Essential Elements of Data Center Facility Operations

White Paper 196

Revision 0

by Robert Woolley and Patrick Donovan

Executive summary

70% of data center outages are directly attributable to human error according to the Uptime Institute's analysis of their "abnormal incident" reporting (AIR) database[1]. This figure highlights the critical importance of having an effective operations and maintenance (O&M) program. This paper describes unique management principles and provides a comprehensive, high-level overview of the necessary program elements for operating a mission critical facility efficiently and reliably throughout its life cycle. Practical management tips and advice are also given.

APC by Schneider Electric White Papers are now part of the Schneider Electric white paper library produced by Schneider Electric's **Data Center Science Center**
DCSC@Schneider-Electric.com

Schneider Electric

Introduction

A properly designed, implemented, and supported operations and maintenance (O&M) program will minimize risk, reduce costs, and even provide a competitive advantage for the overall business the data center serves. A poorly organized program, on the other hand, can quickly undermine the design intent of the facility putting its people, IT systems, and the business itself at risk of harm or interruption. The importance of an effective and efficient data center O&M program is further illustrated by considering the following points:

- Most facility outages are attributable to human (i.e., operator) error[1], much of which occurs as a result of poor operations and maintenance practices
- Majority of data center facility TCO is in OPEX, not CAPEX, which is also where most of the potential cost savings reside
- Energy costs represent the largest portion of OPEX, and the cost of energy is rising
- Drive for energy efficiency is reducing capacity safety margins and system redundancy, increasing the importance of proactive maintenance and data center infrastructure management (DCIM)
- High levels of facility automation and equipment performance data have created new opportunities for enhancing reliability while reducing costs, when properly managed

This paper describes a balanced critical facility management program and mindset with twelve essential program elements, while providing practical tips and advice throughout. Data center facility managers and operators can use this information for O&M program development, or as a tool for performing a gap analysis on an existing program. In addition, White Paper 197, *Facility Operations Maturity Model for Data Centers*, provides a detailed framework for both establishing and evaluating data center O&M programs, recognizing that there is no "one size fits all" solution for every organization. The purpose of this "Essential Elements" paper is to describe the key components of an effective data center O&M program, while the Maturity Model provides a framework for their implementation and measurement based on the specific requirements and stage of development for a given business. Using these tools, organizational managers can determine which level of maturity is right for them at any given time based on their unique needs and available resources, and also chart their progress. Note that the topics covered in this paper by no means represent a complete list of every process, task, procedure, or system involved with critical facility Operations and Maintenance. Rather, a perspective is offered on the most critical elements to consider when developing or evaluating O&M programs in new or existing data centers.

Principles of the "mission critical mentality"

Managing and operating a mission critical facility is very different from managing a commercial office building or a factory. For most data centers, failure is not an option. Some liken it to "maintaining an airplane while flying it". Today, businesses are often either wholly dependent on their data center or the data center IS the business. Complexity is much higher and the pace of change within the data center is much greater than in most other types of facilities. Increasingly software defined data centers (i.e. virtual machines, virtual storage, and virtual networks) and workload movement combined with short IT refresh cycles make for a challenging management environment. These challenges require careful coordination and planning with the Facilities team. The potential impact on system availability can be so severe that each operational task must be carefully evaluated in terms of its net effect on availability. There are also unique outside pressures. Government regulations and customer audits require detailed processes and procedures that are properly documented

[1] http://blog.uptimeinstitute.com/2011/03/

and conscientiously observed. The high criticality and cost of data center operations often invokes an intense focus from the CxO level of the organization.

Effectively managing and operating in this type of environment dictates that facility management and their staff adapt a "mission critical mentality" that focuses on risk mitigation and grasps the interconnectedness of facility and IT systems. This operating philosophy forms the foundation of an effective O&M program. **Table 1** describes its core principals and outcomes.

Table 1

The mission critical code of conduct and its impact on data center operations

"Mission Critical Mindset" principles	Impact
Focused on risk mitigation in all operational and maintenance activities, work processes, and procedures	Proactively deals with all potential threats to system availability and worker/occupant safety
Acting with confidence and patience that is an outgrowth of careful planning and preparation	Prevents risks from becoming problems; enables faster response times and fewer errors if problems do arise
Analytical, process-driven approach to risk avoidance and problem solving	Helps identify and mitigate risk in complex environments; ensures predictable and safe operation
Comprehensive understanding of the function and interconnectedness of facility systems and components	Quickly identify and resolve potential threats or actual problems; avoid or reduce system downtime
Commitment to continuous learning and process improvement	Increases skills and operational efficiency to maintain an edge in a constantly changing environment

The facilities team that embodies this mindset will be in a much better position to successfully implement and manage an effective O&M program built on the twelve essential elements. The twelve are: environmental health and safety, personnel management, emergency preparedness and response, maintenance management, change management, documentation management, training, infrastructure management, quality management, energy management, financial management, and performance monitoring and review. Each is described below.

12 essential elements

Environmental health and safety

Every data center facility contains electrical, chemical, and mechanical safety hazards that can cause injury, illness, or even death if they are not properly identified and mitigated. A comprehensive workplace safety program is, therefore, an essential component of any data center O&M program. The key tasks for a safety program include injury and illness prevention, electrical safety, hazard analysis, and hazard communication. An effective program not only protects the workforce from harm and lost time, but it also helps avoid possible fines and citations by government authorities, as well as reduce equipment damage and system interruptions that often result when accidents occur. **Table 2** lists and describes the critical attributes of an effective safety program.

Table 2

The critical attributes of an environmental health & safety program

Key Program Attributes	Description
Safety plans and training	Written safety plans must be established that describe the safe work practices and procedures to be observed by all workers. Regular training on the program elements must also be conducted.
Hazard analysis	All operational procedures shall start with an analysis of the possible hazards involved. Risks must be identified and safety measures assigned.
Lockout/tagout procedures	Proper procedures to prevent the unexpected energizing or startup of machines or equipment (or which causes a release of stored energy) shall be used when servicing or maintaining equipment.
Personal protective equipment (PPE)	Appropriate protective equipment should be provided, properly sized, stored, maintained, and utilized as required to mitigate identified safety hazards.
Hazardous material handling	Hazardous materials must be properly identified, labeled, stored, maintained, and used in conformance with manufacturer's requirements, local laws, and ordinances.
Hazard communications program	Includes a list of hazardous chemicals, use of material safety data sheets (MSDS), proper labeling of all hazardous materials containers, and employee training on use of and protection from hazardous materials.
Compliance with all applicable health and safety laws and regulations	Requirements will likely vary by region and by level of government (e.g., local, state, federal).

Personnel management

Humans are still required to install, maintain, and operate data center facility systems. Eliminating human error as the number one cause of system interruptions requires the hiring and development of competent, team-oriented people who embody the "mission critical mentality" described above. A well-rounded team includes subject matter experts in the following disciplines: electrical, mechanical, controls, fire detection/suppression, quality management, training, as well as computerized maintenance management systems (CMMS), and other operational support systems such as data center infrastructure management (DCIM) and building management systems (BMS). Facilities teams require extensive initial and on-going training, which is further discussed later in the paper.

In addition to hiring and training, another key task of personnel management is to develop a staffing model which is specific to the facility systems, business functions, and operational mandates of the organization. The important factors in determining staffing levels are coverage requirements (e.g. weekday only, 24x7), emergency response requirements, maintenance activity workload, project supervision needs, and the operations budget. An

analysis must be performed of the facility maintenance scope, which determines how many man-hours of maintenance are required, factoring in administrative time for change management and training tasks. The objective should be to right-size the staff for normal operations, and to augment it with subcontractor personnel for peak maintenance and project work.

The coverage requirement is fundamentally driven by mission criticality and the perceived cost of downtime. Having at least two technicians per shift with both electrical and mechanical expertise on a 24x7 basis will ensure the highest level of emergency response capability. Some risk profiles and/or budgets allow for a more relaxed model that only requires a minimum of one technician on shift nights and weekends. Others may be willing to assume the higher risk of less than 24x7 coverage with an after hour on-call option. All are valid models for specific risk profiles. The important thing is to match them up properly.

Lastly, it is crucial to have clearly defined roles and responsibilities for each individual position as well as a clearly defined team and organizational mission statement. Well defined position descriptions provide a benchmark for evaluating skills and setting goals for growth and training needs. As a consequence, job satisfaction and employee retention will be improved. A well adjusted and trained staff focused on a common mission will provide the foundation that a successful mission critical O&M program must be built upon.

Emergency preparedness and response

Regardless of how good the infrastructure design and personnel capabilities are, it is impossible to eliminate all risk of unexpected system interruption. Good preparation is the best defense, and will help ensure responses are timely, effective, and error-free. Emergency preparedness begins with developing emergency operating procedures (EOPs) for all high-risk failure scenarios such as the loss of a chiller plant, failure of the generator to start, and so on. EOPs establish a detailed plan of action for safely isolating faults and restoring service or redundancy when possible. These procedures should be posted in areas where the response is likely to be conducted. Escalation procedures also need to be developed and rehearsed to ensure the chain of command is informed and the appropriate resources are brought to bear as the situation develops. Scenario drills should be regularly conducted to rehearse and evaluate both team and individual emergency response effectiveness. Once an incident has been dealt with and its effects mitigated, an analysis should be conducted to understand what the root causes were and how effective the emergency response was in dealing with the problem. Formal failure analysis for significant facility events is a fundamental part of the overall continuous improvement process that is needed to reduce failures and improve response effectiveness in future events.

For a more detailed description of the emergency preparedness and response element including sample EOPs and emergency drill procedures, see White Paper 217, *Data Center Emergency Preparedness and Response*.

Maintenance management

The facility maintenance program helps ensure power and cooling systems continuously perform as expected throughout the life cycle of the data center. Good asset intelligence combined with a proactive preventative and predictive maintenance plan boosts equipment reliability and system availability. As a result, maintenance budget forecasts become more accurate, while total cost of ownership and downtime are both minimized. A poorly managed program, on the other hand, increases operating costs due to higher failure rates that can result in costly repairs and extended periods of downtime. Maintenance management encompasses three key tasks: **asset management, work order management, and spare parts management**.

Recommended asset database information

At a minimum, each asset record should contain the following information:

- Type - top level classification (e.g. electrical, mechanical, fire system)
- Sub-type (e.g. PDU, UPS, CRAH)
- Text description of asset
- Make - asset manufacturer name
- Model - manufacturer model #
- Size or rating
- Location ID (room/area)
- Trade responsible for maintenance
- Manufacturer serial #
- Install date
- Warranty expiration date
- Date asset to be replaced

Asset management

Accurate and consistent tracking of all critical facility assets is the foundation of a good maintenance program. While a well maintained asset database provides the building blocks for effective maintenance, an inaccurate one will result in inefficiency or even equipment failures. To address this, a computerized maintenance management system (CMMS) should be used to record, track, and manage asset data and maintenance history. See the sidebar for a list of recommended asset attributes to be recorded. In addition, each unique make and model of asset should have a documented scope of service (SOS). This document defines the maintenance scope in terms of frequency and the specific activities required in each maintenance event, along with the number of man-hours needed to perform each service. Its function is to establish a standard that is used in the procurement of service agreements, maintenance scheduling, procedure development, and continuous program improvement.

Work order management

Work orders provide a tool for service process management from work initiation through planning, scheduling, execution, and completion. This allows work to be prioritized correctly, assigned the right resources, and completed on schedule. If poorly managed, maintenance may be missed, go unfinished, or result in wasted staff effort. Either a standalone ticketing system or an integrated work order module in a CMMS or DCIM system can be used for work order management. These tools allow facility personnel to spot trends, identify problem equipment, track labor utilization, efficiently manage resources, and more accurately forecast maintenance budgets and equipment "end of life" replacement needs.

Spare parts management

Typically the same tools listed above are also used for the purpose of spare parts management. Maintaining a well-documented inventory of critical spare parts will make mean time to recovery (MTTR) much shorter. The spare parts inventory should include select components whose procurement lead times exceed the maximum acceptable downtime period for the associated system. Prior to the start of operations, an evaluation should be performed to build a recommended spares list that is derived from manufacturer and vendor recommendations, specific mission goals, plant design, parts availability, and past experience. Frequently used items may also be stocked to take advantage of bulk discounts. Re-evaluation of the spares inventory for item selection and stocking levels should take place on an annual basis. As equipment ages, the likelihood of component failure increases while parts availability can decrease, which along with maintenance history may affect the decision on which items to stock, and in what quantities. These items should be stored in a safe, clean, and stable environment with periodic inspections, audits, and even testing to assure readiness.

MOP checklist

A MOP is created for each maintenance activity and is based on the equipment's scope of service (SOS). A MOP should contain:

- Date and time of activity
- Site and contact information
- Procedure overview
- Predicted effects on facility
- Supporting documentation
- Safety requirements
- Risks and assumptions
- Step-by-step work details
- Back-out procedures
- Approvals
- Completion sign-offs
- Feedback

Change management

Any work on or around mission critical equipment and its support systems requires special precautions and coordination with the affected stakeholders (clients/IT groups) to ensure that the intended results are achieved without any unwanted or unexpected consequences. Poor management of this process may result in failures such as turning a wrong valve, cutting power to the wrong feed, or accidental exposure to a live electrical conductor. The primary mechanism for managing change in the mission critical facilities arena is the **Method of Procedure (MOP)** process. A MOP is essentially a detailed checklist (see sidebar) of each step in a specified task such as a preventative or corrective maintenance activity. The MOP itself is an important tool for controlling the work activity, but it is only part of a larger change management process that includes key items such as operational procedure development and review, risk analysis and communication, structured work practices, and vendor/contractor supervision.

Change management starts with developing and conducting peer reviews of the work procedures. These should be based in part on vendor recommendations for the specific

devices being serviced, but must also take into account the overall system dependencies along with any unique site characteristics or equipment configuration. Risks to safety and system availability need to be identified, documented, and communicated in the MOP. Planned change activities need to be clearly communicated to the appropriate individuals in a timely manner so that no one is caught off guard by the change or by any problems that might occur when the change is made. Finally, since OEM vendors and third party service providers often are involved in these procedures, it's important that they are carefully managed and supervised. To this end, vendor orientation must take place to introduce individual vendor technicians to the facility and its work rules, the required work and safety procedures, as well as the MOP and vendor supervision process. A change management program that includes all of these items will minimize errors resulting in downtime, rework, and the associated costs. The number of change windows will be reduced and costs to re-dispatch vendors will diminish.

Documentation management

There should be a system in place to keep the critical infrastructure records well organized and up-to-date. Accurate information that is readily available to anyone in the organization needing access is a fundamental operational goal. Ideally this is accomplished through a document management software application that can automate processes and facilitate document processing, storage, retrieval, and archiving. Not everyone's budget can accommodate such a system, however. A more manual process may be less convenient and feature rich, but it can still work if it includes the elements listed in the sidebar. Whether automated or manual, a good document management program will facilitate the development of accurate procedures, proper training, workplace safety, and process improvement, all of which contribute to facility uptime and efficiency.

Document management process

Should include:

- A catalog that lists each piece of documentation by category and lists its location
- A version control system that shows…
  - Document author
  - Current version
  - Owner
  - Revision dates
  - Change history
  - Next review date
- A quality assurance procedure for peer and/or management review of document changes, additions, and deletions

In addition to the operational procedures and maintenance records that have been already discussed, there are other important documents to manage, such as the critical facility work rules, facility drawings, engineering studies, shift turnovers, and rounds logs. The facility work rules are the established rules governing safety, security, operations, cleanliness, and proper documentation. All personnel entering the data center to perform work must sign off on understanding and observing them. The facility drawings are the current and historical electrical and mechanical one-lines, piping diagrams, and floor space layout of the facility. Engineering studies include items such as arc flash studies, breaker coordination studies, and so on.

Logs of shift changes and inspection rounds describe all activities and events that occurred during a particular shift including maintenance, training, special projects, failures, and any other notable observations. This helps provide real-time knowledge of the facility status and should be continuously maintained and made available for all concerned parties. Conscientious use of this documentation will ensure mission continuity as shifts change.

Training

Maximizing availability and minimizing human error in the critical systems environment depends, in large part, on well trained staff. A suitable training program must be established that organizes all of the operational and maintenance tasks into categories that correspond to specific levels of capability (e.g. Basic, Intermediate, and Advanced). All operations and maintenance activities should be mapped to one of these levels. This provides the ability to control work assignments and ensure that all activities are being carried out by properly qualified personnel.

The training should be administered in a manner that allows new technicians to be quickly brought to a minimum level of competency and achieve steady progress until they are fully qualified in all facets of site operation. Upon completing the course material for each training

level, trainees should be evaluated using a combination of written and oral examinations that include practical demonstrations of knowledge. Examination materials must be secured and randomized to ensure the integrity of the process. Any missed questions should be reviewed and a supplemental evaluation done to ensure that all required knowledge has been acquired, even when a passing score is obtained. Upon successful completion of the evaluation, personnel are certified to perform or supervise any activity associated with that level of training. All personnel should be required to maintain their certification by exhibiting sustained proficiency by passing annual recertification exams.

All personnel must be required to stay current in the knowledge, licenses, and certifications needed to operate and maintain the facility equipment and systems to the current state of the art. In addition, team managers and lead personnel need to stay abreast of industry trends and solutions. To that end, ongoing education needs to take place to maintain team members' capabilities. A training program conducted in this way helps prevent errors, increase worker confidence and satisfaction, as well as increase the amount of maintenance that can be done in-house, thereby reducing maintenance costs.

Infrastructure management

The fundamental purpose of data center facilities is to provide uninterrupted power, cooling, network and space resources in the right amounts, at the right redundancy level, and at the right time to IT servers, storage, and networking gear. However, this purpose is complicated by the fact that the IT gear and their workloads can undergo frequent change and variation both in time and location. And too often, this is further complicated by a "silo mentality" where Facilities and IT (and sometimes upper management) act in isolation from each other. This can make effective capacity management, planning, and other important functions requiring on-going communication extremely difficult. An infrastructure management system is necessary to efficiently match the facility's resources with changing IT requirements. And particularly in an environment where there isn't gross over provisioning of excess safety capacity and where there is not a high degree of redundancy, an infrastructure management system can prevent downtime, improve resiliency and response, reduce operating expenses, and provide a sound basis for capacity planning decisions.

In the context of an O&M program, there are three key tasks to focus on within an infrastructure management program: facility monitoring, capacity management, and IT/ Facilities integration. The ideal platform to address these requirements is a data center infrastructure management (DCIM) software suite. Providing centralized, real-time monitoring of all facility assets, visually mapping dependencies of the IT workloads to the physical infrastructure, as well as showing current, historical, and future power consumption trends are all typical functions of modern DCIM suites. For more information about the functions of today's DCIM tools, see White Paper 104, *Classification of Data Center Infrastructure Management Software (DCIM) Tools*. To understand the potential benefits of these functions, see White Paper 107, *How Data Center Infrastructure Management Software Improves Planning and Cuts Operational Costs*. White Paper 170, *Avoiding Common Pitfalls of Evaluating and Implementing DCIM Software* advises on what to look for in an effective solution and how to ensure the implementation is successful over the long term.

Quality management

A focus on quality and continuous improvement will lead to a more efficient, reliable, and productive data center facility that is less costly to operate. A good facility management program should have an integrated and pervasive quality system that includes the following key components:

- Quality Assurance (QA): Typified by process and procedure standardization

- Quality Control (QC): Quality checks, inspections, and audits
- Continuous Quality Improvement

QA methods help prevent errors from being introduced into a system. The facility processes, procedures, documentation, and training all fall into this category, helping ensure accuracy and consistency in the staff's actions and responses. **QC** is concerned with detecting errors that have been introduced in a system, preferably at an early stage. Regular, on-going checks, inspections, and audits are all used to "inspect what we expect". This pertains to the facility staff as well as the infrastructure. Knowledge must be continuously evaluated to identify gaps in training. **Quality Improvement** occurs when the output of a QC activity is used to modify and improve a QA process. When significant incidents occur or errors are detected, there should be formal efforts made to understand the root cause. The resulting lessons learned are used to adapt existing rules, policies, or procedures to avoid future occurrences. A quality program that focuses on these key tasks eliminates the repetition of costly errors, increases productivity, and creates a path towards standardized best practices and best-in-class operations.

Energy management

With energy typically being the single largest operational expense for a data center, energy management deserves to be listed as an essential element of any O&M program. Energy costs can be significantly lowered in many cases with efforts that produce a very favorable ROI. Depending on where the facility is located, regulatory burdens can also be lessened, and the company's image enhanced.

There are three core tasks involved in an effective energy management program: **performance benchmarking, efficiency analysis, and strategic energy sourcing**. A comprehensive benchmarking program must be implemented to document the facility's energy use, which will be used to formulate energy efficiency and cost reduction plans. The benchmarking process depends on accurate and timely data. The power system must be adequately instrumented to provide the necessary inputs, and the sensors properly calibrated when installed and at recalibrated regularly to achieve the maximum benefit.

Once the data is accurately collected, analysis must take place to uncover energy savings opportunities and to plan for their realization. The preferred toolset to manage and automate an energy management program is DCIM software. Modern DCIM tools will proactively gather power and energy data and present it in a clear, easy to understand manner. Energy consumption and cost per kWh can be determined down to the rack level in many cases. If metered data is not available, power draw data can be estimated based on the equipment nameplate ratings.

A modern energy management program should go beyond just looking at internal opportunities to increase energy efficiency by optimizing the power and cooling infrastructure components. Today's de-regulated energy procurement market also offers opportunities to reduce energy bills. Optimized energy sourcing can reduce exposure to price volatility and can secure pricing that fits budget and business objectives. Accomplishing this requires activities on a variety of fronts including: contract/credit negotiation, demand response program participation, supplier management, analysis of market opportunities, and more. For those who lack the knowledge or bandwidth to pursue this type of energy savings, note that these energy outsourcing activities are available in the market today from third party service providers.

Financial management

Financial Management is an essential element due to the sheer size of data center operating expenses, and also because financial-related issues can have a direct impact on the facility's day-to-day availability and resiliency. Procurement delays, ordering mistakes, unplanned partial shipments, and a multitude of other possible mishaps can delay critical maintenance and facility projects that could jeopardize availability and meeting service level agreements (SLAs). Therefore financial management processes should be in place that focus on purchasing, invoice matching, and financial reporting/analysis.

Note that this element requires close cooperation with the Purchasing department, with whom Facility Managers should maintain a close and open working relationship. Good communication and planning will help ensure orders are placed in a timely and correct fashion, and when issues arise (e.g., backorder, partial shipment, etc) they are communicated quickly to provide time for alternative actions.

Invoice matching is an important element, where vendor invoices are matched to purchase orders and proof of delivery. This process should also be applied to service reports, to ensure that service delivery is performed in accordance with contractual obligations. Effective purchasing techniques, such as using ROI calculations for system upgrades, and standardized RFPs for "apples to apples" comparison of services to be procured, all help to ensure that the maximum value can be obtained and waste minimized. Finally, financial reporting and analysis is very useful for understanding program performance and to potentially uncover unhealthy trends that would lead to repetitive delays, less predictable delivery times, and inefficient ordering.

Performance monitoring & review

Regularly monitoring and reviewing facility performance will determine what the health and effectiveness of the overall O&M program is and where it is trending. It is an integral part of the quality process, which should encompass every element described in this paper. This is most effectively done though the use of key performance indicators (KPIs) (see sidebar), which are used to provide focus and drive program improvements. This yields several benefits, including the alignment of operational activities with business goals and providing positive reinforcement for innovation and process improvement.

The structuring and measurement of KPIs and their associated SLAs is the key to a good performance monitoring & review program. Each metric should be clearly defined in discrete terms that are quantifiable, rather than being based on subjective criteria. Metrics should be derived from measured data that comes from facility monitoring and control systems such as DCIM software, CMMS tools, security logs, and other operational support systems. Each metric should have success target and failure levels defined including what levels are considered "acceptable". A common pitfall is to make the "success" and "failure" thresholds nearly identical to each other (which is a characteristic of SLA-centric systems). The result is that everyone assumes the situation is fine until suddenly and unexpectedly the facility is in a "failure" mode even though from a metrics perspective, little has changed. Good KPIs provide leading indicators of failure that make them more predictable and preventable. These metrics should be collected continuously and tabulated on a monthly basis, with a formal quarterly review recommended. Deviations from "acceptable" levels of performance should be noted and addressed immediately. Finally, the program should be administered in a way that fosters an atmosphere of teamwork and cooperation rather than one of fear. Focus should be placed on providing positive monetary incentives to meet or surpass goals and targets instead of punishing people, departments, or vendors who fail to reach these goals.

Recommended facility KPIs...

- Critical load uptime
- Load redundancy maintained
- Support system uptime
- Maintenance completion
- Staffing coverage
- Security policy conformance
- Emergency preparedness drills
- Emergency response procedure adherence
- Safety policy and procedure adherence
- Procedure development, management and use
- Quality control/improvement
- Training compliance
- Process improvement
- Operational reporting
- Proper event notification and escalation
- Timely and accurate cost reporting

Common mistakes

Research and experience has shown that there are several O&M program-related mistakes that can undermine the effectiveness of a program, potentially leading to system interruptions, avoidable expenses, or staff injuries. **Table 3** below summarizes these pitfalls…

Table 3

A description of the common mistakes made in the management of an O&M program

Common Mistakes	Description
Maintenance program is not driven by metrics	• Often the result of poor asset management • No linkage made between break/fix maintenance activities and preventative maintenance
Poor training	• Training is not formalized and/or is not taken seriously • Over-reliance on technician "shadowing" • No linkage between certification level and tasking
Ineffective change management	• Inadequate risk analysis • Poor or non-existent procedures • No defined process for performing critical work tasks
Failure to consistently test & evaluate skills	• Existing skills/training level not formally evaluated • Scenario drills are not employed • Incident and drill results are not evaluated
Poor documentation	• No coherent sequence of operations • Drawings and schedules are outdated • Lack of revision control and/or lack of digitization
Failure to develop and implement a quality control system	• Lack of governance or resources to measure, monitor, and review performance
Stuck in manual mode	• Failure to implement CMMS, EDMS, DCIM, etc
Overconfidence	• Assumption that future performance can be predicted by past experience

Facility operations services

As the Operations and Maintenance program is being considered and developed, the organization may come to the realization that professional help is required. Project goals could determine that there's not enough time to develop and implement the program internally. There may not be enough in-house expertise or the time to develop it. There might also be a desire to minimize the errors that would likely occur as the team built experience operating the new facility. There are vendors who offer services to advise on, develop, implement, and operate O&M programs for both existing and new data centers. To learn more about these services and how to effectively write an RFQ for them, see White Paper 198, *How to Write an Effective RFP for Data Center Facility Operations Services*.

Conclusion

Human error and inattention can compromise the performance of any data center design. Mitigating these threats and their effects requires an effective and efficient operations and maintenance program that focuses on and attends to the twelve elements described in this paper. The very foundation of that program, however, rests on having a facilities operations team that manages and acts with a “mission critical mindset”. This operational philosophy is focused on risk mitigation, preparedness, standardized processes, and continuous improvement. A well constructed and managed program will reduce operating expenses while maintaining the high level of performance expected by the design of the facility.

About the authors

Robert Woolley has been involved in critical facilities management for over 20 years. Robert has served as Senior Vice President Critical Environment Services at Lee Technologies and Vice President of Data Center Operations for Navisite, as well as Vice President of Engineering for COLO.COM. He was also a Regional Manager for the Securities Industry Automation Corporation (SIAC) telecommunications division and operated his own critical facilities consulting practice. Mr. Woolley has extensive experience in building technical service programs and developing operations programs for mission critical operations in both the telecommunications and data center environments.

Patrick Donovan is a Senior Research Analyst with Schneider Electric’s Data Center Science Center. He has over 18 years of experience developing and supporting critical power and cooling systems for Schneider Electric’s IT Business unit including several award-winning power protection, efficiency, and availability solutions.

Resources

Facility Operations Maturity Model for Data Centers
White Paper 197

How to Write an Effective RFP for Data Center Facility Operations Services
White Paper 198

Data Center Emergency Preparedness and Response
White Paper 217

Classification of Data Center Infrastructure Management (DCIM) Tools
White Paper 104

How Data Center Infrastructure Management (DCIM) Software Improves Planning and Cuts Operational Costs
White Paper 107

Avoiding Common Pitfalls of Evaluating and Implementing DCIM Software
White Paper 170

Browse all white papers
whitepapers.apc.com

Browse all TradeOff Tools™
tools.apc.com

Contact us

For feedback and comments about the content of this white paper:

Data Center Science Center
dcsc@schneider-electric.com

If you are a customer and have questions specific to your data center project:

Contact your Schneider Electric representative at
www.apc.com/support/contact/index.cfm