EVALUATING DATA CENTER AND COLOCATION HIGH-AVAILABILITY SERVICE DELIVERY

A FORTRUST White Paper

Original March, 2008
Revised March, 2013
Revised June, 2016

FORTRUST™
premium data center services

When companies evaluate potential data centers and colocation service providers, they customarily create a checklist of criteria to compare their options. However, many of these efforts fail to delve into the depths of detail necessary to make a sufficient evaluation, rendering a well informed decision impossible.

This white paper examines several key criteria as they relate to service delivery from a data center or colocation provider. Specifically, this paper examines the importance of factors such as risk mitigation, operational processes, service assurance, and maintenance and life cycle strategies that directly contribute to "high-availability service delivery."

If you have any questions about this white paper or FORTRUST, please visit us at
www.FTDC.com

INTRODUCTION

The search for the right data center or service provider to support colocation or hosting requirements is a challenging endeavor. Companies rely on data centers or colocation service providers to support mission critical information technology (IT) infrastructure and maintain business continuity. A high-availability data center or colocation service provider minimizes the chances of downtime occurring for critical applications and makes it easier to secure and manage a company's IT infrastructure. As a result, choosing a data center and/or a colocation service provider to entrust and house their business or mission critical IT applications becomes a very important decision.

These highly reliable or high-availability data centers must have a combination of:

- Certified as built site infrastructure design and construction - normally Tier III or Tier IV Constructed Facility Certified
- Outstanding management and operations
- Superior risk mitigation from natural and man-made disasters

While the choices are plentiful, only a few can truly provide high-availability and choosing the wrong data center or colocation service provider can prove costly to the business.

That's why companies spend considerable time and resources selecting data centers or colocation providers. They conduct research, tour facilities, submit requests for information, review proposals and check references.

The key to making the right decision often depends on asking the right questions.

But how do you know if you're asking questions that truly help you make an informed decision? Asking potential data center and colocation service providers' questions uncovers important information about the facility, network access, operations, performance history and the quality of service delivery.

As a premium data center and colocation services provider, FORTRUST has worked closely with companies of all sizes to ensure they're making the right choices for their businesses. In doing so, FORTURST has answered and responded to many questions that help companies make those choices. Leveraging this experience, FORTRUST has compiled a list of questions companies should be asking but often don't. This list is far from exhaustive and is not intended to be applicable in every situation or to every data center or colocation service provider; instead, it is designed to help companies make the right decisions for their businesses.

In this white paper, you'll read and learn about important criteria companies should evaluate when choosing a data center or colocation service provider. At the end of the paper is a workbook/checklist where you'll find a list of evaluation questions. These questions may help you gather the important information you need to make a well-informed decision about your data center or colocation service provider.

The information provided in this document is intended only to be a starting point. For more information, we suggest you examine the excellent work performed by organizations such as Uptime Institute, the American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE) and others on the subjects of reliability and critical systems infrastructure design.

A CLOSER LOOK AT RELIABILITY AND "HIGH-AVAILABILITY SERVICE DELIVERY"

Each company has unique IT and network requirements, and many look for different attributes from a data center or colocation service provider. Most companies, however, are looking for a data center that offers reliability and "high-availability service delivery."

FORTRUST defines "High-Availability Service Delivery" as the manner and means in which the data center or colocation service provider delivers the expected availability or uptime to the end-user.

In many cases, companies looking for a data center or colocation provider primarily examine the data center's critical systems infrastructure design through facility tours, one-line diagrams and visual inspections. Additionally, companies will collect and review information about:

- The data center's third party certifications and compliance
- The data center's location, facility, and risk mitigation features
- Business stability
- The data center IT equipment space and environment
- Access and connectivity
- Physical security

However, some key factors and practices are typically overlooked. While all the above attributes are important when evaluating data centers or colocation providers, companies should also focus on two additional areas that play a critical role in ensuring "high-availability service delivery." These two key areas are:

- Operational processes and service assurance
- Maintenance and life cycle strategies

Even though data centers are designed and built to provide different levels of expected availability, "high-availability service delivery" is not achieved by critical systems infrastructure design alone. In fact, it is only one part of the equation. **See FIGURE 1.0**

Reliability and uptime stem from a combination of many factors starting with the design of the critical systems infrastructure. However, there are several other factors and practices that contribute to "high-availability service delivery." These include:

1. Operational process controls for the critical systems infrastructure including:
    - Change management
    - Staff training on processes and procedures that mitigate or eliminate errors and ensure high levels of service delivery
2. Equipment commissioning and integrated systems testing of the critical system's infrastructure
3. A comprehensive preventive and predictive maintenance strategy combined with:
    - Meaningful testing and trend analysis
    - A commitment to replacing or repairing equipment before it fails
4. Critical systems infrastructure management and capacity planning
5. A Data Center Infrastructure Management (DCIM) system that fully integrates into the operations and service delivery functions that provides a continuous, comprehensive and accurate monitoring and data collection system for all critical and essential systems
    - The DCIM must be combined with a process for notification, escalation and resolution to be effective
6. The use of infrastructure standards for the uniform identification and management of equipment throughout the following systems:
    - Electrical distribution
    - Heating, Ventilation and Air Conditioning (HVAC)
    - Connectivity and access
    - Fire and life safety
7. Risk Mitigation

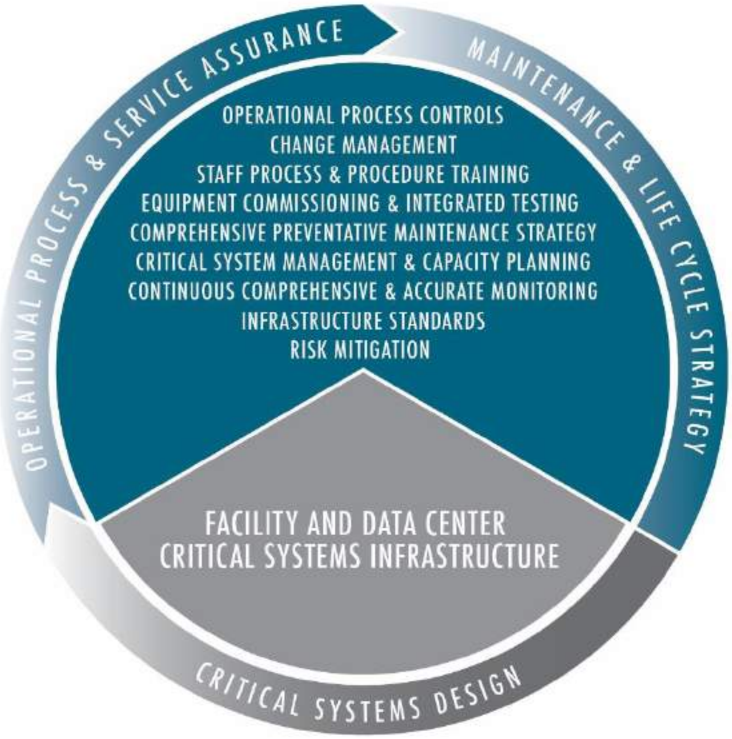
OPERATIONAL PROCESS & SERVICE ASSURANCE
MAINTENANCE & LIFE CYCLE STRATEGY
CRITICAL SYSTEMS DESIGN
OPERATIONAL PROCESS CONTROLS
CHANGE MANAGEMENT
STAFF PROCESS & PROCEDURE TRAINING
EQUIPMENT COMMISSIONING & INTEGRATED TESTING
COMPREHENSIVE PREVENTATIVE MAINTENANCE STRATEGY
CRITICAL SYSTEM MANAGEMENT & CAPACITY PLANNING
CONTINUOUS COMPREHENSIVE & ACCURATE MONITORING
INFRASTRUCTURE STANDARDS
RISK MITIGATION
FACILITY AND DATA CENTER
CRITICAL SYSTEMS INFRASTRUCTURE

FIGURE 1.0: FORTRUST's High-Availability Service Delivery Model

(Source: FORTRUST)

“The concepts of reliability and “high-availability service delivery” are facilitated through an operational mindset in which attention to detail, process discipline and procedural compliance emanate from every aspect of the provider’s approach to operations and service delivery.” – Robert McClary Executive Vice President and General Manager, FORTRUST

KEY DATA CENTER OR COLOCATION EVALUATION CRITERIA

Third Party Certifications and Compliance

Third party certifications can abbreviate, assist and augment your due diligence efforts when evaluating whether or not the data center or colocation provider is aligned with your business needs.

Known as the Global Data Center Authority, Uptime Institute provides the accepted standard for reliability or expected availability for data centers. Uptime Institute's Tier Standard defines the Tier Classifications for the site infrastructure of a data center, either Tier I, Tier II, Tier III, or Tier IV. Uptime Institute's Tier Certification of Constructed Facility (TCCF) is used to validate the site infrastructure, ensuring the as-built data center performs to the Tier objective. Uptime Institute is the only organization that can certify a data center to this standard.[1]

In addition to the Tier Certification of Constructed Facility, Uptime Institute will also certify a data center or colocation provider for Tier Certification of Operational Sustainability (TCOS). The Operational Sustainability rating is only given in addition to the Tier Certification of Constructed Facility Certification.[1]

The Tier Certification of Operational Sustainability criteria pinpoint those elements that impact long-term data center availability in three key categories:

- **Management & Operations**, which evaluates the staffing levels, skills, training, and qualifications of the data center staff; assesses the effectiveness of the maintenance and processes supporting data center operations; and reviews the policies that affect the planning and coordination of activities.

- **Building Characteristics**, which assesses the purpose design and construction of the physical facility and infrastructure.

- **Site Location**, which includes an assessment of potential risks associated with natural and man-made disasters and the levels of risk mitigation in place. [1]

The Tier Certification of Operational Sustainability rating (Bronze, Silver or Gold), when determined by Uptime Institute, becomes a suffix to the Tier Certification of Constructed Facility. Uptime Institute Tier Certification of the installed infrastructure Tier Certification of Design Documents followed by Tier Certification of Constructed Facility is a prerequisite to the Operational Sustainability rating.[1]

The following link can be used to verify all Uptime Institute's data center certifications and is located on Uptime Institute's website: https://uptimeinstitute.com/TierCertification/

[1] Used with permission from *Uptime institute* - June, 2016.

Additionally, organizational controls over the business, operations and security are also important to understand. Many data centers and colocation providers will have audits performed by third parties. Compliance reports such as SSAE 16 SOC 1, Type 2, SOC 2 Type 2 and SOC 3 SysTrust for Service Organizations may be available for review by customers.

Letters of compliance or letters of attestation may be available for industry or organizational specific compliance requirements applicable to data centers such as:

- Payment Card Industry Data Security Standard (PCI-DSS)
- HIPPA
- The Gramm-Leach-Bliley Act (GLBA)
- FISMA
- NIST

Location, Facility, and Risk Mitigation

One of the first factors you should consider when evaluating a data center or colocation service provider is the facility and its location. While it may be important to choose a data center that's easy for your support staff to access, the location of the data center is also significant for a number of other reasons.

Geographic location of the facility and the potential for natural disasters is a key factor of evaluation criteria. Investigate whether the data center is in a zone or region that is at risk to the possibility of natural disasters. Earthquakes, hurricanes, floods, and tornadoes can all damage—if not destroy—even the most reliably built data center.

Location is important to consider in terms of climate as well. If the data center you're evaluating is in a cold-weather region, check to see if it is located on an emergency route. These roads are normally cleared during snowstorms, so it is more likely that your data center will be staffed and able to accept deliveries (such as re-fueling and supplies.) Moreover, it will be easier for you to access in inclement weather. Data centers not positioned on emergency routes may not be so lucky during the next blizzard.

The facility's proximity to other resources or potential hazards is important to evaluate. Obviously, facilities located close to the local fire department will benefit from faster response during emergencies. On the other hand, proximity to airports may present potential risks by putting the facility under the flight path of arriving and departing airplanes. Proximity of the facility to other high risk elements such as nuclear power plants, refineries, dams etc. should also be considered and reviewed.

The **Tier Certification of Operational Sustainability (TCOS)** awarded by Uptime Institute includes a comprehensive review of those elements that impact long-term data center availability with respect to Site Location including an assessment of potential risks associated with natural and man-made disasters and the levels of risk mitigation in place.

Another factor to consider is the facility's construction. Some data centers were built or designed specifically to be data centers, while others were renovated shells or existing multi-use commercial property structures that became data centers. Because existing commercial property structures may be missing key structural elements, they may be more susceptible to storms and problems with ongoing sustainability and may lack the necessary physical security and risk mitigation measures. Inquiring about the facility's construction can provide a large amount of information on its structural integrity and its ability to withstand a natural disaster. Reliability of the critical systems infrastructure design without the thought of risk mitigation tempts the possibility of significant downtime.

The **Tier Certification of Operational Sustainability (TCO**S) awarded by Uptime Institute includes a comprehensive review of those elements that impact long-term data center availability with respect to Building Characteristics which assesses the purpose design and construction of the physical facility and infrastructure.

The utility grid that provides power to the facility is also an important factor to evaluate. Data centers should be designed for uninterrupted power to the critical IT load when a utility power disruption occurs. Repeated interruptions or poor utility power quality can take a toll over time on the data center's infrastructure components like generators, uninterruptible power supplies (UPSs), and switchgear. To minimize the chances of disruptions in your data center's power supply, look for a data center fed by a reliable utility grid. Even though data centers in newer developed areas may be less likely to be connected to a well-established utility power supply, you can best determine the reliability of the grid by contacting the local utility provider. Most will provide information and reports on their performance. The data center or colocation service provider should also be able to supply this information.

Although utility outages should not necessarily translate to data center outages or even critical equipment downtime, unstable utility power can be a sign of capacity and power quality issues. Area construction also can affect the reliability and power quality of the utility grid. So whether the data center is located close to residential areas with new construction or in a zone undergoing revitalization, these factors can potentially impact the quality of the facility's utility power supply, and possibly your server's uptime.

Risk Mitigation integrated into the data center's design and operations is a key to "high-availability service delivery."

Business Stability and Ownership

Business stability is also an important factor to consider when selecting a data center or colocation service provider. Being forced to relocate critical IT equipment should the data center service provider suddenly go out of business is, in many cases, an undesirable evolution. Direct ownership and control of the facility, data center and the property should be reviewed and evaluated.

Data Center IT Equipment Space & Environment

Data centers are traditionally built using raised floors, which provide a plenum for cooling. Data center experts recommend a minimum of 18 inches above the sub floor for raised floors, but 24”, 36” and even 48” are becoming the desired height. The reason for the higher raised floors is clear: the more space there is for air to flow, the easier it is to cool the data center. That’s why newer data center designs often feature cabling that runs above the equipment racks or cabinets, rather than below the raised floors. Cabling, conduit, raceways and other items placed underneath the raised floors take up valuable space used for cooling that can impede the flow of air and potentially cause variations in plenum pressure, hot spots and potentially cleanliness issues.

When evaluating data centers with raised floors, it is important to evaluate if the raised floor is attached to a concrete slab, which provides improved stability and support for heavy equipment. Additional stability is offered by equipment cabinets or racks that are anchored directly to the slab rather than simply sitting on or directly attached to the raised-floor tiles.

Some newer data centers may feature IT equipment spaces that are not traditional raised floor. Over the past few years, different approaches to data center design, construction and deployment have become increasingly popular for a number of reasons including:

- Greater efficiencies, specifically in cooling methods
- Higher power densities (i.e. watts per square foot) and greater per rack kW densities
- Modular deployment of data center capacity to reduce capital costs
- Just-in-time provisioning of IT equipment space and associated capacity

When touring prospective data centers, it is important to understand how much space is available for new equipment and how it can be configured. Having ready-to-use space and a variety of set-up options to choose from, such as individual cabinets, cages with racks, data modules and private rooms is important because it not only means the data center can meet your needs now, but can easily meet your needs in the future. However, physical IT equipment space does not always equate to sufficient power and cooling capacity. All must be discussed, understood and reviewed thoroughly.

Space considerations can go far beyond the amount of available raised-floor or IT equipment space. Access to onsite office space and temporary storage space is also important. Office space can be used in the event of a disaster or when you are at the data center working on equipment. Secure onsite storage space and round-the-clock receiving services provided by the data center or colocation provider can allow you to have equipment shipped directly to the data center without having to worry about your employees being on-site to receive it.

Access and Connectivity

It is critical to understand the connectivity and access options offered by each data center or colocation service provider. Because of this, many companies ask questions associated with the carriers present in the facility such as whether or not they have fiber in the facility and at what capacities.

Multiple and diverse fiber facilities offered by different telecommunication providers or carriers add the benefit of redundancy. For companies who choose to take advantage of such an option, this means that should one carrier or provider’s backbone fail, traffic can be switched over to another provider’s network if configured appropriately.

Also, to optimize physical diversity, the data center should bring fiber into its facility from at least two separate and diverse locations. This ensures traffic will continue to flow even if all the conduits or fiber coming through one of the entrance points is cut or damaged.

Carrier neutrality is another important factor to look for and evaluate. The term “carrier neutral” should not only mean that the customer can use any carrier or telecommunication provider that they desire, but also that the data center or colocation service provider makes it as easy as possible for its end-users to do so.

Many define “carrier neutral” as the capacity to allow the end-user’s direct access to any carrier in the facility without erecting significant logistical or financial barriers for them to do so.

To support true carrier neutrality, data center or colocation service providers should have fiber facilities provided by several redundant carriers installed in the facility and will help their customers gain access to any other carrier they choose that may not already be present in the facility. By choosing a carrier-neutral provider, you are able to use the carrier (or combination of carriers) that makes the most sense for your Wide Area Network (WAN) and business.

Physical Security

Physical security is just as important as digital security when it comes to protecting data housed in a data center. Physical security approaches can differ greatly from one data center to the next. More rigorous approaches rely on a multi-layered security strategy that provides a wide variety of surveillance, multiple points and types of two-factor authentication that make it more difficult for unauthorized access to occur. Biometric devices should also be multi-layered. Additionally, mantraps and security checkpoints should be integrated into the access control design.

The surveillance component of a security system should also have multiple points and “multiple sets of eyes” tasked with monitoring cameras. Another layer of physical security that creates redundancy in the security posture of the data center is the employment of both on-site and off-site monitoring.

One of the best ways to help secure a facility is to make it practically disappear by keeping a low profile. Unfortunately, some data centers and colocation service providers post signage above their facilities that draw attention to themselves—and their customers.

OTHER FACTORS AND PRACTICES THAT LEND TO “HIGH AVAILABILITY SERVICE DELIVERY”

Operational Process and Service Assurance Controls

Even though data centers are designed and built to provide different levels of expected reliability, “high-availability service delivery” is not achieved by critical systems design alone.

How a data center or colocation service provider handles its operations can greatly impact your experience and your equipment at the facility. One important factor to consider is the data center’s processes associated with maintenance and day-to-day operations that surround service assurance and delivery controls.

Process control and documentation of processes are critical because many unplanned downtime incidents are the result of human error.

Documented, validated and repeatable processes create a standardized approach to service delivery and mitigate risk associated with human error. Procedures and processes should be documented and all personnel associated with those processes should be trained appropriately. The structure in which the data center or provider handles their process controls and procedures should be thoroughly reviewed. A strict program for the documentation and revision of procedures will ensure the likelihood that they will be followed and thus reduces the likelihood that human error will cause a disruption in service.

It is critical that the data center or colocation service provider has a primary focus on implementing procedural compliance throughout its operations and service delivery functions. Equally important is how well these procedures are disseminated. The data center or colocation service provider must provide adequate training on their use to be able to ensure that the procedures are followed.

A formal change management process and procedure that fully integrates into all aspects of operations and service delivery is essential.

Change Management should be a routine part of the operations and service delivery of a data center or colocation provider. It should consist of a documented process that includes participation from all levels of management on a consistent basis. Change Management Boards for levels of review and approval are one way to identify that there are participation and compliance throughout an organization. Review of the data center or colocation provider’s change management process helps you to understand the methodology used to implement change to critical systems. This will also aide in the identification of potential impacts to end-users that may occur and how to mitigate them, as well as how the change itself is communicated to customers.

Service Level Agreements (SLAs) are another operational consideration to take into account.

While many people ask about SLAs, very few inquire about how maintenance windows will affect or exempt the data center or colocation services provider's power availability, temperature and relative humidity SLAs. Tier III and Tier IV certified data centers are "concurrently maintainable" by definition, so maintenance windows should not be routine, but rather, rarely needed for planned routine maintenance. Additionally, downtime for routine maintenance should not be needed or should not be an exception to the provider's obligation to their service level agreements for the electrical and mechanical infrastructure.

In contrast, a Tier I or II data center will need to have planned site wide outages to do required and routine maintenance—that is, unless they are neglecting or deferring the required maintenance. The consequences of deferring maintenance can be detrimental to reliability and over time may lead to a catastrophic unplanned downtime event.

Tier I and II data centers may use frequent maintenance windows in order to:

- Conduct routine maintenance activities
- Eliminate responsibility or financial penalties from SLAs if downtime occurs due to the maintenance
- Eliminate responsibility for downtime or financial penalties that may be caused by human error during the maintenance
- Mask a lack of redundancies due to over-subscription of redundant capacities

It is also important to understand in detail how these SLAs are monitored and measured. A thorough review should be conducted of all SLAs associated with the service delivery. Real-time visibility or, at the very least, reports on adherence to SLAs should be required upon request or on a routine basis.

Maintenance and Life Cycle Strategies

Maintenance and life cycle strategies are core to a data center's critical systems infrastructure's ability to continuously provide high-availability service delivery over a long period of time.

The commissioning of equipment and its initial validation or integrated systems testing are extremely important.

These tasks are normally accomplished at the completion of initial construction or additional space and infrastructure expansions. This testing should also be conducted by a third party to provide a comprehensive and unbiased evaluation of the systems and components of the electrical, HVAC and critical systems infrastructure working in an integrated fashion.

Detailed commissioning levels 1 through 5 should include an extensive integrated systems test that provides information and data on how the systems react together in different load and potential failure scenarios. Commissioning with a complete integrated systems test will also validate design capacities, redundancies, reliabilities, and the sequencing of building management systems to determine whether or not the systems can produce the desired results as designed and constructed.

Any level of commissioning should not be considered a valid substitute or even near the same level of comprehensive performance validation as provided by Uptime Institute's Tier Certification of Constructed Facility (TCCF). Commissioning should be considered a pre-requisite to Tier Certification of Constructed Facility.

Regular preventive and predictive maintenance combined with a life cycle strategy is critical to ensuring the reliability of equipment and systems.

Because maintenance procedures and processes differ dramatically from one data center or colocation service provider to the next, it is important to closely evaluate each provider's procedures to determine if the provider has them and, if so, what they are and who performs the work. The frequencies and periodicities of the preventive and predictive maintenance should be reviewed to ensure that OEM recommendations are being met or exceeded.

CRITICAL SYSTEMS INFRASTRUCTURE MANAGEMENT AND CAPACITY PLANNING

In addition to the actual Tier Certification of Constructed Facility that Uptime Institute has awarded to the data center, there are five key areas to the critical systems infrastructure that should be reviewed and considered when choosing a data center or colocation service provider:

- Critical equipment
- Critical and essential electrical systems
- Critical HVAC systems
- Fire and life safety equipment
- Critical systems and equipment monitoring

Critical Equipment

There are several factors that affect the performance of a data center's critical equipment, such as UPS devices, generators, switchgear, chillers, and other associated equipment. These factors include: the age of the equipment, the process by which the equipment is selected, and the redundancies in the design. Additionally, performance is impacted by how equipment is maintained, monitored, inspected, and tested.

- **Age.** All too often, data center or colocation service providers rely on equipment that has exceeded its useful life. This puts end-users at risk because as a piece of equipment gets older, the chances of it failing increase. Newer equipment, on the other hand, normally has less risk of failure, so there are fewer chances of downtime occurring.

- **Selection process.** As data center and colocation service providers replace or buy new equipment, the selection process becomes more important to the performance and reliability of critical systems. Some providers select equipment for the facility based on the lowest bid they receive, while others take a best-in-class approach. Best-in-class equipment selection protects the end-user rather than the bottom line. However, many data centers do not consider the long term costs associated with lower-end equipment over the course of time. Performance, reliability, and mean time between failures (MTBF) should be considered when making critical equipment choices.
- **Redundancy.** Expressions such as N+1, 2N, 2N+1 are often used to describe the level of redundancy data center providers rely on for back-up, or to provide redundancy for critical components. They describe a configuration in which necessary or needed components, referred to as N have a back-up or redundant component or distribution path. When configured correctly, this type of redundancy helps reduce the chances of equipment failure affecting data center end-users. The level of redundancy also enables routine preventive or corrective maintenance to be performed while minimizing impact to end-users. Tier III and Tier IV certified data centers are “concurrently maintainable” by definition, so maintenance windows should not be routine, but rather, rarely needed for planned routine maintenance.

Critical and Essential Electrical Systems

The quality of the electrical distribution systems can make or break a data center or colocation service provider’s performance, reliability, and service delivery. When evaluating data centers or providers, it is important to look at the power available to the data center from the utility. It is also necessary to understand the number of utility feeds received by the facility, how they are used, and the capacity available on each feed in addition to the voltage received from the utility provider. Data centers designed to a premium level should not be impacted by a utility provider outage whether or not it occurred on one or more feeds. Equally important are the data center or colocation provider’s process and procedures for handling utility power disruptions. Tier III and Tier IV data centers use their generators as their primary source of reliable power and those generators should be continuous run-rated.

Data center or colocation service providers should have generators installed and ready to go at all times as their primary source of reliable power.

Generators are at the core of reliability for data centers. However, some emergency or standby generators have run-time limitations and may not be rated for continuous operations. The data center’s generator ratings should be reviewed to ensure it meets the level of reliability and service delivery needed. Redundancy should also be designed into the generator scheme in some manner.

Generators are vital to providing power during utility provider outages; however, they do not normally provide power to the critical loads instantaneously upon a utility power disruption. Understanding the sequence of events during a power disruption and the generators' integration with UPS devices is extremely important.

Generators are powered by fuel—usually diesel. It is a good idea to discover how long each generator can run at full rated load, how much fuel the provider keeps on site and how the provider plans on getting more fuel in the event of a longer utility outage.

Uninterruptable power supply (UPS) devices are equally as critical to reliability. UPS devices will provide continuous power to the critical systems and IT equipment in the event the utility power is disrupted, and as the data center transitions to and from the utility and generator power sources. They can also help alleviate problems with power quality, such as voltage sags or spikes, which can damage IT and network equipment. UPS devices and systems must be maintained and inspected at regular and frequently recurring intervals.

Critical HVAC Systems

Keeping data center space cool is a critical component of any provider's operations. When evaluating data center or colocation service providers, be sure to review a detailed description of the facility's cooling systems, its capacity and redundancies.

HVAC and cooling equipment should also be reviewed for performance and reliability relative to the extreme ambient temperatures or conditions it operates and is exposed to, depending on the geographic location of the data center. The outside ambient conditions of the geographic location may impact operations and the capacities of the equipment.

Thorough review of the cooling system's capacity and how the provider controls and monitors temperature and humidity in the raised-floor or IT equipment areas is essential. Understanding how the monitoring and control of temperature and humidity at the intake of the end-user's equipment, in delivery aisles, or within the IT equipment space is vital as well.

Fire and Life Safety Equipment

Being able to respond quickly to a potential fire is critical in a data center. The data centers or providers you are considering should not only have smoke detection and fire suppression systems in place, but also early warning systems that continuously sample the air for early indications of smoke. This allows the provider to quickly respond to potential problems. In addition, data centers should make portable extinguishers readily available and test them routinely.

Critical Systems and Equipment Monitoring

Critical systems require constant, accurate, and reliable monitoring.

In a highly reliable environment that is focused on high-availability service delivery, monitoring systems become as important as the critical equipment.

Data Center Infrastructure Management (DCIM) and monitoring systems alert personnel to changes or issues often before they become critical or possibly impact availability. Properly configured monitoring systems can be used to provide real-time visibility, and track and report on adherence to SLAs. They also can be used for systems and performance analysis and for immediate notification of potential issues. Trend analysis and equipment performance information can alert operations personnel to potential failures of equipment far in advance of the equipment needing corrective maintenance or replacement.

Infrastructure Management Standards

The use of infrastructure standards for the uniform identification and management of equipment throughout the electrical distribution, heating, ventilation and air conditioning, connectivity and access, and fire and life safety systems is fundamental to an operational environment that has strict process control.

The data center or colocation services provider must keep standards and policies that describe:

- Proper installation and management of cabling in the data center
- Uniform numeration, color coding and labeling throughout the entire critical systems infrastructure
- Visible and easily referenced in-place diagrams and drawings
- Accurate electrical and branch circuit panel schedules and management

The **Tier Certification of Operational Sustainability (TCOS)** awarded by Uptime Institute includes a comprehensive review of those elements that impact long-term data center availability with respect to Management and Operations. This review evaluates the staffing levels, skills, training, and qualifications of the data center staff; assesses the effectiveness of the maintenance and processes supporting data center operations; and scrutinizes the policies that affect the planning and coordination of activities.

CONCLUSION

It is important to understand that not all data centers are designed, built, managed or operated alike. An examination based solely on the data center's critical systems infrastructure design and other attributes will not provide a complete review of "high-availability service delivery."

Companies should also focus on additional factors and practices that play an important role in ensuring high-availability service delivery, such as:

1. Operational processes and service assurance
2. Maintenance and life cycle strategies

Every data center and colocation service provider is unique. Some offer greater reliability and security than others, but this disparity is not always easy to determine. That is why selecting a data center and colocation provider can be such a long and arduous process. However, by asking the right questions, you have a better chance of ensuring that you are making the right decision.

LEARN MORE ABOUT FORTRUST

FORTRUST is one of the most progressive high-availability data center services providers in North America, serving clients across the globe who depend on colocation services for the critical lifeline of their business. FORTRUST was awarded a Tier III Gold Certification of Operational Sustainability and a Tier III Certification of Constructed Facility by Uptime Institute. FORTRUST Denver is the largest colocation data center in the region. FORTRUST offers agile, reliable, sustainable and secure raised floor and modular data center capacity for any-size enterprise supported by optimal power infrastructure and connectivity to safeguard mission-critical business services.

More information is available by visiting www.FTDC.com

FOOTNOTES

[1] Used with permission from *Uptime institute* - June, 2016.

FORTRUST™
premium data center services

QUALITY AND
CUSTOMER SERVICE
MATTER

DATA CENTER EVALUATION WORKBOOK/CHECKLIST

Consider using the following questions when evaluating data centers and colocation service providers. More information about each of the subject areas can be found in the FORTRUST white paper titled: *Evaluating Data Center and Colocation High-Availability Service Delivery* available at **www.FTDC.com**

How to use this checklist:

1. A number of the questions contained within this workbook/checklist will lead to a variety of different answers or responses, many of which are neither right nor wrong. It is the user's responsibility to determine whether the questions or the subsequent responses address your organization's requirements for its future data center or colocation service provider.
2. Prioritize the evaluation criteria based on the factors that matter or apply to your company's unique business requirements.
3. Establish a methodology for the selection process that helps you arrive at the best fit for your organization's needs.

KEY DATA CENTER EVALUATION CRITERIA

Third Party Certification and Compliance	
Has the data center been awarded a Tier Certification of Constructed Facility (TCCF) by Uptime Institute? If so, to what Tier classification (Tier I, II, III, IV) is the data center certified for "Constructed Facility" by Uptime Institute? Has the data center been awarded a Tier Certification of Operational Sustainability (TCOS)? If so, what Operational Sustainability Rating (Bronze, Silver or Gold) was awarded by Uptime Institute?	

NOTE: Self certifications or statements of compliance to the Tier Standard are not valid in lieu of the actual Tier Certification of Constructed Facility (TCCF) awarded by Uptime Institute. **The link to verify all data center Constructed Facility Certifications awarded by Uptime Institute is located at Uptime Institute's website: https://uptimeinstitute.com/TierCertification/**	
Are there other 3rd party audits, reports, certifications that the data center holds? Are the reports able to be reviewed?	
Are there 3rd party audits and/or letters of attestation or compliance for the following? • SSAE 16 SOC 1 Type 2 • SOC 2 Type 2 • SOC 3 • Payment Card Industry Data Security Standard (PCI-DSS) • HIPPA • The Gramm-Leach-Bliley Act (GLBA) • FISMA • NIST Are the audit reports and/or letters able to be reviewed?	

Location, Facility, and Risk Mitigation

Location, Facility, and Risk Mitigation	
Is there construction in progress near the data center? Is there risk? If so, how is it mitigated?	

Does the data center have access to more than one utility grid or separate feeders from different substations? How are they used (i.e. for capacity or redundancy?) What is the designated “source of reliable power” for the data center? Describe in detail the exact demarc point from the utility provider to data center (i.e. meter set, utility provider automatic throw-over (ATO) switch, transformer, etc.) If applicable, how does the switching work? Who owns, controls, and maintains the equipment that does the switching?	
Is the data center located on an emergency route?	
What is the zoning classification?	
Is the data center located in an area that puts it at risk of: Earthquakes? Hurricanes? Floods? Tornados? Wildfires? If yes, how would you rate that risk? Describe any associated risk mitigation efforts.	

Has the data center been awarded a Tier Certification of Operational Sustainability (TCOS) from Uptime Institute in which all natural and man-made disasters were evaluated and assessed? If so, what Operational Sustainability Rating (Bronze, Silver or Gold) was awarded by Uptime Institute? Which natural disasters were evaluated and assessed during the Tier Certification of Operational Sustainability (TCOS) by Uptime Institute? Which man-made disasters were evaluated and assessed during the Tier Certification of Operational Sustainability (TCOS) by Uptime Institute? What were the results and assessments made of each of the above natural and man-made disasters during the Tier Certification of Operational Sustainability (TCOS) by Uptime Institute?	
What are the sources of your data about natural disaster risks associated with the geographic location of the data center?	
What is the history of storms, floods, tornados, hurricanes or other natural disasters at that location?	
Where is the facility located in relation to the 100-year and 500-year floodplain for the location?	
What is the FEMA maximum predicted flood elevation in the data center's location?	
What is the probability of seismic activity in the data center's location? Is the data center located at a site that is < 0.8 m/s² Peak Ground Acceleration (PGA) expected in 50 years with 10% probability?	

Are there seismic enhancements to the facility's construction or within the critical systems infrastructure? If yes, provide a detailed description of the facility's seismic enhancements.	
Is a lightning protection system in place for the entire facility?	
What are the company's contingency procedures for other events or potential risks associated with the data center's location? Are these procedures documented?	
How old is the building in which the data center is housed?	
Was the facility purpose built or designed as a data center or is it a multi-use or other type of commercial building? Has the data center been awarded a Tier Certification of Operational Sustainability (TCOS) from Uptime Institute in which Building and Infrastructure Characteristics were evaluated and assessed as "purpose built"? If multi-use or commercial, what was its original purpose?	
How is the facility constructed? (For example, what were the exterior walls constructed of and what are the interior wall fire ratings?)	
What materials were used in the roof construction?	
Are there windows or glass located in the data center or Mechanical/Electrical Plant (MEP), IT equipment or raised-floor areas?	

If there are windows in the facility but not necessarily in the raised-floor or IT equipment areas, are they hardened or treated from a physical security standpoint?	
Is the building or facility structurally reinforced in any way? If yes, provide a detailed description of the building/facility reinforcements.	
Can the facility's construction documentation and as-built drawings be made available for review?	
How close is the nearest fire department or first responders?	
Is the facility near or in the flight path of an airport?	
How are potential risks from the local area mitigated?	
Is there a hazmat spill procedure that can be reviewed?	
What are the operational profile and contingency plans in case the facility and surrounding area must be evacuated?	
Are there any other businesses or operations occurring at the facility or neighboring locations that are in conflict or pose a threat to data center operations? Has the data center been awarded a Tier Certification of Operational Sustainability (TCOS) from Uptime Institute in which all man-made disasters were evaluated and assessed? If so, what Operational Sustainability Rating (Bronze, Silver or Gold) was awarded by Uptime Institute?	

Business Stability and Ownership

Business Stability and Compliance	
Is the company privately or publicly held? If privately held – Does the data center have financial information it could provide that would indicate the health of the company? Describe the legal ownership of the business.	
How long has the business been operating in the data center or colocation services business?	
Is the business fully funded for growth? If so, to what extent?	
Is the data center, its equipment and facility wholly owned and operated by the business? Is the building structure and property wholly owned by the business? Describe the ownership of the data center facility and all assets associated with the operation of the data center.	
Are there any major components of the electrical or HVAC system that are owned and therefore maintained by someone other than the owner/operator?	
Are high-availability data center and colocation services the primary focus from a services standpoint?	
Is there a disaster recovery and business continuity plan in place?	

Data Center IT Equipment Space and Environment

Data Center IT Equipment Space and Environment	
What is the electrical and cooling density in watts per square foot and/or BTUs per square foot in the raised floor or IT equipment areas?	
Are there restrictions or limits on power and subsequent cooling capabilities to an individual cabinet or rack? If yes - What are those limits? What is the maximum kW per rack that is available?	
What is the height of the data center's raised floors?	
Is cabling run under the floors? If yes: - How do you keep cabling from restricting airflow and creating potential pressure differences? - What are the cleanliness standards and how are they achieved? What is contained under the raised floor or delivery aisles for cooling in IT equipment areas?	
At what pressure is the raised-floor plenum maintained?	
What is the designed or desired cubic feet per minute (CFM) of air flow in the delivery aisle per tile? In other IT equipment area? How is this monitored?	
Is the entire data center space built on the ground floor? On concrete slab? Is data center multi-floor at any point in the IT equipment areas?	

Is your raised floor attached to the concrete slab?	
Do cabinets or racks sit un-anchored on raised floors? If they are anchored, are they anchored only to the raised floor or are they anchored to the concrete slab or floor?	
What is the load capacity of your raised floor in concentrated load? And uniform load?	
Is your raised floor grounded?	
What are your minimum ceilings heights (measured from the top of the raised floor)?	
Is the ceiling over the raised floor susceptible to radiant heat changes and condensation issues? If yes: - How do you counteract this? - Does water from a source other than an extinguishing system run over the raised-floor areas in any fashion?	
How much IT equipment space and associated capacity (power and cooling) do you have available in your data center? How quickly can you build out and deliver the space?	
Is there adequate space for critical components and systems infrastructure to support growth and density?	
What is the ratio of raised floor space to mechanical, electrical, and critical systems space?	
Do you offer customers access to onsite office or drop in space? If yes - Is this permanent, temporary or a disaster recovery-type of offering?	

Is there a charge associated with any of these?	
Under what conditions can a customer gain access to the onsite office space?	
Can we have equipment drop-shipped to the data center? Are there restrictions on the hours available to receive equipment? Are there any costs?	
What is your process for handling customer equipment drop-shipped to the data center?	
What is the security protocol around items being received at the location?	

Access and Connectivity

Access and Connectivity	
Is your data center carrier neutral? If yes - How do you define the term "carrier neutral"?	
What carriers have installed fiber in your data center?	
How does the fiber enter the facility and how is it secured?	
Is the fiber exposed at any point inside the facility so that someone can gain access to it?	
Does the fiber enter the building in more than one location?	
Are the fiber entrances secured and separated at the exterior of the facility? If yes - In what manner and at what distance?	

Is the fiber transported in conduit? If yes: - Can it be accessed within the facility or is it secured? - Does the conduit run under the slab of the facility?	
What is the bandwidth capacity at the facility, per carrier?	
Can I use a carrier other than those that already service the data center?	
Are you open to having different carriers have a presence in the data center?	
How do you allow for the use of other carriers in the facility?	
What is the data center's policy on cross-connects? What are the costs involved?	
Does the data center provide a Managed Internet Access (house, blended) service that is comprised of redundant and diverse carriers?	

Physical Security

Physical Security	
What types of physical security measures are in place?	
Please describe in detail the data center's approach to physical security including the administrative processes for granting access to people such as customers, vendors, and visitors.	
Are the data center's access controls multi-layered? Please describe in detail the layers and how they are configured?	

What type and how many layers of 2-factor authentication are employed?	
Is there around-the-clock dedicated security personnel onsite? If yes - Do the security personnel have other duties assigned to them? What are these duties? Are they third party or FTE employees?	
Are all of the facility's exterior entrances and exit points monitored by cameras?	
Are exterior entrances and exit points alarmed? If yes - How often are the alarms tested?	
Is power for the physical security system on a UPS?	
Is there camera monitoring throughout the data center and IT equipment areas? If yes: - How are the cameras monitored? - Are they monitored around the clock? - Are they monitored by others in addition to the assigned security personnel? - Is the video from the cameras recorded? If yes— how long is it stored?	
Are there manned security checkpoints and/or traps?	
How often are security tours through the facility conducted?	
Are the windows alarmed?	

What areas are accessible via windows?	
Are the facility's walls and windows resistant to explosions?	
Is roof access restricted, alarmed or monitored?	
Are customer and IT equipment areas, including cabinets, cages, and rooms secured in multiple layers? If so, what are those layers specifically?	
Does the data center use an offsite monitoring company to provide additional layers of security?	
Does the data center use any forms of biometric access controls? If yes - What types and in what fashion?	
Is the facility location susceptible to crimes?	
What is your procedure for items shipped to and received at the facility?	
Are the receiving areas monitored by security personnel?	
Has the data center ever experienced any security incidents?	
Who is responsible for developing the facility's security procedures? Is there an Executive Steering Committee that meets on a regular basis to review all physical and logical security practices and policies? If yes - Please explain in detail.	
Is the data center's security procedures documented?	
How often does the data center have outside third parties audit its security practices?	

Are there any signs on the exterior of the facility that may indicate that it's a data center?	
Will our company's presence in the facility be advertised in any fashion?	
Does the data center list its customers housed in the facility anywhere, such as on marketing materials?	

Operational Process and Service Assurance Controls, Maintenance and Life Cycle Strategies

Operational Process and Service Assurance Controls, Maintenance and Life cycle Strategies	
Operational Processes, Change Management, and SLAs	
What are the data center's change management controls? Is there a documented process for change management? Is this available for review?	
Does the data center document maintenance and operational procedures? If yes - Are the documented procedures available for review?	
Are there procedures or contingency plans for identified potential risks?	
Are revisions to the documented procedures controlled? How?	
How is staff training conducted for processes and procedures?	
What are the SLAs for electrical power availability?	

What are the SLAs for temperature and relative humidity (RH) availability in the equipment spaces?	
Does the data center have SLAs for temperature and relative humidity ranges? If yes - what are they?	
Are there penalties (such as service credits) for exceeding the ranges established by the SLAs? If yes, is the customer required to request an SLA credit if applicable or does the data center automatically provide the credit?	
Are 7x24 Remote or Smart hands available? What are the data center's SLAs for technical response and/or remote/smart hands? What are the costs?	
How are the data center's temperature and relative humidity SLAs measured and monitored?	
Are temperatures and relative humidity measured in the delivery aisles above installed computer equipment?	
Has the data center been awarded a Tier Certification of Constructed Facility (TCCF) by Uptime Institute? If so, to what Tier classification (Tier I, II, III, IV) is the data center certified for "Constructed Facility" by Uptime Institute? Is the data center certified by Uptime Institute as "Concurrently Maintainable" (Tier III or Tier IV) for Constructed Facility? Are maintenance windows for electrical and mechanical (cooling) critical systems infrastructure "routine" or "rare"? Please describe in detail how and when maintenance windows are used and their impact on SLAs or service credits?	

Do declared maintenance windows exempt or provide an exception to SLAs and/or service credits for electrical and mechanical (cooling) related SLAs?	
Is there around-the-clock facilities staff onsite besides security or network operations staff?	
Please provide a description, matrix, or documented procedure of the escalation processes for all operational events and customer service delivery issues.	
Equipment Commissioning and Initial Validation or Integrated Systems Testing	
Was an electrical short-circuit coordination study conducted? If yes - Is it available for review?	
Were the data center facility and critical systems infrastructure commissioned by a third party or commissioning agent? If yes: - Did the commissioning include an integrated systems test (level 5) to validate the design capacities, redundancies and reliabilities of critical equipment in different modes of failure? - Are the commissioning and integrated systems test reports available for review? Has the data center been awarded a Tier Certification of Constructed Facility (TCCF) by Uptime Institute? If so, to what Tier classification (Tier I, II, III, IV) is the data center certified for Constructed Facility by Uptime Institute?	
Preventive and Predictive Maintenance and Life Cycle Strategies	

How is the scheduling for the data center’s preventive and/or predictive maintenance managed? For example, is it automatically generated by a software program? Does the data center use hard-copy scheduling or does it use an outside vendor to manage it?	
Does the data center keep a maintenance history for all critical equipment? If yes - Can the maintenance history for a specific piece of equipment be reviewed? Are maintenance schedules and equipment history records available for review?	
What kind of documented preventive and predictive maintenance procedures does the data center have in place?	
Does the data center conduct maintenance in-house or is it outsourced? If maintenance is outsourced - Who does the work and at what intervals?	
Has the data center been awarded a Tier Certification of Constructed Facility (TCCF) by Uptime Institute? If so, to what Tier classification (Tier I, II, III, IV) is the data center certified for Constructed Facility by Uptime Institute? Is the data center certified by Uptime Institute as “Concurrently Maintainable” (Tier III or Tier IV) for Constructed Facility? What types of maintenance activities are performed during the maintenance windows? Are they routine or corrective?	

What are the frequencies of facility-related (electrical or mechanical) maintenance windows? Does this maintenance work affect redundant circuits or distribution paths to computer racks or cabinets?	
Can the data center provide a list and description of all the facility-related (electrical or mechanical) maintenance windows for the prior year?	
Please provide a list of all the scheduled preventive and predictive maintenance and testing frequencies for critical infrastructure components such as: - Electrical systems (infrared testing) - Electrical systems (all other maintenance and testing) - Generators - UPS devices - Switchgear and transformers - Automatic transfer switches - Static transfer switches - Power distribution units (PDUs) - Remote power panels or circuit breaker panels - Other electrical distribution equipment - HVAC system equipment - Fire and life safety equipment	
Are the data center's generators tested at a significant (>90%) of their rated load? If yes: - How often is this performed and what is the tested load percentage of their full-rated load?	

Is the facility load used for load testing? Or does the data center use a load bank? - How often is end-to-end utility outage testing performed? - What items are inspected and recorded during testing? - Can the most recent test results be reviewed?	
What is the percentage of accomplishment of all preventive and predictive maintenance? Is any preventive or predictive maintenance not accomplished or deferred? Has the data center been awarded a Tier Certification of Operational Sustainability (TCOS) from Uptime Institute in which all preventive and predictive maintenance programs were evaluated and assessed? If so, what Operational Sustainability Rating (Bronze, Silver or Gold) was awarded by Uptime Institute?	
What are the cleanliness standards for the raised-floor areas?	
How does the facility manage airborne particulates in the raised-floor or IT equipment areas?	
How does the data center control and manage installation and maintenance activities in the raised-floor or IT equipment areas and in the mechanical and electrical areas? Is there a documented procedure of the above that can be reviewed?	

Critical Systems Infrastructure Management and Capacity Planning

Critical Systems Infrastructure Management and Capacity Planning	
Critical Equipment	
Has any of your critical equipment (UPS devices, generators, chillers, etc.) exceeded its useful life?	
What is the data center's policy for replacing critical equipment?	
What is the data center's process for evaluating and choosing critical equipment?	
Who are the manufacturers of the data center's critical infrastructure equipment?	
How is the data center's redundant critical equipment configured?	
Is any of the data center's equipment reused or refurbished?	
Critical and Essential Electrical Systems	
How many utility feeds does the facility receive? How are they used? (i.e. redundancy, or capacity) Is there an ATO switch between feeders? If so, who owns and maintains it?	
What are the feeder sizes in MVA?	
What is the current capacity in MVA available from the utility provider on each feeder?	
Is there reserved capacity for the facility?	
What is the voltage received from the utility service?	

What types of switchgear are used (such as transformers and automatic transfer switches)?	
At what points is transient voltage surge suppression (TVSS) equipment used in the electrical distribution system?	
How many generators does the data center have in place? Are your generators considered the primary source of reliable power to the entire facility? Are the data center's generators continuous run rated? Are the data center's generators rated as emergency or standby? - If so, what are the run-time limitations?	
What are the capacities and ratings of the generators?	
How are the generators configured in terms of redundancy?	
What type of fuel do the generators use?	
Are the generators tied to a common bus?	
Do the generators use paralleling gear? If yes - What are the redundancies of the paralleling gear?	
How long does it take for the generators to go online and supply the facility with power in the event of a utility outage?	
What is the run time for each generator at full load before needing to refuel?	
What is the onsite fuel storage capacity?	

In the event of an extended utility interruption, what is the refueling plan? For example, what are the fuel supply sources?	
How many UPS devices service the data center? What is the total MVA capacity of UPS available to the IT critical load? How is the UPS capacity expressed? N, N+1 or 2N?	
What are the capacities and ratings of the UPS devices in kW of output?	
If flywheels are used in UPS devices, what are the ratings and time limits? Please provide a detailed description of the operation of these units.	
If batteries are used in UPS devices: -What types of batteries are used? (VRLA or wet cell) -What is the expected range of life of the batteries?	
What is the battery discharge time at full load?	
What is the data center's policy on UPS battery replacement?	
When was the last time the batteries were replaced?	
How does the data center manage load capacity on the UPS devices?	
What is the current capacity available on the UPS devices?	
What are the UPS redundancies?	

How many UPS devices can fail without impacting critical load to the data center floor?	
How are multiple UPS devices configured? (Single module or common bus?)	
Do the UPS devices feed straight to the PDUs or are static transfer switches used to provide multiple source UPS devices to the PDUs?	
Can we review a one-line drawing of the data center's electrical distribution system?	
Can we be provided a drawing and description of the data center's grounding system? Is the grounding system designed for a data center? Are there redundancies in the grounding system?	
What was the grounding system tested to?	
Are cabinets and racks individually grounded?	
Critical Mechanical (HVAC) Systems	
Describe in detail the facility's cooling systems for the data center and IT equipment areas.	
What is the total designed cooling capacity of the cooling system?	
What are the redundancies?	
Is refrigerant used on the raised-floor areas in any fashion?	
Are cooling towers used? If yes: - How many utility water taps are supplying the facility? - Provide a detailed description of the system.	

- What is the backup capacity of makeup water on site?	
Is there leak detection under the raised floors, IT equipment areas, and in the mechanical rooms? If yes: - How is it deployed? - Is there redundancy in the leak detection devices? - Is the leak detection system continuously monitored, and, if so, by what means and who is alerted?	
Are there spill containment features in the data center and mechanical plants?	
How is humidity controlled in the raised-floor areas?	
Can we review a drawing of your cooling system?	
What HVAC and cooling equipment is exposed to extreme ambient temperatures or conditions outside of the facility? (i.e. cooling towers, chillers, DX units etc.) What are the ambient condition ratings of the equipment that is exposed outside of the facility? Are the ambient condition ratings of the equipment that is exposed to outside ambient conditions of the facility rated at N=20 per the ASHRAE handbook? What are the ASHRAE N=20 ambient conditions for the data center's location?	

Fire and Life Safety Equipment	
What types of smoke detection and fire suppression systems are in use?	
Is there an early warning system in use? If yes: - What type of system is it? - Where are the sampling points located? - How is it monitored? - What is the process in the event of an early warning alarm? - What is the process for identifying the source?	
How often are the fire and life safety systems inspected and tested?	
Can we review the maintenance, inspection, and testing records?	
Are portable extinguishers used? If yes: - What types are used? - What type is used in the IT equipment areas? - Where are they located? - How often are they tested and inspected? - Is onsite staff trained in portable extinguisher use?	
What are the fire ratings of internal walls throughout the facility?	
Are fire drills conducted on a recurring basis? If yes - What are the process and schedule for fire drills?	
Critical Systems and Equipment Monitoring	

What types of critical infrastructure monitoring or DCIM systems are in use?	
What equipment is continually monitored?	
How are monitoring system alerts and alarms disseminated, escalated and resolved?	
Please provide a description of all facility, building management, Data Center Infrastructure Management (DCIM) and critical systems monitoring systems.	
Are individual electrical branch circuits to equipment racks and cabinets monitored continuously by the monitoring system or DCIM? Can the colocation customer have real-time visibility to relevant SLAs and adherence to those service levels from the DCIM system? Are monitoring reports available for review? Are historical or trend analytics available to the customer from the DCIM system? Please describe in detail all the information around SLA adherence provided to the customer via the DCIM system.	
Infrastructure Management Standards	
What is the data center's cable management policy? How is it enforced?	
How are critical infrastructure equipment and components labeled? (This includes electrical systems including branch circuits, HVAC systems and fire and life safety equipment.)	
How are circuit breaker panels and panel schedules managed and maintained?	