Avoiding Common Pitfalls of Evaluating and Implementing DCIM Solutions

White Paper 170

Revision 0

by Patrick Donovan

> Executive summary

While many who invest in Data Center Infrastructure Management (DCIM) software benefit greatly, some do not. Research has revealed a number of pitfalls that end users should avoid when evaluating and implementing DCIM solutions. Choosing an inappropriate solution, relying on inadequate processes, and a lack of commitment / ownership / knowledge can each undermine a chosen toolset's ability to deliver the value it was designed to provide. This paper describes these common pitfalls and provides practical guidance on how to avoid them.

Contents

Click on a section to jump to it

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

Link to resource
White Paper 104
Classification of Data Center Management Software Tools

An **effective and well-implemented** Data Center Infrastructure Management (DCIM) system helps operators safely maximize the efficient use of power, cooling, and space capacities now and in the future. Availability of the physical infrastructure systems and the IT workloads that are supported by them is enhanced. Many data center management activities are simplified or automated allowing operators to focus on other issues and tasks. White paper 104, *Classification of Data Center Management Software Tools*, describes the core functions that enable these and other benefits:

Monitoring and Automation functions

- Visibility to the status and configuration of physical infrastructure systems
- Proactive notification of changing status and alarm conditions
- Remote configuration of facility power, cooling, and security system settings

Planning and Implementation functions

- Tracking of assets and their dependencies in the data center
- Facilitating efficient deployment of new equipment
- Execution of planning in order to facilitate changes in the data center
- Simulation of potential changes in order to analyze impact to data center operations

The problem, of course, is that not all solutions are effective (or appropriate) and they can be poorly implemented and maintained. Although they may understand the necessity and value of DCIM, some customers fail to obtain much value or benefit. Research has determined there are three common pitfalls that users can fall into when evaluating and implementing DCIM tools. These traps interfere with the tools' functions listed above. **Choosing an inappropriate solution, relying on inadequate or mismatched processes, and a lack of commitment / ownership / knowledge can each undermine a chosen toolset's ability to deliver the value and benefits it was designed to provide.** This paper describes these pitfalls and provides practical guidance on how to avoid them.

Pitfall 1: Choosing an inappropriate solution

At the time of this writing, there are a large and growing number of DCIM vendors and solutions. Some of the available tools are focused on specific measurement functions, or are slanted towards managing specific power or cooling devices, while others may provide a broad capability, such as workflow management or energy management, over the whole data center. Some may allow remote control, while other tools only collect and report data. Functions are provided at different levels of depth across different products, and there is often overlap or gaps when assembling various DCIM tools into a suite. To help make sense of the various types of tools and their functions, consult white paper 104, *Classification of Data Center Management Software Tools,* linked above in the Introduction.

As data centers increasingly become standardized and modular, the need to assemble a suite of DCIM solutions will be reduced, as some functions become implemented as firmware within data center modules, and other DCIM functions, such as analytics, become available via cloud services. It is important to recognize this trend now and assure that the kinds of solutions implemented now will seamlessly carry over into next-generation data centers, without dramatically changing data center operating practices and processes. Although the exact methods and standards used in future data centers are not yet determined, it is

possible to identify a number of key characteristics that tools selected today must have, in order to be prepared for the future and be effective today:

- Scalable, modular, flexible system
- Open communication architecture
- Standardized, pre-engineered design
- Active vendor support structure

Choosing DCIM tools today with these characteristics ensures that the business processes, data, and methods will be in-line with the expected evolution of DCIM; solutions without these attributes are likely to be dead-end choices. More than that, these attributes play a significant role in helping ensure the solution is effective **today**. These four critical attributes, their impact on system effectiveness, and the steps to confirm their presence in a given DCIM solution is explained in the sections below.

Scalable, modular, flexible system

This attribute speaks to the toolset being easy to implement, expand (or shrink), or customize. On the surface, this trait may seem to be a "nice to have" luxury or simply a matter of convenience. But, indeed, a system which lacks this trait is more likely to lose its value over time and end up falling out of use. The common benefits of modularity and scalability are widely known today: ability to pay-as-you-grow, increased fault tolerance, reduced mean time to recovery, etc. But, particularly for software suites whose value is dependent to a significant extent on user action and ongoing process (discussed in detail later) flexibility also helps ensure there is continuous value even as the data center evolves and changes over time. If the software is difficult and/or expensive to expand or upgrade, there is a risk it will be abandoned as compatibility issues arise or functionality is lost. The DCIM system's map of managed assets will become incomplete and inaccurate over time. The inability to easily add additional tools as an organization grows in maturity and complexity could force that organization to buy and implement upfront an entire suite of products they aren't ready for or that aren't necessarily needed. In all of these cases, value of the software decreases and this can lead to eventual abandonment of the management system altogether.

Table 1 lists suggested questions to ask the vendor to help determine whether and to what degree their proposed offer is scalable, modular and flexible.

Table 1

Questions to ask the vendor to help identify whether (and to what degree) a solution is scalable, modular, and flexible

Scalable, modular, and flexible?
What is the cost and process for upgrades and additional licenses?
Is service required to perform an upgrade or can I simply self-install a patch or update?
Can I pick and choose only the tools I need now and add more later? Or do I have to implement the full suite now?
How disruptive is expansion to my current operations?
Can reporting tools and results be customized to meet the needs of my stakeholders?
How difficult is it to add/remove IT systems and infrastructure components within the system?

Link to resource
White Paper 160
Specification of Modular Data Center Architecture

For more information regarding the benefits of modularity in the data center and how to specify it in the design of the infrastructure, see white paper 160, *Specification of Modular Data Center Architecture.*

> Infrastructure Communication

The most effective DCIM solutions work off the continuous input of live data from the physical infrastructure devices and other management systems. UPSs, PDUs, power meters, environmental sensors/probes, security cameras, cooling units, flow meters, BMSs, CMDBs, and more can be setup to communicate with a DCIM server.

Monitoring and some planning functions requires this on-going communication. Not having a clear picture of power, cooling and environmental conditions at the rack level leads to an inaccurate picture of infrastructure capacity and status upon which the DCIM software will make erroneous assumptions, calculations and recommendations.

- At a minimum, UPSs, cooling units, rack PDUs*, and temp / humidity sensors should be enabled for network communication.
- Ensure DCIM server initially discovers necessary devices
- If BMS is the system monitoring power and/or cooling, make sure DCIM server communicates with BMS
- Configure each device with appropriate settings, thresholds, access rights and security settings to ensure system responds as expected
- Ensure communication is maintained as the data center changes and evolves over time

*Some systems enable you to get power and temp data directly from the server. In this case, metered rack PDUs are unnecessary.

Open communication architecture

This refers to the ability of the system to interact with third party devices and software over a multitude of standard communication protocols. Highly effective DCIM systems require a full and accurate picture of power, cooling, space, and IT usage, as well as knowing their dependencies on each other, ideally in real time. These modern systems proactively gather all the data points it needs to present the user with a sound basis for planning and operation-related decisions. If the DCIM software is unable to communicate with a particular cooling unit or UPS, for example, then it will be unable to determine accurate capacities or their current status (see the sidebar on this page). This then makes sound planning decisions hard or impossible to make in real-time. Answering important questions such as where to place the next server, when will power/cooling capacity be exhausted, or what the impact of a particular change will be, all become hard to answer if communication is limited. DCIM's reporting and dashboard functions will also be fatally flawed if inputs are missing or are wrong. For example, reporting PUE (Power Usage Effectiveness) is a higher level metric often reported through a DCIM dashboard that is wholly dependent on the collection and understanding of the connections of many lower level sensor readings. If the system is unable to communicate with all of the necessary sensors, then obviously the PUE metric reported would be incorrect. Therefore, it is important that the DCIM solution be capable of communicating with all the physical infrastructure devices and the building management system (BMS) that exists (or will exist) at the location to be managed.

It should be noted, however, that the need to meter and monitor all devices and systems can be lessened if the DCIM system is capable of effective modeling and accurately simulating the potential effects of moves, adds, and changes. This ability means that these solutions are less dependent on live measurements and can often give good approximations with fewer meters. This is useful if the data center is not fully instrumented and additional meters cannot be implemented, or if the site is not metered at a few crucial, but hard to meter points.

Some DCIM suites also enable communication with IT management systems such as Configuration Management databases (CMDB) which (to varying degrees) can help automate at least some of the collection of IT systems data. This data is used to determine IT dependencies on power, cooling, and space at a device level. Otherwise, the IT systems data may need to be manually entered into the DCIM software. It is, therefore, recommended to choose a solution with this ability to help make implementation easier and to better ensure asset information is kept up to date over time.

To understand more about the importance of DCIM's ability to incorporate both facilities and IT layer information, see white paper 107, *How Data Center Infrastructure Management Software Improves Planning and Cuts Operational Costs*, linked on the next page.

The extent to which a given offer has this capability should be determined by asking the vendor directly. **Table 2** describes how to do this.

Link to resource
White Paper 107
How Data Center Infrastructure Management Software Improves Planning and Cuts Operational Costs

Table 2

Questions to ask the vendor to help determine to what degree a given solution will be capable of providing a complete picture of both IT and facility systems

Open communication architecture?
Ask the vendor to provide a list of supported protocols.
Compare this list to the protocols supported by the devices and systems to be managed.
Describe categories of available APIs (application programming interfaces) or provide a list of actual APIs, as well as typical examples of usage.
Ask vendor to describe process required to share and/or receive data between the DCIM server and other management systems being used (e.g., BMS, or VM Manager).

Standardized, pre-engineered design

Management systems and software that are highly customized, "one off" designs created on site should be avoided. Those that are standardized and pre-engineered are easier to implement, operate, and maintain, as well as being more reliable and flexible. Being overly complicated, difficult to use, and fragile will obviously make it more likely the solution will fail to offer the value it is capable of providing.

Being standardized implies the system is built on previous experience and field-proven best practices. Being pre-engineered indicates that much, if not all, of the complex programming work to enable the software to communicate with and understand the outputs from the power, cooling, and IT systems has already been done. In contrast, a SCADA system requires complex custom programming just to account for the basic logic of a given device. Whereas a standardized, pre-engineered DCIM system already knows, for example, what a UPS is, how to talk to it, how to control it and how to interpret the messages the UPS sends out onto the network. A standardized system will also likely come pre-configured to interact more easily with third party systems (e.g., BMC Remedy or VMware vCenter) requiring only minimal setup procedures. This pre-programmed logic makes a standardized, pre-engineered system faster and simpler to implement.

They are also easier to service and maintain. Someone once said that "unique solutions create unique problems". Fixing a problem or updating a highly customized system could be expensive, invasive, and/or time-consuming. From this perspective, modern standardized DCIM systems are more akin to a mature enterprise IT management software package. It can be changed, updated, or fixed more easily (often through simple patches and mass updates) without the need for specialized personnel.

Being standardized and pre-configured does not mean, however, that it cannot be customized. A well-engineered, modular system should, in fact, facilitate the ability to adapt the toolset to specific needs without compromising the integrity of the overall system. Modularity, as mentioned above, allows for the easy addition or subtraction of individual tools and features. Infrastructure device settings, thresholds, alarm conditions, etc can all be set by the operator. Reporting content, format, and timing can all be typically controlled by the operator as well.

Table 3 lists questions to ask the vendor to help determine the level of standardization.

Table 3

Questions to help verify a given solution is repeatable and based on previous experience and industry best practices

Standardized and pre-engineered?
Is the solution based on an open communication architecture?
Is the solution based on a scalable, modular architecture?
How much configuration or programming is required once installed? Describe the resources (knowledge, skills, time, etc) required to implement and operate
Can the DCIM server auto discover and categorize network-enabled devices including third party equipment?
How easily can I replicate my DCIM system at other sites?
Is the software's default settings based on best practices and real-world experience?

Active vendor support structure

As with any enterprise-level software evaluation, the DCIM vendors themselves should be evaluated and compared based on their general capabilities and support structure. These attributes can have an impact on the long-term effectiveness of their offer once it is implemented. The vendors' level of commitment to the DCIM market segment, participation and cooperation with industry organizations, and their span of interaction between facilities and IT can all give an indication of the level of quality and the amount of long term support that can be expected. The user should feel confident the vendor will be there to support them over the lifespan of their data center and that the management system can be updated or adapted to changing technology trends or business conditions with minimal interference. Many vendors offer services to implement, configure, train, and even operate these systems. The extent and cost of these services is an additional item to consider during the evaluation phase. Particularly for organizations that are low in process maturity, lack resources or who simply lack the knowledge to do this management for themselves, these software services may be the right course of action for ensuring the value of a DCIM system is realized. **Table 4** lists questions to help determine the level and quality of vendor support that can be expected.

Table 4

Questions to ask the vendor to help determine level and quality of support to be expected

Questions to determine level and quality of vendor support
Does the vendor support commonly used open communication protocols that will ensure solution is ready for the future?
Does the vendor have a long-term strategy for the DCIM market or are they a startup with a more short-term focus and an exit strategy?
Does the vendor's expertise span both realms of Facilities and IT?
Does the vendor offer local support in the local language for fast and clear response to issues?
What is the vendor's escalation path for support issues and how well trained are the reps in DCIM implementation and operations?
Are services available to install, configure, educate, and operate DCIM systems?

This consideration of process maturity is an important step when evaluating vendors and their toolsets. It is critical to have an understanding of what is required on the user side to make the management system work. And these participation requirements can vary significantly from one vendor's toolset to another; in other words, the level of automation and guidance varies. These requirements should be compared to what the organization can realistically do given their knowledge and manpower constraints. **Selecting a system that requires on-going processes that the user is not willing or able to maintain is perhaps another form of "choosing an inappropriate solution".** This critical role of process is discussed in the next section.

Pitfall 2: Relying on inadequate or mismatched processes

DCIM solutions are often sought by data center managers to fill a gap in their operational processes. Vendors often sell them on this basis. And, indeed, **effective** DCIM does simplify, facilitate, and provide a clear view of what would otherwise be a very complex and diverse ecosystem of disparate facilities and IT systems. But this ability is still dependent on operators doing their part by following good processes to implement, operate and maintain the DCIM system. Even the best solutions do not eliminate the need for management processes. Poor process is a common cause of failing to achieve the desired value of DCIM.

The amount of operator effort and process will vary from one vendor's offer to another. This is yet another point upon which to compare solutions during the evaluation phase. Knowing the specific operator requirements of a given offer typically means interviewing the vendor directly. Some vendors will even offer training programs on how to operate and maintain the management system. And it is very important to ensure there will be enough resources (and the on-going discipline to use them) to meet the effort and process required.

Here are four common DCIM-related processes that, if neglected, will undermine the functioning and benefits of the management system:

- Inventory/asset management
- System configuration
- Alarm integration
- Reporting for management or other stakeholders

Each of these is described below along with the impact of poor management.

Inventory/asset management

Some of the most valuable functions of today's DCIM tools include modeling proposed changes or moves, impact analysis of potential problems, and mapping IT device dependencies to specific power and cooling resources. Because IT is so dependent on the physical infrastructure, these functions are critically important. They play a crucial role in ensuring power, cooling, and space is available and in the amount needed as physical and virtual servers are added, removed or are exposed to physical infrastructure problems (e.g., loss of redundancy, CRAH fan failure, etc). In order for these DCIM functions to succeed in doing this, however, IT and facility infrastructure asset information, including their location and interdependencies on each other, must be accurately recorded and continuously maintained over time. This asset management requires on-going process and some action on the part of the operator. Some DCIM solutions, it should be noted, can help in this process by constantly checking measured values against modeled data in order to detect discrepancies. If any are found, a warning notification can be sent to the operator.

As soon as the map of assets within the DCIM software becomes inaccurate, then like a house of cards, these DCIM functions will fail to work properly. They could even possibly cause harm by making faulty recommendations (due to bad input) that could result in wasted effort or even downtime. The output of any modeling function would be seriously flawed if the inputs into the model were wrong or inaccurate - "garbage in, garbage out" as they say. This could lead to making – or trying to make - a change in the IT space that the physical infrastructure may not have been designed to accommodate. For example, some DCIM solutions make recommendations for where to place new equipment based on available power, cooling, rack space, floor weight capacity and network port availability. These recommendations would obviously be wrong and lead to wasted effort if these recommendations were based on bad information about what was already installed in each of the racks. Also, it would be impossible to know the possible impact of an infrastructure system failure (e.g., UPS inverter fault, cooing fan failure, etc) for a given IT load if it is not known where that load is at any given time. Or if the information was believed to be correct, it is possible one might have assumed the load was safe when, in fact, it was not. Imagine someone assuming an important application was running on servers located on power path "A" when it was actually located on power path "B" which had just experienced an infrastructure failure. Once confidence and trust in the DCIM system is lost in this way, it will likely be discarded or ignored in the future. So, establishing and maintaining an accurate map of all IT and infrastructure assets within the DCIM software is important to that management system's long-term success.

System configuration

Once the DCIM software is installed and asset information is collected and mapped, the management system needs to be configured and tailored to the user's requirements. This configuration can span several areas. This would include setup items like determining alarm thresholds, alarm notification policies, defining user access rights and system security, device/location labeling within the GUI, report definition/frequency, UPS and cooling unit operating parameters, and so on. Like the asset management piece, this configuration requires initial action from the operator and on-going process to account for new equipment or changed requirements. Doing so ensures the system responds and acts in expected and useful ways.

These configuration parameters can go beyond just basic setup activities like assigning user access rights or setting polling rates for data logs. Sometimes core and vital functions of the software - see example in the next paragraph - also require initial setup and configuration that may not be obvious at first. Again, it is important to get from the vendor or consultant the full requirements for implementation and use. Standardized, pre-engineered systems can make configuration easier by offering default settings based on best practices and prior experience. Users who may not be sure what settings to make can start with these default settings, monitor the results, and then make adjustments as needed. As DCIM toolsets evolve and standardize, it is likely that the amount of configuration and set-up required will diminish.

To convey the importance of spending the time and resources on initial setup, consider the following example. A newer function of some of the leading DCIM solutions is the ability to automatically initiate the movement of virtual machines (VMs) away from areas with power or cooling alarms by directly communicating with the VM manager. This feature can help ensure VMs always have enough power and cooling capacity, as well as any required redundancy even if they are created and moved suddenly in real-time without user intervention. This capability, of course, does not work "out of the box", but rather requires some setup work. Communication between the DCIM server and the VM manager server needs to be configured. The DCIM vendor's application needs to be imported into the VM manager. On the DCIM side of the equation, the software needs to be populated with live modeled data representing the physical infrastructure (e.g., the servers' location in the racks, rack layout in the room, power connections to the racks, etc. Once this is modeled with the correct

inventory, VM hosts can be associated to the graphical objects in the layout representing the actual servers. This data is then made available to the VM manager through Web Services (for example). The VM manager then needs to be configured to react to any alarms (location, power, and impact data) sent by the DCIM system. The user needs to decide what events warrant an alarm and how to react to it. For example, they can decide to manually act on the alarms or to allow the VM manager to automatically respond in user defined ways. They can create a policy that defines the level of redundancy required for a given VM or application. This policy can then be used to drive the VM manager to move VMs based on the information it receives from the DCIM server.

Alarm integration

Today's DCIM systems are capable of collecting, analyzing, and reporting a lot of information. Based on the particular thresholds and settings chosen by the operator during the system configuration phase, the software can notify operators and managers of changing device and environmental conditions. These alarms can appear in the DCIM dashboard itself or they can appear in other management systems such as a BMS or IT application systems (e.g., HP Openview) if they are linked to the DCIM software. Some DCIM platforms also allow alarms to be sent to remote clients or mobile devices such as an iPhone or Android OS-based device. Most systems will not just show an alarm condition but will time and date stamp the event while storing it in a log file. Some systems are even capable of using this historical information in an analytical way to generate and present recommendations for how to prevent the alarm condition from occurring in the future.

The pitfall is that these alarms can go unnoticed or be simply ignored. There are two basic reasons why this happens. The first is because DCIM alarms and messages are not included in existing issue resolution processes or a new process to accommodate the alarms has not been implemented. The operations team needs to identify and agree on what constitutes an alarm, who should be notified, how (and how often) they are notified, who should act, and how is it confirmed the alarm condition has been resolved. These notification policies will need to be setup and configured within the DCIM system. Using default settings can simplify this process.

The second reason has to do with the sheer volume of data and a lack of context that can exist. Increasing device intelligence and decreasing sensor costs means a typical data center today is capable of feeding many tens of thousands of data points into a DCIM server. If thresholds and notification policies are too broad, this reported data could be overwhelming and, perhaps, even largely irrelevant. This then leads to the data being ignored while critical information (such as a UPS fault) goes unnoticed. Therefore it is important that alarm policies and thresholds be designed to only broadcast an alarm when it is truly important or critical. And only those who really need to know should be notified. If you are unsure of what constitutes an important or critical alarm, choose the system default or contact the vendor.

Alarms which lack context can compound this problem of volume. Receiving raw data from an infrastructure device may not be very helpful especially if the operator is not an expert on that device. Alarms that fail to indicate what to do or what is impacted are obviously less effective in helping to get a problem resolved. Today's modern DCIM systems offer context-aware alarms thanks to its mapping of IT resources with physical infrastructure systems discussed previously. If there is a UPS fault that results in a lack of redundancy, for example, the operator will know which servers (physical or virtual) are affected. And they will know where there is available capacity elsewhere. In some DCIM systems, these context-aware alarms can automatically initiate actions to protect against the impact of a given alarm. In this example, the VM manager could be notified and the "at risk" VMs moved to a safe location in a different physical host with adequate power and cooling resources.

Reporting for management or other stakeholders

Similarly, in order to help ensure that the value of DCIM is realized, it is important that reporting also be considered, planned for, and incorporated into a formal process of on-going review. These reviews can then generate positive actions that can improve and maintain the operations of the data center. Most DCIM toolsets include a reporting function and some allow for their reports to be customized in terms of time period, content and format. Reports can often be exported into other programs to allow for further customization. Some allow for inclusion of external data from other management systems (e.g., a BMS) via web services or databases. The point of tailoring these reports, of course, is to enable management teams to focus on the particular data they care about and review it in a format that is most efficient for them. These reports can typically be easily configured, saved and auto-generated on a user-defined time interval. This can eliminate or greatly reduce the time operators previously spent preparing reports for management.

DCIM reports can convey very useful information that can be used not only to judge the on-going health and effectiveness of the infrastructure, but also to drive preventative actions that help sustain the integrity of the physical infrastructure over time. For example, some systems enable you to run reports on capacity history. This makes it possible to monitor over time how measured loads are tracking towards power and cooling capacities. This knowledge can help prevent an unintended loss of redundancy and provide enough visibility to begin plans for expanding capacity proactively versus reactively. The information in this example also serves to provide real data for determining a growth plan into the future. Failing to pay attention to this important data or to use it to drive corrective action is another manifestation of the “inadequate process” pitfall.

In summary, despite the much higher level of automation found in today’s DCIM systems, on-going process and action from operators is still very much required to make the whole system work and be effective. Assets need to be accurately documented in the system and maintained over time. The system needs to be configured with the appropriate settings and thresholds based on operating requirements. Alarms need to be incorporated into an issue resolution process. And reports need to be customized based on local requirements and regularly reviewed by the appropriate personnel. At a fundamental level, making all of this happen requires:

- Agreement between facilities, IT, and management on operating parameters, metrics, and goals for the data center power and cooling systems and their management.
- A review of existing processes and comparison to DCIM requirements. (Can DCIM-related processes be incorporated into existing practices or are new ones required?)
- New processes should be formally defined (who, what, when, where), resources committed and specific owners assigned.

Starting out “small and simple” is an effective and less risky way to implement a new management solution. Determine the core functions and features that are most important and start with that. Particularly for an organization that is low in process maturity, it may not make sense to try to implement an entire DCIM toolset for the entire data center all at once. The complexity and the amount of new process requirements may be overwhelming and result in the tools never being fully implemented or being used at all. Getting it right for a few select functions and/or for a smaller area (e.g., a row, pod or room) of the data center might better ensure the system provides the value expected. This initial management success can then be later built upon and done so more easily, particularly if the software is modular in nature. **Table 5** summarizes the guidance for avoiding pitfall 2.

Table 5

Basic advice for ensuring key processes are created, implemented and maintained over time

Tips to Avoid Pitfall 2
1. Learn from vendor what processes and resources are required for the implementation and operation of a given solution
2. Compare this to existing capabilities and resources and determine what new or additional process(es) or resources are needed
3. If unable to develop new processes or add additional resources (see Pitfall #3), then choose a solution that matches current capabilities
4. Formally define new processes (who, what, when, where), seek Management commitment of resources and assign specific owners
5. Focus efforts on asset management, system configuration, reporting to stakeholders, and alarm integration processes
6. Start out small by implementing a few select DCIM functions for a smaller area (e.g., a row, pod or room) and then grow from there

Pitfall 3: Lack of commitment, ownership, and knowledge

"Pitfall 3" is, perhaps, a sign or result of poor process as described above. A lack of commitment, ownership, and knowledge can seriously limit any management system's success and, so, deserves some specific attention here in this paper. Because there is a common cause, these three items have been grouped together. It would be obvious to most readers, at least, that a process without an owner or the resources to carry it out almost certainly dooms that process to failure. But, if this is so obvious, then why is it a common pitfall?

The main reason for this - and the common cause for these pitfalls - has to do with the scope of DCIM combined with a "silo mentality" that often exists within an organization. DCIM's functions, tools, and effects span across both facilities and IT – two realms that have traditionally been isolated or segregated from each other. Given IT's reliance on the facility for power, cooling, and space and given that IT is a customer (of sorts) for the facility, there has been much written in the industry press over recent years about the need for these two groups to work together. Management can be another "silo" in the organization that if isolated can sabotage the effectiveness of DCIM tools. This lack of teamwork and communication can, of course, appear within any team - cross-functional or not. DCIM systems have been viewed and touted, at least by some, as a tool for eliminating this "silo mentality". But, sometimes, the isolation can be so great that DCIM tools are unable to bridge this gap as there is neither commitment to use nor clear ownership of the system and its processes. When writing about the risk of data center downtime, David Boston, President of David Boston Consulting, wrote "[T]he potential for confusion and error is high. That's unless the [facilities and IT] groups work together to clearly define detailed processes and ownership of key tasks."[1]

Facilities teams may have their own existing management system (i.e., a BMS) that is currently serving their needs. And IT has their own separate management systems and processes, too, of course. However, neither are really capable of helping to maintain or balance power, cooling and space supply with demand within the data center. This is fundamentally why DCIM toolsets exist, after all. But, sometimes the familiarity and habitual use of these existing tools and processes combined with a "well-its-worked-fine-before" mindset has meant that DCIM did not get fully implemented or used. It is important, there-

[1] "IT and Facilities: how to work together to avoid downtime", Datacenter Dynamics article, accessed March 22nd 2012

fore, for facilities, IT and management to all work together early on and come to agreement on the adoption and use of DCIM tools in conjunction with their existing tools. It's a mistake for management to decide to use a DCIM system without the buy-in from those who will be required to implement and operate it. All sides should be involved in the early evaluation phase to ensure everyone's needs and expectations are met. Each group should come to see and understand the value of the proposed solution upfront. There also needs to be agreement and management support for committing the necessary resources to implement and operate the management system. All of this upfront discussion and buy-in ensures on-going cooperation and participation well beyond the implementation phase.

Owners for the tools and their associated processes should be explicitly named before the system is implemented. This may be tricky since facilities personnel may be unfamiliar with IT systems while IT personnel may have little knowledge of power and cooling. For this reason among others, it is recommended that evaluation and operation teams include people from both sides to help close any knowledge gaps. They should work closely with the vendor to understand all the requirements for making the system work effectively. This information will help the evaluation team decide what level of vendor (or consultant)-provided training and support will be needed, if any. This early involvement and consensus-building between facilities and IT should make on-going cooperation and coordination easier. All of this makes it more likely that the DCIM system is fully implemented, regularly used and, therefore, effective in delivering on its promises. **Table 6** summarizes the guidance for avoiding pitfall 3.

Table 6

Basic steps to ensure on-going commitment and ownership of key processes

Tips to Avoid Pitfall 3	
1.	Involve IT, Facilities and Management from start of evaluation phase
2.	Obtain "buy-in" from all sides on need for DCIM
3.	Come to agreement on DCIM requirements and goals
4.	Work with vendor to understand specific requirements needed to achieve goals
5.	Obtain Management commitment to provide necessary resources
6.	Name specific owners for processes and procedures
7.	Leverage vendor to develop required knowledge on how to operate and maintain system

Conclusion

The benefits of a data center infrastructure management system are achievable, but action on the part of users is still required. This is the underlying theme of this paper. At first glance, the need for significant user action may seem counterintuitive since effective DCIM solutions can, in fact, simplify and automate many aspects of infrastructure management. With the right systems in place, for example, there is no need to have people in the data center white space checking on the status of individual power, cooling and security devices. Guesswork as to where to place the next physical or virtual server is removed. Developing an internal system to create and manage work orders is unnecessary. There's no longer the need to monitor temperature, humidity or look for hotspots using primitive, labor-intensive methods. Reports can be easily and quickly created at any time without having to collect lots of data manually.

This ability to automate and greatly simplify infrastructure management can cause users to underestimate or not properly account for the effort still required on their end. This paper tries to point out what needs to be done by describing the traps that lead to disuse and then offering simple tips on how to avoid them. The bullet points below summarize what is needed to avoid these common pitfalls of evaluating and implementing DCIM solutions:

- Solution should embody certain fundamental properties – scalable, modular, standardized, pre-engineered, open communication architecture with a strong vendor support structure.

- Processes required for implementation and on-going operations needs to be determined, created and supported for the long term; focus on asset management, system configuration, reporting and alarm integration.

- Facility, IT and management should all be involved in the evaluation stage; they must come to agreement on needs, goals and implementation plans, as well as determine ownership for all processes.

About the author

Patrick Donovan is a Senior Research Analyst with Schneider Electric's Data Center Science Center. He has over 16 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

Click on icon to link to resource

Virtualization and Cloud Computing: Optimized Power, Cooling and Management Maximizes Benefits
White Paper 118

Classification of Data Center Management Software Tools
White Paper 104

Power and Cooling Capacity Management for Data Centers
White Paper 150

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

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