



Ensuring Your Data Center is in Compliance

By **TODD BERMONT**

With Sarbanes-Oxley, SAS70, HIPAA and scores of other government and industry regulations, data center and facility managers are under more scrutiny than ever before. While these regulations always start out as well meaning, invariably they end up putting onerous responsibilities on targeted organizations.

As most of us now know, data centers have become the true heartbeat of most businesses and public sector agencies. Imagine a day without e-mail or a phone call. Imagine a day without clients, members and users being able to access your Web site for information or purchases. In some industries such as financial services and manufacturing, the cost of downtime can be measured in millions of dollars per minute.

Given the importance of data centers, it is no surprise that regulators and auditors are giving a tremendous amount of focus to this area. Ensuring compliance to regulations can be a Herculean effort. However, there are three areas that you can focus on to ease the burden of compliance: procedures, documentation and ongoing risk mitigation.

Typically, the goal of most government regulations centers on the tightening of internal controls, increasing the accuracy of reporting, and fully disclosing outstanding risks. By focusing on procedures, documentation and ongoing risk mitigation data center and facility managers can ease the burden of compliance. Let's take a look at these in more detail.

Procedures

Most any repetitive or mission-critical task in a data center should have a fully tested and documented procedure. According to many studies, human error is the No. 1 cause of havoc in the data center. There are many ways to reduce the potential of human error. One of those is through training. Another is by ensuring compliance with all safety codes and regulations. However, the single most important measure that can be taken to reduce human error is to maintain and enforce procedures.

The most common procedures found in data centers are methods of procedures (MOP) for maintaining the equipment and standard operating procedures (SOP) for operating equipment. Many firms make the

mistake of either not having these procedures in place or not keeping them up to date.

During a recent conversation with a CIO of a major Midwestern manufacturer, he mentioned that their data center experienced a 36-hour outage because the technician who was working on the HVAC system inadvertently pressed the emergency power off button and brought down the entire data center. It took a full 36 hours to bring everything back online all because someone did something that could easily have been prevented with a proper MOP on maintaining that particular piece of equipment.

Outages like this are not only a major inconvenience, they can actually impact profitability and earnings per share.

Consequently, it is imperative for every major task and component in a data center to have a fully documented and tested procedure. These procedures should be tested at a minimum of once per year because facility composition, personnel, and equipment change. You want to test for accuracy and results.

If you don't have the bandwidth to create and/or test procedures in your facility, there are several third-party providers that can assist. The bottom line is procedures help ensure that rigid internal controls are being followed and can mitigate the potential risk of human error impacting mission-critical operations.

Documentation

The second critical area of compliance is in documentation. We discussed the importance of documenting procedures. However, there are several other areas that need to be fully documented and up-to-date.

Maintenance Records

Anyone who has ever had maintenance performed on anything, such as an automobile or an uninterruptible power supply, knows that trying to read the handwriting of the maintenance technician to figure out what was done can be a bit challenging to say the least. However, without knowing what maintenance was actually performed, this could severely impact your ability to predict failure and be proactive about future maintenance. Consequently, it is crucial to keep maintenance records in a concise, consistent, and fully readable format.

In some large data centers, more than

1,000 maintenance activities need to be performed in a given year. If just one of those maintenance activities is not performed correctly, or at all, there is the possibility of a major event occurring that could bring down the entire facility. Comprehensive maintenance records should be kept online and reviewed on a regular basis.

Facility Diagrams

When is the last time your facility's electrical single-line and "as-built" drawings were updated to reflect the current status of your data center? Why is this critical? Safety, security, and reliability are all impacted. Power distribution units and breakers can easily be overloaded and fail due to poor documentation and not knowing exactly what is connected to what.

Safety can be impacted during routine maintenance or something catastrophic such as a fire. Without proper documentation of the facility, where the high voltages and hazardous materials are, safety can be compromised and could not only cause an issue with compliance but with human life.

At least once a year, facility diagrams should be fully scoured to ensure that they are brought up to date.

Procedures

We talked earlier about the importance of having documented MOPs and SOPs.

Other procedures that should be fully documented include safety related procedures such as "lock-out/tag-out" (LOTO) procedures. According to the Occupational Safety and Health Administration (OSHA), LOTO refers to specific practices and procedures to safeguard employees from the unexpected energization or startup of machinery and equipment or the release of hazardous energy during service or maintenance activities.

As many as 3 million workers service equipment and face the greatest risk of injury if lockout/tagout procedures are not properly implemented. According to OSHA, compliance with the lockout/tagout standard prevents an estimated 120 fatalities and 50,000 injuries each year. Workers injured on the job from exposure to hazardous energy lose an average of 24 workdays for recuperation.

In a study conducted by the United Auto Workers, 20 percent of the fatalities (83 of 414) that occurred among their members between 1973 and 1995 were attributed to inadequate hazardous energy control procedures (specifically lock-out/tag-out procedures).

Additional areas of focus for procedures should include the security of the facility and the scheduling of staff. Inadequate security or staffing could present compliance and operational issues if not properly mitigated.

Training

Besides procedures, training is perhaps one of the most effective means of mitigating the risk of human error in data centers. For each critical component in the data center, you should have a fully documented training module, centered around procedures, to ensure your staff is adequately trained and prepared to operate within your facility.

Ongoing Risk Mitigation

Most any government regulation at its core was created to reduce the risk of something. Be it the risk of faulty financial reporting, the risk of injury or the risk to the nation as a whole.

As human beings, we mitigate risk by going to the doctor to take a physical. We subject ourselves to a litany of tests to hopefully get a clean bill of health. If not, we hope to identify something in the early stages so that it can be addressed before becoming life threatening.

Mission-critical facilities are the heartbeat of our economy and government. Just like people need a physical, so do data centers and other mission-critical facilities. At least once a year, a complete assessment should be done of your critical facilities to ensure that there are no core vulnerabilities that could potentially cause havoc.

As with a physical, you hope that the assessment will turn up nothing. However, more times than not, a trained, third-party expert will find something that can be addressed to mitigate risk to the ongoing operations of your facility.

Just like a doctor won't perform a physical on themselves, neither should you have your own employees conduct an assessment of your facilities. It is important to have a trained professional, who is unbiased, to conduct a thorough review of not only the physical infrastructure of the facility but also of the procedures and documentation.



Todd Bermont is director of business development, marketing, and communications for Lee Technologies, a firm that specializes in protecting technology infrastructure from disaster. Bermont has more than 20 years of experience in the IT industry. Prior to joining Lee Technologies, Bermont worked for NCR, IBM, and APC. He is also an author and has worked with clients in 21 countries across the globe. Bermont can be reached at tbermont@leetechologies.com.

"Let there be a plan!"

When orders come from above, you need DSPN.

Disaster Survival Planning Network
Consulting - Workshops - Exercises
800.601.4899 www.dspnetwork.com