A Framework for How to Modernize Data Center Facility Infrastructure

White Paper 272

Revision 0

by Patrick Donovan and Wendy Torell

Executive summary

Aging data centers represent a downtime risk to business operations. In this paper, we lay out a framework for modernizing a facility. This framework includes (1) defining performance standards, (2) benchmarking the facility to identify gaps and health risks, (3) determining modernization options, and (4) prioritizing actions based on business objectives. Modernization should include not only the hardware, but also the software management tools, and operations & maintenance programs. This complete approach ensures the facility continues to meet its IT objectives, including availability, efficiency, and operational cost targets.

RATE THIS PAPER ★★★★★

Introduction

A significant downtime risk exists when physical infrastructure systems approach the end of their useful life, software management tools no longer reflect or comprehend reality, and operations & maintenance programs become outdated. Aging data centers must either be modernized or have their business functions outsourced to cloud or colocation service providers to minimize the risk of disruption. Sites that postpone modernizing also fail to benefit from recent technological advances. These improvements make data centers simpler, more efficient, easier to manage, and more cost effective to operate today. In addition, IT demands change over time, and modernizing represents an opportunity to re-assess the requirements of the data center, such as redundancy and capacity needs. Fundamentally, you have a choice of buying new, upgrading/fixing what you have, or doing nothing. The right answer might depend on your future growth and outsourcing plans.

In this white paper, we present a simple **four-step framework** for how to modernize a data center facility (**Figure 1**). **Often, when modernization is discussed, the focus is only on upgrading the equipment hardware, but as we discuss in this paper, these steps should be carried out for three key domains** – equipment hardware (electrical & mechanical), software management systems, and operations & maintenance programs, since keeping the IT systems running depends on all three.

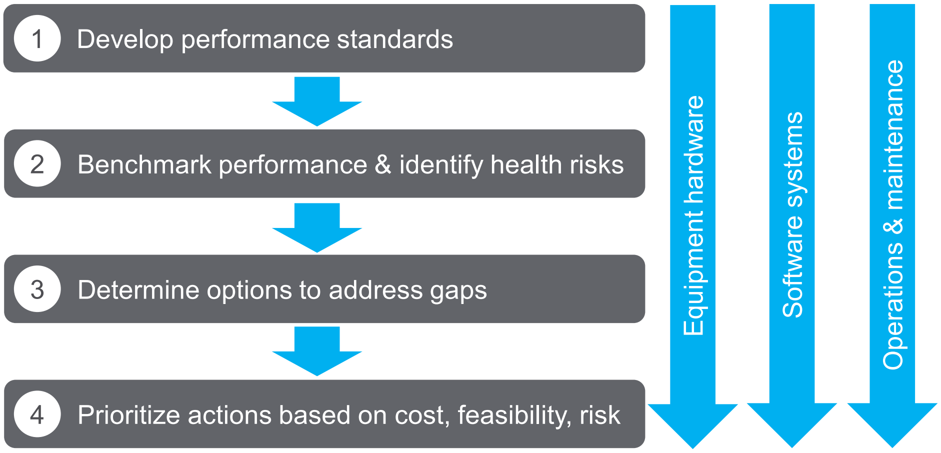

1 Develop performance standards
2 Benchmark performance & identify health risks
3 Determine options to address gaps
4 Prioritize actions based on cost, feasibility, risk
Equipment hardware
Software systems
Operations & maintenance

Figure 1
Four-step framework for modernization

One of the biggest obstacles to modernizing a facility is securing the funding for the project. This holistic and structured approach helps in justifying data center upgrades by documenting the budget required for each improvement as well as the risks of not implementing them. This also makes it easy to select certain improvements and exclude others in order to fit a certain budget.

Note, this paper assumes you've decided on modernizing an existing data center facility. White Paper 171, *Considerations for Owning versus Out-sourcing Data Center Physical Infrastructure*, is a useful reference before going through this modernization process, to weigh the tradeoffs of keeping your own facility vs. outsourcing to a service provider. White Paper 142, *Data Center Projects: System Planning*, is also a useful reference for practical advice on streamlining the planning process.

Four-step framework

The four-step framework is a measured and methodical process to determine what to modernize in your facility, and how and when to do it. It is best applied holistically, across domains, but can be applied to a single domain within your data center as well. The evaluation of a site can be very time consuming. There are 3rd party vendors who can assist you or even lead this process for you. Not only would they simplify and likely accelerate the process, but you would benefit from their experience with other data centers. Also, their independence can result in a more impartial judgement of what risks might exist in your facility.

Step 1 – Develop performance standards

The performance characteristics required of a data center facility (whether a new site or one in need of modernization) should be driven by the business and IT objectives. Keep in mind that for an existing site, these may well have changed since you first built the data center. Re-evaluating your needs in the context of today's organizational objectives will help you figure out, for example, what level of electrical redundancy is really needed or what the operations team staffing levels should be at a given site. A design standard for each of the key domains should be written down and documented.

We often hear the needs of the facility focused around availability or criticality, but a complete performance standard considers other business needs or mandates such as energy efficiency or carbon emissions.

Below are key drivers to think about as you begin to define your performance standard(s).

- Cost/risk of downtime to the business, both tangible and intangible costs
- Capex and opex budgets and/or cost reduction initiatives
- "Green" initiatives like carbon reduction or PUE targets
- Industry expectations (what are your peers doing?)

This is very much an iterative process as you consider the trade-offs between highly available systems, highly efficient systems, and cost. The budget often becomes the constraint, but methodically going through this process can also justify larger budgets and help align all your project parameters.

For a company with more than one data center site, it is likely you will have more than one standard. Not all sites serve the same business function, and some may be more critical than others. Defining different levels or tiers of standards allows you to match your sites to the appropriate standard.

Table 1 is an example of some common performance standards broken into 3 levels. Notice this is focused on the hardware, and only includes some example power and cooling specifications. It's important to have access to deep knowledge on data center design to ensure the performance standards are complete and align to your business objectives, so you aren't left with weak links. There are several criticality specifications out there that can be used as a starting point for this step in the process. White Paper 122, *Guidelines for Specification of Data Center Criticality / Tier Levels*, describes these common methods used.

Table 1
Example of performance standards

System	Attribute	Level 1 Standard	Level 2 Standard	Level 3 Standard
Power	UPS redundancy	N	N+1	2N
	UPS battery runtime	5 min	10 min	15 min
	UPS battery type	VRLA or Li-ion	Li-ion	Li-ion
	Generator redundancy	N	N+1	2N
	Generator fuel onsite	24 hours	48 hours	72 hours
	Branch circuit monitoring	No	Yes	Yes
Cooling	Heat rejection redundancy	N	N+1	2N
	Air distribution redundancy	N	N+1	N+1
	CRAH fans	Fixed speed	VFD	VFD
	Economizer mode	No	Yes	Yes
	Thermal storage	No	30 min	1 hour
	Aisle containment	No	Yes	Yes

In the example, you'll notice many of the items are focused on availability, like specifying 2N redundancy, or a certain amount of runtime. Others are focused on efficiency like economizer modes and type of fans. The priorities of your business must be understood as you develop these standards. Make sure you have buy-in from all key stakeholders as well as an understanding of what the IT outsourcing strategy is. Your outsourcing strategy directly impacts your capacity and redundancy needs moving forward.

Step 2 – Benchmark performance & identify health risks

With a performance standard in place, you can now begin to benchmark how your facility compares to that standard and identify any gaps that exist. This step involves physically investigating the infrastructure equipment, collecting device data, and verifying their interconnections. It involves tracing circuits throughout the electrical infrastructure and piping connections throughout the mechanical system, so you know exactly what loads are plugged in where, what redundancy levels you're currently operating at, what runtime you have, and so on.

You should not just rely on drawings or written reports, as these often become outdated as changes are implemented in the data center. It means interviewing the operations and maintenance (O&M) team and reviewing their methods of procedure and training documentation. Note, outdated drawings are a gap in itself from an operations and maintenance perspective, since it is essential to have "as is" drawings for effective low risk maintenance. Likewise, the software management tools (data center infrastructure management or DCIM) should be checked against the equipment benchmark to see how well the software map of assets and their interconnections match reality. Use the design standard documents as scorecards to record the current reality.

In addition to benchmarking against your performance standard, a basic "health check" should be conducted to identify systems at risk. This health check should evaluate:

- age of devices and warranty status
- maintenance history and service contract status
- current load vs. capacity of systems

As devices age, they present greater downtime risks. Components are more likely to fail or require maintenance. Many devices as they age are also not under maintenance contracts.

Evaluating the current and expected loads are essential to the health of the site. If loads have grown since the original design of the data center, certain systems may become overloaded, or systems that were once used for redundancy now become necessary to support the load (i.e. you lose your redundancy). On the other extreme, your system may be significantly over-sized due to loads being virtualized and outsourced over time. While these oversized systems can support the load, it may not be cost effective to continue to operate them. It's therefore important to fully understand your load today and your growth plan moving forward.

If you're using DCIM monitoring tools, they can be a valuable resource in identifying the health risks. For example, run reports to determine which units are out of warranty, which units have failed a self-test, when batteries have been replaced, etc.

The process of documenting the gaps can be as simple as a table comparing the as-is to the desired performance standard, and noting which rows represent gaps, or you can use a scoring system where you weight each item and assign risk scores. Vendors and consultants may use more sophisticated means of identifying and ranking the gaps.

Step 3 – Determine options to address gaps

Once you've identified all the performance gaps and health risks, the next step is determining what your options are for addressing them. Vendors and consulting engineers may be needed to clearly understand what your options are, as well as their costs. This effort will begin to form a picture of what it will take in terms of time, money, and labor to achieve the project goals. This, in turn, could lead you to re-evaluate the performance standards. And that's OK, this is designed to be an iterative process.

Consider the scenario of a fleet of aging UPSs. I have options to:

1. **Buy new** – Should the UPS be replaced with a new one?
2. **Upgrade** - Can it be revitalized in some way to extend the life and performance for several more years?
3. **Do nothing** - Or is it better to do nothing beyond the most basic maintenance and just let it, in effect, "run-to-fail"?

Investing in a new UPS might make sense if capacity requirements have changed significantly (up or down), if redundancy needs have changed, if maintenance opex is a concern, and if you're looking to improve your energy efficiency since devices have improved significantly over the last 10 years. White Paper 214, *Guidance on What to Do with an Older UPS*, goes through this scenario in detail and helps you weigh the pros and cons of each. While it focuses only on UPSs, the same logic applies to all subsystems in the data center.

Step 4 – Prioritize actions based on cost, feasibility, risk

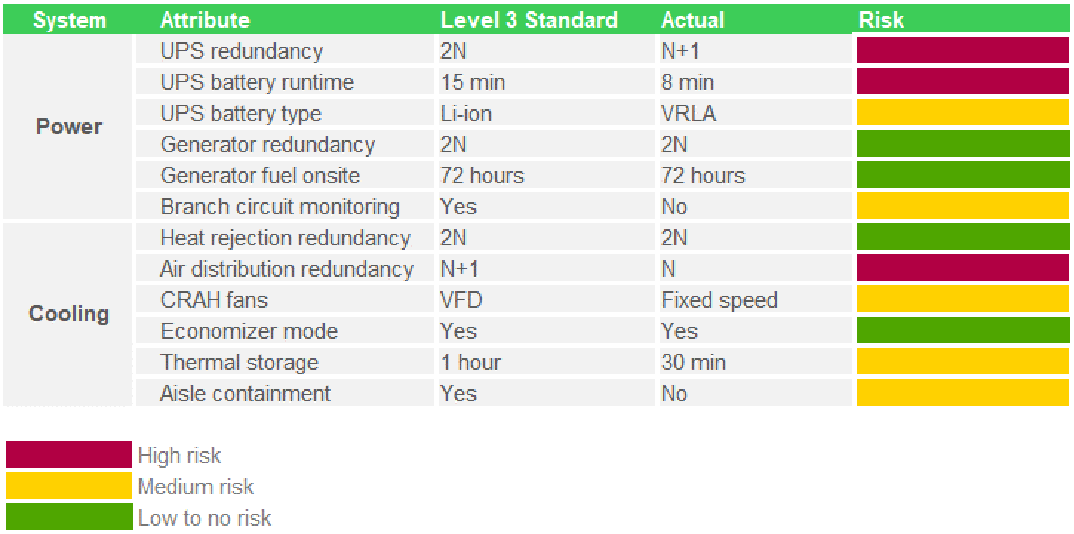
The final step before the actual implementation of upgrades and replacements is to prioritize the actions needed to close the gaps to bring the data center to the performance levels spelled out in the standards. All potential actions need to be evaluated based on:

- the amount of **risk** they represent to the continued functioning of the IT
- the **cost** to implement the change
- the **time** (man-hour resources) to implement the change
- **feasibility** of implementing the change in a live facility with minimal disruption

For each gap uncovered in the audit, you must calculate the risk of not addressing it. Obviously, gaps with the biggest risk go to the top of your list of needs to focus on. This risk needs to be balanced against cost, time, how disruptive it might be to on-going operations, and any other objectives deemed important, such as energy efficiency goals.

Although sometimes hard to quantify, going through the exercise of assigning risk to each gap will help in the process. **Table 2** is a simple example of gaps identified against a standard and a red, yellow, green color coding to determine urgency of closing the gap. In general, the gaps with highest urgency represent the biggest risk of downtime to the data center. Again, a vendor or consultant guiding you through this process will likely quantify the risk with a scorecard, to better rationalize the priority order. Depending on the cost of downtime to your business, it may make sense for you to pay for a probabilistic risk assessment (PRA)[1] to quantify the risk of all the major subsystems in terms of reliability. The higher your cost of downtime, the more this PRA cost is justified.

Table 2
Example of risk assessment for each gap



System	Attribute	Level 3 Standard	Actual	Risk
Power	UPS redundancy	2N	N+1	🟥
	UPS battery runtime	15 min	8 min	🟥
	UPS battery type	Li-ion	VRLA	🟨
	Generator redundancy	2N	2N	🟩
	Generator fuel onsite	72 hours	72 hours	🟩
	Branch circuit monitoring	Yes	No	🟨
Cooling	Heat rejection redundancy	2N	2N	🟩
	Air distribution redundancy	N+1	N	🟥
	CRAH fans	VFD	Fixed speed	🟨
	Economizer mode	Yes	Yes	🟩
	Thermal storage	1 hour	30 min	🟨
	Aisle containment	Yes	No	🟨

🟥	High risk
🟨	Medium risk
🟩	Low to no risk

If you have a large facility, broken into IT pods or rooms, you may be able to prioritize based on which one(s) are supporting the most critical IT loads.

You also will likely identify a lot of "quick fixes" that have low or minimal cost to implement. While these may or may not have the highest level of urgency based on risk to downtime, they represent opportunities to improve the data center without securing significant funding. Examples of these are described in the following section.

[1] Probabilistic risk assessment (PRA) is a systematic and comprehensive methodology to evaluate risks associated with a complex engineered technological entity.

Identify and address the basics

During the process we just described, you will likely uncover easy-to-fix issues, i.e., items involving relatively little to no capex or executive buy-in and time to implement. These should be addressed right away, of course. Low-hanging-fruit actions we often see include:

- **Power** – conducting preventative maintenance (PM) services on hardware systems that are past due, removing unused power modules from UPSs (to reduce electrical losses), redistributing unbalanced loads (for 3-phase power), correcting mistakes in PDU/Rack PDU assignment if redundancy rules are found to be broken, etc.
- **Cooling** – conducting past-due PM services, adding blanking panels to racks, plugging holes in raised floors, removing obstructions from underfloor air pathways, making sure floor tiles are in the right places, making sure racks are aligned properly, adding aisle containment, etc. White Paper 153, *Implementing Hot and Cold Air Containment in Existing Data Centers*, is a helpful reference when thinking about containment upgrades. See also White Paper 40, *Cooling Audit for Identifying Potential Cooling Problems in Data Centers*.
- **Software management systems** – reviewing and making sure all software tools have an accurate map of assets, resources and their dependencies are mapped correctly; reviewing alarm thresholds and notification policies.
- **Operations** – updating/correcting as-built drawings, ensure methods of procedures (MOPs) and emergency operating procedures (EOPs) are correct and in the right places, verify staff is properly trained on emergency procedures.

The three domains

While the physical equipment (hardware) is generally the first thing people think of when it comes to upgrades and modernization, it represents only one leg of the 3-legged stool. Software management tools and operations & maintenance procedures are equally important in ensuring your facility meets the performance standards in terms of availability, efficiency, and cost. The four-step process described above should be followed for all three domains described here.

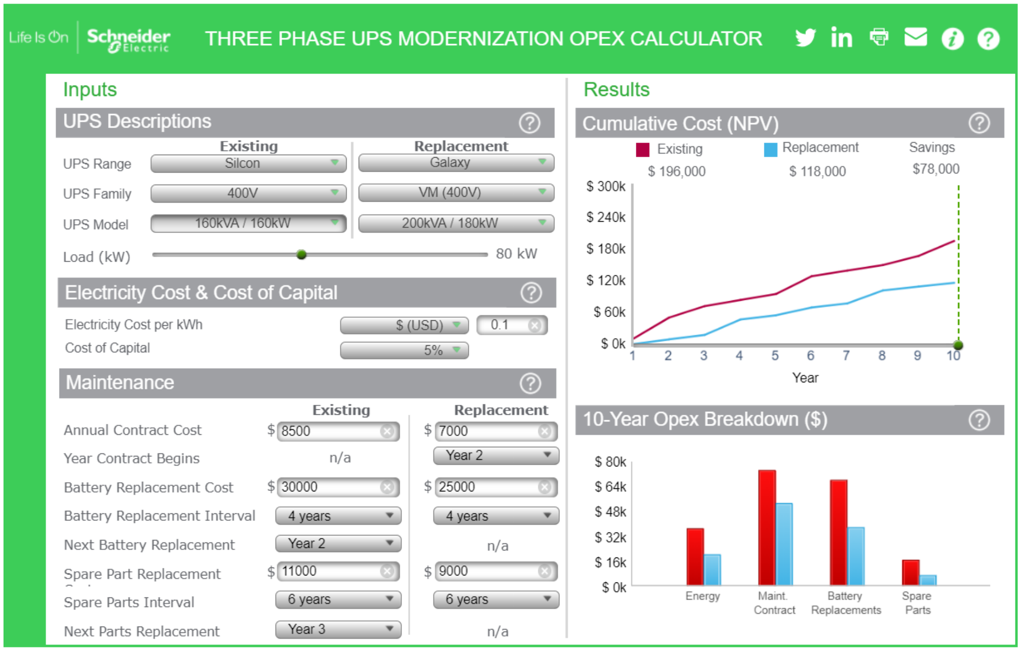
Domain 1 – Equipment hardware

When you're going through the four-step modernization process, it's important to consider all hardware that plays a part in supporting the IT equipment. This includes:

- **Power** – the entire electrical train from utility entrance to IT load
- **Cooling** – the mechanical cooling plant, economizers, air distribution, and cooling controls
- **Physical security & safety** – the racks, sensors, fire detection/suppression, cameras ensuring IT is safe from environmental and human threats

Equipment assessment should include the age, operating conditions, installation condition, and operating efficiency. It should highlight the most significant opportunities for improvement or include specific energy saving calculations and detailed recommendations for remedy.

There are resources to help quantify the value of making improvements. For example, Schneider Electric's online TradeOff Tool, *Three Phase UPS Modernization Opex Calculator* (shown in **Figure 2**), helps to quantify the cost of operating an existing older UPS vs. a newer one, based on efficiency improvements as well as maintenance and parts cost savings. This allows you to determine if it makes sense to replace the system. New technology in many cases also simplifies operations, requires a smaller footprint, and offers feature enhancements, so that should factor into the decision. A UPS with li-ion batteries is an example of a technology improvement compared to older UPSs with VRLA batteries. Li-ion provides longer battery life expectancy, less maintenance, 50-80% smaller footprint, and 3x less weight.



THREE PHASE UPS MODERNIZATION OPEX CALCULATOR

Inputs

UPS Descriptions

	Existing	Replacement
UPS Range	Silcon	Galaxy
UPS Family	400V	VM (400V)
UPS Model	160kVA / 160kW	200kVA / 180kW
Load (kW)	80 kW	

Electricity Cost & Cost of Capital

Electricity Cost per kWh	$ (USD)	0.1
Cost of Capital	5%	

Maintenance

	Existing	Replacement
Annual Contract Cost	$ 8500	$ 7000
Year Contract Begins	n/a	Year 2
Battery Replacement Cost	$ 30000	$ 25000
Battery Replacement Interval	4 years	4 years
Next Battery Replacement	Year 2	n/a
Spare Part Replacement	$ 11000	$ 9000
Spare Parts Interval	6 years	6 years
Next Parts Replacement	Year 3	n/a

Results

Cumulative Cost (NPV)

Existing	Replacement	Savings
$ 196,000	$ 118,000	$78,000

10-Year Opex Breakdown ($)

Figure 2
Online Calculator to help determine whether UPS should be maintained or replaced

It's helpful to create a lifecycle "heat map" (**Table 3**) to help get a visual of aging equipment in the data center. It is advisable to monitor maintenance and repair budgets while beginning to plan for replacement.

Table 3
Example heat map to highlight aging equipment

System description	Max age	Life expectancy range		2018	2019	2020	2021	2022	2023	2024	2025	2026	2027
UPS systems	12	11	15	🟨	🟨	🟨	🟨	🟥	🟥	🟥	🟥	🟥	🟥
UPS Batteries (VRLA)	5.2	4	5.5	🟨	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥
CRAC/CRAH units	16	13	18	🟨	🟨	🟨	🟥	🟥	🟥	🟥	🟥	🟥	🟥
Generators	22	26	35	🟩	🟩	🟩	🟩	🟨	🟨	🟨	🟨	🟨	🟨
Chiller	18	21	25	🟩	🟩	🟩	🟨	🟨	🟨	🟨	🟨	🟥	🟥

🟥 Life expectancy = end of life; Capital replacement should be planned
🟨 Life expectancy = near end of life; Capital budget should be planned
🟩 Life expectancy = New / prime; No action required at this time

While the modernization process may sound simple and straightforward, the actual implementation requires significant coordination and project management to make the upgrade as seamless as possible. For the example of a UPS system replacement, there are several actions that can be done to mitigate risks to your critical loads:

- selecting a replacement that fits in the footprint available and with the input/output gear of the previous system
- performing work during a maintenance window
- generating procedures to transfer mission critical loads to another source of power prior to the initiation of work and returning the load to the UPS
- notifying all users of loads impacted by the replacement project
- ensuring that the standby generator is properly functioning and has adequate fuel supplies for the duration of the project
- performing the UPS replacement when storms are not forecasted nor being experienced
- ensuring new asset(s) are updated in management software and operations documentation

Domain 2 – Software management systems

Data center infrastructure management (DCIM) tools, building management systems (BMS), and electrical power monitoring systems (EPMS) have been important tools for ensuring data centers remain operational and resources are efficiently used. But to remain effective, your existing tools require regular maintenance. Better software management tools have also emerged that take advantage of newer technologies. So, efforts to modernize a facility should include a review of management software and the processes used to operate and maintain them. Users must decide whether to:

- only maintain and update the existing software tools
- keep existing software tools, but add (or remove) functions or apps
- remove existing software tools and migrate to completely new, modern tools

Regardless of the modernization path taken, it is always important to review the processes for operating and maintaining the tools that ensure the tools do what they’re supposed to.

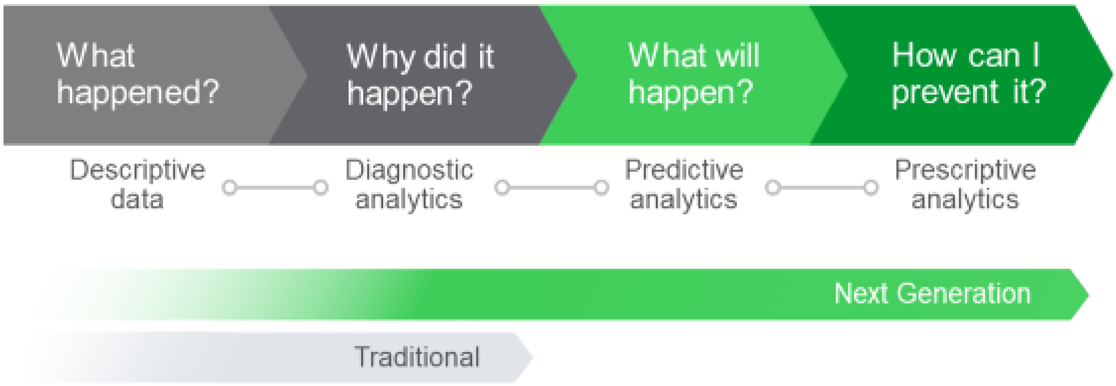
Any enterprise-grade program must be maintained. On-premise DCIM apps, for example, run on their own appliance or exist as a virtual machine (VM). These must be maintained by provisioning the necessary compute and storage resources, performing regular data backups, and implementing new patches and upgrades. The firmware of the infrastructure devices (e.g., UPSs, cooling units, etc.) also need to be checked regularly to make sure the latest version is in use. Lack of maintenance can cause the tool to perform improperly, or worse, create a cyber security vulnerability.

Software, server, and device maintenance aside, the information within the tools requires regular upkeep, too. **The value in the output of management tools is wholly dependent on the accurate mapping of assets, resources, and their dependencies.** DCIM, BMS, EPMS systems are subject to slow drift out of calibration due to changes that occur after the system is commissioned. Some of the causes of the decay in the performance of a system include moves/adds/changes, setpoints being adjusted/overridden, functions put in hand and forgotten, loss of operating knowledge through attrition of staff, and loss of system expertise over time. Addressing this takes discipline and well-managed processes. When this process beaks down, management tools lose their effectiveness and inevitably fall out of use by operators. A facility modernization project is a good time to perform an audit to make sure they reflect the current reality of your data center. Note, there are vendors who can perform this service for you, if preferred.

Part of the management software modernization process should be to consider whether additional infrastructure management functions (e.g., capacity planning) should be added. Many organizations find it best to start out with just basic monitoring capabilities until the operations team becomes proficient at using the app. And once mature with that, they add additional functions. Conversely, some have invested in apps that later proved to be unnecessary or too burdensome given the available staff resources. In this case, it might make sense to simplify and remove software tools to only the core functions needed. For data center facility management, this comes down to monitoring and alarming functions.

Considering entirely new replacement options (vs. upgrading what you have) is part of the modernization framework too. Tools are now available that are cloud-based, mobile-friendly, and take better advantage of data analytics and artificial intelligence technologies. These newer apps offer greater scalability and remove some of the procurement and maintenance burdens by changing to an OPEX model and by putting the server (or management gateway) in the hands of the app vendor who provides them as a service. Cloud-based "data lakes" provide the basis for analytics engines to glean insight and for the development of predictive analytics algorithms. Using these new technologies, DCIM tools will be able to proactively predict UPS battery failures, consolidate device alarms, and point out the root cause of incidents, for example. Modernization projects, in this way, provide an opportunity for data center owners to evolve their management from just basic monitoring and alerting of raw device data, to one that is more proactive and predictive in nature. **Figure 3** highlights the likely evolution path of data center infrastructure management tools that the industry is headed towards.

Figure 3
DCIM evolution



Domain 3 – Operations & maintenance program

Every data center relies on effective operation, maintenance, and management by well-trained, organized human beings. Operations and maintenance (O&M) programs play a critical role in how successful a data center is in meeting its design goals and business objectives. White Paper 196, *Essential Elements of Data Center Facility Operations*, describes twelve key components that make up an effective O&M program. This information can be used to develop a program or be used as a tool for performing a quick and basic gap analysis on an existing program. White Paper 197, *Facility Operations Maturity Model for Data Centers*, on the other hand, moves beyond just describing the high-level elements of a good program. The paper provides a very detailed framework for evaluating and benchmarking all aspects of an existing program. This comprehensive and standardized framework (embedded in the resource section of White Paper 197) offers a means to determine to what level or degree the program is implemented, used, managed, and measured. Armed with this information, facility operations teams can better ensure their O&M program continuously lives up to their data center's specific design and business goals throughout the life cycle of the facility.

As facilities age and mature, management of the facility may become lax and/or too dependent on the institutional knowledge of one or two seasoned facility operators. The following is a list of common O&M program deficiencies we see in older data centers.

- As-built drawings and DCIM map of resources do not match current reality
- MOPs and EOPs do not match the installed devices and their current firmware level
- On-going staff training and emergency response drills are no longer carried out
- Change management process is ineffective due to inadequate risk analysis, poor procedures, and lack of defined process for performing critical work tasks

Preventing or reducing the impact of human error and system failures, as well as managing the facility efficiently, all requires an effective and well-maintained O&M program. Ensuring such a program exists and persists over time requires periodic reviews and effort to reconcile assessment results with business objectives. With an orientation towards reducing risk, the facility operations maturity model presented and attached to *White Paper 197* is a useful framework for evaluating and grading an existing program. Use of this assessment tool enables teams to thoroughly understand their program including:

- whether and to what degree the facility is in compliance with statutory regulations and safety requirements
- how responsive and capable staff is at handling and mitigating critical events and emergencies
- the level of risk of system interruption from day-to-day operations and maintenance activities
- levels of staff knowledge and capabilities

Grading and assessment of results is best done by an experienced, unbiased assessor. There are third party vendors who offer facility operations assessment services.

Conclusion

Following and adhering to the four-step framework for modernizing a data center facility reduces downtime risk and ensures business objectives for availability, “green” initiatives, and efficiency are met. This process must include not only the hardware, but also the software management tools, and operations & maintenance program. For each of these domains, the process should include:

- developing performance standards
- benchmarking performance & identifying health risks
- determining options to address gaps
- prioritizing actions based on cost, feasibility, risk

Risk mitigation is core to data center management and operation. A modernization plan identifies and organizes risk exposure that arises from aging assets and growth. A modernization plan built on quality assessments enables effective budgeting, planning, and intermediate steps for remediation. It optimizes costs by focusing spending on process improvements, hardware upgrades, and replacements that have the biggest impact on reducing critical incidents and failures. And new business requirements may mean that the infrastructure capacity needed today is much less than what you needed when it was first built. When you combine that with the likely efficiency gains that modern infrastructure and their management tools bring, the real total cost of ownership (TCO) of a newly modernized facility is often less than expected.

Assessments can range from basic, low to no cost evaluations of existing conditions, to advanced evaluation of customer design requirements and performance against that criteria. Vendors and partners such as Schneider Electric offer a suite of assessment services to support modernization goals and objectives.

About the authors

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.

Wendy Torell is a Senior Research Analyst at Schneider Electric’s Data Center Science Center. In this role, she researches best practices in data center design and operation, publishes white papers & articles, and develops TradeOff Tools to help clients optimize the availability, efficiency, and cost of their data center environments. She also consults with clients on availability science approaches and design practices to help them meet their data center performance objectives. She received her bachelor’s of Mechanical Engineering degree from Union College in Schenectady, NY and her MBA from University of Rhode Island. Wendy is an ASQ Certified Reliability Engineer.

RATE THIS PAPER ★★★★★

Resources

Considerations for Owning versus Out-sourcing Data Center Physical Infrastructure
White Paper 171

Data Center Projects: System Planning
White Paper 142

Guidelines for Specification of Data Center Criticality / Tier Levels
White Paper 122

Guidance on What to Do with an Older UPS
White Paper 214

Implementing Hot and Cold Air Containment in Existing Data Centers
White Paper 153

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

Three Phase UPS Modernization Opex Calculator
TradeOff Tool 25

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