Liebert®

IT White Paper

REGULATORY COMPLIANCE AND CRITICAL SYSTEM PROTECTION:

The Role of Mission-Critical Power and Cooling in Data Integrity and Availability

EMERSON™
Network Power

Summary

Regulatory compliance has become a legal and necessary extension of business continuity and disaster recovery planning for IT departments as they take steps to ensure their companies do not run afoul of an increasingly complex set of laws and regulations relating to data integrity and availability. Business continuity and systems security are also being driven by the Department of Homeland Security for both government and commercial operations. New laws and regulations not only mandate effective integrity, availability, and accountability of systems and processes relating to data, they set severe civil – and in some cases, criminal – penalties for failure.

The good news is that high availability and continuous availability protection strategies will help you meet these regulatory requirements . . .

This white paper is designed to help identify the regulatory compliance issues that impact business continuity planning and increase the understanding of how mission-critical power, cooling, and monitoring strategies support business continuity. It is intended primarily for:

- IT professionals, CIOs, Business Continuity Managers, Disaster Recovery Managers, Emergency Preparedness and Response Managers, Data Center Managers, Audit Managers, and Facilities Managers.
- CEOs, CFOs and Boards of Directors in these same organizations, including Audit Committee members.
- Outsourcers of data services affected by various regulations.

When it comes to ensuring the integrity and availability of data systems, there is both bad news and good news about regulatory compliance. The bad news is that the regulations do not provide a "blueprint" for protection— just the penalties if you fail to protect your critical data. The good news is that high availability and continuous availability protection strategies will help you meet these regulatory requirements, eliminating the risk that under-protected systems will create breaks in the "chain of data integrity" caused by power outages and other anomalies. It is important to note that compliance is a moving target; both government and industry leaders will continue to move toward more specific regulations and standards.

This paper was developed by Liebert Corporation with assistance from Network Frontiers, whose principals Dorian Cougias and Lynn Heiberger are experts in the realm of business continuity planning and regulatory compliance relating to IT. They are authors of a leading book on business continuity, The Backup Book, and will soon be releasing The Compliance Book.

Introduction

In the past few years, regulatory compliance has become a larger concern for IT departments as they have taken steps to ensure their companies do not run afoul of an increasingly complex set of laws and regulations relating to data integrity and availability.

The issue became more acute in 2002 when the Sarbanes-Oxley Act— described as the most significant change to securities law in 70 years— went into effect. Sarbanes-Oxley sent a chill through corporate boardrooms and triggered sweeping reviews of organizational policies and procedures. This review is ongoing, with increasing attention being paid to data standards and IT processes.

A key part of that review process is how vital corporate data is stored, managed and protected. The major requirements of data protection are ensuring its integrity, availability, accountability and confidentiality. From a power protection standpoint, confidentiality is less important, but availability, integrity and accountability have the following implications:

- Critical data is not lost or corrupted
- A "chain of integrity" exists that can show data was not tampered with or subject to unauthorized disclosure
- Data can be made available under conditions mandated by law or regulation
- Systems and management processes ensure that actions relating to data and systems availability, integrity and confidentiality can be traced to a person or system

No law or regulation goes so far as to set a specific process or architecture for data protection, including power protection. But the laws do describe expected outcomes and the penalties for failure to meet them, and the regulations that accompany each law are broad and sweeping.

The regulations often refer to existing standards for more specific compliance expectations. For the astute IT professional, this means being especially aware of standards on data integrity and availability.

This white paper identifies the laws, regulations and standards that specifically impact power and cooling strategies for mission-critical data systems. It is meant to help you understand the impact of regulations as they affect power protection and cooling programs.

The major requirements of data protection are ensuring its integrity, availability, accountability and confidentiality.

Defining Terms:

Availability: Systems and their data are protected against either accidental or intentional attempts to perform unauthorized deletion, cause denial of service, or use the systems or data for unauthorized purposes.

Integrity: Systems remain operable through organizational life-cycle management and data integrity is not impaired.

Accountability: The actions of anyone (or any system) can be uniquely traced to that person or system at the individual level.

Confidentiality: Data is protected while it is in storage, being processed, and in transit.

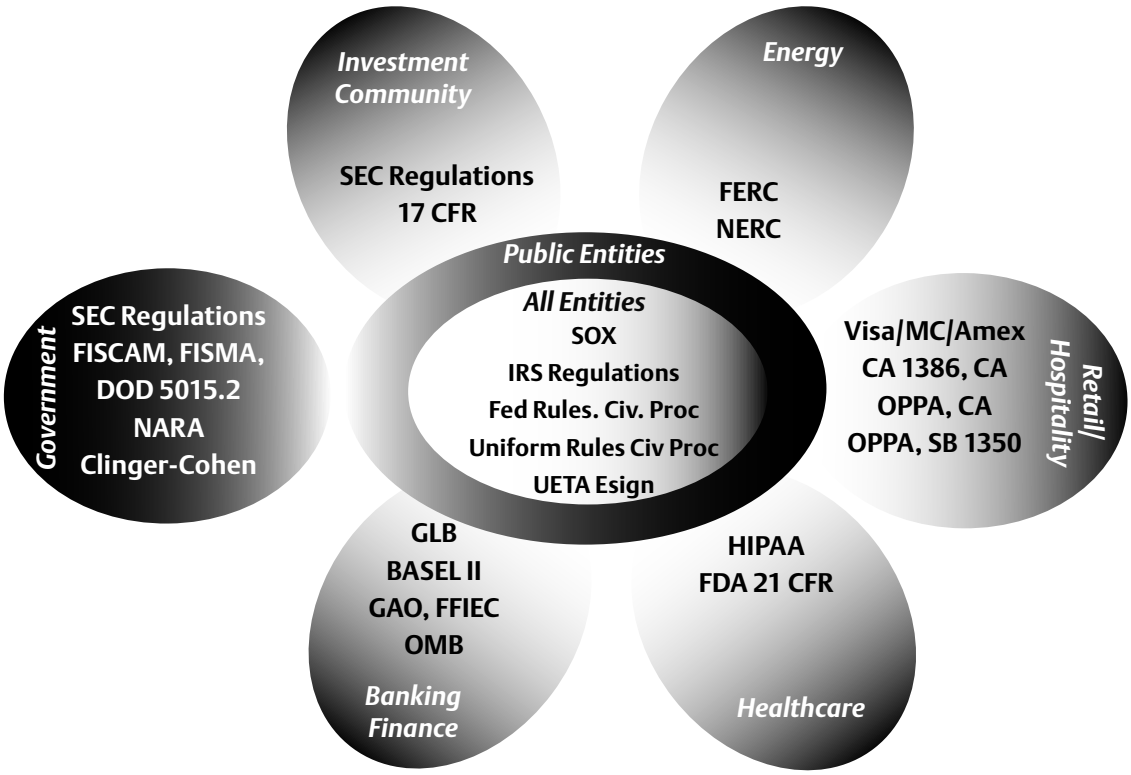

Figure 1. Many companies are now subject to multiple, overlapping regulations.

The Regulatory Framework for Power and Cooling of Mission-Critical Networks

There are various laws, regulations, and international conventions that impact the protection of mission-critical networks. These laws and regulations are listed here and described in more detail in Appendix A.

- HIPAA: The Health Insurance Portability and Accountability Act of 1996 states that whenever patient data is recorded, stored, or transmitted there must be a record of the change and an associated permission linked to a document that has been signed by the patient. From the standpoint of data and system availability, considerable attention is being paid to "life-safety" data. Organizations that collect or maintain life-safety data need continuous availability to be HIPAA compliant.
- FDA 21 CFR, Part 11: These U.S. Food and Drug Administration regulations outline criteria for accepting electronic records and electronic signatures as equivalent to paper-based records and handwritten signatures, and for documenting and validating authorized change processes to systems and software involved in the creation of electronic documents.
- SEC 17 CFR 240: This portion of Securities and Exchange Commission regulations deals with controls and procedures over electronic securities transactions.

- Sarbanes-Oxley
  The Sarbanes-Oxley Act addresses security and controls of accounting and auditing processes, as well as all of their supporting IT processes for publicly traded companies. Sarbanes-Oxley is also driving compliance for private companies that may elect to go public, and for very large private organizations whose activities draw public scrutiny. Over time, Sarbanes-Oxley may become the de-facto standard for all companies that grow beyond the definition of small business.

- Basel II: The Basel Capital Accord, introduced by the Bank for International Settlements (BIS), applies primarily to the largest banks in the U.S. It isolates measurement structures and introduces new direction for managing capital risk, supervisory interaction, and public risk disclosure.

- Gramm-Leach-Bliley
  Gramm-Leach-Bliley focuses on requirements for maintaining the privacy of customer data in the banking arena. In addition, financial firms must assure— on an annual basis— that all of their subcontractors and vendors have appropriate processes in place to maintain the security of this data.

- Clinger-Cohen Act of 1996: The Clinger-Cohen Act, also known as the Information Management Reform Act, regulates firms providing IT products and services to the U.S. Government, but may be of interest to any firm in the supply chain of a government supplier.

- FISMA: The Federal Information Security Management Act of 2002 focuses on information security and appoints the National Institute of Standards and Technology (NIST) through the NIST Act (15 U.S.C. 278g-3) to develop technical, management, physical, and administrative standards and guidelines for the cost-effective security of sensitive information. The Federal Information Processing Standard Publication 199 (FIPS PUB 199) supports FISMA and states that information security requires that integrity, confidentiality, and availability are maintained.

- Visa CISP
  Visa Cardholder Information Security Program* defines a standard of due care for securing Visa cardholder data, wherever it is located. CISP compliance is required of all entities storing, processing, or transmitting Visa cardholder data. Auditors address power system issues such as firewall continuity plans, managed-device passwords, and implementation of key controls, including UPS and battery shutdown tests.

- MasterCard SDP
  The MasterCard Site Data Protection program calls for members to implement and maintain data security compliance programs for themselves and their electronic commerce merchants and Member Service Providers. A series of manuals** provide security requirements and best practices.

Over time, Sarbanes-Oxley may become the de-facto standard for all companies that grow beyond the definition of small business.

* (2004). Cardholder Information Security Program. VISA.
** (2003). Electronic Commerce Security Architecture Best Practices. MasterCard, (2003). MasterCard Security Standard Applicable to Merchants and Member Service Providers. MasterCard, (2003). MasterCard Security

In general, all standards call for emergency mode operations plans, such as business continuity plans and disaster recovery plans.

Supporting Standards

The laws and regulations described above refer to standards, assessment processes, and risk management tools being published by industry groups. There are four standards bodies referred to by these laws or regulations, which have specific guidance relative to power protection. These standards are listed here and described in more detail in Appendix B.

* COSO: Committee of Sponsoring Organizations of the Treadway Commission. COSO calls for data center operations controls and transaction management controls in order to ensure both availability and integrity within its control activities section.

- ISO 17799: The information security standard of the International Standards Organization (ISO). ISO 17799 calls for power supplies to be applied correctly under the heading of its Equipment and Security section. ISO 17799 also has an entire section entitled Business Continuity Management wherein testing, maintaining, and reassessing the plan are called for directly.

- ISACA CobiT: The Information Security & Audit Control Association's Control Objectives for Information Technology. CobiT details uninterruptible power supply needs in section 12.6 under Manage Facilities. CobiTs Continuity Framework, section 4.0, deals specifically with the creation, testing, and monitoring of a continuity and contingency plan.

- FIPS Pub 199: The documents supporting FISMA are the Federal Information Processing Standard Publication 199 (FIPS PUB 199) Standards for Security Categorization of Federal Information and Information Systems and the NIST 800 series on security most especially 800-14, Risk Management Guide for Information Technology Systems.

  As stated in Section 3542 of FISMA, information security ensures that integrity, confidentiality, and availability are maintained. The FIPS Publication 199 assigns this level of criticality and sensitivity to data based on the potential impact on agency operations (mission, functions, image, or reputation), agency assets, or individuals should there be a breach in security due to the loss of confidentiality, integrity, or availability. In short, FIPS Publication 199 draws out the specific implications of the regulation so that NIST can offer standards of best practices.

- NIST Special Publication 800-14: The Generally Accepted Principles and Practices for Securing Information Technology Systems of the U.S. National Institute of Standards & Technology. NIST 800-14 calls for uninterruptible power supplies under its Failure of Supporting Utilities section within Physical & Environmental Security. NIST 800-14's section on Preparedness for Contingencies and Disasters covers the identification and development of various contingency and continuity plans and procedures.

Regulation	Relevant Requirements	Power Implications
HIPAA	Where patient data is recorded, stored or transmitted there must be a record of the change and an associated permission linked to a document that has been signed by the patient	Power interruptions or disturbances can break the chain of integrity. Life safety data must be continuously available
FDA 21 Part CFR 11	Outlines criteria for accepting electronic records and signatures and for documenting and validating authorized change processes to systems and software involved in the creation of electronic documents	Requires formal risk evaluation and compliance with "current good practices." Secondary power for manufacturing considered good current practice
SEC 17 CFR 240	Establishes controls and procedures for electronic securities transactions	Power failures or disturbances can result in an organization being unable to verify the existence or accuracy of transaction histories
Sarbanes-Oxley	Guidelines for corporate governance and oversight of accounting and audit practices as well as financial record retention	Power interruptions or disturbances can break chain of integrity of data
Basel II	Provides direction for managing capital risk, supervisory interaction, and public risk disclosure for large banks	Power systems must provide protection across far flung enterprises
Gramm-Leach-Bliley	Assure privacy of customer data for financial institutions	Breaches of data security will result in regulatory scrutiny
Clinger-Cohen Act	Regulates firms providing IT products and services to the U.S. government	Requirements may emerge regarding data availability and security
FISMA	Federal Information Security Act: Focuses on what should be secured and who should secure it	Supporting standards reinforce connection between security and data integrity and availability
VISA CISP	CISP defines a standard for securing Visa cardholder data for all entities storing, processing, or transmitting that data	Requires effective management of network devices, including power protection systems, and continuity planning for security systems
MasterCard SDP	Ensures that online merchants and Member Service Providers are adequately protected against hacker intrusions and account data compromises	Requires effective management of network devices, including power protection systems, and continuity planning for security systems

Summary of regulatory and legal requirements with implications for the power system.

In large measure, regulatory compliance involves power and security issues.

In addition to these standards, the U.S. government has created the Federal Financial Institute Examination Council (FFIEC) and Federal Information Systems Audit Control Manual.

- FFIEC
  FFIEC is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the National Credit Union Administration, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision. The FFIEC Information Security Examination Handbook is derived from NIST's underlying models for IT ensuring data availability, integrity, confidentiality , accountability and assurance. The FFIEC also provides a complete Audit booklet that covers internal, and third party, auditing.

- FISCAM
  The General Accounting Office issued the Federal Information Systems Audit Controls Manual (FISCAM), which provides guidance for evaluating internal controls over the integrity, confidentiality, and availability of data maintained in financial information systems. The manual outlines steps that auditors should follow to review general and application controls for computer systems. This document has been the basis for the system security review co-performed by USAAA and GAO since its release.

Complying with Standards and Regulations

No current regulations spell out, in legal terms, the need for secondary power or uninterruptible power. But neither do they call for any specific IT controls such as password management, backups, or security logging that are typically implemented by companies.

Instead, the regulations focus specifically on the need for the fundamentals of availability, integrity, confidentiality, and accountability in the realms of physical, technical and operational security. For example, following is one of the most detailed standards for power availability, from ISACA CobiT:

> **12.6 Uninterruptible Power Supply**
> Management should assess regularly the need for uninterruptible power supply batteries and generators for critical information technology applications to secure against power failures and fluctuations. When justified, the most appropriate equipment should be installed.

The term "most appropriate equipment" leaves room for judgment— and error.

Therefore, it is imperative to understand the frameworks recommended by HIPAA, SOX, GLB, Basel II, as well as most others. These frameworks suggest a standardized IT operating structure for ensuring that control objectives are defined, implemented, managed, and monitored within the organization.

These frameworks establish the IT guidelines for best practices and here is where the need for power management is spelled out in great detail. In general, all standards call for emergency mode operations plans, such as business continuity and disaster recovery plans.

Assessing Your Critical System Protection Strategy

Good compliance starts with high availability or continuous availability protection systems, along with good processes and complete documentation. You can have bulletproof protection and still fall short of compliance, if you do not have compliant policies, procedures and practices. Moreover, you may still run afoul of regulations if you have good processes in place but they are not documented and reported.

And you are not off the hook, yet. You will need to review current protection against any recent changes in your data system architecture to ensure your network has not outgrown its protection.

Regulatory compliance requires a good-sense approach to business continuity and high availability. Most organizations already know which systems are mission-critical and must be protected from downtime to ensure that critical business functions are available. The challenge to IT departments is to layer compliance issues over those and determine whether current protection is adequate. In terms of compliance, consider these three broad levels of protection:

1. If you are not impacted by regulation, you may not be required to address system or data availability. Any requirements would be governed by your own business imperatives.
2. If regulations require you to maintain data integrity, you must ensure your systems can be shut down and restarted safely.
3. If regulations require you to maintain data availability, then your standard should be at least high availability (99.999 percent or better), if not continuous availability.

In large measure, regulatory compliance involves power and security issues. If high or continuous availability is necessary, physical security and environmental protection are also necessary.

Following are some considerations for determining the adequacy of your power and cooling protection:

Ten Questions to Ask

1. **If you rely on backup generators, is your generator sized adequately to power the cooling system and critical computer systems?**

   It may seem basic, but ensure that not only your critical computer systems, but your cooling systems, are supported by back-up generators. With the densities of today's computer systems, computer rooms can heat up fast if computers continue to operate on backup power without precision cooling. Also, be sure your automatic transfer switch is configured so that the lag time between switching from generator back to utility is short enough not to disrupt UPS power to your computer systems.

2. **Is mission-critical network equipment— whether in the data center or at remote locations— being protected by line-interactive UPS systems?**

   If so, your network may be at risk. Liebert recommends against using line-interactive UPS systems for mission-critical applications. Line-interactive UPS units are only 85 percent effective against power anomalies in general and have little protection against surges, harmonics and frequency variations. In high-speed networks, some Liebert customers have found that in going to battery, line-interactive UPS systems drop loads, resulting in data losses. Use of double-conversion on-line UPS systems ensures continual power conditioning and maximum protection against even daily power anomalies.

3. **Are you relying on UPS batteries to ride through daily power fluctuations?**

   If you are using line-interactive UPS units, these units go to battery every time a power anomaly occurs, which wears down the batteries more quickly than the batteries of double-conversion UPS systems. Perform a cost-benefit analysis, including battery replacement costs, for switching to double-conversion online UPS systems, which do not go to battery as often.

4. **Are your UPS batteries fully charged and do you have a testing and replenishment plan in place?**

   It sounds elementary, but many IT managers do not know the status of their UPS batteries. Be sure to implement a policy of regular battery inspections, and have a replacement program that makes replacement manageable.

5. Have you performed an analysis of your power protection strategy to ensure that you are not sacrificing reliability as you build out your network?

Building redundancy into the power system is a proven strategy for increasing power system reliability and, consequently, network availability. Redundancy enables maintenance of a UPS module without affecting power to connected equipment and also increases fault tolerance.

Redundancy is typically achieved though either an N + 1 or a 1 + 1 design. In an N + 1 design, also known as a parallel-redundant system, multiple UPS modules are sized so that there are enough modules to power connected equipment (N), plus one additional module for redundancy (+ 1). During normal operation, the load is shared equally across all modules. If a single module fails or must be taken offline for service, the system can continue to power connected systems.

In a 1 + 1 design, two UPS modules are sized so that either module is capable of carrying the entire load. While 1 + 1 systems deliver a significant improvement in availability over N + 1 systems and are regularly specified for the most critical applications, N + 1 remains a viable and popular option for applications seeking to balance cost, reliability and scalability. However, a statistical analysis of the projected reliability for multi-module systems reveals the point at which the risks of power system scalability to network availability clearly outweigh the benefits.

Downtime attributed to additional modules remains fairly flat — and acceptable for many applications — up to the 3 + 1 level. At 4 + 1 and beyond, power system availability begins to drop dramatically and downtime increases substantially for each module added.

For instance, if UPS reliability is .9995, a 13 + 1 architecture will be down about 90 times as often as a 1 + 1 system. This is particularly problematic because modules are added to an N + 1 system as the load increases. Typically, a load increase correlates with an increase in network criticality. So, a “scalable” N + 1 architecture is actually responding to an increase in network criticality by reducing system availability.

6. **Are you monitoring for heat and humidity in critical computer areas, including small rooms and server closets?**

   Temperature increases of 10 degrees above 75 degrees F reduce the lifespan of network equipment by 50 percent, and heat is the biggest threat to UPS battery life. Yet, heat density is becoming a bigger issue, as more and denser equipment is packed into small spaces. Without temperature and humidity monitoring these spaces are at risk of overheating and the downtime that may result. Small-space precision cooling solutions can help you overcome these risks.

7. **Is there sufficient circulation of air to cool the computer systems area and the UPS system room, especially if you are using blade servers or other high-density equipment?**

   The use of blade servers has increased heat densities in data centers and computer rooms. When heat densities approach 100 watts per square foot, it's time to consider spot cooling systems to resolve hot spots. Also, ensure that you have proper air circulation and configurations to help resolve these increased densities. The rule of thumb for cooling computer equipment is one air change per minute. Do not allow hot air from computer systems to be forced back onto the computer systems or the device can ultimately be damaged. Racks should be configured in a hot aisle / cold aisle arrangement to ensure that cold supply air is directed to the cold aisle through perforated tile or an overhead system.

8. **Do you have dual UPS units for all network equipment that has dual power supplies?**

   Network equipment manufacturers specify that their dual power supplies are for dual UPS units to ensure redundancy. Some equipment requires that both power supplies be used for the equipment to operate, and some equipment has three power supplies and requires two for operating.

   There are several ways to protect this equipment. You may want to use a different UPS for each power supply and provide separate circuits for each UPS. You may also want to run communications software between dual UPS units supporting a single load to ensure that if one UPS goes down, the other UPS will continue to support the load and not initiate a graceful shutdown if not desired.

Ten Questions to Ask

9. Can you keep mission-critical loads online while doing UPS maintenance?

Even in applications where UPS redundancy is not feasible, solutions are available that allow mission-critical systems to continue to operate during UPS maintenance. A maintenance bypass switch provides the capability to switch mission-critical loads to utility power during UPS maintenance.

10. Is your UPS monitoring application set to notify you when the load has exceeded 80 percent of the UPS system's maximum capacity?

Many IT professionals prefer to set alarms to trigger when loads reach less than 80 percent of capacity. Above this threshold, the UPS system may be forced to go to unplanned bypass. To avoid this, reallocate power or add power equipment as necessary instead of resorting to an unplanned transfer to bypass.

There are other considerations in determining the right protection strategy for your network. Thanks to Liebert's nationwide network of skilled, experienced protection specialists, you have local access to the information and application capabilities needed to develop and implement your own roadmap for protecting data and applications. Every organization is different, so solutions that work for one company may not be the right approach for another.

Your local Liebert Representative can help you evaluate your protection strategy and make appropriate recommendations for ensuring high availability. For more information on Liebert solutions, call 800-877-9222.

Appendix A
Laws, Regulations and International Conventions

Following is more detailed information on the laws, regulations, and international conventions that impact the protection of mission-critical networks. See Appendix C for links to the actual laws and regulations.

HIPAA

HIPAA (Health Insurance Portability and Accountability Act of 1996) is a broad set of regulations for managing patient information within the healthcare industry. It states that whenever patient data is recorded, stored, or transmitted there must be a record of the change and an associated permission linked to a document that has been signed by the patient.

Power Protection Implications. If the data and the linked permission are lost or become corrupted because of a power outage or other anomaly, the "chain of integrity" for the data has been broken and the company is in violation of HIPAA.

From the standpoint of data and system availability, considerable attention is being paid to what the healthcare industry is calling "life-safety" data. This is critical patient information that must be available at all times, e.g. lab test data that doctors rely upon for the diagnosis and survival of their patients. Organizations that collect or maintain life-safety data need continuous availability to be HIPAA compliant.

21 CFR, Part 11

The U.S. Food and Drug Administration (FDA) has issued a set of regulations, collectively called 21 CFR 11. These regulations outline criteria for accepting electronic records and electronic signatures as equivalent to paper-based records and handwritten signatures. The 21 CFR11 also provides guidelines for documenting and validating authorized change processes to systems and software involved in the creation of electronic documents.

These regulations, which apply to all FDA program areas, are intended to permit the widest possible use of electronic technology, compatible with the FDA's responsibility to promote and protect public health. Because of this, the FDA includes Part 11 in its formal review of current good practice (cGxP) regulations which include the good clinical practice (GCP), good laboratory practice (GLP) and good manufacturing practice (GMP).

Power Protection Implications. Because Part 11 is predicated on the GxPs, the FDA expects each firm that is subject to GxP regulations to develop a risk evaluation of its products and manufacturing processes and then to mitigate the identified risks. Clearly, having secondary power for critical manufacturing facilities falls within the GxP and therefore Part 11 regulations.

SEC 17 CFR 240

This portion of Securities and Exchange Commission regulations deals with controls and procedures over electronic securities transactions. It mandates— among other things— that "underlying control systems" such as secondary power systems be implemented as necessary to maintain the continuity of the system. In the area of broker-dealer records retention, CFR 240 also requires that transaction recording systems have quality control processes that verify the accuracy of the recording.

Power Protection Implications. Unexpected power failures or other anomalies that lead to a corruption or loss of data may result in an organization not being able to verify the existence or accuracy of their transaction histories.

Sarbanes-Oxley

Signed into law in 2002, the Sarbanes-Oxley Act was designed to protect investors by improving the accuracy and reliability of disclosures by publicly traded corporations. This act addresses security and controls of accounting and auditing processes, as well as all of their supporting IT processes. The act provides strict guidelines for corporate governance and oversight of accounting and audit practices as well as financial record retention. Sections 302 and 404 of this act require companies to disclose their internal financial reporting controls as well as an assessment of how well those controls are working. In fact, the wording in Section 404 is the same as portions of SEC 17 CFR 240 (see previous), as SEC 17 CFR 240 is a derivative work of Sarbanes-Oxley.

Sarbanes-Oxley is also driving compliance for private companies that may elect to go public, and for very large private organizations whose activities draw public scrutiny. Over time, Sarbanes-Oxley may become the de-facto standard for all companies that grow beyond the definition of small business.

Power Protection Implications. Policies and practices for ensuring data integrity and confidentiality in handling complaints create risk for under-protected systems for the same reasons of security law: the potential for breaking the "chain of integrity" of vital data.

Basel II

The Basel Capital Accord, introduced in 1988 by the Bank for International Settlements (BIS) and updated in Basil II, applies primarily to the largest banks in the U.S. It is structured around three components called Pillars that isolate measurement structures and introduce new direction for managing capital risk, supervisory interaction, and public risk disclosure.

Power Protection Implications. Basel II impacts IT precisely because of the organization-wide need for banks to amass and process a historical-loss data. This data must be

built into and integrated with the banks' global processes and therefore is reliant upon technologies and processes in the many localities where these banks operate. As a result, power protection strategies must be implemented in ways that ensure data availability across far-flung financial organizations.

Gramm-Leach-Bliley

Signed into law in 1999, Gramm-Leach-Bliley focuses on requirements for maintaining the privacy of customer data in the banking arena. In addition, financial firms must assure – on an annual basis— that all their subcontractors and vendors have appropriate processes in place to maintain the security of this data.

Power Protection Implications: Any emergency-mode or disaster recovery operation that compromises security could bring regulatory scrutiny to the data protection systems.

Clinger-Cohen Act of 1996

The Clinger-Cohen Act, also known as the Information Management Reform Act, specifically regulates firms providing IT products and services to the U.S. Government, but may be of interest to any firm in the supply chain of a government supplier. Passage of this act is causing a major paradigm shift in the process for acquiring and managing information technology within the federal government.

Power Protection Implications: As currently constructed, it has no immediate impact on power protection strategies. However, regulatory experts expect requirements for availability, integrity, or confidential to emerge, and therefore this regulation bears watching.

Appendix B
Industry Standards

Laws and regulations mandating the integrity and availability of data and applications often refer to key industry standards that address power protection. Information on these standards follows. See Appendix C for links to the actual standards:

COSO

COSO (Committee of Sponsoring Organizations of the Treadway Commission) released the Enterprise Risk Management (ERM) Framework providing information on enterprise risk management for all organizations. The Framework also identifies the inter-relationships between enterprise risk management and internal control. Internal control is broadly defined as a process, driven by an entity's board of directors, management and their personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- Effectiveness and efficiency of operations.
- Reliability of financial reporting.
- Compliance with applicable laws and regulations.

COSO's internal control framework deals with the needs and expectations of management and others. It defines and describes internal control to:

- Establish a common definition serving the needs of different parties.
- Provide a standard against which business and other entities— large or small, in the public or private sector, for profit or not— can assess their control systems and determine how to improve them.

COSO is referred to in regulations that govern public companies and the investment, healthcare and finance industries.

ISO 17799

The International Standards Organization (ISO) adapted British Standard 7799 as a basis for establishing its information security standard 17799. ISO 17799 is an extremely comprehensive and detailed standard. Compliance with this standard, therefore, will require both a methodical and measured approach. It will also require commitment, as well as appropriate policies, procedures, and managerial follow-through. At the highest level are ten topic areas:

- Security Policy
- Organizational Security
- Asset Classification & Control

- Personnel Security
- Physical & Environmental Security
- Communications & Operations Management
- Access Control
- Systems Development & Maintenance
- Business Continuity Management
- Compliance

ISO 17799 is referred to more than any other standard. It is a guiding standard for all industries that have regulated data.

ISACA CobiT

The Information Security & Audit Control Association's (ISACA) Control Objectives for Information Technology (CobiT) was among the earliest efforts to establish guidance for auditors to use in addressing information security. CobiT includes four domains:

* Planning & Organization
* Acquisition & Implementation
* Delivery & Support
* Monitoring

Each domain contains multiple processes, and each process can contain multiple control objectives.

Regulations that govern data of the energy, retail, and finance industries reference CobiT. The CobiT handbook is recognized by the US Treasury Department, FDIC, Federal Reserve Bank and the World Bank.

NIST Special Publication 800-14

The US National Institute of Standards & Technology (NIST) has issued the Generally Accepted Principles and Practices for Securing Information Technology Systems, one of the most comprehensive of the NIST SP 800 series. It includes 14 "Common IT Security Practices," four of which are directly impacted by data protection systems: Preparing for Contingencies & Disasters, Physical & Environmental Security, Identification & Authentication, and Audit Trails.

Like ISO 17799, the NIST 800 Series is referenced by all regulations for data handling and management.

Appendix C

Links to additional information on products and services from Liebert:

www.liebert.com

Links to additional information on laws and regulations relating to IT's role in ensuring data integrity and availability:

www.netfrontiers.com

Links to additional information on laws and regulations:

Health Insurance Portability and Accountability Act (HIPAA): http://aspe.hhs.gov/admnsimp/index.shtml

Clinger-Cohen Act: http://wwwoirm.nih.gov/policy/itmra.html

Graham-Leach-Bliley Act (GLBA): http://www.senate.gov/~banking/conf/confrpt.htm

Sarbanes-Oxley Act: http://www.law.uc.edu/CCL/SOact/soact.pdf

Basel II: http://www.bis.org/bcbs/index.htm

US FDA 21 CFR, Part 11 http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm

Links to additional information on standards:

COSO (Committee of Sponsoring Organizations): http://www.coso.org/publications/executive_summary_integrated_framework.htm

ISO 17799: http://www.17799.com/

ISACA CobiT (The Information Security & Audit Control Association's Control Objectives for Information Technology): www.isaca.org/cobit.htm

NIST Special Publication 800-14 (US National Institute of Standards & Technology): http://www.hipaadvisory.com/regs/finalsecurity/nist/800-14.pdf

LIEBERT CORPORATION

1050 DEARBORN DRIVE

P.O. BOX 29186

COLUMBUS, OHIO 43229

800.877.9222 (U.S. & CANADA ONLY)

614.888.0246 (OUTSIDE U.S.)

FAX: 614.841.6022

www.liebert.com

Printed in U.S.A. 0405