements. The National Fire Protection Association's (NFPA) *70B Recommended Practice for Electrical Equipment Maintenance* and *RSMMeans Facilities Maintenance and Repair Book* give guidance for testing and maintenance tasks and periodic schedules to incorporate into maintenance programs.

Testing and service individuals should have the highest education, skills, training, and experience available. Their conscientiousness and decision-making abilities are a key to avoiding potential problems with perhaps the most crucial equipment in a facility. Most importantly, learn from previous experiences and from the experiences of others so that operational and maintenance programs continuously improve as knowledge increases. If a task has historically not identified a problem at the scheduled interval, consider adjusting the schedule. Examine maintenance programs on a regular basis and make appropriate adjustments.

Routine shutdowns of a facility should be planned to accommodate preventive maintenance of electrical equipment. Neither senior management nor facility managers should underestimate the cost-effectiveness of a thorough preventative maintenance program.

Initial equipment acceptance testing and ongoing maintenance will not return maximum value unless the test results are evaluated and compared with standards and previous test reports that have established benchmarks. It is imperative to recognize failing equipment and to take appropriate action as soon as possible. All too commonly, maintenance personnel perform maintenance without reviewing prior maintenance records. This approach must be avoided because it defeats the value of benchmarking and trending and must be avoided. By reviewing past maintenance reports, staff can keep maintenance objectives in perspective and rely upon the accuracy of the information contained in these reports when faced with a real emergency.

Every preventative maintenance opportunity should be thorough and complete, especially in mission critical facilities. If they are not, the next opportunity will come at a much higher price: downtime, lost business, and the loss of potential clients. In addition, safety issues arise when technicians rush to repair high voltage equipment.

ITEM	DESCRIPTION
	Strategic
127.	Is there a documented maintenance and testing program based on your business risk assessment model?
128.	Is an audit process in place to ensure that this maintenance and testing program is being followed rigorously?
129.	Does the program ensure that maintenance test results are benchmarked and used to update and improve the maintenance program?
130.	Is there a program in place that ensures periodic evaluation of possible equipment replacement?
131.	Is there a process in place that ensures the spare parts inventory is updated when new equipment is installed or other changes are made to the facility?
132.	Have you evaluated the impact of loss of power in your institution and other institutions because of interdependencies?
133.	Has your facility developed Standard Operating Procedures (SOPs), Emergency Action

ITEM	DESCRIPTION
	Procedures (EAPs), and Alarm Response Procedures (ARPs)?
134.	Are the SOP, EAP, and ARP readily available and current?
135.	Is your staff familiar with the SOPs, EAPs, and ARPs?
	Planning
136.	Does the system design provide redundancy so all critical equipment can be maintained without a shutdown if required?
137.	Are there adequate work control procedures and is there a change management process to prevent mistakes when work is done on critical systems and equipment?
138.	Are short circuit and coordination studies up to date?
139.	Do you have a Service Level Agreement (SLA) with your facilities service providers and contractors?
140.	Is there a change management process that communicates maintenance, testing, and repair activities to both end users and business lines?
141.	Do you have standard operating procedures to govern routine facilities functions?
142.	Do you have emergency response and action plans developed for expected failure scenarios?
143.	Have you prepared an emergency telephone contact list that includes key service providers and suppliers?
	Safety
144.	Is there a formal and active program for updating the safety manual?
145.	Are electrical work procedures included in the safety manual?
146.	Has an arc-flash study been performed?
147.	Are specific PPE requirements posted at each panel, switchgear, etc?
148.	Is there a program in place to ensure studies and PPE requirements are updated when system or utility supply changes are made?
149.	Are workers trained regarding safety manual procedures?
150.	Are hazardous areas identified on drawings?
151.	Are hazardous areas physically identified in the facility?
	Testing
152.	Have protective devices been tested or checked to verify performance?
153.	Is a Site Acceptance Test (SAT) and a Factory Acceptance Test (FAT) performed for major new equipment such as UPS systems and standby generators?
154.	Is an annual “pull the plug” test performed to simulate a utility outage and ensure that the infrastructure performs as designed?
155.	Is an annual performance and recertification test conducted on key infrastructure systems?
156.	Is there a process in place that ensures personnel have the proper instrumentation and that it is periodically calibrated?
	Maintenance
157.	Does the program identify all critical electrical equipment and components?
158.	Is there a procedure in place that updates the program based on changes to plant equipment or processes?
159.	Does a comprehensive plan exist for thermo infrared (IR) heat scan of critical components?

ITEM	DESCRIPTION
	Is an IR scanning test conducted before a scheduled shutdown?
160.	Are adequate spare parts on hand for immediate repair and replacement?
161.	Is your maintenance and testing program based on accepted-industry guidelines such as NFPA 70B and on equipment supply recommendations?
162.	Do you incorporate Reliability Centered Maintenance (RCM) philosophy in your approach to maintenance and testing?
163.	When maintenance and testing is performed, do you require preparation of and adherence to detailed work statements and method of procedures (MOPs)?
164.	Do you employ predictive maintenance techniques and programs such as vibration and oil analysis?

VI – TRAINING AND DOCUMENTATION

Millions of dollars are invested in the infrastructure supporting 24/7 applications, with major commitments made in design, equipment procurement, and project management. However, investment in documentation, training, and education has been minimal despite the fact that they are essential to achieving and maintaining optimum levels of reliability.

As equipment reliability increases, a larger percentage of downtime results from actions by personnel who are inadequately trained or who lack access to accurate, comprehensible data during crisis events. Keeping on-site staff motivated, trained, and ready to respond to emergencies is a challenge. Years ago most organizations relied heavily on their workforce to retain much of the information regarding the mission critical systems. A large body of personnel had a similar level of expertise and remained with their company for decades. Therefore, little emphasis was placed on creating and maintaining a fluid and living document repository for critical infrastructure.

Today's diversity among mission critical systems severely hinders employee ability to fully understand and master all necessary equipment and the information required to keep that equipment running. We can no longer allow engineers and operators to acquire their knowledge of increasingly sophisticated power supply and distribution technology from "on the job training," which proves woefully inadequate in time of crisis. Instead, a clear plan must be put into place to develop a critical document repository and to continually educate and train employees while enhancing real time experiences.

Elements of a comprehensive training and certification program could include:

- Providing fundamental training on facility electrical, mechanical, and life safety systems.
- Determining staff qualification criteria.
- Identifying training topics and developing specific modules.
- Creating testing content and certification methods.
- Maintaining employee training records and ongoing training requirements.

Prudent business practice recognizes the need to plan for employee succession, unexpected staff departure, orientation/training of new employees, as well as education of seasoned employees. An education and training program, coupled with a document management system, can address these concerns. Site-specific training courses can be developed to target subjects such as UPS switching procedures, emergency generator operation and testing, company policies and procedures, safety, and critical environment work rules.

In the financial services industry, education and training that is standardized, comprehensive, and focused on the job at hand will create a pool of talented individuals possessing the knowledge and information necessary to solve problems during power emergencies. This will lead to shorter and less frequent unplanned downtime. Documentation is essential not only to facilitate the ongoing education and training requirements of a company's personnel, but also to maintain safety and to minimize risk to the company, assuring the integrity of a robust mission critical infrastructure and the institution's bottom line.

A “database” of perpetually refreshed knowledge can be achieved by creating a living document system that provides the level of granularity necessary to operate a mission critical infrastructure. Such a system should be supplemented with a staff training and development program. Keeping the living document and training programs current can then be addressed each time a capital project is completed or an infrastructure change is made. Accurate and up-to-date information provides first responders with the intelligence and support necessary to make informed decisions during critical events.

ITEM	DESCRIPTION
	Documentation
165.	What emergency plans, if any, exist for the facility?
166.	Where are emergency plans documented (including the relevant internal and external contacts for taking action)?
167.	How are contacts reached in the event of an emergency?
168.	How are plans audited and changed over time?
169.	Do you have complete drawings, documentation, and technical specifications of your mission critical infrastructure including: electrical utility, in-facility electrical systems (including power distribution and ATS), gas and steam utility, UPS/battery/generator, HVAC, security, and fire suppression?
170.	What documentation, if any, exists to describe the layout, design, and equipment used in these systems?
171.	How many forms does this documentation require?
172.	How is the documentation stored?
173.	Who has access to this documentation and how do you control access?
174.	How many people have access to this documentation?
175.	How often does the infrastructure change?
176.	Who is responsible for documenting change?
177.	How is the information audited?
178.	Can usage of facility documentation be audited?
179.	Do you keep a historical record of changes to documentation?
180.	Is a formal technical training program in place?
181.	Is there a process in place that ensures personnel have proper instrumentation and that the instrumentation is periodically calibrated?
182.	Are accidents and near-miss incidents documented?
183.	Is there a process in place that ensures action will be taken to update procedures following accidents or near-miss events?
184.	How much space does your physical documentation occupy today?
185.	How quickly can you access the existing documentation?
186.	How do you control access to the documentation?
187.	Can responsibility for changes to documentation be audited and tracked?
188.	If a consultant is used to make changes to documentation, how are consultant deliverables tracked?
189.	Is your organization able to prove what content was live at any given point in time, in the event such information is required for legal purposes?

190.	Is your organization able to quickly provide information to legal authorities including emergency response staff (e.g., fire, police)?
191.	How are designs or other configuration changes to infrastructure approved or disapproved?
192.	How are these approvals communicated to responsible staff?
193.	Does workflow documentation exist for answering staff questions about what to do at each stage of documentation development?
194.	In the case of multiple facilities, how is documentation from one facility transferred or made available to another?
195.	What kind of reporting on facility infrastructure is required for management?
196.	What kind of financial reporting is required in terms of facility infrastructure assets?
197.	How are costs tracked for facility infrastructure assets?
198.	Is facility infrastructure documentation duplicated in multiple locations for restoration in the event of loss?
199.	How much time would it take to replace the documentation in the event of loss?
200.	How do you track space utilization (including cable management) within the facility?
201.	Do you use any change management methodology (i.e., ITIL) in the day-to-day configuration management of the facility?
	Staff & Training
202.	How many operations and maintenance staff do you have within the building?
203.	How many of these staff do you consider to be facilities "subject matter experts?"
204.	How many staff members manage the operations of the building?
205.	Are specific staff members responsible for specific portions of the building infrastructure?
206.	What percentage of your building operations staff turns over annually?
207.	How long has each of your operations and maintenance staff, on average, been in his or her position?
208.	What kind of ongoing training, if any, do you provide for your operations and maintenance staff?
209.	Do training records exist?
210.	Is there a process in place to ensure that training records are maintained and updated?
211.	Is there a process in place that identifies an arrangement for training?
212.	Is there a process in place that ensures the training program is periodically reviewed and identifies changes required?
213.	Is the training you provide general training, or is it specific to an area of infrastructure within the facility?
214.	How do you design changes to your facility systems?
215.	Do you handle documentation management with separate staff, or do you consider it to be the responsibility of the staff making the change?
	Network and Access
216.	Do you have a secured network between your facility IT installations?
217.	Is this network used for communications between your facility management staff?
218.	Do you have an individual on your IT staff responsible for managing the security infrastructure for your data?
219.	Do you have an online file repository?

220.	If so, how is use of the repository monitored, logged, and audited?
221.	How is data retrieved from the repository kept secure once it leaves the repository?
222.	Is your file repository available through the public Internet?
223.	Is your facilities documentation cataloged with a standard format to facilitate location of specific information?
224.	What search capabilities, if any, are available on the documentation storage platform?
225.	Does your facility documentation reference facility standards (e.g., electrical codes)? If so, how is this information kept up-to-date?

VII – CONCLUSION

The following highlights have been distilled from the prior sections of this *Guide*. They are baseline observations and recommendations intended to provide financial institutions with industry business practices for understanding, evaluating, and managing risks associated when the predicted reliability and availability of the electrical system is disrupted.

GENERAL COMMENTS
<ul style="list-style-type: none">• Financial institutions need to constantly and systematically evaluate their mission critical systems, assessing and reassessing their level of risk tolerance versus the cost of downtime.
<ul style="list-style-type: none">• Providing continuous operation under all foreseeable risks of failure is a nontrivial matter and requires a holistic, enterprise approach.
<ul style="list-style-type: none">• Communication between managers of business lines, business continuity and facilities is vital.
THE GRID AND POWER UTILITY COMPANIES
<ul style="list-style-type: none">• The grid is inherently subject to external factors that can cause outages, and there is only so much that feasibly can be done to secure it against these possible problems.
<ul style="list-style-type: none">• Guaranteeing supplies of critical power at high-demand, high-reliability locations ultimately means adding increasingly sophisticated on-site generating capacity and storage to back up whatever is being done to improve reliability higher in the grid.
<ul style="list-style-type: none">• Financial institutions should be in touch with their electric power utility to establish the working relationship needed to help through real or potential service interruptions, including becoming involved in crisis management testing performed by the utility and understanding the power utility’s operating strategy and position within any larger regional or national infrastructure.
NEEDS ANALYSIS/RISK ASSESSMENT
<ul style="list-style-type: none">• Today’s risk profile includes the possibility that outages may last a long time and extend over wide areas. The planning challenge shifts from issues of power <i>quality</i> or <i>reliability</i> to issues of business <i>sustainability</i>. Planning must take into account outages that last not for seconds, or for a single hour, but for days.
<ul style="list-style-type: none">• The first step in the needs analysis process is to determine the level of criticality. Individual institutions establish their level of criticality based on their own criteria and their customers’ criteria. The primary criterion is availability.
INSTALLATION
<ul style="list-style-type: none">• Financial institutions require highly sophisticated uninterruptible power systems, generators, HVAC systems, transfer switches, and other high-voltage electrical and mechanical systems to ensure fail safe power delivery and operation.
<ul style="list-style-type: none">• Security requirements may include capabilities to prevent and protect against intrusion, hazards, threats, and incidents—both physical and cyber—and to expeditiously recover and reconstitute critical services.
<ul style="list-style-type: none">• It is essential to include representation from the financial institution security department from the onset of initial design.
MAINTENANCE AND TESTING
<ul style="list-style-type: none">• An effective maintenance and testing program for a mission critical electrical load is key to protecting the investment by safeguarding against power failures.

<ul style="list-style-type: none"> • Routine shutdowns of a facility should be planned to accommodate preventive maintenance of electrical equipment. Neither senior management nor facility managers should underestimate the cost-effectiveness of a thorough preventative maintenance program.
<ul style="list-style-type: none"> • Maintenance procedures and schedules must be developed, staff properly trained, spare parts provisioned, and mission critical electrical equipment performance tested and evaluated regularly.
<p>TRAINING AND DOCUMENTATION</p>
<ul style="list-style-type: none"> • A large percentage of downtime results from actions by personnel who are inadequately trained or who lack access to accurate comprehensible data during crisis events.
<ul style="list-style-type: none"> • A clear plan must be put into place to develop a critical document repository and to continually educate and train employees while enhancing real time experiences.

Prudent planning and an appropriate level of investment will help ensure uninterrupted power supply. Minimizing unplanned downtime reduces risk. Financial institutions must consider a proactive rather than a reactive approach. Strategic planning can identify internal risks and provide a prioritized plan for reliability improvements that identify the root causes of failures before they occur. Planning and careful implementation will minimize disruptions while making the business case to fund necessary capital improvements and implement comprehensive maintenance strategies. When the business case reaches the board room, the entire organization can be galvanized to prevent catastrophic losses, damage to capital equipment, and physical danger to our employees and customers.

APPENDIX A

ACKNOWLEDGEMENTS AND REFERENCES

The *BITS Guide to Business-Critical Power* was developed by a small, dedicated team of professionals from BITS member organizations, the Critical Power Coalition, Power Management Concepts and BITS staff. It is based on meetings and calls and it draws on the following sources:

- “Maintaining Mission Critical Systems in a 24/7 Environment,” Peter M. Curtis (to be published in 2006)
- BITS white paper, “Telecommunications for Critical Infrastructure: Risks and Recommendations” (December 2002)
- *BITS Guide to Business-Critical Telecommunications Services* (2004)
- BITS Forums on Telecommunications Resiliency (June 2002 and June 2004)
- Securities Industry Association Business Continuity Committee “Critical Infrastructure Guidelines” (May 2004 draft)
- BITS Lessons Learned: Northeast Blackout of 2003 (October 2003)
- Digital Power white paper, “Critical Power” (August 2003)

Peter M. Curtis, Power Management Concepts, and Teresa C. Lindsey, BITS, served as the principal authors of this document. Additionally, the following individuals made significant contributions:

Warren Axelrod, Pershing
Mike Carano, LaSalle Bank Corporation
Don Donahue, DTCC and FSSCC
Jim Driscoll, Commerce Bancshares
Kfir Godrich, EYP MCF
Howard Goodman, Securities Industry Association
Patti Harris, Regions Financial Corporation
Sue Kerr, Capital One Financial Corporation
Paul LaPierre, The Critical Power Coalition
Joe Lee, Wachovia Corporation
Lou Leffler, NERC
Mark Mills, The Critical Power Coalition
Melvyn Musson, Edward Jones
Charles Rodger, The PNC Financial Services Group, Inc.
Jim Sacks, Fifth Third Bank
Howard Sprow, Securities Industry Association
Chris Terzich, Wells Fargo & Company
Tom Weingarten, Power Management Concepts
John Carlson, BITS
Cheryl Charles, BITS
John Ingold, BITS
Heather Wyson, BITS

About BITS

BITS was created in 1996 to foster the growth and development of electronic financial services and e-commerce for the benefit of financial institutions and their customers. A nonprofit industry consortium that shares membership with The Financial Services Roundtable, BITS seeks to sustain consumer confidence and trust by ensuring the security, privacy and integrity of financial transactions. BITS works as a strategic brain trust to provide intellectual capital and address emerging issues where financial services, technology and commerce intersect, acting quickly to address problems and galvanize the industry. BITS' activities are driven by the CEOs and their appointees—CIOs, CTOs, Vice Chairmen and Executive Vice Presidents—who make up the BITS Advisory Board and BITS Advisory Council. For more information, go to www.bitsinfo.org.

BITS
1001 PENNSYLVANIA AVENUE, NW
SUITE 500 SOUTH
WASHINGTON, DC 20004
202-289-4322
WWW.BITSINFO.ORG

About the Critical Power Coalition

The Critical Power Coalition (CPC) was formed by leading providers, and users, of critical-power products and services. Over the course of the past decade, telecommunications facilities, financial institutions, hospitals, airports, data centers, emergency response centers, manufacturing plants, and other U.S. enterprises and government agencies have invested some \$250 billion in hardware, systems, software, and engineering services to ensure the uninterrupted supply of high-quality power to critical facilities and equipment when grid power fails. The pace of investment is rising as government and the private sector grow increasingly dependent on digital equipment, and as concerns rise about the grid's potential vulnerabilities. CPC is focused on the urgent policy, technology, and regulatory issues that must be addressed to ensure the quality, reliability, and continuity of power where it is needed the most.

CRITICAL POWER COALITION
1615 M STREET NW, SUITE 400
WASHINGTON DC 20036
[HTTP://WWW.CRITICALPOWERCOALITION.ORG](http://WWW.CRITICALPOWERCOALITION.ORG)

About Power Management Concepts

Power Management Concepts (PMC) is an engineering and technology company dedicated to preventing costly downtime for clients operating mission critical facilities. "Mission-Critical" is a broad categorization of ultra-high reliability and availability of electrical and mechanical systems that must meet stringent operating criteria to maintain continuous functionality and eliminate costly unscheduled downtime. PMC provides a fully integrated continuum of services including planning, design, project management, preventive maintenance, mission critical technology solutions and training.

POWER MANAGEMENT CONCEPTS
20 CROSSWAYS PARK NORTH
SUITE 130
WOODBURY, NY 11797
[HTTP://WWW.POWERMANAGE.COM](http://WWW.POWERMANAGE.COM)

A

AC or ac Abbreviation for alternating current.

Alternating current Electrical current which periodically reverses direction, usually several times per second.

Ampere The measurement unit for electrical current.

Automatic transfer switch A switch that automatically transfers electrical loads to alternate or emergency-standby power sources.

B

Black-out A complete loss of power lasting for more than one cycle. A black-out can damage electronics, corrupt or destroy data, or cause a system shutdown. Blackouts can result from any of a number of problems, ranging from natural events (hurricanes or other high winds, ice storms, lightning, trees falling on power lines, floods, geomagnetic storms triggered by sunspots and solar flares, etc.) to situations such as cables being cut during excavation, equipment failures at the utility, vandalism, corrosion, etc. Also known as an outage.

Brown-out A prolonged sag, occurring when incoming power is reduced for an extended period. Usually caused when demand is at its peak and the line becomes overloaded.

C

Capacitor Any AC circuit element possessing the property of capacitance (i.e., the ability to store a charge). Normally a capacitor is a dedicated device, designed for the prime purpose of exhibiting the property of capacitance (as opposed to inductive devices, in which inductance is used by the device to produce other results, such as turning a motor shaft).

Critical load Equipment that must have an uninterrupted power input to prevent damage or loss to a facility or to itself, or to prevent danger of injury to operating personnel.

Current The flow of electricity in a circuit. The term current refers to the quantity, volume or intensity of electrical flow, as opposed to voltage, which refers to the force or "pressure" causing the current flow. Current may be either direct or alternating. Direct current refers to current whose voltage causes it to flow in only one direction. Common direct current sources are batteries. Alternating current refers to current whose voltage causes it to flow first in one direction, then the other, reversing direction periodically, usually several times a second. A common alternating current source is commercial/household power. This current reverses direction 120 times each second, thus passing through 60 complete cycles each second for a frequency of 60 Hertz.

¹⁴ Glossary reproduced courtesy of Liebert Corporation.

D

Direct current Electrical current which flows consistently in one direction.

E

EMI/RFI Electromagnetic/Radio Frequency Interference. These high frequency signals are generally low level (<1V) and range from 1MHz up. EMI/RFI filters are generally not suitable for large amplitude surge suppression.

H

Harmonic distortion A measure of the degree to which the impedance of a UPS affects the shape of the output voltage waveform. Distortion is stated as a percentage and may refer to any single harmonic or to the total waveform, in which case it is referred to as "total harmonic distortion" (THD).

I

Inverter The DC to AC power converter driven by the UPS rectifier-charger or battery via the DC bus. The inverter output drives the critical load.

IEC555 A German standard that requires power factor corrected (PFC) loads.

K

KVA Abbreviation for kilovolt-amperes. (1000 x volt-amperes)

L

Line disturbance analyzer A tool used in analyzing problems in a facility's incoming power. The line disturbance analyzer is connected at the power input to measure and record incoming power, then left in place for long enough to gather data typical of the site.

N

Noise Noise is the result of distortion of the normal line power sine wave by hundreds or thousands of small increases in voltage similar to EMI/RFI, though it encompasses lower frequencies. The amplitude of this type of disturbance is less than a surge but may be as low as EMI/RFI.

Normal line power Commercial electricity supplied by U.S. power utilities is generally delivered as 60 cycle (Hz) alternating current (AC).

O

Overload capacity A UPS's overload capacity is its ability to respond to sudden surges in load current without allowing the output voltage level to decrease.

P

Power conditioning systems A broad class of equipment that includes filters, isolation transformers, and voltage regulators. Generally, these types of equipment offer no protection against power outages.

Power factor corrected (PFC) supply A recently developed type of computer power supply, which exhibits an input power factor equal to one. IEC 555 will force most computers to use a power supply of this type at some point in the future.

Power synthesizer Power synthesizers actually use the incoming utility power as an energy source to create a new sine wave that is free from power disturbances. They can be as much as 99% effective against power disturbances. Types of power synthesizers include magnetic synthesizers (capable of generating a sine wave of the same frequency as the incoming power - 60 Hz), motor generators (which use an electric motor to drive a generator that provides electrical power), and UPSs.

S

Sag A momentary decrease from nominal voltage lasting one or more line cycles. Severe conditions may indicate a need for a UPS or voltage regulator. Also known as a temporary undervoltage (TUV).

Sine wave A periodic oscillation. The fundamental waveform from which other waveforms may be generated by combinations of various group of harmonics. The voltage and current waveforms produced from the power company generators (alternators) are basic sine waves.

Surge A surge is a prolonged over-voltage condition. Surges can damage electronics and corrupt or destroy data.

Spike A spike involves a sudden marked jump in voltage, which can damage electronics and corrupt or destroy data.

Spike/surge protector These products are inexpensive solutions that provide minimal protection against surges, but no protection against sags and outages.

Suppressed voltage ratings Several ranges are assigned by UL for grading transient suppression voltages. For instance, a 400 volt rating indicates a maximum peak voltage between 330 and 400 volts. These ratings appear between 330 volts peak and 6000 volts peak.

Swell An increase from nominal voltage lasting one or more line cycles.

T

Transfer time Transfer time can refer to either the speed with which an off-line UPS transfers from utility power to battery power, or to the speed with which an on-line UPS switches from the

inverter to utility power in the event of an inverter failure. In either case, the time involved must be shorter than the length of time that the computer's switching power supply has enough energy to maintain adequate output voltage. This hold-up time may range from eight to 16 milliseconds, depending on the point in the power supply's recharging cycle that the power outage occurs, and the amount of energy storage capacitance within the power supply. A transfer time of 4ms is most desirable, however, it should be noted that an oversensitive unit may make unnecessary power transfers.

Transient suppression voltage (let-through voltage) The maximum peak voltage occurring within 100 μ s after the test wave.

Transient voltage surge suppressor (TVSS) A device used to reduce voltage surges. Products may be wired in series or in parallel with the AC electrical conductors.

U

UL 1449 United Laboratories, Inc.'s Standards for Safety of Transient Voltage Surge Suppressors (TVSS).

UPS Uninterruptible power supplies (sometimes called uninterruptible power systems). A system designed to protect against short-term power outages.

V

Volt The quantitative unit of measurement of electrical voltage.

Voltage A term referring to the electrical force or potential. A technical synonym for voltage is emf or "electromotive force." Voltage is the parameter of electricity which causes current to flow when a circuit is completed. Voltage is always presented in an energized line, whether or not the circuit is complete (i.e., whether or not current flows).

Voltage regulator A device designed to regulate RMS voltage by removing swells and sags (such as an automatic tap-switching transformer or ferroresonant transformer).

W

Watt The quantitative unit of measurement of actual power. Actual power in an AC circuit is the measurement of the effective energy available for doing work, and is normally less than apparent power (volt-amperes) because of power factor considerations. Watts may be measured directly, by means of a wattmeter, or may be calculated by multiplying volt-amperes by the power factor of the equipment.

This case study highlights key lessons learned from the power outage that affected the Northeast from August 14 through 16, 2003. This case study does not represent the efforts of the other financial services industry associations and/or coordinating bodies. This only reflects the BITS perspective and lessons learned relevant to its crisis management coordination process and its members' experiences.

On August 14, 2003, a cascading blackout struck a large portion of the northeast United States and eastern Ontario. The outages began just after four o'clock Thursday afternoon and affected financial services institutions through the following day. Although most financial operations suffered only brief interruptions and no data loss, the financial services industry can learn from both the sound planning and from the handful of planning oversights revealed by the blackout.

Most institutions, particularly the exchanges and institutions involved in payment, clearing, and settlement, successfully continued operations utilizing backup power and facilities. Some bank branches and many ATMs (especially stand alone machines) were forced to suspend operations until regular power was restored. However, there were no runs on banks or market panics. Most attribute the calm to timely communication from the government assuring the public that the blackout was not caused by terrorism.

The blackout did cause some unanticipated problems. Telecommunications problems stemmed from insufficient backup power at the central office switch and internal telecommunication system levels. Despite communication protocols that generally permitted a successful level of communication in the industry and between the industry and government, it is evident that communication systems and protocols warrant closer scrutiny.

One financial institution experienced an unanticipated problem when its steam provider was unable to continue delivery. Because the financial institution relied on steam to power its electronics cooling system, it was forced to install a boiler for cooling and open late on Friday. Institutions should learn from this instance that continuity plans should encompass more remote potentialities.

In general, the nation's financial services sector withstood the massive power outage with little or no disruption. Verification and notification by Department of Homeland Security (DHS) officials that the power outage was not terrorism-related provided the public with important assurance. Clearly, the nation's power grid and transmission network should be strengthened to prevent power outages of this magnitude. Further research is needed to understand whether software security weaknesses contributed to the outage.

Contingency Planning and Third Party Providers

- Financial institutions relied on business continuity plans to respond to the power outage and related consequences.

¹⁵ Compiled by the BITS Crisis Management Coordination and IT Service Providers Working Groups.

- Data-protection schemes worked almost flawlessly for most large companies affected by the power outage. Recovery planning efforts made by financial institutions since 9/11 enabled them to respond to the crisis effectively.

Recommendations

- Ensure all critical systems are located in facilities with adequate backup power capacity.
- *Evaluate single points of failure, redundancy, and single-provider implications.*
- Evaluate, define and test procedures for operating and restarting equipment during power failures.
- Ensure financial institution patch-management programs include software at contingency sites or vendor-controlled sites.
- Validate emergency building access policy/procedures with third-party building management services.
- Establish and maintain strong relationships with critical partners and suppliers such as power, water, and telecommunications providers.
- Maintain quick-ship/contingency agreements with suppliers.

Communication

- Many member organizations have automated notification systems that provided paging services and 800 numbers for associates to use to receive information.
- Alternate communication devices allowed financial institutions to communicate with employees, third parties, customers and regulators. With limited cell phone service, Blackberries became a primary and important means of communication for many members whose internal communications servers were not disabled.
- Most Government Emergency Telecommunications Services (GETS) Cards worked.
- Some satellite phones did not work in the New York City area because tall buildings and other environmental factors can affect the phones' ability to receive a signal.
- Reported telecommunications problems included inadequate backup power at telecommunications companies and a spike in the volume of calls. (In the hours after the blackout hit, leading wireless carriers reported three to four times the normal volume of calls, a load that virtually guaranteed that many people would hear busy signals and not be able to get through.)
- Many cell tower generators failed due to insufficient fuel to operate and support the increase of wireless communications. Many of the trucks that service these towers depend on commercial power to refuel and encountered roadblocks in their attempts to reach the towers. The National Coordinating Center of the National Communications System coordinated efforts to get the trucks through the roadblocks and helped secure generators for those carriers in need.
- Because so many thousands of servers were effectively "removed" from the Internet so quickly, it caused a sustained surge in BGP (Border Gateway Protocol) traffic to update router tables, effectively blocking other traffic temporarily and slowing the Internet.

Recommendations

- Obtain as many means of communication with key individuals at third-party service providers as possible (including home phones, cell phones, and email addresses).

- Ensure alternative communication channels to communicate with the media, third party providers, customers, and government agencies.
- Develop an improved system for communicating emergency and building evacuation instructions and employee protocols.

Coordination with Federal, State and Local Government

- Government officials provided accurate and timely information, which helped to maintain order. Increased presence by public safety officials helped to alleviate fears and minimize looting and civil unrest.
- Overall communication between government officials and the private sector was successful. Officials from the Federal Reserve, DHS, and Treasury were very responsive to BITS' requests for information and coordinated effectively with the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC).
- All of the major cities affected by the blackout had post-9/11 emergency procedures in place. When electric water pumps shut down in Cleveland, authorities tapped private water trucks the city had arranged to be available in emergencies. Communities in suburban Detroit collaborated to evacuate residents living near a potentially dangerous gasoline plant.

Recommendations

- Establish and maintain strong relationships between the industry and federal, state and local governments.

Transportation, Water and Fuel

- There was widespread disruption to transportation systems, including trains, subways and air travel. Limited and often conflicting or inaccurate information was provided to air travel customers.
- Some companies encountered problems with armored car companies or courier services that would not deliver to locations where power had not been restored. Additionally, some couriers could not gain access to areas due to curfews – or were not able to obtain fuel to complete deliveries.
- Some companies reported a shortage of fuel for generators and difficulty in obtaining additional fuel for their generators.
- In some states, water supplies were affected because water is distributed through electric pumps.
- The inability to pump water and use electronic flushing devices rendered many buildings uninhabitable. High-rise buildings were evacuated due to their inability to run fire pumps.

Recommendations

- Ensure there is adequate food and water at key locations.
- Ensure ATMs in key locations have an alternative power source in the event of a power failure.
- Ensure that critical business units/facilities functions are adequately protected by standby power generation and/or power protection systems.
- Test power generation and/or power protection systems regularly at full capacity for extended periods of time.

APPENDIX D – CAUSE AND EFFECT OF RECENT POWER OUTAGES

LOCATION	RECENT POWER OUTAGES	
	CAUSE	EFFECT
Los Angeles	<ul style="list-style-type: none"> Massive Power Outage – Utility Worker wiring error (9-12-05) 	<ul style="list-style-type: none"> Traffic and public transportation problems and fears of a terrorist attack
Gulf Coast (Florida/New Orleans)	<ul style="list-style-type: none"> 2004/05 Hurricanes: Ivan, Charley, Frances, Katrina, etc. 	<ul style="list-style-type: none"> Millions of customers without power, water, food and shelter, government records lost due to flooding
China	<ul style="list-style-type: none"> 20-million kilowatt power shortage – Equivalent to the typical demand in the entire state of New York (Summer 2005) 	<ul style="list-style-type: none"> Multiple sporadic brownouts Government shutdown least energy efficient consumers
Greece	<ul style="list-style-type: none"> Temperatures near 104°F Mismanagement of electric grid (7-12-04) 	<ul style="list-style-type: none"> Over half of the country left without power
O’Hare Airport	<ul style="list-style-type: none"> Electrical explosion (7-12-04) 	<ul style="list-style-type: none"> Lost power to two terminals Flight delays over course of a day
Logan Airport	<ul style="list-style-type: none"> Electrical substation malfunction (7-5-04) 	<ul style="list-style-type: none"> Flight delays and security screening shutdown for 4 hours
Italy	<ul style="list-style-type: none"> Power line failures Bad Weather (9-29-03) 	<ul style="list-style-type: none"> Nationwide power outage 57 million people effected
London	<ul style="list-style-type: none"> National grid failure (8-29-03) 	<ul style="list-style-type: none"> Over 250,000 commuters stranded
Northeast, Midwest and Canada	<ul style="list-style-type: none"> Human decisions by various organizations, corporate & industry policy deficiencies, inadequate management (8-14-03) 	<ul style="list-style-type: none"> 50 Million People effected due to the 61,800 MW of capacity not being available

APPENDIX E

CONSOLIDATED LIST OF KEY QUESTIONS

Below is a consolidation of the questions that appear in the body of this *Guide*. The questions are the starting point for a rigorous examination of a financial institution’s critical power environment. The answers will help financial institutions achieve the necessary levels of diversity, recoverability, redundancy and resiliency.

The questions are presented in a “worksheet” format providing space so that financial institutions:

- Can indicate whether the question is applicable; and
- Can record comments germane to the question.

	QUESTION	APPLICABLE? (Y/N)	COMMENTS
	QUESTIONS 1 THROUGH 28 APPLY TO POWER UTILITIES – SECTION II OF THE GUIDE		
	General		
1.	Do you have a working and ongoing relationship with your electric power utility?		
2.	Do you know who in your financial institution currently has a relationship with your electric power utility – i.e., facilities management or accounts payable?		
3.	Do you understand your electric power utility’s “Electric Service Priority” (ESP) protocols?		
4.	Do you understand your electric power utility’s restoration plan?		
5.	Are you involved with your electric power utility’s crisis management/disaster recovery tests?		
6.	Have you identified regulatory guidelines or business continuity requirements that necessitate planning with your electric power utility?		

	QUESTION	APPLICABLE? (Y/N)	COMMENTS
	Specifically for an Electric Power Utility		
7.	What is the relationship between the regional source power grid and the local distribution systems?		
8.	What are the redundancies and the related recovery capacity for both the source grid and local distribution networks?		
9.	What is the process of restoration for source grid outages?		
10.	What is the process of restoration for local network distribution outages?		
11.	How many network areas are there in (specify city)?		
12.	What are the inter-relationships between each network segment and the source feeds?		
13.	Does your infrastructure meet basic standard contingency requirements for route grid design?		
14.	What are the recovery time objectives for restoring impacted operations in any given area?		
15.	What are recovery time objectives for restoring impacted operations in any given network?		
16.	What are the restoration priorities to customers – both business and residential?		
17.	What are the criteria for rating in terms of service restoration?		
18.	Where does the financial services industry rank in the priority restoration scheme?		
19.	How do you currently inform clients of a service interruption and the estimated time for restoration?		

	QUESTION	APPLICABLE? (Y/N)	COMMENTS
20.	What are the types of service disruptions, planned or unplanned, that (specify city) could possibly experience?		
21.	Could you provide a list of outages, type of outage and length of disruption that have affected (specify city) during the last 12 months?		
22.	What are the Reliability Indices and who uses them?		
23.	During an outage, would you be willing to pass along information regarding the scope of interruptions to a central industry source, e.g., a financial services industry business continuity command center?		
24.	Are the local and regional power utilities cooperating in terms of providing emergency service? If so, in what way? If not, what are the concerns surrounding the lack of cooperation?		
25.	Would you be willing to provide schematics to select individuals and/or organizations on a non-disclosure basis?		
26.	Could you share your lessons learned from the events of 9/11 and the regional outage of 8/14/03?		
27.	Are you familiar with the “Critical Infrastructure Assurance Guidelines for Municipal Governments” document written by the Washington Military Department Emergency Management Division? Is so, would you describe where (specify city) stands in regard to the guidelines set forth in that document?		
28.	Independent of the utility’s capability to restore power to its customers, can you summarize your internal business continuity plans, including preparedness for natural and manmade disasters (including but not limited to weather-related events, pandemics and terrorism)?		
	QUESTIONS 29 THROUGH 55 APPLY TO NEEDS ANALYSIS/RISK ASSESSMENT – SECTION III OF THE GUIDE		

	QUESTION	APPLICABLE? (Y/N)	COMMENTS
29.	How much does each minute, hour or day of operational downtime cost your company if a specific facility is lost?		
30.	Have you determined your recovery time objectives for each of your business processes?		
31.	Does your financial institution conduct comprehensive business impact analyses (BIA) and risk assessments?		
32.	Have you considered disruption scenarios and the likelihood of disruption affecting information services, technology, personnel, facilities, and service providers in your risk assessments?		
33.	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 failure, power outages, equipment and software failure), and malicious activity (e.g., network security attacks, fraud, terrorism)?		
34.	Does this BIA identify and prioritize business functions and state the maximum allowable downtime for critical business functions?		
35.	Does the BIA estimate data loss and transaction backlog that may result from critical business function downtime?		
36.	Have you prepared a list of “critical facilities” to include any location where a critical operation is performed including all work area environments such as branch backroom operations facilities, headquarters or data centers?		
37.	Have you classified each critical facility using a critical facility ranking/rating system such as the Tier I, II, III, IV rating categories?		
38.	Has a condition assessment been performed on each critical facility?		
39.	Has a facility risk assessment been conducted for each of your key critical facilities?		
40.	Do you know the critical, essential and discretionary loads in each critical facility?		

	QUESTION	APPLICABLE? (Y/N)	COMMENTS
41.	Must you comply with the regulatory requirements and guidelines discussed in this chapter?		
42.	Are any internal corporate risk and compliance policies applicable?		
43.	Have you identified business continuity requirements and expectations?		
44.	Has a gap analysis been performed between the capabilities of each company facility and the corresponding business process recovery time objectives residing in that facility?		
45.	Based on the gap analysis, have you determined the infrastructure needs for your critical facilities?		
46.	Have you considered fault tolerance and maintainability in your facility infrastructure requirements?		
47.	Given your new design requirements, have you applied reliability modeling to optimize a cost effective solution?		
48.	Have you planned for rapid recovery and timely resumption of critical operations following a wide-scale disruption?		
49.	Following the loss of accessibility of staff in at least one major operating location, how will you recover and timely resume critical operations?		
50.	Are you highly confident, through ongoing use or robust testing, that critical internal and external continuity arrangements are effective and compatible?		
51.	Have you identified clearing and settlement activities in support of critical financial markets?		
52.	Do you employ and maintain sufficient geographically dispersed resources to meet recovery and resumption activities?		
53.	Is your organization sure that there is diversity in the labor pool of the		

	QUESTION	APPLICABLE? (Y/N)	COMMENTS
	primary and backup sites, such that a wide-scale event would not simultaneously affect the labor pool of both sites?		
54.	Do you routinely use or test recovery and resumption arrangements?		
55.	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 in private and public sectors by providing common program elements, techniques, and processes?		
	QUESTIONS 56 THROUGH 126 APPLY TO INSTALLATION – SECTION IV OF THE GUIDE		
	Design		
56.	Has the owner, working with an engineering professional, developed a Design Intent Document to clearly identify quantifiable requirements?		
57.	Have you prepared a Basis of Design document that memorializes, in a narrative form, the project intent, future expansion options, types of infrastructure systems to be utilized, applicable codes and standards to be followed, design assumptions, and project team decisions and understandings?		
58.	Will you provide the opportunity to update the Basis of Design to reflect changes made during the construction and commissioning process?		
59.	Are the criteria for testing all systems and outlines of the commissioning process identified and incorporated into the design documents?		
60.	Have you identified a qualified engineering and design firm to conduct a peer project design review?		
61.	Have you considered directly hiring the commissioning agent to		

	QUESTION	APPLICABLE? (Y/N)	COMMENTS
	provide true independence?		
62.	Have you discussed and agreed to a division of responsibilities between the construction manager and the commissioning agent?		
63.	Do you plan to hire the ultimate operating staff ahead of the actual turnover to operations so they will benefit from participation in the design, construction and commissioning of the facility?		
64.	Have you made a decision on the commissioning agent early enough in the process to allow participation and input on commissioning issues and design review by the selected agent?		
65.	Is the proper level of fire protection in place?		
66.	Is the equipment (UPS or generator) being placed in a location prone to flooding or other water damage?		
67.	Do the generator day tanks or underground fuel cells meet local environmental rules?		
68.	Does the battery room have proper ventilation?		
69.	Has adequate cooling or heating been specified for the UPS, switchgear or generator room?		
70.	Are the heating and cooling for the mechanical rooms on the power protection system?		
71.	Have local noise ordinances been reviewed and does all the equipment comply with the ordinances?		
72.	Are the posting and enforcement of no-smoking bans adequate, specifying, for example, no smoking within 100 feet?		
73.	Are water detection devices used to alert building management of flooding issues?		
	Procurement		
74.	Is there a benefit to using an existing vendor or supplier for standardization of process, common spare parts, or confidence in service response?		

	QUESTION	APPLICABLE? (Y/N)	COMMENTS
75.	Have the commissioning, factory, and site testing requirement specifications been included in the bid documentation?		
76.	If the project is bid, have you conducted a technical compliance review which identifies exceptions, alternatives, substitutions, or non-compliance to the specifications?		
77.	Are the procurement team members versed in the technical nuances and terminology of the job?		
78.	If delivery time is critical to the project, have you considered adding late penalty clauses to the installation or equipment contracts?		
79.	Have you included a bonus for early completion of project?		
80.	Have you obtained unit rates for potential change orders?		
81.	Have you obtained a GMP (Guaranteed Maximum Price) from contractors?		
82.	Have you discussed preferential pricing discounts that may be available if your institution or your engineer and contractors have other similar large purchases occurring?		
	Construction		
83.	Do you intend to create and maintain a list of observations and concerns that will serve as a check list during the acceptance process to ensure that these items are not overlooked?		
84.	Will members of the design, construction, commissioning agent, and operations team attend the factory acceptance tests for major components and systems such as UPS, generators, batteries, switchgear and chillers?		
85.	During the construction phase, do you expect to develop and circulate for comment the start up plans, documentation formats and pre-functional checklists that will be used during startup and acceptance testing?		
86.	Since interaction between the construction manager and the		

	QUESTION	APPLICABLE? (Y/N)	COMMENTS
	commissioning agent is key, will you encourage attendance at the weekly construction status meetings by the commissioning team?		
87.	Will an independent commissioning and acceptance meeting be run by the commissioning agent ensuring that everything needed for that process is on target?		
88.	Will you encourage the construction, commissioning, and operations staff to walk the job site regularly to identify access and maintainability issues?		
89.	If the job site is an operating critical site, do you have a risk assessment and change control mechanism in place to ensure reliability?		
90.	Have you established a process to have independent verification that labeling on equipment and power circuits is correct?		
	Commissioning and Acceptance		
91.	Do testing data result sheets identify expected acceptable result ranges?		
92.	Are control sequences, check lists, and procedures written in plain language, not technical jargon that is easily misunderstood?		
93.	Have all instrumentation, test equipment, actuators and sensing devices been checked and calibrated?		
94.	Is system acceptance testing scheduled after balancing of mechanical systems and electrical cable/breaker testing are complete?		
95.	Have you listed the systems and components to be commissioned?		
96.	Has a detailed script sequencing all activities been developed?		
97.	Are all participants aware of their responsibilities and the protocols to be followed?		
98.	Does a Team Directory with all contact information exist and is it available to all involved parties?		
99.	Have you planned an “all hands on deck” meeting to walk through and finalize the Commissioning schedule and Scripted Activities?		
100.	Have the format and content of the final report been determined in		

	QUESTION	APPLICABLE? (Y/N)	COMMENTS
	advance to ensure that all needed data is recorded and activities are scheduled?		
101.	Have you arranged for the future facility operations staff to witness and participate in the commissioning and testing efforts?		
102.	Who is responsible for ensuring that all appropriate safety methods and procedures are deployed during the testing process?		
103.	Is there a process in place that ensures training records are maintained and are updated?		
104.	Who is coordinating training and ensuring that all prescribed training takes place?		
105.	Will you videotape training sessions to capture key points and for use as refresh training?		
106.	Is the training you provide both general systems training as well as specifically targeted to types of infrastructure within the facility?		
107.	Have all vendors performed component level verification and completed pre-functional check lists prior to system level testing?		
108.	Has all system level acceptance testing been completed prior to commencing the full system integration testing and “pull the plug” power failure scenario?		
109.	Is a process developed to capture all changes made and to ensure that these changes are captured on the appropriate built drawings, procedures, and design documents?		
110.	Do you plan to re-perform acceptance testing if a failure or anomalies occur during commissioning and testing?		
111.	Who will maintain the running punch list of incomplete items and track resolution status?		
	Transition to Operations		
112.	Have you established specific Operations Planning meetings to discuss logistics of transferring newly constructed systems to the facility		

	QUESTION	APPLICABLE? (Y/N)	COMMENTS
	operations staff?		
113.	Is all as-built documentation, such as drawings, specifications, and technical manuals, complete and has it been turned over to operations staff?		
114.	Have position descriptions been prepared that clearly define roles and responsibilities of the facility staff?		
115.	Are Standard Operating Procedures (SOP), Emergency Action Procedures (EAP), updated policies, and change control processes in place to govern the newly installed systems?		
116.	Has the facility operations staff been provided with warranty, maintenance, repair, and supplier contact information?		
117.	Have spare parts lists, setpoint schedules after Cx is complete, TAB report and re-commissioning manuals been given to operations staff?		
118.	Are the warranty start and expiration dates identified?		
119.	Have maintenance and repair contracts been executed and put into place for the equipment?		
120.	Have minimum response times for service, distance to travel, and emergency 24/7 spare stock locations been identified?		
	Security Considerations		
121.	Have you addressed physical security concerns?		
122.	Have all infrastructures been evaluated for type of security protection needed (e.g., card control, camera recording, key control)?		
123.	Are the diesel oil tank and oil fill pipe in a secure location?		
124.	If remote dial in or Internet access is provided to any infrastructure system, have you safeguarded against hacking or do you permit read only functionality?		
125.	How frequently do you review and update access permission authorization lists?		
126.	Are critical locations included in security inspection rounds?		

	QUESTION	APPLICABLE? (Y/N)	COMMENTS
	QUESTIONS 127 THROUGH 164 DEAL WITH MAINTENANCE AND TESTING – SECTION V OF THE GUIDE		
	Strategic		
127.	Is there a documented maintenance and testing program based on your business risk assessment model?		
128.	Is an audit process in place to ensure that this maintenance and testing program is being followed rigorously?		
129.	Does the program ensure that maintenance test results are benchmarked and used to update and improve the maintenance program?		
130.	Is there a program in place that ensures periodic evaluation of possible equipment replacement?		
131.	Is there a process in place that ensures the spare parts inventory is updated when new equipment is installed or other changes are made to the facility?		
132.	Have you evaluated the impact of loss of power in your institution and other institutions because of interdependencies?		
133.	Has your facility developed Standard Operating Procedures (SOPs), Emergency Action Procedures (EAPs), and Alarm Response Procedures (ARPs)?		
134.	Are the SOP, EAP, and ARP readily available and current?		
135.	Is your staff familiar with the SOPs, EAPs, and ARPs?		
	Planning		
136.	Does the system design provide redundancy so all critical equipment can be maintained without a shutdown if required?		
137.	Are there adequate work control procedures and is there a change management process to prevent mistakes when work is done on critical systems and equipment?		
138.	Are short circuit and coordination studies up to date?		

	QUESTION	APPLICABLE? (Y/N)	COMMENTS
139.	Do you have a Service Level Agreement (SLA) with your facilities service providers and contractors?		
140.	Is there a change management process that communicates maintenance, testing, and repair activities to both end users and business lines?		
141.	Do you have standard operating procedures to govern routine facilities functions?		
142.	Do you have emergency response and action plans developed for expected failure scenarios?		
143.	Have you prepared an emergency telephone contact list that includes key service providers and suppliers?		
	Safety		
144.	Is there a formal and active program for updating the safety manual?		
145.	Are electrical work procedures included in the safety manual?		
146.	Has an arc-flash study been performed?		
147.	Are specific PPE requirements posted at each panel, switchgear, etc?		
148.	Is there a program in place to ensure studies and PPE requirements are updated when system or utility supply changes are made?		
149.	Are workers trained regarding safety manual procedures?		
150.	Are hazardous areas identified on drawings?		
151.	Are hazardous areas physically identified in the facility?		
	Testing		
152.	Have protective devices been tested or checked to verify performance?		
153.	Is a Site Acceptance Test (SAT) and a Factory Acceptance Test (FAT) performed for major new equipment such as UPS systems and standby generators?		
154.	Is an annual “pull the plug” test performed to simulate a utility outage and ensure that the infrastructure performs as designed?		
155.	Is an annual performance and recertification test conducted on key infrastructure systems?		

	QUESTION	APPLICABLE? (Y/N)	COMMENTS
156.	Is there a process in place that ensures personnel have the proper instrumentation and that it is periodically calibrated?		
	Maintenance		
157.	Does the program identify all critical electrical equipment and components?		
158.	Is there a procedure in place that updates the program based on changes to plant equipment or processes?		
159.	Does a comprehensive plan exist for thermo infrared (IR) heat scan of critical components? Is an IR scanning test conducted before a scheduled shutdown?		
160.	Are adequate spare parts on hand for immediate repair and replacement?		
161.	Is your maintenance and testing program based on accepted industry guidelines such as NFPA 70B and on equipment supply recommendations?		
162.	Do you incorporate Reliability Centered Maintenance (RCM) philosophy in your approach to maintenance and testing?		
163.	When maintenance and testing is performed do you require preparation of and adherence to detailed work statements and method of procedures (MOPs)?		
164.	Do you employ predictive maintenance techniques and programs such as vibration and oil analysis?		
	QUESTIONS 165 THROUGH 225 APPLY TO TRAINING AND DOCUMENTATION – SECTION VI OF THE GUIDE		
	Documentation		
165.	What emergency plans, if any, exist for the facility?		
166.	Where are emergency plans documented (including the relevant internal and external contacts for taking action)?		
167.	How are contacts reached in the event of an emergency?		

	QUESTION	APPLICABLE? (Y/N)	COMMENTS
168.	How are plans audited and changed over time?		
169.	Do you have complete drawings, documentation, and technical specifications of your mission critical infrastructure including: electrical utility, in-facility electrical systems (including power distribution and ATS), gas and steam utility, UPS/battery/generator, HVAC, security, and fire suppression?		
170.	What documentation, if any, exists to describe the layout, design, and equipment used in these systems?		
171.	How many forms does this documentation require?		
172.	How is the documentation stored?		
173.	Who has access to this documentation and how do you control access?		
174.	How many people have access to this documentation?		
175.	How often does the infrastructure change?		
176.	Who is responsible for documenting change?		
177.	How is the information audited?		
178.	Can usage of facility documentation be audited?		
179.	Do you keep a historical record of changes to documentation?		
180.	Is a formal technical training program in place?		
181.	Is there a process in place that ensures personnel have proper instrumentation and that the instrumentation is periodically calibrated?		
182.	Are accidents and near-miss incidents documented?		
183.	Is there a process in place that ensures action will be taken to update procedures following accidents or near-miss events?		
184.	How much space does your physical documentation occupy today?		
185.	How quickly can you access the existing documentation?		
186.	How do you control access to the documentation?		
187.	Can responsibility for changes to documentation be audited and tracked?		

	QUESTION	APPLICABLE? (Y/N)	COMMENTS
188.	If a consultant is used to make changes to documentation, how are consultant deliverables tracked?		
189.	Is your organization able to prove what content was live at any given point in time, in the event such information is required for legal purposes?		
190.	Is your organization able to quickly provide information to legal authorities including emergency response staff (e.g., fire, police)?		
191.	How are designs or other configuration changes to infrastructure approved or disapproved?		
192.	How are these approvals communicated to responsible staff?		
193.	Does workflow documentation exist for answering staff questions about what to do at each stage of documentation development?		
194.	In the case of multiple facilities, how is documentation from one facility transferred or made available to another?		
195.	What kind of reporting on facility infrastructure is required for management?		
196.	What kind of financial reporting is required in terms of facility infrastructure assets?		
197.	How are costs tracked for facility infrastructure assets?		
198.	Is facility infrastructure documentation duplicated in multiple locations for restoration in the event of loss?		
199.	How much time would it take to replace the documentation in the event of loss?		
200.	How do you track space utilization (including cable management) within the facility?		
201.	Do you use any change management methodology (i.e., ITIL) in the day-to-day configuration management of the facility?		
	Staff & Training		
202.	How many operations and maintenance staff do you have within the		

	QUESTION	APPLICABLE? (Y/N)	COMMENTS
	building?		
203.	How many of these staff do you consider to be facilities "subject matter experts?"		
204.	How many staff members manage the operations of the building?		
205.	Are specific staff members responsible for specific portions of the building infrastructure?		
206.	What percentage of your building operations staff turns over annually?		
207.	How long has each of your operations and maintenance staff, on average, been in his or her position?		
208.	What kind of ongoing training, if any, do you provide for your operations and maintenance staff?		
209.	Do training records exist?		
210.	Is there a process in place to ensure that training records are maintained and updated?		
211.	Is there a process in place that identifies an arrangement for training?		
212.	Is there a process in place that ensures the training program is periodically reviewed and identifies changes required?		
213.	Is the training you provide general training, or is it specific to an area of infrastructure within the facility?		
214.	How do you design changes to your facility systems?		
215.	Do you handle documentation management with separate staff, or do you consider it to be the responsibility of the staff making the change?		
	Network and Access		
216.	Do you have a secured network between your facility IT installations?		
217.	Is this network used for communications between your facility management staff?		
218.	Do you have an individual on your IT staff responsible for managing the security infrastructure for your data?		
219.	Do you have an online file repository?		

	QUESTION	APPLICABLE? (Y/N)	COMMENTS
220.	If so, how is use of the repository monitored, logged, and audited?		
221.	How is data retrieved from the repository kept secure once it leaves the repository?		
222.	Is your file repository available through the public Internet?		
223.	Is your facilities documentation cataloged with a standard format to facilitate location of specific information?		
224.	What search capabilities, if any, are available on the documentation storage platform?		
225.	Does your facility documentation reference facility standards (e.g., electrical codes)? If so, how is this information kept up-to-date?		