

How to Prepare and Respond to Data Center Emergencies

White Paper 217

Revision 0

by Leonid Shishlov
Mark Rentzke
Zhang Yong Ping
Patrick Donovan

Executive summary

Data center operations and maintenance teams should always be prepared to act swiftly and surely without warning. Unforeseen problems, failures, and dangers can lead to injury or downtime. Good preparation and process, however, can quickly and safely mitigate the impact of emergencies, and help prevent them from happening again. This paper describes a framework for an effective emergency preparedness and response strategy for mission critical facilities. This strategy is composed of 7 elements arranged across 3 categories: Emergency Response Procedures, Emergency Drills, and Incident Management. The paper describes each element and offers practical advice to assist in implementing this strategy.

Introduction

“Even an expertly engineered and thoroughly commissioned Tier IV-certified data center cannot guarantee 100% availability.”

As stated in White Paper 196, [Essential Elements of Data Center Facility Operations](#), even an expertly engineered and thoroughly commissioned Tier IV-certified data center cannot guarantee 100% availability. Business interruptions due to the unplanned downtime of IT systems will always remain a risk. Good preparation is the best defense, and will help ensure responses are timely, effective, and error-free. Preparedness begins with developing emergency operating procedures (EOPs) for all identified high-risk failure scenarios, such as the loss of a chiller plant, failure of the generator to start, and so on. 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.

Table 1 gives a short overview of key aspects of an effective emergency preparedness and response program for data centers. There are seven key elements, which are grouped within three higher-level categories.

Category	Element	Short description
Emergency response procedures	Emergency operating procedures (EOPs)	EOPs provide a plan of action for safely isolating faults and restoring service or redundancy
	Crisis management plan (CMP)	A detailed step by step plan of action on what to do in the event of a crisis situation
	Escalation procedures	Escalation procedures are documented, prioritized contact lists that outline internal contact requirements for specific situations related to data center operations
Emergency drills	Emergency drills	Emergency drills scheduled and performed in line with top 10 identified operational risks, help ensure readiness
Incident management	Incident notification	A process that ensures any safety or mission critical event is made known to appropriate personnel
	Incident identification and reporting	All incidents must be reported immediately once the situation is stabilized. A brief summary of the incident should be sent to the appropriate distribution list as defined by the incident's level of severity
	Failure analysis	A comprehensive program to determine a root cause is required for any incident that involves an injury or system downtime, or has the likelihood of doing so

Table 1
Overview of key elements of an emergency preparedness and response strategy for data centers

EOPs are discussed first since quickly and safely isolating a fault, restoring service, and rendering first aid is obviously the most critical and urgent aspect of emergency response procedures. Next, a crisis management plan (CMP) is described as the

overall plan for dealing with urgency and crisis in a data center that, if left unchecked, will lead to a disaster. (See sidebar for an explanation of the terms “crisis” and “disaster”.) Finally, the role of emergency drills and incident management is explained as important aspects of a program to be continuously prepared for problems and to be better able to detect issues before they become a crisis or worse yet, a disaster.

Emergency operating procedures

Key definitions

Crisis – An urgent, critical event or situation that if not responded to properly **will eventually result** in system interruption, loss of business, and/or injury to personnel.

A **Crisis management plan (CMP)** deals with preparing, detecting, and mitigating crisis. Emergency Operating Procedures (EOPs) are used to respond to a crisis as it is developing in the hopes of preventing a disaster.

Examples: Loss of UPS redundancy, not having fuel for generator, failed UPS battery string

Disaster or emergency – An event or situation that **has resulted** in severe damage, system downtime, loss of business, or personal injury.

Emergency operating procedures (EOPs)

are used to respond to disasters.

Examples: Failure of genset to start after UPS batteries are exhausted during outage, fire, arc flash explosion in switchgear...anything that results in immediate downtime or injury.

NOTE: What constitutes a “crisis” and “disaster” may vary from organization to organization depending on what they deem to be critical and urgent. A Tier IV data center might have a different definition than a Tier I site with site and software redundancy in place.

Emergency operating procedures (EOPs) are used for handling crisis and disasters as soon as they are detected. EOPs should exist as documents and preferably maintained through a computerized document management system (CDMS). Each procedure describes an approved set of actions for how to respond to a crisis or disaster. The response should cover how to safely isolate the fault and how to restore service or redundancy. The EOP aims to have facility operators respond in the correct sequence of events for the purpose of safety and minimizing the duration and impact of the emergency.

An EOP has multiple functions. First, it assists operators in placing the affected system(s) into a controlled and stabilized condition as quickly as possible. Second, it provides step-by-step guidance to ensure all activities are carried out in a safe and deliberate manner. This is done to prevent further (or wider) service interruption, equipment damage, or personal injury. These negative or possibly even devastating effects result from performing work in an uncontrolled manner, by omitting essential steps, or by performing them incorrectly, or half-heartedly. A third function of EOPs is as a training tool for new operators. They should be used as the basis for scenario drills and testing in staff training programs (as discussed later in the paper). They are also important to have when audited or evaluated by customers or management to demonstrate effective emergency preparedness and response.

It is a common mistake to equate EOPs as being the same thing as standard operating procedures (SOPs). SOPs provide generic guidance or instructions on performing more mundane, day-to-day normal operation type tasks, such as putting a UPS into bypass or other maintenance tasks. An SOP is concerned with how to operate or maintain a system. It does not describe how to deal with and recover from a failure or emergency situation. If operators only rely on SOPs to give them an understanding of how the equipment works and is maintained, the result is a reduced state of readiness for real emergencies. Critical failures often have causes and effects that span across multiple systems. SOPs, on the other hand, generally only address specific pieces of gear. So SOPs are not a good tool to help people understand the dependencies that each of the components and sub-systems have on each other. This knowledge is critical for being able to quickly diagnose and resolve problems. Furthermore, without having specific EOPs for high-risk failure scenarios, there’s likely no scenario drilling taking place. This lowers readiness even further.

Copies of EOP documentation should be posted in areas where they will be executed. A master reference copy should be maintained in the facilities office. Continued tracking of performance metrics and revision of EOPs should be completed as needed to ensure that the instructions are clear and concise.

The EOP is the most important recovery tool in ensuring operational stability and recovery after a failure event. It should be a well-practiced and rehearsed procedure to ensure that all facility staff is aware of their responsibility and tasks in the EOP process. Before any EOPs are developed, first draw up a list of all the likely and/or high-risk failure scenarios. Most commonly occurring examples are listed in **Table 2** by system. An EOP should be written for each one. Of course, data center

operators and their managers cannot foresee all problems, but they can prepare for the worst and hope for the best.

“For each known or anticipated system and/or equipment malfunction, there must be an EOP written.”

All these documents should be maintained in a central document management library. To learn an effective methodology for putting together a site documentation and training program, see White Paper 4, [The Importance of Critical Site Documentation and Training](#). EOP activities are performed exclusively by dedicated and trained data center staff located on site. Outside contractors may in certain circumstances execute some of the steps outlined in the EOP at the direction of the onsite staff. Experience has shown that proper training can effectively counteract the sense of panic that can ensue in an emergency. Good preparation can literally mean the difference between a close call and a complete loss of load in a critical environment.

An effective training method is to create realistic drills that are scripted to simulate the conditions of a particular event. When necessary, props such as colored sticky notes can be used to simulate panel indicators or switch positions. The drills are administered to individuals in order to exercise their abilities and evaluate their responses, and are an excellent measurement of operational readiness.

System	Common failures requiring EOPs
HV/MV electrical services	<ul style="list-style-type: none"> • Utility failure - complete (feeder A and B) • Utility failure - feeder A only • Utility failure - feeder B only • Transformer failure • Load centre bus-coupler circuit breaker failure • Failure of load centre energy building A or B side • Cooling towers switchboard failure • Pumps switchboard failure • Generator switchboard failure
Standby generators and fuel systems	<ul style="list-style-type: none"> • Generator alarm / failure • Generator manual start • Fuel delivery pump failure • Water delivery pump failure • Failure of generator system PLC • Air compressor system failure
Uninterruptable Power Supply (UPS)	<ul style="list-style-type: none"> • UPS unit alarm • UPS unit failure • UPS system failure • DC power plant failure
Central refrigeration & associated systems	<ul style="list-style-type: none"> • Cooling tower failure • Hydraulic system pump failure • Hydraulic system pump VFD failure • Pressurization unit failure
CRAC & critical environment A/C	<ul style="list-style-type: none"> • Water leak in hydraulic pipe • CRAC alarm / failure • Loss of CRAC unit redundancy • AHU failure • VRV system failure
Mechanical services	<ul style="list-style-type: none"> • Loss of water supply to building • Hydraulic pipe leak
General	<ul style="list-style-type: none"> • Elevator entrapment / safe release of passengers • Freight elevator lift failure • Access control failure • Earthquake alarm • Heavy rain alarm

Table 2

Common failures by system that require the development and implementation of documented EOPs (emergency operating procedures)

Crisis management plan

Key elements of good CMP

- Planning
- Procedures Implementation
- Testing and Training
- Crisis types
- Disaster Types
- First response
- Notification
- Consultation
- Delegation
- Mitigation
- Iteration
- Post incident analysis
- Reporting

The crisis management plan (CMP) is a set of policies and procedures to help data center operators prepare for, respond to, and learn from crisis situations that could eventually lead to a true emergency or disaster that would then require the execution of EOPs. The CMP should be closely reviewed by all major stakeholders who would participate in the process. This includes facility managers, operators, as well as IT managers and their staff who work in the white space. The plan is designed to instruct people on how to detect/prevent and react to a variety of crisis scenarios, with the goal of providing a safe, timely, and sound resolution that prevents the crisis from evolving into a total disaster.

Preparation and prevention

The best crisis management tool is prevention. It is commonly known that most data center outages are a direct or indirect result of human error. Many of these errors occur during installation and maintenance, activities that are performed or supervised by the Facility Engineering staff. To minimize errors, data center personnel should undergo intensive training in change management procedures to ensure proper behavior and execution for work in or around critical facility systems. All data center work procedures (standard operating procedures, or “SOPs”) should be created with safety and operational risk mitigation as the primary goal. It is recommended that all procedures be peer reviewed on site and undergo an additional review by a Quality Assurance specialist for technical and procedural accuracy. In particular, they should be scrutinized for proper risk categorization, safety preparation, work task sequencing, and back-out procedures.

Another important activity is the identification of probable and/or consequential system failure modes, which is a precursor to development of emergency operating procedures (EOPs). This exercise not only identifies what EOPs are needed as previously explained, but it will also help prevent such incidents from occurring as a natural consequence of the identification and preparation process. Once established, regular drills of EOPs will maximize preparation and staff coordination.

Detection and incident classification

How do you recognize a crisis when it occurs? Not all events appear out of nowhere or are easily identifiable at first glance. Quite often, a manageable situation will transform into a crisis over time, possibly catching the participants off guard. It is important to be able to recognize their early warning signs and threshold qualities.

There is a distinction between an urgent situation and a crisis. An urgent situation that is being managed with a proven process or procedure would not normally be considered a crisis. For instance, the loss of redundant UPS or Chiller capacity might be considered a crisis, and result in Emergency Operations Procedures being immediately implemented. However these are events that typically have a defined response plan that is well documented and rehearsed. Provided EOPs are implemented as planned, the situation can be resolved in an orderly and controlled manner without reaching the level of being a disaster where downtime and/or injury has already occurred.

In fact, one of the defining characteristics of a crisis is a loss of control. If a situation passes outside the boundaries of what can be reliably managed and becomes, or threatens to become out of control, a crisis may ensue. Another characteristic of a crisis would be a high level of severity. For example, even though there may be an incident response plan in place for a critical load outage, the severity of the event dictates that crisis management take place immediately.

Data center infrastructure management (DCIM) software tools can be an effective way to centrally monitor data center system state changes and alarms to provide more proactive notification of problems and conditions that could lead to a crisis or disaster. Many DCIM suites also offer Change Management and work order functions, as well as the ability to simulate adds, moves, and other changes to ensure such actions will not cause any problems.

In either the event of a crisis or disaster, the ability to quickly recognize and classify the event is the crucial first step in the process, which is necessary for an effective response and communication strategy.

Response and mitigation

Once a crisis or disaster has been declared, the first inclination on the part of well-meaning operators might be to immediately jump in and take action to fix the problem. Until the situation is fully understood and a well-considered response plan created, however, such actions run the risk of causing further harm or downtime. Except in obvious cases requiring immediate action (e.g., fire), the proper course of action is to circle the wagons and craft a plan of action with subject matter experts and key stakeholders. The time invested in these activities will often, in the long run, provide a safer, surer, and longer lasting solution than hasty action.

However, of course, if there is an immediate threat to human safety or the physical plant that can be safety mitigated, immediate action should be taken. Common sense dictates that if someone is or is about to be injured the need for action outweighs the need for deliberation - provided that the consequences of such actions do not recklessly endanger anyone. Similarly, if there were a containable fire and the safe means to extinguish it, doing so would take precedence over anything else. These are just two possible examples where a first response would be justifiable and prudent. That being said, extreme caution should be employed in any situation where the need for an immediate first response is indicated. Only when the stakes are high and the consequences predictable should such actions be considered.

After any first response activities, the primary task is to assess the situation. Basic information must be put together about the scope and severity of the incident, as well as the state and stability of the plant. This data must be quickly established and continuously updated in order to ensure good decision making and accurate communications. Doing this well requires staff who are well trained, drilled, and who are quick thinking and calm under pressure.

Recovery and analysis

Once the incident has been fully resolved, a failure analysis report should be prepared and issued to key stakeholders. It is best to do this quickly - within one week of the incident's resolution – while the experience is still fresh in people's minds. The Failure Analysis Report should also include:

- Root Cause analysis
- Lessons learned report – Participants reflection on what happened and what was learned
- After action plan document – contains specific recommendations and a set of actions for improving the team's response to a given event.
- Training program update for existing operators and new hires to ensure analysis is understood

All of this is aimed at preventing the same crisis or emergency from happening ever again.

Escalation procedures

As situations go from normal to urgent to potential crisis or even disaster level, escalation of the problem must take place. This is to assure the right know-how and resources are brought to bear at the right time. Escalation management can be a stressful task, but having a formal process in place will help to manage escalations as easily and effectively as possible.

Proper escalation of business-impacting incidents as well as “near-misses” is an important element of an emergency preparedness and response strategy. Communication between data center staff, management, customers and vendors is crucial business success and relations to ensure that the situation is under control and all necessary resources are being focused on the incident. While there is no single step-by-step escalation procedure that guarantees successful resolution for every issue, there are essential ingredients to ensure success for your own internal process. Escalation procedures should be implemented that provide a framework for, at least, typical situations. **Table 3** below provides an example of escalation procedure and timelines. It can be modified to suit any organization’s specific requirements and expectations.

Table 3

An example escalation procedure and timelines based on the level of severity (incident class)

Incident class	Facility manager	Service manager	Operations manager	Operations director
Class 1 Life Safety	Immediate	+20 minutes	+30 minutes	+1hour
Class 2 Critical	Immediate	+30 minutes	+1 hour	+2 hours
Class 3 Serious	Immediate	+1 hour	+4 hours	+24 hours
Class 4 Significant	Immediate	Next business day	+ 2 business days	+5 business days
Class 5 Advisory	Advisory			

All incidents should be assigned a “Class” level based on severity, Class 1 being the most serious and Class 5 being the least serious. Summary definitions of the Event Class are as follows:

Class 1: Life safety

This class overrides all other classes. Threat to human life is more important than threats to the IT load. The data center team’s responsibility is to notify emergency response teams, call 911, assist Security as needed, and pass the responsibility on to Security. This class covers Fire, natural disasters, threat to human life, and physical security threats. After a Class 1 event has been stabilized by Security, the Fire Department, or the Police, the decision must be made by data center management as to how to proceed with any other needed recovery work for their critical environments.

Class 2: Critical

Defined as an event that interrupts IT function, or if “N” is lost in any building system, Mechanical or Electrical. A Class 2 situation can be determined by asking one of 2 questions: Have we lost “N” redundancy in cooling or electrical support for the IT load? Or have we lost ANY critical IT load in the building? Class 2 events will

mainly be “recovery” situations that will need direct data center management decision making before recovery actions can be performed.

Class 3: Serious

No further backup systems are available; i.e., redundancy has been reduced from “N+1” to “N”. Also covers any non-scheduled generator runs. When defining this class the question that needs to be asked is: “Do we have additional backup or capacity?” if the answer is “no”, then Class 3 must be assumed.

Class 4: Significant

Critical systems redundancy is still available, i.e., “N+1” exists. Class 4 may be difficult to define due to the many definitions of “redundancy” that may exist. For example, at Building 11, the loss of a CRAC unit on the server floor would be a class 4. This is due to the fact that there are many other units that will be able to take over cooling without much impact due to the loss. There is still backup, however the failure was significant. Sudden power draw increases on the UPS system could be considered a class 4.

Class 5: Advisory

This class is designed to notify the immediate supervisors of the data center team. Examples would be: strong wind warning, lightning storm warning. This class is mainly for notification of situations that could have the possibility of escalating to a higher class. Also covered under this class is maintenance work that could possibly escalate to a higher class as well as plant lineup changes, i.e. chiller plant, UPS etc.

Similar escalation procedures as shown in **Figure 1** should be put into place for facility incidents and for vendor escalation. For multi facility data centers, a 24x7 Operations Center should be available as a centralized resource to coordinate escalation procedures.

Data Center Event Escalation List

Name	Title	Mobile / Cell	Office	Home	Other	Class 4	Class 3	Class 2	Class 1	Call Order
	Shift Supervisor					X	X	X	X	
	Facilities Manager					X	X	X	X	
	Data Center Manager					X	X	X	X	
	Operations Director						X	X	X	
	Operations VP							X	X	
	Operations Center				email			X	X	

Figure 1

Example of a Data Center Escalation List

Emergency Vendor Contact List

System	Company	Phone
UPS		
Switchgear		
Electrical		
PDU		
Generator		
Mechanical		
Chillers		
Fuel		
Controls		
Fire		

Data Center Operations Staff Contact List

Name	Title	Mobile / Cell	Home
	Team Lead		
	Technician		
	Specialist		

Command Center: (XXX) XXXx-XXXX

Emergency drills

The primary function of a drill is to evaluate the proficiency of an operator's response to emergency events. Written and oral tests can demonstrate knowledge, but more importantly, drills show both knowledge and proficiency of action. Safely resolving a crisis or emergency depends in large part on bodily action and knowing where things are physically. Drills can identify areas of skill and knowledge deficiency, and thus create an opportunity for training to address those deficiencies before a real emergency occurs.

The drills should be based on real world conditions and an understanding of the underlying principles of how the equipment and systems function. A drill report document allows for the evaluation and recording of individual performance. It is also useful to use some drills as an opportunity to train and enhance the individual's knowledge of the data centre environment and installed equipment.

Drills should be mandatory and should be created for each emergency operating procedure (EOP) that addresses anticipated events of high probability and/or high severity. Each facility should establish a goal of each data center operations team member participating in at least one drill per month, but must in all circumstances meet any contractual obligations regarding drill requirements. Emphasis should be placed on the top 10 EOPs, in combination with the current threat evaluation. Drills can be grouped based on complexity or level of difficulty such as, "basic", "intermediate", and "advanced".

The drill evaluator must indicate if the drill is being used for evaluation or training purposes prior to the start, and maintain that focus throughout the session. Ability to accurately execute the documented procedure in a safe and timely manner depends on the operators who need to be keen with the following:

- Knowledge of equipment and systems functionality
- Understanding of equipment operation and systems integration.
- Familiarity and proper use of reference materials (EOPs, SOPs, operator manuals, etc)

When drills are used as an evaluation tool, the evaluator strictly assesses and records the data center operations team's performance without providing any coaching, hints, or corrections during the drill session. It is not expected that data center staff will pass every evaluation the first time. If an evaluation is not passed, it is the responsibility of the evaluator or Critical Facility Manager to develop a training plan of action to address all deficiencies identified by the drill. Upon completion of the specified remedial training, the trainee may perform one or more training drills, but must eventually repeat and pass the evaluation drill. This above process is repeated until the trainee achieves a passing score.

In the case of a drill conducted for training purposes, the instructor would take on the role of coach and participant, actively assisting and directing the trainee during the drill. As the training drill is repeated and the operator learns, instructor participation would decrease until the trainee could do it on their own.

Combining multiple failures into a single drill can make them much more challenging. This makes for a more thorough test of prioritization, teamwork, and incident management skills. Combining a mains failure with a subsequent start-up failure of a standby emergency generator would be a good example.

The following bullets are considered best practices when conducting drill evaluations:

- Hold a pre-drill briefing and provide an evaluation scorecard beforehand to explain the test to the engineer(s).
- Technically knowledgeable evaluators familiar with conducting scenario drills should administer and record the drill.
- Signs should be installed prior to the training scenario to signify drill and alarm conditions to the engineer(s) being assessed.
- The evaluator plays the role of announcing changing alarm conditions and equipment state changes in real time as dictated by the drill, such as “the generator will not synchronize to the bus bar” or “there is an alarm sound coming from the UPS panel”.
- The observers should not assist the engineer with determining resolution except to provide information that would be available to the engineer, for example, “that gauge is at 1 Bar”.
- The drill ends when resolution is obtained or no additional actions by the engineering team are required.
- Observers should evaluate and record the engineer(s) against the criteria detailed on the evaluation scorecard and then go over it in detail with the engineer. The evaluator should re-enforce what they did right and explain where they went wrong. This should be done immediately following the drill.

Incident management

What is an incident?

An “**incident**” in a mission critical facility is any unplanned, unusual, or unexpected event that occurs that could impact operations or safety.

Example incidents:

- Equipment or system failures
- Operator hurts themselves
- Infrastructure device loses network communication
- UPS sounding an alarm
- Temperature threshold exceeded
- UPS switching to battery
- Panel circuit breaker trips
- Smoke alarm goes off
- Intrusion alert
- Water leak sensor alarm

Mission critical facilities expend large amounts of capital and human effort to ensure continuous operation. These environments should be highly controlled and monitored as a result. As part of that control scheme, it is important to be aware of, document, and report on any unexpected events that might affect operations or safety (see **sidebar**). These incidents if poorly handled could become a crisis or even a disaster. An organization with good emergency preparedness and response capabilities will have an Incident Management process that provides a standardized method for handling these events. An effective process has three elements: incident notification, incident reporting, and failure analysis.

Incident notification and identification

Incident notification includes the systems, process, and people involved in alerting stakeholders that an incident has occurred. It is important for notification of events to be timely. What exactly is meant by “timely” will depend on the severity and urgency of the incident. Smoke in the white space will obviously require more immediate notification than will an incident involving a loss of communication with a single environmental sensor. Who should be alerted needs to be determined and planned for ahead of time. As previously shown in **Table 3**, incidents can be classified by level of urgency or criticality. This classification system can then govern who needs to be notified, when, and how often.

Data Center Infrastructure Management (DCIM) software including Building Management Systems (BMS) can be very helpful in simplifying and automating incident notification (and reporting) assuming infrastructure systems are metered, instrumented, and communicating with the software, of course. Alarm thresholds and notification policies can be centrally configured and managed. Too many alarms or improper notification can render the system ineffective. See White Paper 170, [Avoiding Common Pitfalls of Implementing Data Center Infrastructure Management \(DCIM\) Software](#) for information on how to do this properly.

Incident reporting

Incident reporting is a generic process that may be augmented or superseded by an existing system (e.g., DCIM or BMS) or an existing process. The following sections cover the incident reporting process from incident occurrence through event response and follow-up actions.

Once the initial incident has been detected, responded to, and the right people notified; it is recommended that an incident report be completed within 24 hours and sent out to all appropriate stakeholders. It is a good practice to start filling the report out as soon as there is time to do so (while the event is still fresh in people's minds), and to continue updating it throughout the event, if the situation allows.

A standardized template should be used to report all incidents. This helps ensure all of the relevant information is gathered every time. It should be stored in computerized document management system (CDMS). The report should contain the following information.

Report information

- Report title
- Submittal report date
- Date and time of report creation
- Date and time of report submittal

Site information

- Site identifier
- Site address, city, state or province, zip or post code, country
- Site point of contact (POC)
- Incident report author

Incident overview

- Brief description of incident
- Location affected by incident (e.g. generator bay, UPS room, or entire facility)
- Equipment involved
- Incident attributes

Incident details

- Time/date of incident and duration
- Who discovered it
- Who was present
- Describe initial response actions
- Who was notified and when
- How the situation was stabilized or resolved
- What resources were brought to bear
- The time that each step in the narrative occurred

Incident follow up

Once the initial incident is reported, follow-up activities may occur that are recorded in this section. For instance, an incident may occur when a system component fails and service is restored through a redundant unit, and a vendor is called in to repair

the failed component. The Incident Report would be filled out right away and can be approved and distributed prior to the repair being affected. Once the vendor shows up and performs the work, the Incident Report can be updated in this section.

Action items

These are specific actions that need to take place in response to the incident.

- Specific task(s) to correct or provide additional information about the incident (e.g. ordering a part, calling a vendor, long term monitoring of the issue).
- Name of the person or persons who are responsible for carrying out the task.
- Expected or required completion date for the task.

Recommendations

Any recommended action or actions that should be taken to prevent future incidents. This may be skipped if a Failure Analysis Report will cover the subject, but it may be used in any event to recommend short-term activities to mitigate the risk of complications.

Support information

This is the place to add any supportive information like insert photos, diagrams, attachment file names, links, etc.

The language must be professional, accurate, concise, and limited to the facts at hand. It should communicate all of the necessary information without elaborating in ways that do not add to the narrative. Reports are typically viewed by a wide cross section of people that want a summary of the pertinent facts, not a novel, or an apology for anyone's actions. Avoid long rambling commentaries in favor of breaking it up into a series of time-stamped steps that show the progression of the activity.

Any speculation of the cause of the incident should be postponed unless it is completely obvious and understood. The purpose of the report is to inform all interested parties in what actually happened as opposed to the root cause analysis, which generally is provided in a follow-up Failure Analysis Report. Pictures can be very useful.

Each step should have a time stamp when known. When an incident spans more than one day, a date separator should be inserted with the first entry of the new day, as provided in the template.

Failure analysis & lessons learned

The Failure Analysis process is designed to provide a standard method for determining and documenting the root cause of an incident, whenever it is determined such an investigation is necessary. It focuses on the WHY the situation occurred rather than the WHO, WHAT, HOW, WHEN and WHERE, which are the focus of the Incident Report. The Failure Analysis report should still provide a description of what happened where and when, and how it was responded to. This can be done by simply referring to the Incident Report or attaching the Incident Report as a reference document.

Accurate detailed documentation of problems can provide valuable "Lessons Learned" to operators. A Failure Analysis Report shall be required whenever a full understanding of the event is not complete at the time the Incident report is completed.

"Incident Report focuses on the WHY the situation occurred rather than the WHO, WHAT, HOW, WHEN and WHERE."

Once the incident has been resolved, there are several items to consider:

- Failure analysis: Full Failure Analysis Report should be created if the root cause is not determined in the Incident Report. This will require the input of the incident report author and anyone involved in the incident itself.
- Integration: Existing policies and procedures should be examined to determine if changes are needed to prevent or mitigate future incidents.
- Lessons Learned: In cases where spreading the word about a particular incident would have widespread benefit, a Lessons Learned document should be created. It is a good practice to cross reference the Lesson Learned documents in training materials, EOPs and SOPs where appropriate.
- Archiving: All closed out Incident Reports should be uploaded to the Document Management System and noted properly.

Conclusion

For now, companies must understand the importance of preparedness and response strategy for their sustainable operations. To effectively respond to all different kinds of risks and crises in data centers, organizations must act quickly and know what to expect in unexpected situations. Proper operational methodology will avoid common mistakes. A good Emergency Preparedness Plan is a key element of such methodology and includes integration of people, processes, and systems, which help the data center operators run their facilities in a more predictable and effective way.

Companies who struggle with adequate response to natural and man-made risks should seek the assistance of critical facility operations subject matter experts. By implementing the best practices developed over the many years in Schneider Electric, organizations can protect their expensive assets like data centers and ensure the best returns of investments.

About the authors

Leonid Shishlov joined Schneider Electric in 2013. He is responsible for establishing the Data Center Critical Facility Operations and Managed Services' offer globally. This includes managing a Quality Management System to ensure the highest standards of delivery. He resides in Singapore in Schneider Electric's DC Center of Excellence. Leonid has 10 years of experience in the data center industry spanning IT, Data Center Management, Facilities Operations, as well as design and consulting services. He holds a number of industry recognized certifications. Before joining Schneider Electric, Leonid worked for Intel Corporation as a data center manager.

Mark Rentzke is a Senior Manager for the Global Data Center Services responsible for the global development, implementation and deployment of the advanced Data Center Critical Facility Operations Services program that Lee Technologies brought to Schneider Electric in the 2010 acquisition. He resides in Dublin, Ireland and reports directly into the Schneider Electric Global Solutions Line of Business. Mark has over 25 years of experience in the data center industry spanning, Telecoms, Networking, IT, Data Center Management, Facility Operations, Business Development, Quality Management and Consulting Services. Before joining Schneider Electric, Mark worked for Lee Technologies as a Data Center Operations Consultant, prior to this he was the Data Center Manager for EIR (previously known as Eircom).

Zhang Yong Ping is the Manager of Global Data Center Services responsible for the global development, implementation and deployment of the Data Center Critical Facility Operations Services program at Schneider Electric focusing on the Greater China region. He joined Schneider Electric in 1994 and has worked in many areas, including as a UPS field service technical trainer, Quality Assurance Manager, Product Marketing Manager, Data Center Operations Manager, Contract Manager, and Data Center Engineering Manager. Before joining Schneider Electric, Zhang went to Antarctica three times as a member of the Chinese Antarctic Expedition and researched Antarctic meteorology for ten years in the Chinese Academy of Meteorological Sciences.


Patrick Donovan is a Senior Research Analyst for the Data Center Science Center at Schneider Electric. He has over 20 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. An author of numerous white papers, industry articles, and technology assessments, Patrick's research on data center physical infrastructure technologies and markets offers guidance and advice on best practices for planning, designing, and operation of data center facilities.




 [Fundamentals of Managing the Data Center Life Cycle for Owners](#)
White Paper 195

 [Essential Elements of Data Center Facility Operations](#)
White Paper 196

 [Facility Operations Maturity Model for Data Centers](#)
White Paper 197

 [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