BICSI 009-2019

Data Center Operations and Maintenance Best Practices

DEMONSTRATION VERSION NOT FOR RESALE

Committee Approval: March 27, 2019

First Published: May 1, 2019

BICSI International Standards

BICSI international standards contain information deemed to be of technical value to the industry and are published at the request of the originating committee. The BICSI International Standards Program subjects all of its draft standards to a rigorous public review and comment resolution process, which is a part of the full development and approval process for any BICSI international standard.

The BICSI International Standards Program reviews its standards at regular intervals. By the end of the fifth year after a standard's publication, the standard will be reaffirmed, rescinded, or revised according to the submitted updates and comments from all interested parties.

Suggestions for revision should be directed to the BICSI International Standards Program, care of BICSI.

Copyright

Published by:

BICSI
8610 Hidden River Parkway
Tampa, FL 33637-1000 USA

Notice of Disclaimer and Limitation of Liability

BICSI standards and publications are designed to serve the public interest by offering information communication and technology systems design guidelines and best practices. Existence of such standards and publications shall not in any respect preclude any member or nonmember of BICSI from manufacturing or selling products not conforming to such standards and publications, nor shall the existence of such standards and publications preclude their voluntary use, whether the standard is to be used either domestically or internationally.

By publication of this standard, BICSI takes no position respecting the validity of any patent rights or copyrights asserted in connection with any item mentioned in this standard. Additionally, BICSI does not assume any liability to any patent owner, nor does it assume any obligation whatever to parties adopting the standard or publication. Users of this standard are expressly advised that determination of any such patent rights or copyrights, and the risk of infringement of such rights, are entirely their own responsibility.

This standard does not purport to address all safety issues or applicable regulatory requirements associated with its use. It is the responsibility of the user of this standard to review any existing codes and other regulations recognized by the national, regional, local, and other recognized authorities having jurisdiction (AHJ) in conjunction with the use of this standard. Where differences occur, those items listed within the codes or regulations of the AHJ supersede any requirement or recommendation of this standard.

All warranties, express or implied, are disclaimed, including without limitation, any and all warranties concerning the accuracy of the contents, its fitness or appropriateness for a particular purpose or use, its merchantability and its non-infringement of any third-party's intellectual property rights. BICSI expressly disclaims any and all responsibilities for the accuracy of the contents and makes no representations or warranties regarding the content's compliance with any applicable statute, rule, or regulation.

BICSI shall not be liable for any and all damages, direct or indirect, arising from or relating to any use of the contents contained herein, including without limitation any and all indirect, special, incidental, or consequential damages (including damages for loss of business, loss of profits, litigation, or the like), whether based upon breach of contract, breach of warranty, tort (including negligence), product liability or otherwise, even if advised of the possibility of such damages. The foregoing negation of damages is a fundamental element of the use of the contents hereof, and these contents would not be published by BICSI without such limitations.

TABLE OF CONTENTS

INDEX OF FIGURES

This page intentionally left blank

PREFACE

Revision History

May 1, 2019 First publication of this standard, titled BICSI 009-2019, *Data Center Operations and Maintenance Best Practices*

Translation Notice

This standard may have one or more translations available as a reference for the convenience of its readers. As that act of translation may contain inconsistencies with the original text, if differences between the translation and the published English version exist, the English text shall be used as the official and authoritative version.

1 Introduction

1.1 General

This standard is written with the expectation that the reader is familiar with the different facets of operating and maintaining data center IT systems and supporting facility systems. The reader should understand from which role and point of view he or she intends to use this document (e.g., information technology, facilities, other corporate internal or external to the owner). Refer to Sections 1.2.1 –1.2.3 below.

1.2 Purpose

This standard provides a reference of common terminology and operating practices. It is not intended to be used by managers, administrators or technicians as their sole reference or as a step-by-step operations guide, but may be used by such persons to determine operation requirements in conjunction with the data center owner, management, administrators, technicians, and in the case of data center outsourcing vendors - customers.

This standard is intended primarily for:

- Data center owners
- Data center management
- Data center operations
- Project managers
- Information and communications technology (ICT) project managers, technicians and system administrators

Additionally, individuals in the following groups are also served by this standard.

1.2.1 ICT Operations

1.2.1.1 ICT Representatives

ICT operations that may use BICSI 009 to develop policies and procedures include:

- Application developers
- Server, storage and network system administrators
- Network Security
- ICT network cabling technicians
- Network operations center (NOC) technicians
- Rack & stack technicians
- IT service desk support and knowledge management
- Change management
- Project management
- Risk management

1.2.1.2 ICT Groups

Each of the ICT representatives listed above may work within one or more of the following areas of responsibility:

- Planning and design
- Intake and transition
- Release management
- Change management
- General operations
- Risk management

ICT operations should coordinate policies and procedures with Facility operations to ensure the policies and procedures of one discipline does not introduce unnecessary risk on the data center operations.

1.2.2 Facilities Operations

1.2.2.1 Facilities Management Representatives

Facilities operations that may use BICSI 009 to develop policies and procedures include:

- Computer room layout
- Electrical engineers/technicians
- HVAC engineers/technicians
- Plumbing engineers/technicians
- Physical security
- Shipping and receiving
- Change management
- Project management
- Risk management
- Ground support
- Housekeeping

1.2.2.2 Facilities Groups

Each of the Facility representatives listed above may work within one or more of the following areas of responsibility:

- Planning and design
- Maintenance
- General operations

Facilities operations should coordinate policies and procedures with ICT operations to ensure the policies and procedures of one discipline does not introduce unnecessary risk on the data center operations.

1.2.3 Data Center Management

The data center manager is typically responsible for the overall performance of the data center including the facility infrastructure and ICT infrastructure. The data center manager would be responsible for:

- Operations and maintenance plan and budget
- Reliability and availability of systems and services
- Energy efficiency
- Resource effectiveness
- Capacity planning and forecasting
- Internal operations personal
- Solicit, review, approve and manage outside vendor support
- Risk management

The data center manager is not typically responsible for IT service delivery.

1.2.3.1 ICT Infrastructure

ICT infrastructure would typically include computational, storage and network hardware deployments, network cabling infrastructure, and technology hardware refresh activities.

1.2.3.2 Facility Infrastructure

The facility infrastructure would typically include all electrical, mechanical, and fire systems operations and maintenance, physical security, and general building and site maintenance.

1.3 Impact of Redundancy on Operations and Maintenance Procedures

Redundancy is the addition of components that are either instantly operational or are continuously operational to achieve a higher degree of reliability, so that the failure or maintenance activity of the primary component does not result in mission failure. Since data center components require maintenance, upgrade, replacement, and may fail, redundancy is required to reduce downtime. There are many combinations of components possible to achieve higher reliability, with each combination having maintenance, operation, and cost advantages and disadvantages.

1.3.1 Standard Operating Procedures

Standard operating procedures are written for all personnel working within the data center or responsible for providing data center services. The procedures address safety requirements, code of conduct of personnel, quality of work, and work order request, approval and implementation process.

The required and recommended standard operating procedures, and the expectations of all personnel are independent of the level of redundancy of the critical data center systems. The general expectations of personnel within a data center should be the same, whether the data center is a BICSI Class 0, Class 1, Class 2, Class 3 or BICSI Class 4.

1.3.2 Maintenance Operating Procedures

Maintenance operating procedures are written to address specific components or systems, and for the specific technicians trained in working on those components or systems.

A significant contributor to unplanned data center service outages is human error. Data centers and data center services are designed with significant automation to reduce the need for human interaction in order to operate under normal and component or system failure modes of operation. Maintenance tasks represent activities when there is an elevated level of human interaction with the critical components and systems, and therefore can affect the level of risk present related to an unplanned outage.

When conducting maintenance tasks on a BICSI Class 0/1 data center, or on non-redundant systems within a BICSI Class 2 data center, a planned outage is required to complete the maintenance. If human error results in an unplanned failure of completing the maintenance tasks, the result is the planned outage will be extended.

When conducting maintenance tasks on a BICSI Class 3/4 data center, or on redundant components within a BICSI Class 2 data center, a planned outage is not required to complete the maintenance. If human error results in an unplanned failure of completing the maintenance tasks, the result could be an unplanned outage if the error cascades and impacts the redundant components or systems.

1.3.3 Emergency Operating Procedures

Emergency operating procedures are written to address specific events and includes procedures for all personnel regarding how to respond to those events.

Emergency events consist of service failures such as utility outages, man-made events such as injured personnel or fire, and natural events such as natural disasters that are prone within the data center region.

The required and recommended emergency operating procedures, and the expectations of all personnel are independent of the level of redundancy of the critical data center systems. The general expectations of personnel within a data center should be the same, whether the data center is a BICSI Class 0, Class 1, Class 2, Class 3 or BICSI Class 4.

1.4 Categories of Criteria

Two categories of criteria are specified – mandatory and advisory.

- Mandatory criteria generally apply to protection, performance, administration and compatibility; they specify the absolute minimum acceptable requirements.
- Advisory or desirable criteria are presented when their attainment will enhance the general performance of the data center infrastructure in all its contemplated applications.

Mandatory requirements are designated by the word *shall*; advisory recommendations are designated by the words *should*, *may*, or *desirable*, which are used interchangeably in this standard. Where possible, requirements and recommendations were separated to aid in clarity.

Notes, cautions and warnings found in the text, tables, or figures are used for emphasis or for offering informative suggestions.

This page intentionally left blank

2 Scope

This standard provides best practices, implementation requirements and guidelines related to the operations and maintenance of data centers. BICSI 009 was written as a complement to ANSI/BICSI 002, *Data Center Design and Implementation Best Practices*. As such, information related to the initial planning, design, construction and commissioning of a data center may not be present within this standard, except as summarized to provide additional information and reference to a specific data center operational or maintenance topic.

This standard has been developed to address data centers built with traditional building construction methods. The requirements and recommendations within this standard could be applicable to other types of data centers (e.g. containerized, modular).

This page intentionally left blank

3 Required Standards and Documents

The following standards and documents contain provisions that constitute requirements listed within this standard. Unless otherwise indicated, all standards and documents listed are the latest published version prior to the initial publication of this standard. Parties to agreement based on this standard are encouraged to investigate the possibility of applying a more recent version as applicable.

Where equivalent local codes and standards exist, requirements from these local specifications shall apply. Where reference is made to a requirement that exceeds minimum code requirements, the specification requirement shall take precedence over any apparent conflict with applicable codes.

ASTM International

- ASTM F2413, *Standard Specification for Performance Requirements for Protective (Safety) Toe Cap Footwear*

BICSI

- ANSI/BICSI 002, *Data Center Design and Implementation Best Practices*

Canadian Standards Association

- C22.1, *Canadian Electrical Code, Part I, Safety Standard For Electrical Installations*
- Z93.4, *Eye and Face Protectors*
- Z195, *Protective Footwear*

European Committee for Electrotechnical Standardization (CENELEC)

- EN 50174-2, *Information technology – Cabling installation – Installation planning and practices inside buildings*

International Code Council (ICC)

- *International Fire Code (IFC)*

Institute of Electrical and Electronics Engineers (IEEE)

- IEEE 142, *IEEE Recommended Practice for Grounding of Industrial and Commercial Power Systems*
- IEEE 450, *IEEE Recommended Practice for Maintenance, Testing, and Replacement of Vented Lead-Acid Batteries for Stationary Application*
- IEEE 1100 (The IEEE Emerald Book), *IEEE Recommended Practice for Powering and Grounding Electronic Equipment*
- IEEE 1106, *IEEE Recommended Practice for Installation, Maintenance, Testing, and Replacement of Vented Nickel-Cadmium Batteries for Stationary Applications*
- IEEE 1188, *IEEE Recommended Practice for Maintenance, Testing, and Replacement of Valve-Regulated Lead-Acid (VRLA) Batteries for Stationary Applications*
- IEEE 3003 series, *IEEE Power Systems Grounding, previously published as IEEE 142 (The IEEE Green Book), IEEE Recommended Practice for Grounding of Industrial and Commercial Power Systems*
- IEEE 3004 series, *IEEE Protection & Coordination*

Institution of Engineering and Technology (IET)

- *Requirements for Electrical Installations BS 7671:2018 (IET Wiring Regulations 18th Edition)*

International Organization for Standardization (ISO)

- ISO 13999-2*, Protective clothing – Gloves and arm guards protecting against cuts and stabs by hand knives – Part 2: Gloves and arm guards made of material other than chain mail*
- ISO 14520, *Gaseous fire-extinguishing systems – Physical properties and system design*
- ISO/IEC 14763-2, *Information technology – Implementation and operation of customer premises cabling – Part 2: Planning and installation*
- ISO 20345, *Personal protective equipment – Safety footwear*
- ISO 27001, *Information technology – Security techniques – Information security management systems – Requirements*

International Safety Equipment Association (ISEA)

- ANSI/ISEA 105, *American National Standard for Hand Protection Classification*
- ANSI/ISEA 107, *American National Standard for High-Visibility Safety Apparel and Accessories*
- ANSI/ISEA Z87.1, *American National Standard for Occupational and Educational Personal Eye and Face Protection Devices*
- ANSI/ISEA Z89.1, *American National Standard for Industrial Head Protection*

National Fire Protection Association (NFPA)

- NFPA 70®, *National Electrical Code® (NEC®)*
- NFPA 70E, *Standard for Electrical Safety in the Workplace*
- NFPA 72®, *National Fire Alarm and Signaling Code*
- NFPA 1600, *Standard on Disaster/Emergency Management Business Continuity Programs*
- NFPA 2001, *Standard on Clean Agent Fire Extinguishing Systems*

Telecommunication Industry Association (TIA)

- ANSI/TIA-569-D, *Telecommunications Pathways and Spaces*
- ANSI/TIA-942-B, *Telecommunications Infrastructure Standard for Data Centers*

4 Definitions, Acronyms, Abbreviations, and Units of Measurement

4.1 Definitions

For the purposes of this document, the following terms and definitions apply. Some terms and definitions may also be represented by an acronym as listed in Section 4.2.

abandoned cable — Installed cables that are not terminated at both ends at a connector or other equipment and not identified 'For Future Use' with a tag.

access floor — A system consisting of completely removable and interchangeable floor panels that are supported on adjustable pedestals or stringers (or both) to allow access to the area beneath the floor (also known as raised floor).

administration — (1) The method for labeling, identification, documentation and usage needed to implement moves, additions and changes of the telecommunications infrastructure (2) The body of persons or the actions thereof that establish and execute goals, policies and procedures for the functional areas or organizations for which they have authorized to operate.

alarm — An electrical, electronic, or mechanical signal that serves to warn of danger or abnormal condition by means of an audible sound or visual signal.

asset — Anything tangible or intangible that has value.

availability — The probability that a component or system is in a condition to perform its intended function, which is calculated as the ratio of the total time a system or component is functional within a specified time interval divided by the length of the specified time interval.

backbone — (1) A facility (e.g., pathway, cable, conductors) between any of the following spaces: telecommunications rooms (TRs), common TRs, floor-serving terminals, entrance facilities, equipment rooms, and common equipment rooms. (2) In a data center, a facility (e.g., pathway, cable, conductors) between any of the following spaces entrance rooms or spaces, main distribution areas, horizontal distribution areas, and TRs.

blanking panel (or filler panel) — (1) A panel that may be plastic or finished metal and is not integral to any discrete electronic component or system. (2) A barrier installed in information technology equipment cabinets, racks, or enclosures for maximizing segregation for optimized cooling effectiveness.

bonding — The permanent joining of metallic parts to form an electrically conductive path that will ensure electrical continuity and the capacity to conduct safely any current likely to be imposed.

building systems — The architectural, mechanical, electrical, and control system along with their respective subsystems, equipment, and components.

bundled cable — An assembly consisting of two or more cables, of the same or different types of cable media, continuously bound together to form a single unit. Bundled cable may be created by the original cable manufacturer, a third-party facility, or during installation. See also *hybrid cable.*

cabinet — A container with a hinged cover that may enclose telecommunications connection devices, terminations, apparatus, wiring, and equipment.

cable	(1) An assembly of one or more insulated conductors or optical fibers within an enveloping sheath. (2) An assembly of one or more cable units of the same type and category in an overall sheath. It may include overall screen. (3) The act of installing cable.
cable management	Physical structures attached to, within, or between cabinets and racks to provide horizontal and vertical pathways for guiding and managing cabling infrastructure.
cable tray	A support mechanism used to route and support telecommunications and other cable. Cable trays may be equipped with side walls or barriers to constrain a cable's horizontal placement or movement.
cabling	A combination of all cables, jumpers, cords, and connecting hardware.
Class	An abbreviation of Data Center Facility Availability Class—the characteristic uptime performance of one component of the critical IT infrastructure. A quantitative measure of the total uptime needed in a facility without regard to the level of quality required in the IT functions carried on during that uptime. As used in this standard, it applies to scheduled uptime. Class is expressed in terms of one of five Data Center Facility Availability Classes. This classification reflects the interaction between the level of criticality and the availability of operation time.
clean agent	An electrically nonconductive, volatile, or gaseous fire extinguishant that does not leave a residue upon evaporation.
client	(1) An internal or external customer. (2) A hardware or software entity, as in "client/server."
colocation	A data center, managed by a vendor, that provides one or more services (e.g., space, power, network connectivity, cooling, physical security) for the server, storage, and networking equipment of one or more customers. A colocation data center is often called a *colo*.
command center	A location where network and IT systems are managed and monitored. A command center is commonly referred to as a network operations center (NOC).
commissioning, building	A process for achieving, verifying, and documenting that the performance of a building and its various systems meet design intent and the owner and occupants' operational needs. The process ideally extends through all phases of a project, from concept to occupancy and operations.
component redundancy	A configuration designed into a system to increase the likelihood of continuous function despite the failure of a component. Component redundancy is achieved by designing and deploying a secondary component so that it replaces an associated primary component when the primary component fails.
computer room	An architectural space with the primary function of accommodating information technology equipment (ITE).
concurrently maintainable	A configuration where system components may be removed from service for maintenance or may fail in a manner transparent to the load. There will be some form of state change, and redundancy will be lost while a component or system is out of commission. This is a prime requirement for a Class 3 facility.
conduit	(1) A raceway of circular cross section. (2) A structure containing one or more ducts.
connecting hardware	A device providing mechanical cable terminations.
connectivity	Patch panels, cabling, connectors, and cable management used to create and maintain electrical and optical circuits.

cord	A length of cable with connectors on one or both ends used to join equipment with cabling infrastructure (i.e., patch panel or cross-connect), a component of cabling infrastructure to another component of cabling infrastructure, or active equipment directly to active equipment.
countermeasures	The procedures, technologies, devices or organisms (e.g., dogs, humans) put into place to deter, delay or detect damage from a threat.
criticality	The relative importance of a function or process as measured by the consequences of its failure or inability to function.
cross-connect	A facility enabling the termination of cable elements and their interconnection or cross-connection.
data center	A building or portion of a building with the primary function to house a computer room and its support areas.
demarcation point	A point where the operational control or ownership changes, typically between the service provider and the customer.
design document	The record that details the design intent.
design intent	Design intent is a detailed technical description of the ideas, concepts, and criteria defined by the building owner to be important.
emergency systems	Those systems legally required and classed as emergency by municipal, state, federal, or other codes or by any governmental agency having jurisdiction. These systems are intended to automatically supply illumination, power, or both to designated areas and equipment in the event of failure of the normal supply or in the event of accident to elements of a system intended to supply, distribute, and control power and illumination essential for safety to human life.
entrance room or space (telecommunications)	A space in which the joining of inter or intra building telecommunications backbone facilities takes place. Examples include computer rooms and server rooms.
equipment cord	See *cord*.
equipment distribution area	The computer room space occupied by equipment cabinets or racks.
failure mode	A system state resulting from an unanticipated system outage and typically an automatic system response to that failure.
fault tolerant	The attribute of a concurrently maintainable and operable system or facility where redundancy is not lost during failure or maintenance mode of operation.
fiber management	Hardware designed and manufactured for keeping optical fiber patch cords neat and orderly. Most termination frame manufacturers provide optical fiber management components designed to work in conjunction with their termination frames. Fiber management may also refer to other types of hardware for securing optical fiber cable to the building.
fiber optic	See *optical fiber*.
flexibility	A design's ability to anticipate future changes in space, communications, power density, or heat rejection and to respond to these changes without affecting the mission of the critical IT functions.
frame	A special purpose equipment mounting structure (e.g., IDC blocks, fiber termination hardware not meant to be mounted in standard 19 inch or 23 inch racks).
ground	A conducting connection, whether intentional or accidental, between an electrical circuit or equipment and the earth or to some conducting body that serves in place of earth.

grounding	The act of creating a ground.
higher Class	Within this standard, a higher Class data center is a data center that meets the requirements of either Class 3 or Class 4.
horizontal cabling	(1) The cabling between and including the telecommunications outlet/connector and the horizontal cross-connect. (2) The cabling between and including the building automation system outlet or the first mechanical termination of the horizontal connection point and the horizontal cross-connect. (3) Within a data center, horizontal cabling is the cabling from the horizontal cross-connect (in the main distribution area or horizontal distribution area) to the outlet in the equipment distribution area or zone distribution area.
horizontal distribution area	A space in a computer room where a horizontal cross-connect is located and may include LAN switches, SAN switches, and keyboard/video/mouse (KVM) switches for the equipment located in the equipment distribution areas.
hybrid cable	A manufactured assembly of two or more cables of the same or differing types of media, categories designation, covered by one overall sheath. See also *bundled cable.*
identifier	A unique item of information that links a specific element of the telecommunications infrastructure with its corresponding record.
information technology equipment	Electronic equipment used for the creation, processing, storage, organization, manipulation and retrieval of electronic data.
infrastructure (telecommunications)	A collection of those telecommunications components, excluding equipment, that together provides the basic support for the distribution of all information within a building or campus.
label	A piece of paper or other material that is fastened to something and gives predefined information about it. Describes its identity, path, location, or other important information about the product or material.
ladder rack	A cable tray with side stringers and cross members, resembling a ladder, which may support cable either horizontally or vertically.
luminaire	An electric light and its components; an electrical lighting fixture.
main cross-connect	A cross-connect for first level backbone cables, entrance cables, and equipment cords.
main distribution area	The space in a computer room where the main cross-connect is located.
maintenance mode	A system state resulting from an anticipated system outage or routine maintenance activity and typically a manual system response to that activity.
media (telecommunications)	Wire, cable, or conductors used for telecommunications.
mission critical	Any operation, activity, process, equipment, or facility that is essential to continuous operation for reasons of business continuity, personnel safety, security, or emergency management.
module	The incremental development size of a storage or computer node, electrical or mechanical system, or data center area.
network operation center	See *command center.*
normal mode	The steady-state system configuration while under load.
optical fiber	Any filament made of dielectric materials that guides light. An optical fiber may be designated single mode (i.e., carrying only one path or mode of light) or multimode (i.e., carrying many paths or modes of light

optical fiber cable	An assembly consisting of one or more optical fibers.
panelboard (electrical)	A single panel, or groups of panel units, designed for assembly in the form of a single panel, including buses and automatic overcurrent devices such as fuses or molded-case circuit breakers, accessible only from the front.
patch cord	See *cord*.
patch panel	A connecting hardware system that facilitates cable termination and cabling administration using patch cords.
pathway	A facility for the placement of telecommunications cable.
performance test	A series of tests for specified equipment or systems, which determines that the systems are installed correctly, started and are prepared for the functional performance tests. Often these tests are in a checklist format.
plenum	A compartment or chamber that forms part of the air distribution system.
power distribution unit	Typically expressed as *PDU*, this is a floor- or rack-mounted enclosure for distributing branch circuit electrical power via cables, either overhead or under an access floor, to multiple racks or enclosures of information technology equipment (ITE). A PDU includes one or more distribution panelboards and can include a transformer, monitoring, and controls. PDUs may also be called a computer power center or a power distribution center.
power strip	A device mounted onto or within an information technology equipment (ITE) rack or enclosure, supplied by a single branch circuit, and containing power receptacles into which multiple IT devices can be plugged. A power strip can include metering, controls, circuit protection, filtering, and surge suppression. A power strip is identified within IEEE 1100 as a power outlet unit or POU. A power strip may also be called a rack-mount PDU, rack power distribution unit, ITE-PDU, cabinet distribution unit, or plug strip.
power usage effectiveness	Typically expressed as *PUE*, power usage effectiveness is an efficiency metric for an entire data center calculated as the total facility power usage divided by the information technology equipment power usage. PUE is the reciprocal of data center infrastructure efficiency (DCIE).
quality control	One of the four major strategies for increasing reliability by ensuring that high quality is designed and implemented in the facility, thus reducing the risk of downtime because of new installation failures or premature wear.
raceway	An enclosed channel of metal or nonmetallic materials designed expressly for holding wires or cables. Raceways include, but are not limited to: rigid metal conduit, rigid nonmetallic conduit, rigid nonmetallic conduit, intermediate metal conduit, liquid tight flexible conduit, flexible metallic tubing, flexible metal conduit, electrical nonmetallic tubing, electrical metallic tubing, underfloor raceways, cellular, cellular concrete floor raceways, cellular metal floor raceways, surface raceways, wireways, and busways. NOTE: Cable tray is not considered a type of raceway.
rack	An open structure for mounting electrical and electronic equipment.
rack unit	The modular unit on which panel heights are based. One rack unit is 45 mm (1.75 in) and is expressed in units of U or RU
raised floor	See *access floor.*
record	A collection of detailed information related to a specific element of the infrastructure.

record drawing	A plan, on paper or electronically, that graphically documents and illustrates the installed infrastructure in a building or portion thereof. Also known as an *as-built drawing*.
redundancy	Providing secondary components that either become instantly operational or are continuously operational so that the failure of a primary component will not result in mission failure. See also *component redundancy*.
reliability	The probability that a component or system will perform as intended over a given time period.
remote power panel	A power distribution cabinet downstream from a PDU or UPS, typically containing circuits and breakers, without a transformer, located near the load.
report	Presentation of a collection of information from various records.
riser	(1) Vertical sections of cable (e.g., changing from underground or direct-buried plant to aerial plant). (2) The space used for cable access between floors.
risk	The measure of the likelihood that a threat will exploit a vulnerability. Within the context of risk assessment, risk may include the asset subject to the threat, providing a means to determine the severity of the risk.
risk management	The process of identifying, evaluating, mitigating, and monitoring risk that is present in a defined context (e.g., system, site).
service provider	The operator of any service that furnishes telecommunications content (transmissions) delivered over access provider facilities.
sheath, cable	A covering over the optical fiber or conductor assembly that may include one or more metallic members, strength members, or jackets.
space (telecommunications)	An area whose primary function is to house the installation and termination of telecommunications equipment and cable (e.g., MDA, IDA, HDA, TR, entrance room).
storage area network	A high-speed network of shared storage devices. A SAN permits storage devices attached to the SAN to be used by servers attached to the SAN.
surge protection device	A protective device for limiting transient voltages by diverting or limiting surge current. It has a nonlinear voltage-current characteristic that reduces voltages exceeding the normal safe system levels by a rapid increase in conducted current. NOTE**:** A surge protection device may also be known as a *voltage limiter*, *overvoltage protector*, *(surge) arrestor*, or *transient voltage surge suppressor (TVSS)*.
switch (network)	A network access device that provides a centralized point for LAN communications, media connections, and management activities where each switch port represents a separate communications channel.
switchboard	A single-panel frame or assembly of panels, typically accessed from the front, containing electrical disconnects, fuses, and circuit breakers used to isolate electrical equipment. Switchboards are typically rated 400 A to 5,000 A and are characterized by fixed, group-mounted, molded case, or insulated case circuit breakers, but they may include draw-out circuit breakers and usually require work on de-energized equipment only.
switchgear	An electrical enclosure, typically having both front and rear access, containing overcurrent protective devices, such as fuses and circuit breakers, used to isolate electrical equipment. Switchgear is typically rated 800 A to 5,000 A and is characterized by segregated, insulated-case, or low-voltage power circuit breakers, usually draw-out, and frequently contains monitoring and controls as well as features to permit addition or removal of switching devices on an energized bus.

switching	(1) The action of opening or closing one or more electrical circuits. (2) The action of changing state between open and closed in data circuits. (3) A networking protocol in which a station sends a message to a hub switch, which then routes the message to the specified destination station.
telecommunications	Any transmission, emission, and reception of information (e.g., signs, signals, writings, images, sounds) by cable, radio, optical, or other electromagnetic systems.
termination	The physical connection of a conductor to connecting hardware.
test procedures	The detailed, sequential steps to set the procedures and conditions necessary to test the system functionality.
threat	Any circumstance or event with the potential to adversely impact operations, assets, or personnel. A threat requires a related vulnerability to be present before becoming an actual occurrence.
topology	The physical or logical arrangement of a system.
transfer switch	Self-acting equipment that transfers a load from one power source to an alternate power source. Transfer switches may use of electrically operated mechanical moving components, (e.g., switch, breaker) or semiconductor devices, and may by self-acting or manually operated. NOTE: Transfer switches with open transition transfer times exceeding 20 milliseconds will result in a reboot or restart cycle of any loads with electronics or controls utilizing switch-mode power supplies. Automatic transfer switches with open transition transfer times of 16 milliseconds or less will not result in a reboot or restart cycle of any loads with electronics or controls utilizing switch-mode power supplies. Transfer switches with no moving mechanical components (e.g., static) typically have transfer times less than 6 milliseconds in duration.
trunk cables	A type of bundled cable consisting of two or more preconnectorized cabling links of the same or different types cabling media, which may either be covered by one overall sheath or be continuously bound together to form a single unit. A trunk cable may also be termed a *trunk cable assembly*.
uninterruptible power supply	A system that provides a continuous supply of power to a load, utilizing stored energy when the normal source of energy is not available or is of unacceptable quality. A UPS will provide power until the stored energy of the system has been depleted or an alternative or the normal source of power of acceptable quality becomes available.
uptime	The period of time, usually expressed as a percentage of a year, in which the information technology equipment (ITE) is operational and able to fulfill its mission.
validation	The establishment of documented evidence that will provide a high degree of assurance the system will consistently perform according to the design intent.
verification	The implementation and review of the tests performed to determine if the systems and the interface between systems operates according to the design intent.
vulnerability	A weakness within an object, process or other defined element which can fail or be exploited, resulting in injury, death, loss of an asset, or other undesired effect.
wireless	The use of radiated electromagnetic energy (e.g., radio frequency and microwave signals, light) traveling through free space to convey information.
XaaS	A generic representation of services provided by external vendors and data centers. Examples of usages include *Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).*

4.2 Acronyms and Abbreviations

Abbreviations and acronyms, other than in common usage, are defined as follows:

24/7	twenty-four hours a day, seven days a week
AHJ	authority having jurisdiction
BAS	building automation system
BMS	building management system
CBRNE	chemical, biological, radiological, nuclear, or explosive
CFD	computational fluid dynamics
CMMS	computerized maintenance management system
CPU	central processing unit
CRAC	computer room air conditioner; computer room air conditioning
CRAH	computer room air handler; computer room air handling
CRB	change review board
DC	direct current
DCIM	data center integrated management
EMP	equipment maintenance plan
EMS	energy management system
EOP	emergency operating procedure(s)
EPMS	electrical power management system
GPU	graphics processing unit
GUI	graphical user interface
HDA	horizontal distribution area
HMI	human machine interface
HVAC	heating, ventilating, and air conditioning
IDA	intermediate distribution area
IIM	intelligent infrastructure management
IT	information technology
ITE	information technology equipment
ITSM	IT service management
LAN	local area network
LOTO	lockout/tagout
MAC	move, add, change
MDA	main distribution area
MOP	method of procedure
O&M	operation and maintenance
OSHA	Occupational Safety and Health Administration
PAP	preventive action plan
PDU	power distribution unit
PM	preventive maintenance
PPE	personal protective equipment
PUE	power usage effectiveness
RPP	remote power panel
RU	rack unit
SAN	storage area network
SLA	service-level agreement
SNMP	simple network management protocol
SOP	standard operating procedure
TVSS	transient voltage surge suppression
UPS	uninterruptible power supply
VLA	vented lead-acid
VRLA	valve-regulated lead-acid
VSS	video surveillance system
WAN	wide area network
ZDA	zone distribution area

4.3 Units of Measurement

The units of measurement used in this standard are metric. Approximate conversions from metric to U.S. customary units are provided in parentheses; e.g., 100 millimeters (4 inches).

Units of measurement used in this standard are defined below:

CFM	cubic feet per minute
dBA	decibel, A weighted
ft	foot
hr	hour
in	inch
in^2	squared inch
kg	kilogram
kW	kilowatt
kWh	kilowatt hour
lb	pound (weight)
m	meter
mm^2	square millimeter
mm	millimeter
RU	rack unit

5 Governance and Assessment

5.1 Introduction

Governance is the way the rules and actions are structured, regulated and verified as needed. While governance typically derives from a government body, governance may take many forms, driven by different motivations and with desired results.

5.1.1 Public Governance

Public governance is comprised of the administrative and process-oriented elements of a government and occurs in three ways:

- Through top-down methods that primarily involve governments and the state bureaucracy.
- Through networks involving public-private partnerships (PPP) or with the collaboration of community organizations;
- Through the use of market mechanisms whereby market principles of competition serve to allocate resources while operating under government regulation

Public governance can derive from level of recognized governmental body including, country, state/territory, region, district/county, and city/township.

Data centers may be affected by a number of public governance focus areas, including:

- Land use
- Environmental
- Corporate business practice
- Financial and accounting
- Security
- Information privacy

5.1.2 Private Governance

Private governance consists of non-governmental entities, including private organizations, dispute resolution organizations, or other third-party groups, whose decisions may become public policy or affect the larger public. Typically, policies, standards and other guidance are developed by private groups may be voluntarily adopted or may become enforceable by an AHJ in one or more of the following ways:

- By government legislation
  - Standards (e.g., NFPA 70, International Building Code)
  - Professional licenses (e.g., professional engineer [PE])
- Enforcement of privately made rules by a governmental agency (e.g., *International Public Sector Accounting Standards*)
- Legal recognition of the group and its determinations (e.g., credit- rating companies)
- Explicit reference to standards and best practices within determinations made by the judiciary

5.2 Compliance

The need for compliance can be considered as either mandatory or voluntary.

Mandatory compliance arises from regulatory or legislative action, where lack of compliance may result in operational fines, temporary slowing or halting of operations, or if sever enough, permanent stoppage of site operations. Examples of mandatory compliance include adherence to applicable building, electrical and safety regulations, proper reporting of financial and personnel data, and filing of proper permits when making certain type of site improvements.

Voluntary compliance is comprised of the remainder of activities that a data center owner or operator may opt to assess and document activities to a defined list of requirements. Examples of areas where voluntary compliance may occur include:

- Warranties
- Quality and process standards (e.g., ISO 9000)
- Independent/3rd party operation certification
- Internal and operation criteria
- Environmental guidelines (e.g., ISO 14000, Leadership in Energy and Environmental Design [LEED]

5.2.1 Documentation

In areas where governance has been established, there is a related need to assess and document compliance. Assessment and documentation can take many forms, from completing a simple form that is submitted to the governing body, to compilation data, activity logs, results from announced and unannounced inspections, and periodic review of all documentation by an independent reviewer.

For areas with mandatory compliance, the AHJ provides the minimum requirements and types of documentation required. Additionally, some AHJs will provide reporting formats to aid in the review and processing of documentation. Documentation retention requirements may also be defined, as some AHJs require the retention of records for a period of time past the point of initial review.

Documentation requirements for voluntary compliance will differ greatly, depending on the specific area being supported. Documentation for warranties may only require the inclusion of initial testing values and evidence of required actions based upon stated warranty requirements. Independent operation certification may require daily, weekly and monthly data for a number of systems and operational activities. For many voluntary compliance activities, there is typically no need to retain data past the period of review.

5.3 Voluntary Assessment Programs

5.3.1 Overview

Voluntary or optional assessment programs may provide financial or operational benefits. Examples of voluntary assessment programs include:

Environmental

- Building Research Establishment Environmental Assessment Method (BREEAM)
- ISO 14000 Series – Environmental management systems
- U.S. Environmental Protection Agency (EPA): Energy Star for Buildings
- United States Green Building Council (USGBC), Leadership in Energy and Environmental Design [LEED]

Other

- ISO 9000 Series – Quality management systems
- ISO 27000 Series – Information technology – Security techniques – Information security management systems

5.4 Types of Assessments

5.4.1 Introduction

Assessments performed by internal data center personnel or independent 3rd party assessors are often the fastest means to discover potential issues. Conducting assessments may also be part of maintenance planning and strategic planning.

5.4.2 Risk Assessment

Risk can form from one or more factors or potential events, and when not identified and planned for, can lead to relatively minor to major impacts of equipment, systems, personnel and operations. Performing a data center risk assessment provides value as it allows the identification, estimation, and communication of the different risk events and their severity that are present at the data center.

Risk can be defined as the product of the probability of occurrence of an event and its impact. Evaluating the impact of an event requires considering the event's ability to disrupt an organization's entire IT operation or a smaller subset of IT operations, and the potential duration of the disruption.

A systematic analysis and evaluation of threats and vulnerabilities is recommended to understand the risk involved. Organizations and stakeholders may be tolerant to different risk levels for a variety of reasons, such as the impact on the facility, the probability of occurrence of the threat, and the perception of a specific threat, risk attitudes and tolerances.

Multiple international standards and guidelines (e.g., ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005, ISO/IEC 31000, and NIST SP 800-30) can be used to support the risk management process.

5.4.3 Data Center Operations and Maintenance Assessment

5.4.3.1 Introduction

Operations and maintenance assessment are the most common types of assessment within an operating data center

5.4.3.2 Recommendations

The following items should be included within operations and maintenance assessment, as applicable:

- Conduct optimization study to ensure data center meets client goals or requirements
  - Gather client information (e.g., as-built drawings, IT information, floor plan, MOPs, utility bill, client needs)
  - Coordinate with the appropriate disciplines to conduct assessment
- Current system state of data center (e.g., mechanical, electrical, ancillary)
  - Review current system and component availability against original intended design and client need
  - Document findings of performance variance against original intended design and client need
- Current efficiency of data center systems (e.g., mechanical, electrical, ancillary)
  - Review current system efficiency rating against original intended design and client need
  - Document findings of efficiency rating variance against original intended design and client need
- Current capacity and growth capacity level of data center
  - Review current capacity rating against original intended design and client need
  - Document findings of capacity utilization and any variance against original intended design and client need
- Aging of technology and need for refresh
  - Review existing equipment for supportability, age, maintainability, and warranty
  - Document findings of equipment concerns and replacement options
- Utility (e.g., availability and cost of power, telecommunications infrastructure, water, gas)
  - Review existing utility services (e.g., availability and cost of power, telecommunications infrastructure, water, gas)
  - Document findings of utility concerns
- Physical security of data center (e.g., electronic systems, architectural security, bollards)
  - Review current state of the data center physical security (e.g. incident reports, surveillance systems, access control logs)
  - Document findings of physical security concerns
- Operational performance (e.g., personnel, policies, maintenance operations procedures, etc.)
  - Review current state of the data center operational procedures (e.g., personnel, policies, maintenance operations procedures)
  - Document findings of the data center operational procedures
- Data center's current suitability against current IT requirements (e.g., network, disaster recovery plan)
  - Review current state of data center's suitability against client's IT requirements
  - Document findings of the data center IT suitability
- Operations documentation (e.g., historical commission reports and logs)
  - Review operations documentation for currency and accuracy
  - Document findings of the operations documentation
- Safety procedures (e.g., LOTO procedures)
  - Review safety procedures documentation for currency and accuracy
  - Document findings of the safety procedures documentation

5.4.4 Security Assessment

5.4.4.1 Introduction

A data center typically has a defined security plan which includes information concerning ongoing assessment and review of the security plan and of the data center itself

5.4.4.2 Requirements

Security assessments and audits shall be performed as described in the current data center security plan.

5.4.4.3 Recommendations

A data center should perform the following items periodically and after any event with security implications:

- Threat assessment (identification, frequency, impact)
  - Evaluate potential environmental threats to property
  - Identify potential threats to physical access to the DC
  - Evaluate potential threats to data integrity (information assurance)
  - Identify potential threats to human life or safety
  - Evaluate frequency of potential threats
  - Quantify impact if a security breach were to occur
- Security audit (building inspections, security surveys, security analysis)
  - Evaluate current environmental conditions and security controls
  - Controlled access to restricted areas
  - Current security surveillance measures
  - Current network security controls
  - Attempt to gain access to the DC network
  - Analyze and interpret regulations affecting data center operations
  - Verify audit findings against Security Objects
    - Determine threat history
    - Interview data center personnel to ascertain criticality of assets
    - Analyze threat history and current security countermeasures
- Identify countermeasures (physical, electronic, organizational)
  - Determine layers of security plan
  - Environmental security Countermeasures (e.g., site location, fencing, berms, etc.)
  - Manned security countermeasures (e.g., guards)
  - Personal identification requirements (badges)
  - Level of entrance security (locks, mantraps, turnstiles, etc.)
  - Access security systems)
  - Surveillance countermeasures
  - Network security hardware (e.g., firewalls, IDS, IPS)
  - Hardware security
  - Security alert methods (e.g., alarms)
- Review current disaster recovery plan (DRP) requirements into recovery design recommendations
  - Types of potential disasters and the impact to facility
  - Short-term and long-term impact of security breach
  - Personnel required to carry out disaster recovery plan